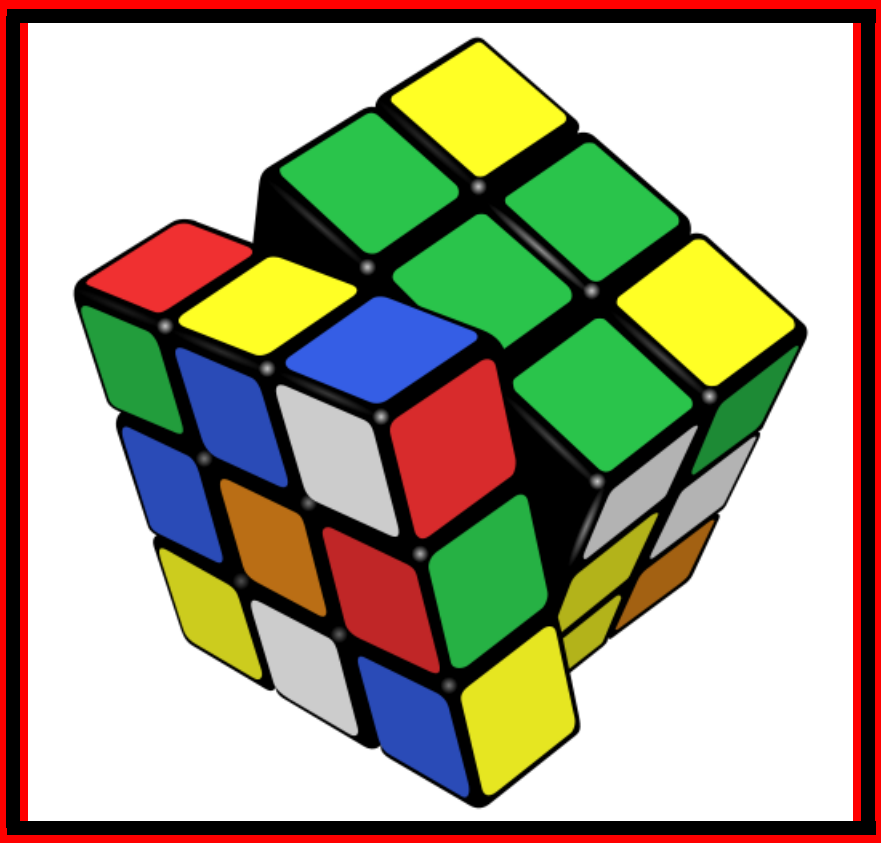
UNIVERSIDAD CENTRAL DE VENEZUELA.
ESCUELA DE MATEMÁTICA.

ÁLGEBRA ABSTRACTA

Notas de curso



MARCO A. PÉREZ B.

Octubre, 2012.

Estas notas están basadas en un curso dado por **Inés Nuñez** en la Universidad Central de Venezuela entre finales de 2005 y principios de 2006. Cualquier error u omisión es responsabilidad del autor.

En la portada: una imagen del cubo de Rubik, cuyas permutaciones forman una estructura de grupo, objeto de estudio fundamental en el álgebra.

TABLA DE CONTENIDOS

1 NÚMEROS ENTEROS **1**

1.1 El Principio del Buen Orden . . . 1
1.2 Divisibilidad . . . 3
1.3 Mínimo común múltiplo . . . 5
1.4 Relaciones de equivalencia y conjunto cociente . . . 5
1.5 Problemas . . . 10

2 GRUPOS **13**

2.1 El concepto de Grupo. Ejemplos . . . 13
2.2 Grupos finitos . . . 16
2.3 Subgrupos . . . 16
2.4 Permutaciones . . . 18
2.5 Homomorfismos . . . 21
2.6 Clases laterales y clases de congruencia . . . 22
2.7 Subgrupos normales . . . 25
2.8 Problemas . . . 28

3 ANILLOS **31**

3.1 El concepto de Anillo. Ejemplos . . . 31
3.2 Subanillos e ideales . . . 32
3.3 Ideales principales y maximales . . . 33
3.4 Anillo cociente . . . 35
3.5 Homomorfismos de anillos . . . 36
3.6 Problemas . . . 39

4 CUERPOS **41**

4.1 El concepto de Cuerpo. Ejemplos . . . 41
4.2 Cuerpo cociente . . . 42
4.3 Característica de un polinomio . . . 44

5 ANILLOS DE POLINOMIOS **45**

5.1 Elementos algebraicos y trascendentes sobre un anillo 45

5.2 Polinomios de varias variables 46

5.3 Anillos euclidianos 48

BIBLIOGRAFÍA **51**

CAPÍTULO 1

NÚMEROS ENTEROS

1.1 El Principio del Buen Orden

Para comenzar estas notas, recordemos al conjunto $\mathbb{N}$ de los números naturales, el cual posee dos operaciones binarias, la suma y la multiplicación:

$$\begin{aligned} + &: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \qquad (a,b) \mapsto a+b, \\ \cdot &: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \qquad (a,b) \mapsto a \cdot b. \end{aligned}$$

Antes de que estudiemos los grupos como una de las estructuras fundamentales en el álgebra, es bueno que sepamos que existen extructuras más simples que el grupo, por ejemplo el **monoide**, que es sencillamente un conjunto no vacío con una operación binaria asociativa. Por ejemplo, $\mathbb{N}$ es un monoide, ya sea con respecto a $+$ o a $\cdot$. Es probable que la propiedad asociativa sea la más importante dentro de las que se estudian en álgebra. La existencia del cero en $\mathbb{N}$ no se fija, existen autores que prefieren incluirlo, otros que no. Por lo tanto es probable que en algunos libros podamos ver la definición $\mathbb{N} = \{1, 2, \dots\}$, o en otros $\mathbb{N} = \{0, 1, 2, \dots\}$. Por convención, trabajaremos con la primera definición de $\mathbb{N}$. Dentro de $\mathbb{N}$ existen ecuaciones que no poseen solución, como por ejemplo $x + 3 = 2$. Todos sabemos que $x = -1$ es una solución para este problema, pero -1 no es un número natural. Es aquí donde entran los números enteros, que estudiaremos en esta primera sección. Sabemos de cursos anteriores que el conjunto de los números enteros se denota por $\mathbb{Z}$ y que se escribe por extensión como $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. La ecuación $x + 3 = 2$ sí tiene solución en $\mathbb{Z}$. Ahora, $\mathbb{Z}$ no resuelve totas las ecuaciones existentes. Por ejemplo, sabemos que $2x + 3 = 8$ tiene por solución $5/2$, el cual no es un número entero, sino racional. Entonces en este punto aparece el conjunto de los números racionales $\mathbb{Q}$ en el cual se puede resolver la ecuación anterior. Hasta el momento, da la impresión de que se "crean" nuevos números, pero en realidad los que se establecen son nuevos axiomas bajo los cuales es posible encontrar soluciones a ciertas ecuaciones que sin tales axiomas serían imposibles de resolver.

Dentro de todas las estructuras que bajos a estudiar, la máxima es aquélla conocida como **cuerpo**. Decimos máxima en el sentido que poseer la mayor cantidad de axiomas. Un ejemplo de cuerpo es el conjunto de los número reales $\mathbb{R}$, el cual posee una suma y una multiplicación $+, \cdot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ que satisface los siguientes axiomas (axiomas de cuerpo):

(1) $a + b = b + a$, para todo $a, b \in \mathbb{R}$.

(2) $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{R}$.

(3) Existe un elemento $0 \in \mathbb{R}$ tal que $a + 0 = a$, para todo $a \in \mathbb{R}$.

(4) Para cada $a \in \mathbb{R}$, existe $-a \in \mathbb{R}$ tal que $a + (-a) = 0$.

(5) $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{R}$.

(6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo, $a, b, c \in \mathbb{R}$.

(7) Existe un elemento $1 \in \mathbb{R}$ tal que $a \cdot 1 = a$, para todo $a \in \mathbb{R}$.

(8) Para cada $a \in \mathbb{R} \backslash \{0\}$, existe $a^{-1} \in \mathbb{R}$ tal que $a \cdot a^{-1} = 1$.

(9) $a \cdot (b + c) = a \cdot b + a \cdot c$, para todo $a, b, c \in \mathbb{R}$.

Esta sección está dedicada al conjunto de los números enteros. Consideremos el conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, \dots\}$. Podemos escribir el conjunto de los números emnteros como $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$, donde $-\mathbb{N} = \{-n : n \in \mathbb{N}\}$. El conjunto $\mathbb{N}$ tiene la siguiente propiedad.

Principio del Buen Orden (o Principio del Elemento Mínimo)**.** Todo subconjunto no vacío de $\mathbb{N}$ tiene un elemento menor.

Ejemplo 1.1.1.

(1) Sea $P(x)$ una propiedad que se cumnple para un cierto subconjunto A de $\mathbb{N}$. Entonces existe $a \in A$ tal que $a \leq r$, para todo $r \in A$.

(2) Todo número natural tiene un sucesor inmediato (único). Demostremos esto: Sea $n \in \mathbb{N}$ y consideremos en conjunto $S = \{x \in \mathbb{N} : x > n\}$. Como $S \subseteq \mathbb{N}$, S posee un menor elemento (por el Principio del Buen Orden), llamémoslo a. Si existiera $x \in \mathbb{N}$ tal que $n < x \leq a$ entonces $x \in S$, por tanto $a \leq x$. Entonces $a = x$. Luego, a es el único sucesor inmediato de n.

Obsérvese que que $\mathbb{Z}$ no vale el Principio del Buen Orden. Por ejemplo, $\{n \in \mathbb{Z} : n < 6\}$ no posee un menor elemento. Sin embargo, hay un segundo principio muy importante, válido para $\mathbb{Z}$, conocido como el Principio de Inducción Completa.

Principio de Inducción Completa. Sea $P(n)$ una propiedad sobre $\mathbb{Z}$. Si:

(1) $P(1)$ es cierta;

(2) $P(n+1)$ es cierta siempre que $P(n)$ lo sea;

entonces $P(n)$ es cierta para todo $n \geq 1$.

Existe otra manera de enunciar este principio, y es la siguiente:

Principio de Inducción Completa. Sea P un subconjunto de los número naturales tales que:

(1) $1 \in P$.

(2) $n \in P \Longrightarrow n + 1 \in P$.

Entonces $P = \mathbb{N}$.

Análogamente, tenemos:

Ejercicio 1.1.1. El Principio de Inducción Completa implica el Principio del Buen Orden.

1.2 Divisibilidad

Comencemos con el objeto de estudio principal de la aritmética, la noción de divisibilidad.

Definición 1.2.1. Sean a y b números enteros, con $a \neq b$. Decimos que a **divide a** b o que b es **múltiplo** de a (y lo denotaremos por $a|b$) si existe un entero c tal que $b = c \cdot a$. En caso contrario, denotamos $a \nmid b$.

Ejercicio 1.2.1. Sean a, b y c números enteros, entonces los siguientes enunciados son ciertos:

(1) Si $a|b$ y $b|c$ entonces $a|c$.

(2) Si $a|b$ y $a|c$ entonces $a|(m \cdot b + n \cdot c)$, para cualquier par de enteros m y n.

(3) Si $a|b$ y $b \neq 0$ entonces $0 < |a| \leq |b|$.

(4) Si $a|b$ y $b|a$ entonces $a = \pm b$.

Teorema 1.2.1 (Algoritmo de Euclides o de la División)**.** Dados $a, b \in \mathbb{Z}$, con $b \neq 0$. Entonces existen enteros q y r (únicos) tales que $a = b \cdot q + r$, donde $0 \leq r < |b|$.

Definición 1.2.2. Un entero positivo distinto de 1 se dice **primo** si sólo tiene como divisores al 1 y a él mismo.

Definición 1.2.3. Sean $a, b \in \mathbb{Z}$, no ambos nulos. El **máximo común divisor** entre a y b, denotado por (a, b), es un número entero positivo c tal que:

(1) $c|a$ y $c|b$.

(2) Si $d|a$ y $d|b$ entonces $d|c$.

Ejercicio 1.2.2. Sean $a, b \in \mathbb{Z}$. Si (a, b) existe entonces es único.

Teorema 1.2.2. Dados $a, b \in \mathbb{Z}$ (no ambos cero), el máximo común divisor entre a y b existe y es de la forma $(a, b) = a \cdot m_0 + b \cdot n_0$, para ciertos $m_o, n_0 \in \mathbb{Z}$.

Demostración: Sea $S = \{a \cdot m + b \cdot n : m, n \in \mathbb{Z}\} \subseteq \mathbb{Z}$. En S existen elementos positivos ya que si $x \in S$, $x = a \cdot m + b \cdot n$, entonces $-x = a \cdot (-m) + b \cdot (-n) \in S$. Sea $A \subseteq S$ el conjunto de los elementos positivos de S. En A vale el Principio del Elemento Mínimo, por tanto A tiene un menor elemento. Sea c ése elemento. Tenemos $c = a \cdot m_0 + b \cdot n_0$, para algún par $m_0, n_0 \in \mathbb{Z}$. Ahora supongamos que $d|a$ y $d|b$. Entonces $a = d \cdot q$ y $b = d \cdot q'$. Tenemos $c = d \cdot q \cdot m_0 + d \cdot q' \cdot n_0 = d \cdot (q \cdot m_0 + q' \cdot n_0)$. Entonces $c|d$. Debemos probar ahora que $c|a$ y $c|b$. Sea $x = a \cdot m + b \cdot n$. Por el Algoritmo de Euclides, $x = c \cdot q + r$, donde $0 \leq r < c$. Es decir $x = q \cdot (a \cdot m_0 + b \cdot n_0) + r$. Luego

$$\begin{aligned} a \cdot m + b \cdot n &= q \cdot (a \cdot m_0 + b \cdot n_0) + r, \\ r &= a \cdot (m - q \cdot m_0) + b \cdot (n - q \cdot n_0) \in A. \end{aligned}$$

Luego, $r = 0$. De donde $x = c \cdot q$ y c divide a todo elemento de S, y luego divide a a y a b. Por lo tanto, $c = a \cdot m_0 + b \cdot n_0$ y c es el máximo común divisor entre a y b. □

Definición 1.2.4. Si $(a, b) = 1$ entonces a y b son **coprimos**.

Ejercicio 1.2.3. Si b es un entero y p es primo entonces $(p, b) = p$ o $(p, b) = 1$ o $p|b$.

(1) $p|b \Longrightarrow (p, b) = p$.

(2) $p \not| \ b \Longrightarrow (p, b) = 1$.

Teorema 1.2.3 (Teorema Fundamental de la Aritmética)**.** Todo entero $a > 1$ se descompone de un modo único en la forma $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, donde $p_1 > p_2 > \cdots > p_r$, cada p_i es primo, y $\alpha_i \in \mathbb{N}$, para cada $1 \leq i \leq r$.

Antes de demostrar esto, establezcamos unos resultados previos.

Lema 1.2.1. Si $a \in \mathbb{Z}$ y $a|bc$, con a y b coprimos, entonces $a|c$.

Demostración: Como a y b son coprimos, existen m_0 y n_0 tales que $1 = m_0 \cdot a + n_0 \cdot b$. Luego, $c = m_0 \cdot c \cdot a + n_0 \cdot b \cdot c$. Como $a|bc$, existe $q \in \mathbb{Z}$ tal que $b \cdot c = q \cdot a$. Entonces $c = c \cdot a \cdot m_0 + a \cdot q \cdot n_0 = (c \cdot m_0 + q \cdot n_0) \cdot a$, es decir $a|c$. □

Corolario 1.2.1. Si p es primo y divide al producto de varios enteros, entonces p divide a uno de esos enteros.

Demostración: Supongamos que $p|(a_1 a_2 \cdots a_r)$. Usemos el Principio de Inducción:

- $r = 2$: Si $p \not| \ a_1$ entonces $(a_1, p) = 1$ y por el lema anterior $p|a_2$. De igual forma se razona si $p \not| \ a_2$.
- Supongamos que si $p|a_1 \cdot a_2 \cdots a_{r-1}$ entonces $p|a_k$ para algún $1 \leq k \leq r - 1$. Sabemos que $p|a_1 \cdot (a_2 \cdots a_r)$. Si $p \not| \ a_1$, $(p, a_1) = 1$ entonces $p|a_2 \cdots a_r$. Por la hipótesis inductiva, se tiene $p|a_j$ para algún $2 \leq j \leq r$. Si $p \not| \ (a_2 \cdots a_r)$ entonces $(p, a_2 \cdots a_r) = 1$ y $p|a_1$.

□

Demostración del Teorema Fundamental de la Aritmética: Usaremos inducción: Si $p(m_0)$ es cierta, y si cada vez que $p(r)$ es cierta para $m_0 \leq r < k$ se tiene que $p(k)$ es cierta, entonces $p(n)$ es cierta para todo $n \geq m_0$.

Si $a = 2$ no hay nada que demostrar. Supongamos que el teorema es cierto para todo entero r, $2 \leq r < k$. Consideremos k. Si k es primo, el teorema vale. Si k no es primo, $k = u \cdot v$, con $u \neq 1$ y $v \neq 1$ con $u < k$ y $v < k$. Por hipótesis inductiva, u y v se escriben como producto de primos: $u = r_1^{\beta_1} \cdot r_2^{\beta_2} \cdots r_s^{\beta_s}$,

$v = q_1^{\gamma_1} \cdot q_2^{\gamma_2} \cdots q_m^{\beta_m}$. Luego, $k = (r_1^{\beta_1} \cdot r_2^{\beta_2} \cdots r_s^{\beta_s}) \cdot (q_1^{\gamma_1} \cdot q_2^{\gamma_2} \cdots q_m^{\beta_m})$. Agrupamos potencias semejantes y reordenando éstas obtenemos la descomposición deseada.

Falta probar la unicidad. Supongamos que $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ y $a = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s}$. Como $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_2^{\beta_2} \cdots q_s^{\beta_s}$, se tiene $p_1 | q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s}$. Como p_1 es primo, por el corolario anterior, $p_1 | q_j$ para algún $j \in \{1, \ldots, s\}$. Luego, $p_1 = q_j \leq q_1$ (1). De igual forma, $q_1 | p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Así que $q_1 | p \cdot t$, para algún $t \in \{1, \ldots, r\}$. Luego, $q_1 = p \cdot t \leq p_1$ (2). De (1) y (2) se concluye que $p_1 = q_1$. Supongamos que $\alpha_1 > \beta_1$. Tenemos $\alpha_1 = \beta_1 + (\alpha_1 - \beta_1)$, por tanto

$$p_1^{\beta_1} \cdot p_1^{\alpha_1 - \beta_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} = p_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$
$$p_1^{\alpha_1 - \beta_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_2^{\beta_2} \cdots q_s^{\beta_s}.$$

Esto no puede ocurrir, así que $\alpha_1 - \beta_1 = 0$, $\alpha_1 = \beta_1$. Hacemos igual con $p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_2^{\beta_2} \cdots q_s^{\beta_s}$. Procediendo inductivamente, se obtiene el resultado, es decir, $p_i = q_j$, $\alpha_i = \beta_j$, $1 \leq i \leq r$, $1 \leq j \leq s$, $r = s$. □

1.3 Mínimo común múltiplo

Definición 1.3.1. Sean a y b enteros no nulos. El **mínimo común múltiplo** entre a y b, denotado por $[a, b]$, es un entero positivo m tal que:

(1) $a|m$ y $b|m$.

(2) Siempre que $a|x$ y $b|x$ para algún x, entonces $m|x$.

Ejercicio 1.3.1. Probar que el mínimo común múltiplo entre a y b es único.

Teorema 1.3.1. Si a y b son enteros no nulos, entonces $|a \cdot b| = [a, b] \cdot (a, b)$.

Demostración: Sea $m = [a, b]$ y $d = (a, b)$. Entonces $\frac{||a \cdot b}{d} = \frac{|a|}{d} \cdot |b| = |a| \cdot \frac{|b|}{d}$. Tenemos $a|(|a \cdot b|/d)$ y $b|(|a \cdot b|/d)$. Luego, $m|(|a \cdot b|/d)$ (1). Por otra parte, $|a \cdot b|$ es un múltiplo común de a y b; por lo tanto $m||a \cdot b|$ y en particular $|a \cdot b|/m$ es un entero. Ahora bien, $m = k \cdot a$. Luego, $\frac{k \cdot |a \cdot b|}{m} = \frac{k \cdot |a| \cdot |b|}{m} = \pm b$. Es decir, $\frac{|a \cdot b|}{m} \mid b$. Análogamente, $\frac{|a \cdot b|}{m} \mid a$. Es decir, $\frac{|a \cdot b|}{m}$ es un divisor común entre a y b. Luego, $\frac{|a \cdot b|}{m} \mid d$ y $\frac{|a \cdot b|}{m} \leq d$ (2). De (1) y (2) se obtiene $\frac{|a \cdot b|}{d} = m$. □

1.4 Relaciones de equivalencia y conjunto cociente

Alguna vez hemos llegado a pensar en la siguiente "definición" de números racionales:

$$\mathbb{Q} = \{a/b : a, b \in \mathbb{Z},\ b \neq 0\}.$$

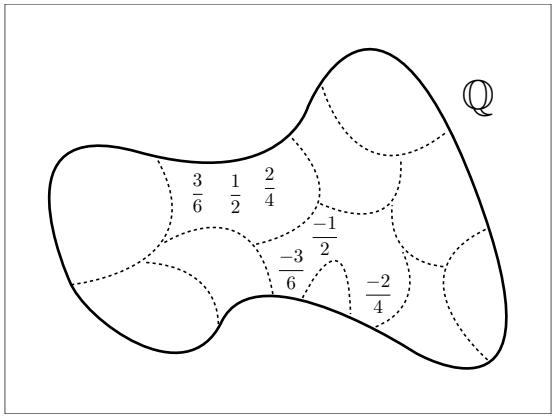
El problema con esta "definición" es que cada punto racional de la recta real tiene asociada una familia de elementos de $\mathbb{Q}$. Por ejemplo, el punto $1/2$ tiene asociados a los números $2/4$, $4/8$, $-8/(-16)$, entre otros. La definición correcta de $\mathbb{Q}$ es la siguiente: Consideremos el conjunto $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ con la siguiente relación:

$$(a, b) \sim (c, d) \Longleftrightarrow a \cdot d = b \cdot c.$$

Esta relación resulta ser una relación de equivalencia. El conjunto de los números racionales está definido por

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})/\sim .$$

Dicho de otra manera, $\mathbb{Q}$ es el conjunto de elementos a/b donde $a \in \mathbb{Z}$ y $b \in \mathbb{Z}\backslash\{0\}$ con la relación de igualdad $a/b = c/d$ si y sólo si $a \cdot d = b \cdot c$. Bajo esta relación, en $\mathbb{Q}$ no se tienen elementos repetidos. Las clases que se producen bajo esta relación de igualdad son disjuntas.



Definición 1.4.1. Sea S un conjunto. Una **partición** de S es una descomposición en bloques de S, tal que:

(1) Todo elemento de S está en un bloque. Denotaremos los bloques de la siguiente forma: $\overline{b}$, para $b \in S$.

Dos bloques $\overline{a}$ y $\overline{b}$ satisfacen:

(2) $\overline{a} \cap \overline{b} = \emptyset$ o $\overline{a} = \overline{b}$.

(3) La unión de todos los bloques de una partición es igual al conjunto S.

Volviendo a $\mathbb{Q}$, tenemos, por ejemplo, $\frac{1909}{4897} = \frac{1403}{3599}$ pues $1909 \cdot 3599 = 1403 \cdot 4897$. Veamos lo siguiente, sea $a \in \mathbb{Q}$:

(1) $a \in \overline{a}$.

(2) Si $a, b \in \overline{x}$, $b, a \in\in \overline{x}$.

(3) Si $a, b \in \overline{x}$ y $b, c \in \overline{y}$, entonces $a \in \overline{y}$ y por tanto $\overline{x} = \overline{y}$.

Entonces denotamos $a \sim b$ si $a, b \in \overline{x}$.

(1) $a \sim a$.

(2) Si $a \sim b$ entonces $b \sim a$.

(3) Si $a \sim b$ y $b \sim c$ entonces $a \sim c$.

Teorema 1.4.1. Sea S un conjunto no vacío y sea $\sim$ una ralación entre elementos de S que satisface las propiedades siguientes:

(1) **Reflexividad:** $a \sim a$ para todo $a \in S$.

(2) **Simetría:** Si $a \sim b$ entonces $b \sim a$, para todo $a, b \in S$.

(3) **Transitividad:** Si $a \sim b$ y $b \sim c$ entonces $a \sim c$.

Entonces $\sim$ produce una partición de S, donde $\overline{a} = \{x \in S : x \sim a\}$ representa el bloque donde está $a \in S$. Recíprocamente, toda partición de S da lugar a una relación natural que verifica las propiedades (1), (2) y (3), definiendo $a \sim b \Longleftrightarrow \overline{a} = \overline{b}$.

Demostración: Ya hemos demostrado la proposición recíproca. Sea $a \in S$, entonces $a \in \overline{a}$ (por (1)). Sea $b \in S$, entonces $b \in \overline{b}$ (por (1)). Supongamos que $\overline{a} \cap \overline{b} \neq \emptyset$, entonces existe $x \in \overline{a}$ y $x \in \overline{b}$. De donde $x \sim a$ y $x \sim b$. Por simetría, $a \sim x$ y $x \sim b$. Se sigue por transitividad que $a \sim b$, es decir $a \in \overline{b}$. Tenemos $\overline{a} \subseteq \overline{b}$. De igual forma se puede probar que $\overline{b} \subseteq \overline{a}$. Luego $\overline{a} = \overline{b}$. Si $S = \emptyset$ no se cumple la propiedad reflexiva. □

Una relación que satisface las propiedades reflexiva, simétrica y transitiva, se llama **relación de equivalencia**. Cada bloque $\overline{a}$ en la partición dada por la relación se llama **clase de equivalencia de** a y al conjunto de clases de equivalencia se denomina **conjunto cociente**.

Ejemplo 1.4.1. Consideremos la relación $\frac{m}{n} \sim \frac{r}{s}$ si, y sólo si, $m \cdot s = n \cdot r$. Veamos que es una relación de equivalencia:

(1) Reflexividad: $\frac{m}{n} \sim \frac{m}{n}$ vale pues $m \cdot n = n \cdot m$.

(2) Simetría: Si $m/n \sim r/s$, entonces ¿$r/s = m/n$?. Tenemos $m \cdot s = n \cdot r$. Luego $n \cdot r = m \cdot s$, es decir $r \cdot n = s \cdot m$, es decir $r/s = m/n$.

(3) Transitividad: Si $m/n \sim r/s$ y $r/s \sim p/q$, entonces ¿$m/n \sim p/q$? Tenemos $m \cdot s = r \cdot n$ y $r \cdot q = p \cdot s$. De donde $(m \cdot s) \cdot q = (r \cdot n) \cdot q$, es decir $(r \cdot q) \cdot n = (p \cdot s) \cdot n$. Se sigue $0 = (m \cdot s) \cdot q - (p \cdot s) \cdot n = (m \cdot q - p \cdot n) \cdot s$. Como $s \neq 0$, nos queda $m \cdot q - p \cdot n = 0$, es decir $m \cdot q = p \cdot n$.

Ejercicio 1.4.1. Defínase en $\mathbb{Z}$ la relación R de la siguiente forma: $aRb \Longrightarrow a \cdot b \geq 0$. Demuestre que R no es una relación de equivalencia.

Ejemplo 1.4.2. Para cada $n \in \mathbb{Z}^+$, tenemos una relación importante, la relación de **congruencia módulo** n. Sean $h, k \in \mathbb{Z}$, decimos que h es **congruente** con k **módulo** n ($b \equiv k \pmod{n}$) si, y sólo si, $h - k = n \cdot r$ para algún $r \in \mathbb{Z}$.

Ejercicio 1.4.2. Demuestre que para $n \in \mathbb{Z}^+$, la congruencia módulo n es una relación de equivalencia para $n = 1, 2, 3, 4$. Generalice lo observado para cualquier n.

Al conjunto de clases de equivalencia de la relación de congruencia (módulo n) se le denota por $\mathbb{Z}_n$.

Definición 1.4.2. Se dice que un conjunto $C = \{x_1, x_2, \ldots, x_m\}$ es un **sistema completo de restos módulo** m si para cualquier entero y existe un único entero $x_i \in C$ tal que $y \equiv x_i \pmod{m}$.

Un **sistema reducido de restos módulo** m es un conjunto $R = \{x_1, x_2, \ldots, x_k\}$ tal que para cualquier número entero y primo con m existe un único entero $x_i \in R$ tal que $y \equiv x_i \pmod{m}$.

Un sistema reducido de restos módulo m puede obtenerse a partir de un sistema completo de restos módulo m, eliminando de este último aquellos enteros que no son primos con m. Si se tienen dos sistemas reducidos de restos módulo m, digamos R y R', cada elemento de R es congruente módulo m con un único elemento de R', y viceversa. Por consiguiente, todos los sistemas reducidos de restos módulo m tienen el mismo número de elementos. A este número se le llama **Indicador de Euler** de m y se denota por $\phi(m)$.

Dado que los elementos de un sistema reducido de restos módulo m pueden obtenerse a partir del sistema completo de restos módulo m formado por los números 1, 2, ..., $m-1$, m, tenemos que $\phi(m)$ indica el número de enteros positivos menores o iguales que m que son coprimos con m. En particular, nótese que si m es primo entonces $\phi(m) = m - 1$.

Si $X = \{x_1, \ldots, x_k\}$ es un sistema completo (o reducido) de restos módulo m y $(a, m) = 1$, entonces $a \cdot x = \{a \cdot x_1, \ldots, a \cdot x_k\}$ es también un sistema completo (resp. reducido) de restos módulo m.

Teorema 1.4.2 (Teorema de Euler)**.** Si $(a, m) = 1$ entonces $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración: Consideremos un sistema reducido de restos módulo m, $R = \{x_1, x_2, \ldots, x_{\phi(m)}\}$. Como $(a, m) = 1$ el conjunto $a \cdot R = \{a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_{\phi(m)}\}$ es también un sistema reducido de restos módulo m. Por consiguiente, a cada $x_i \in R$ le corresponde un y sólo un $a \cdot x_j \in a \cdot R$ tal que $x_i \equiv a \cdot x_j \pmod{m}$. Además, a elementos diferentes de R les corresponderán elementos diferentes de $a \cdot R$, por tanto $a \cdot x_1$, $a \cdot x_2$, ..., $a \cdot x_{\phi(m)}$ son congruentes con x_1, x_2, ..., $x_{\phi(m)}$ módulo m (no necesariamente en ese orden). Luego,

$$(a \cdot x_1) \cdot (a \cdot x_2) \cdots (a \cdot x_{\phi(m)}) \equiv x_1 \cdot x_2 \cdots x_{\phi(m)} \pmod{m}$$
$$x_1 \cdot x_2 \cdots x_{\phi(m)} \cdot a^{\phi(m)} \equiv x_1 \cdot x_2 \cdots x_{\phi(m)} \pmod{m},$$

y como $(x_1 \cdot x_2 \cdots x_{\phi(m)}, m) = 1$ se tiene $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Teorema 1.4.3 (Pequeño Teorema de Fermat)**.** Si p es primo tal que $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Demostración: Como $p \nmid a$ y p es primo, se tiene que $(p, a) = 1$. Además, $\phi(p) = p - 1$. Por el Teorema de Euler, $a^{p-1} \equiv 1 \pmod{p}$. Luego se tiene $a^p \equiv a \pmod{p}$. □

Teorema 1.4.4 (Teorema de Wilson)**.** Sea p un número primo. Entonces $(p-1)! \equiv -1 \pmod{p}$.

Demostración: Sea j un entero tal que $1 \leq j \leq p-1$, entonces $(p, j) = 1$ (porque p es primo). Consideremos $i \cdot j \equiv 1 \pmod{p}$ (1). Se tiene $i \cdot j = 1 + k \cdot p$, con $k \in \mathbb{Z}$. Se sigue $i \cdot j = m_0 \cdot p + n_0 \cdot j + k \cdot p$, con $m_0, n_0 \in \mathbb{Z}$. Nos queda $i \cdot j = n_0 \cdot j + (m_0 + k) \cdot p$. Tenemos $p | j \cdot (i - n_0)$. Como $(p, j) = 1$, nos queda $p | (i - n_0)$. Luego $i = n_0 + \alpha \cdot p$. La ecuación (1) tiene solución única en i tal que $0 \leq i \leq p-1$. Evidentemente, $i \neq 0$. Luego tenemos $1 \leq i \leq p-1$. Si a cada j le asignamos un i correspondiente, como $i \cdot j \equiv j \cdot i \equiv 1 \pmod{p}$ podemos observar que j es el entero asociado con i. Observamos además que $1 \cdot 1 \equiv 1 \pmod{p}$ y $(p-1)^2 \equiv 1 \pmod{p}$, luego 1 y $p-1$ se asocian con ellos mismos. Consideremos los casos en que $2 \leq j \leq p-2$. PAra estos enteros se tiene que $(j-1, p) = 1$ y $(j+1, p) = 1$. Por consiguiente, $(j^2 - 1, p) = 1$ y entonces $j^2 \not\equiv 1 \pmod{p}$. Luego, todo j tal que $2 \leq j \leq p-2$ está asociado con un i tal que $i \neq j$ y $2 \leq i \leq p-2$. Por tanto, los enteros 2, 3, $\ldots$, $p-2$ pueden ser asociados en parejas $\{i, j\}$ tales que $j \cdot i \equiv 1 \pmod{p}$. It follows $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$, and since $1 \cdot (p-1) \equiv -1 \pmod{p}$, we obtain $(p-1)| \equiv -1 \pmod{p}$. □

1.5 Problemas

Problema 1.1. Decida si en los siguientes conjuntos se satisface o no el Principio del Elemento Mínimo:

(a) $\mathbb{R}^+$, el conjunto de los reales positivos.

(b) $A = \{n^2 : n \in \mathbb{Z}\}$.

Problema 1.2. Demuestre que no puede existir una sucesión decreciente infinita de enteros positivos.

Problema 1.3. Demuestre que si $(a, m) = 1$ y $(b, m) = 1$, entonces $(a \cdot b, m) = 1$.

En $\mathbb{Z}_n$, tenemos las siguientes operaciones:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \qquad (\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b} = \overline{a + b}.$$
$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \qquad (\overline{a}, \overline{b}) \mapsto \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Problema 1.4. Demostrar que la operación $+$ definida en $\mathbb{Z}_n$ está bien definida, esto es que si $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$ entonces $\overline{a + b} = \overline{a' + b'}$. Verifique además que $(\mathbb{Z}_n, +)$ se comporta de la misma manera que $\mathbb{Z}$ con respecto a la suma en $\mathbb{Z}$ usual.

Problema 1.5. Verifique que la operación $\cdot$ definida en $\mathbb{Z}_n$ está bien definida. Ver además si esta operación se comporta como el producto usual en $\mathbb{Z}$, y si no lo hace dar las condiciones para que esto suceda.

Sugerencia: Ver que pasa con n primo y con n no primo.

Problema 1.6. Decida si son ciertas o falsas las siguientes afirmaciones:

(a) Si $a|b$ y $b|a$ entonces $a = \pm b$.

(b) Si $a|(c + b)$ entonces $a|b$.

(c) Si $a|(b \cdot c)$ entonces $a|b$ o bien $a|c$.

(d) Si $b|g$ y $b|h$ entonces $b|(r \cdot g + s \cdot h)$, para cualesquiera enteros r y s.

(e) Si $a^2|b^2$ entonces $a|b$.

(f) Si $s|b^2$ entonces $a^2|b^2$.

(g) Si $d = (a, b)$, $a|c$ y $b|c$ entonces $(a \cdot b)|(d \cdot c)$.

Problema 1.7. Demuestre que $n > 1$ es un número primo si, y sólo si, para cualquier entero a se tiene que $(a, n) = 1$ o $n|a$.

Problema 1.8. Demuestre que existen infinitos números primos.

Problema 1.9. Sea n un entero positivo. Demuestre que si n es primo y si $\overline{a} \neq \overline{0}$, entonces existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

Problema 1.10. Si $a \cdot b \equiv a \cdot c \pmod{m}$ y $d = (a, m)$, entonces $b \equiv c \pmod{m/d}$.

Problema 1.11. Supongamos que $(a, m) = 1$. Si $a \cdot b \equiv a \cdot c \pmod{m}$, entonces $b \equiv c \pmod{m}$.

Problema 1.12. La ecuación $a \cdot x \equiv b \pmod{m}$ tiene solución si, y sólo si, $(a, m)|b$.

Problema 1.13. Demuestre que n es primo si, y sólo si, en $\mathbb{Z}_n$ $\overline{a} \cdot \overline{b} = 0$ implica $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$.

Problema 1.14. Demuestre que si n es impar, entonces $\overline{0} + \overline{1} + \cdots + \overline{n-1} = \overline{0}$. ¿Qué pasa si n es par?.

Problema 1.15. Si de una cesta se sacan huevos de 2 en 2, de 3 en 3, de 5 en 5, sobran uno, dos y tres huevos respectivamente. ¿Cuántos huevos había en el canasto?.

Problema 1.16. Encuentre la intersección de la clase del 7 módulo 4 y la clase del 5 módulo 15.

Problema 1.17. Demuestre que si $13 \not| \ a$ y $13 \not| \ b$, entonces $a^{12} \equiv b^{12} \pmod{13}$.

Problema 1.18. Demuestre que si a y b son primos relativos con 91, entonces $a^{12} - b^{12}$ es divisible por 91.

CAPÍTULO 2

GRUPOS

Vagamente hablando, un grupo es un conjunto no vacío junto con una operación benaria que satisface ciertas propiedades. Recordemos que una operación binaria sobre un conjunto S es una función

$$\begin{aligned} * : S \times S &\longrightarrow S \\ (a, b) &\mapsto a * b. \end{aligned}$$

Consideremos los siguientes ejemplos de operaciones binarias en $\mathbb{Z}^+$:

(1) $a * b = \min\{a, b\}$. Por ejemplo, $1 * 10 = 1$, $2 * 2 = 2$, $3 * 1 = 1$.

(2) $a * b = a$, observe que $1 * 3 = 1$ y $3 * 1 = 3$. Note que $*$ no es conmutativa.

(3) $a *' b = (a * b) + 2$, donde $a * b = \min\{a, b\}$. Por ejemplo, tenemos $(2 *' 3) *' 1 = 4 *' 1 = 3$ y $2 *' (3 *' 1) = 2 *' 3 = 4$. En este caso $*'$ no es asociativa.

Recordemos los conceptos usados en los ejemplos anteriores. Una operación binaria $* : S \times S \longrightarrow S$ es:

(1) **conmutativa** si $a * b = b * a$, para todo $a, b \in S$;

(2) **asociativa** si $a * (b * c) = (a * b) * c$, para todo $a, b, c \in S$.

2.1 El concepto de Grupo. Ejemplos

Definición 2.1.1. Un grupo es un par $(G, *)$ donde G es un conjunto no vacío, y $*$ es una operación binaria $G \times G \longrightarrow G$ que satisface los siguientes axiomas:

(1) $*$ es asociativa.

(2) Existe $e \in G$ tal que $a * e = a$ y $e * a = a$, para todo $a \in G$. A tal e se le llama **elemento neutro**, **identidad** o **cero**.

(3) Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$. A a' se le llama **elemento inverso** o **recíproco** de a.

Ejemplo 2.1.1.

(1) Sea $\mathrm{GL}_n(\mathbb{R})$ el conjunto de las matrices de orden n con coeficientes en $\mathbb{R}$ que son invertibles. Con el producto usual de matrices $\mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{R})$, el par $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ es un grupo, conocido como **grupo lineal general**. Es importante recordar que si A y B son matrices invertibles del mismo orden, entonces $A \cdot B$ es invertible y $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

(2) Sea $S = \{-1, 1\}$ y $*$ el producto usual en $\mathbb{Z}$. Entonces $(S, *)$ es un grupo.

(3) El conjunto $\mathbb{Z}$ con la operación usual es también ejemplo de grupo.

(4) El conjunto de los enteros positivos $\mathbb{Z}^+$ es un grupo con respecto a la multiplicación, mientras que con respecto a la suma usual no lo es.

Teorema 2.1.1. Si G es un grupo con operación binaria $*$, entonces valen las leyes de cancelación izquierda y derecha, es decir:

(1) $a * b = a * c \Longrightarrow b = c$.

(2) $b * a = c * a \Longrightarrow b = c$.

Demostración: Sólo probaremos (1), pues (2) es similar. Por la existencia del elemento inverso a^{-1} y por la propiedad asociativa y la del elemento neutro e, tenemos

$$b = e * b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * (a * c) = c.$$

□

Proposición 2.1.1. En un grupo $(G, *)$ la ecuaciones $a * x = b$ y $y * a = b$ tienen solución única en G.

Demostración: Sólo haremos la prueba para la ecuación $a * x = b$. Multiplicamos por el elemento inverso de a y usamos los otros dos axiomas de grupo:

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

Tenemos que $a^{-1} * b$ es una solución para la ecuación anterior. Falta probar que es única. Supongamos que tenemos dos soluciones x_1 y x_2 para la ecuación $a * x = b$. Luego se tiene $a * x_1 = a * x_2$. Por la ley de cancelación izquierda, nos queda $x_1 = x_2$. □

Proposición 2.1.2. Sea $(G, *)$ un grupo, entonces:

(1) e es único.

(2) a^{-1} es único para cada $a \in G$.

(3) $(a * b)^{-1} = b^{-1} * a^{-1}$.

Demostración:

(1) Supongamos la existencia de dos elementos neutros e y e'. Tenemos $e = e * e' = e'$.

(2) Supongamos que a' y a'' son inversos de $a \in G$. Tenemos

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

(3) Tenemos

$$(a * b) * (b^{-1} * a^{-1}) =]a * (b * b^{-1})] * a^{-1} = [a * e] * a^{-1} = a * a^{-1} = e.$$
$$(b^{-1} * a^{-1}) * (a * b) = b^{-1}[(a^{-1} * a) * b] = b^{-1} * (e * b) = b^{-1} * b = e.$$

Por la parte (2), se tiene $(a * b)^{-1} = b^{-1} * a^{-1}$.

□

Definición 2.1.2. Un grupo $(G, *)$ es abeliano si la operación $*$ es conmutativa.

Ejemplo 2.1.2. En conjunto $M_n(\mathbb{R})$ de las matrices cuadradas de orden n con coeficientes en $\mathbb{R}$, equipado con la suma usual, es un grupo abeliano.

Ejercicio 2.1.1. Defínase $*$ en $\mathbb{Q}^+$ por $a * b = \frac{a \cdot b}{2}$. Verifique si $(\mathbb{Q}^+, *)$ es un grupo, y en caso afirmativo vea si es abeliano.

Ejemplo 2.1.3. En $\mathbb{R}^2$, consideremos las rotaciones $\rho_i : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, las reflexiones $\mu_i : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ con respecto a los ejes X e Y, y las reflexiones $\delta_i : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ con respecto a las diagonales. Estos movimientos rígidos conforman el llamado **grupo diedral** de orden 4, $D_4 = \{\rho_i, \mu_i, \delta_i\}$, donde la operación binaria es la composición.

Ejercicio 2.1.2. Describir todas las operaciones ρ_i, μ_i y δ_i posibles. Haga la tabla para el producto $*$ definido en D_4. Describa todas las cosas interesantes que se observen en la tabla. Demuestre que D_4 no es abeliano.

2.2 Grupos finitos

Definición 2.2.1. Un grupo finito $(G, *)$ es aquel tal que la cardinalidad de G es finita. Si G es un grupo finito, se define el **orden** de G como el número de elementos de G. Denotaremos el orden de G por $|G|$.

Sólo existe un grupo de orden 1, en el sentido de que todos los grupos de orden 1 son isomorfos a $(\{x\}, *)$, donde

$*$	x
x	x

También existe sólo un grupo de dos elementos, digamos $G = \{e, a\}$, donde e es el elemento identidad.

$*$	e	a
e	e	a
a	a	e

Lo mismo para grupos de tres elementos, sólo existe uno de ellos, digamos $G = \{e, a, b\}$.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Ejercicio 2.2.1. Demuestre que sólo hay dos grupos con cuatro elementos, uno con cinco elementos, y dos con seis elementos.

Si $(G, +)$ es un grupo abeliano, usaremos la notación $* = +$, $e = 0$, $a^n = n \cdot a$ y $a^{-1} = -a$.

2.3 Subgrupos

Definición 2.3.1. Un subconjunto no vacío H de un grupo G se denomina **subgrupo** de G si H, dotado con la misma operación binaria de G, es un grupo. Esta condición la denotaremos por $H \leq G$.

Ejemplo 2.3.1.

(1) Todo grupo G es un subgrupo se sí mismo.

(2) $\{e\}$ es subgrupo de G, siempre que G sea un grupo y e sea el elemento neutro de G. Los conjunto G y $\{e\}$ son llamados **subgrupos triviales** de G.

(3) $\mathbb{Z}$ es un subgrupo de $(\mathbb{Q}, +)$.

(4) $2 \cdot \mathbb{Z}$ es un subgrupo de $(\mathbb{Z}, +)$.

Ejercicio 2.3.1. Sean

$$H_1 = \{A \in \mathrm{GL}_2(\mathbb{R}) : A \text{ es una matrix triangular superior}\} \text{ y}$$
$$H_2 = \{A \in \mathrm{GL}_2(\mathbb{R}) : \det(A) = 1\}.$$

Verificar que H_1 y H_2 son subgrupos de $\mathrm{GL}_2(\mathbb{R})$ bajo una cierta operación. ¿Cuál es?.

Teorema 2.3.1. Sea $H \subseteq (G, *)$. Una condición necesaria y suficiente para que H sea un subgrupo de $(G, *)$ es que satisfaga:

(1) $H \neq \emptyset$.

(2) $a * b \in H$, para todo $a, b \in H$.

(3) Existe $e \in H$ tal que $a * e = e * a = a$, para todo $a \in H$.

(4) Para cada $a \in H$, existe $a^{-1} \in H$ tal que $a * a^{-1} = a^{-1} * a = e$.

Demostración: La implicación $H \leq (G, *) \Longrightarrow$ (1), (2), (3) y (4) es trivial.

Ahora asumamos (1), (2), (3) y (4). Por (1) y (2), se tiene que $*$ es una operación binaria sobre H, que es asociativa por serlo en G. Como $H \neq \emptyset$, existe $a \in H$. Por (4), $a^{-1} \in H$ y así $e = a^{-1} * a \in H$. □

Ejercicio 2.3.2. Probar que un subconjunto no vacío H de un grupo G es un subgrupo de G si, y sólo si, $a \cdot b^{-1} \in H$ para todo $a, b \in H$.

Teorema 2.3.2. Si H es un subconjunto finito no vacío de un grupo G, y H es cerrado respecto a la operación de G, entonces H es un subgrupo de G.

Demostración: Sea $a \in H$, como la operación de G es cerrada en H, tenemos que $a, a^2, a^3, \cdots \in H$. Pero H es finito, luego debe haber repeticiones de estos elementos. Luego, sean r y s enteros tales que $a^r = a^s$. Supongamos sin pérdida de generalidad que $r > s > 0$.Por la ley de cancelacón, tenemos $H \ni a^{r-s} = e$. Como $r > s$, tenemos $r - s - 1 \geq 0$, por lo que $a^{r-s} \cdot a^{-1} = a^{r-s-1} \in H$. Tenemos $a^{-1} = a^{r-s-1}$ porque $a^{\cdot r-s-1} = a^{r-s} = e$. □

Teorema 2.3.3. Si para cada $i \in I$, H_i es un subgrupo de G, entonces $H = \bigcap_{i \in I} H_i$ es un subgrupo de G.

Demostración: Note que $H \neq \emptyset$ ya que $e \in H_i$ para todo $i \in I$. Ahora, sean $x, y \in H$. Veamos que $x \cdot y^{-1} \in H$. Como $x, y \in H$, se tiene $x, y \in H_i$ para todo $i \in I$. Como cada $H_i \leq G$, se tiene $x \cdot y^{-1} \in H_i$ para todo $i \in I$. Entonces $x \cdot y^{-1} \in H$. Por lo tanto $H \leq G$. □

Definición 2.3.2. Sea G un grupo y $X \subseteq G$ un subconjunto de G. Definimos el **subgrupo de G generado por X** por

$$K = \bigcap \{H : X \subseteq H \text{ y } H \leq G\}.$$

Denotaremos a K por $K = \langle X \rangle$.

Si existiera otro subgrupo H' tal que $X \subseteq H$ y $H' \subseteq \langle X \rangle$, entonces $\langle X \rangle \subseteq H'$, por definición de $\langle X \rangle$. Por lo que $H' = \langle X \rangle$. En otras palabras, $\langle X \rangle$ es el menor subgrupo de G que contiene a X.

Si $X = \{a\}$, entonces $\langle X \rangle \ni a, a^2, a^3, \ldots$. Supongamos que existe $b \in \langle X \rangle$ con $b \neq a$. Tenemos que $\{b, b^2, b^3, \ldots\}$ es un subgrupo que no contiene a X. Por lo que $\langle a \rangle := \langle X \rangle = \{a^i : i \in \mathbb{Z}\}$. A este grupo se denomina **grupo cíclico** de generador a.

Por convención,

$$\begin{aligned} a \cdot a \cdot a &= a^n \text{ si } n > 0, \\ a^n &= e \text{ si } n = 0, \\ a^{-1} \cdot a^{-1} \cdots a^{-1} &= a^n \text{ si } n < 0. \end{aligned}$$

Ejercicio 2.3.3. Si G es un grupo y $X \subseteq G$, entonces el subgrupo generado por X, $\langle X \rangle$, es

$$\langle X \rangle = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : n \in \mathbb{N},\ \alpha_i \in \mathbb{Z},\ x_i \in X,\ 1 \leq i \leq n\}.$$

Ejercicio 2.3.4. Muestre que no existe un análogo para el Teorema 2.3.3 si consideramos $H = \bigcup\{H_i : i \in I\}$.

Ejercicio 2.3.5. Pruebe que todo grupo cíclico es abeliano.

2.4 Permutaciones

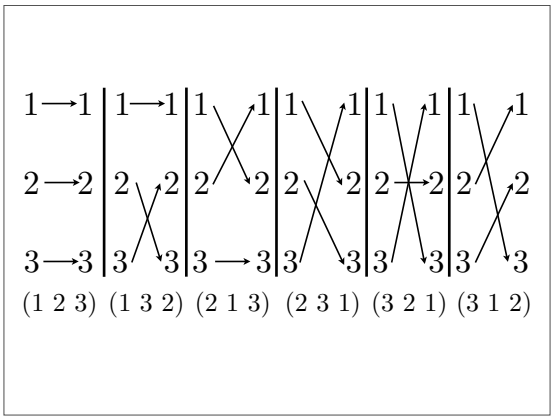
Sea A un conjunto finito $A = \{a_1, a_2, \ldots, a_n\}$. Tenemos la biyección $A \longleftrightarrow [n] := \{1, 2, \ldots, n\}$.

Definición 2.4.1. Sea $A = \{a_1, a_2, \ldots, a_n\}$ un **alfabeto**. Una **palabra de k letras** en el alfabeto A es una sucesión $a_{i_1} a_{i_2} \cdots a_{i_k}$ donde $a_{i_j} \in A$.

Definición 2.4.2. Una **permutación** en $[n]$ es una biyección de $[n]$ en $[n]$. Las podemos identificar con los posibles órdenes que se puedan establecer en n. Al conjunto de todas las permutaciones de $[n]$ lo denotaremos por

$$S_n := \{f : [n] \longrightarrow [n] \ / \ f \text{ es biyectiva}\}.$$

Ejemplo 2.4.1. Para [3], tenemos las permutaciones siguientes:



Si $\sigma, \pi \in S_n$, definimos $\sigma * \pi$ por $\sigma \circ \pi \in S_n$.

Ejemplo 2.4.2. En S_3, $\sigma = (2\ 1\ 3)$ y $\pi = (2\ 3\ 1)$ entonces $\sigma \circ \pi = (1\ 3\ 2)$.

Sabemos que si f, g y h son funciones de A en A, entonces

(1) $(f \circ g) \circ h = f \circ (g \circ h)$.

(2) En general, $f \circ g \neq g \circ f$.

(3) Siempre existe la biyección identidad $\mathrm{Id} : A \longrightarrow A$.

En S_n, tenemos:

(1) $(\sigma \circ \pi) \circ \tau = \sigma \circ (\pi \circ \tau)$.

(2) Existe $\mathrm{Id} \in S_n$ tal que $\sigma \circ \mathrm{Id} = \mathrm{Id} \circ \sigma = \sigma$, para todo $\sigma \in S_n$.

(3) Para cada $\sigma \in S_n$, existe $\sigma^{-1} \in S_n$ tal que $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}$

Ejercicio 2.4.1. Probar (3).

Si $\mathrm{Card}(A) = n$ y σ es una biyección $A \longrightarrow A$. Como hay una biyección entre A y $[n]$ dada por $a_i \longrightarrow i$, entonces podemos escribir σ como una biyección $[n] \longrightarrow [n]$. Entonces

$$S_n = \{\sigma : A \longrightarrow A \ / \ \mathrm{Card}(A) = n \text{ y } \sigma \text{ es biyectiva}\}.$$

Ejercicio 2.4.2. Demuestre que $(S_n, \circ)$ tiene estructura de grupo.

Denotaremos $\sigma \in S_n$ por

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \longrightarrow (\ \sigma(1) \quad \sigma(2) \quad \cdots \quad \sigma(n)\ )$$

Lema 2.4.1. S_n tiene $n!$ elementos.

Ejemplo 2.4.3. Analicemos la estructura de grupo de S_3. Por el lema anterior, S_3 tiene 6 elementos, que son:

$$e = (1\ 2\ 3),\ \rho_1 = (1\ 3\ 2),\ \rho_2 = (2\ 1\ 3),\ \rho_3 = (2\ 3\ 1),\ \rho_4 = (3\ 1\ 2),\ \rho_5 = (3\ 2\ 1).$$

$\circ$	e	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
e	e	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	e	ρ_4	ρ_5	ρ_2	ρ_3
ρ_2	ρ_2	ρ_3	e	ρ_1	ρ_5	ρ_4
ρ_3	ρ_3	ρ_2	ρ_5	ρ_4	e	ρ_1
ρ_4	ρ_4	ρ_5	ρ_1	e	ρ_3	ρ_2
ρ_5	ρ_5	ρ_4	ρ_3	ρ_2	ρ_1	e

Sabemos que los grupos con orden (cardinalidad) del 1 al 5 son abelianos. Como vemos en este ejemplo, no todos los grupos de orden 6 son abelianos.

Sea $\sigma \in S_n$. Existe $a \in [n]$ tal que

$$a \mapsto \sigma(a) \mapsto \sigma \circ \sigma(a) \mapsto \cdots \mapsto \sigma^k(a) = a$$
$$a \mapsto a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k = a$$

donde $a_i \neq a$ para todo $i \in \{1, 2, \ldots, k-1\}$. La sucesión $(a, a_1, a_2, \ldots, a_{k-1})$ se denomina **ciclo** de la permutación σ.

Ejemplo 2.4.4. Sea $\sigma \in S_3$ dada por $\sigma = (1\ 3\ 2)$. Entonces tenemos dos ciclos: $1 \longrightarrow 1$ y $2 \longrightarrow 3 \longrightarrow 2$.

En general, para $a \in [n]$, existe $i \in \mathbb{N}$ tal que $\sigma^i(a) = a$, pues de lo contrario se forma un conjunto infinito. Toda permutación $\sigma \in S_n$ puede escribirse como

$$\sigma = (a_1, \sigma(a_1), \ldots, \sigma^{i_1-1}(a_1))(a_2, \sigma(a_2), \ldots, \sigma^{i_2-1}(a_2)) \cdots (a_r, \sigma(a_r), \ldots, \sigma^{i_r-1}(a_r)).$$

Ejercicio 2.4.3. Demuestre que toda permutación $\sigma \in S_n$ se puede descomponer como producto de ciclos disjuntos.

Ejercicio 2.4.4. Escriba $\sigma = (1\ 3\ 4\ 8\ 9\ 7\ 6\ 2\ 5) \in S_9$ como producto de ciclos.

Definición 2.4.3. A un ciclo de longitud 1 de una permutación σ se le denomina **punto fijo** de σ. A todo ciclo de longitud 2 se le denomina **transposición**.

Ejercicio 2.4.5. Demuestre que $(a_1\ a_2 \cdots\ a_n) = (a_1\ a_2)(a_1\ a_3) \cdots (a_1\ a_n)$.

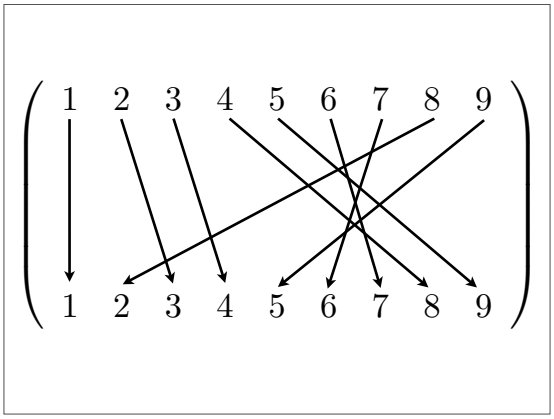
Ejercicio 2.4.6. Toda permutación puede escribirse como producto de transposiciones.

Definición 2.4.4. El signo de una permutación $\sigma \in S_n$ se define como

$$\operatorname{sign}(\sigma) = \begin{cases} 1 & \text{si el número de transposiciones de } \sigma \text{ es par,} \\ -1 & \text{si el número de transposiciones de } \sigma \text{ es impar.} \end{cases}$$

O equivalentemente, $\operatorname{sign}(\sigma) = (-1)^{n-\text{número de ciclos}}$.

Ejemplo 2.4.5. La permutación $\sigma = (1\ 3\ 4\ 8\ 9\ 7\ 6\ 2\ 5)$ tiene 14 transposiciones, de donde $\operatorname{sign}(\sigma) = 1$. Note que el número que transposiciones coincide con el número de cruces entre las flechas de la siguiente representación de σ:



2.5 Homomorfismos

Definición 2.5.1. Sean $(G, *)$ y $(H, \circ)$ grupos. Un **homomorfismo de grupos** entre G y H es una función $f : G \longrightarrow H$ que satisface

$$f(g_1 * g_2) = f(g_1) \circ f(g_2).$$

Ejercicio 2.5.1. Si $f : G \longrightarrow H$ es un homomorfismo de grupos, demuestre que $f(e_G) = e_H$ y $f(g^{-1}) = (f(g))^{-1}$.

Ejemplo 2.5.1.

(1) La función identidad $\mathrm{Id} : G \longrightarrow G$ es claramente un homomorfismo de grupos.

(2) La aplicación constante $E : G \longrightarrow H$ dada por $g \mapsto e_H$ es también un homomorfismo de grupos.

(3) La función exponencial $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$ es un homomorfismo de grupos, pues $\exp(x + y) = \exp(x) \cdot \exp(y)$.

Definición 2.5.2. Dado un homomorfismo $f : G \longrightarrow H$, se define el **núcleo** de f como

$$\mathrm{Ker}(f) := \{g \in G : f(g) = e_H\}.$$

La **imagen** de f es el conjunto

$$\mathrm{Im}(f) := \{f(g) : g \in G\}.$$

Proposición 2.5.1. El núcleo y la imagen de un homomorfismo $f : G \longrightarrow H$ son subgrupos de G y H, respectivamente.

Demostración: Sólo probaremos que $\mathrm{Ker}(f)$ es un subgrupo de G. Primero, $\mathrm{Ker}(f)$ es no vacío pues $f(e_G) = e_H$. Sean $a, b \in \mathrm{Ker}(f)$. Tenemos

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

Entonces $a \cdot b^{-1} \in \mathrm{Ker}(f)$. Por lo tanto, $\mathrm{Ker}(f) \leq G$. □

Definición 2.5.3. Un homomorfismo de grupos $f : G \longrightarrow H$ es un **isomorfismo** (o G y H son **grupos isomorfos**) si f es biyectivo.

Proposición 2.5.2. Un homomorfismo de grupos $f : G \longrightarrow H$ es inyectivo si, y sólo si, $\mathrm{Ker}(f) = \{e_G\}$.

Ahora vamos a probar un resultado conocido como el Teorema de Cayley, que nos da un importante ejemplo de isomorfismo. Este teorema afirma que todo grupo G es isomorfo a un subgrupo de permutaciones de G. Sea G un grupo y $a \in G$ fijo. Sea $T_a : G \longrightarrow G$ la aplicación $g \mapsto a \cdot g$. Note que T_a no es necesariamente un homomorfismo. Definamos

$$L(G) := \{T_a : a \in G\}.$$

Sea $S(G)$ el conjunto de todas las permutaciones de G. Note que cada $T_a \in L(G)$ es una permutación de G, pues la inversa de T_a es $T_{a^{-1}}$. Además, $L(G) \neq \emptyset$ ya que $\mathrm{Id}_G = T_e \in L(G)$. Ahora, sean $T_a, T_b \in L(G)$. Es fácil ver que $T_a \circ (T_b)^{-1} = T_{a \cdot b^{-1}} \in L(G)$. Por lo tanto, $L(G) \leq S(G)$. Esto nos va a permitir demostrar el siguiente resultado.

Teorema 2.5.1 (Teorema de Cayley)**.** Todo grupo es isomorfo a un grupo de permutaciones.

Demostración: Sea G un grupo y definamos una aplicación $\varphi : G \longrightarrow L(G)$ por $a \mapsto T_a$. Tenemos que φ es un homomorfismo de grupos, pues

$$\varphi(a \cdot b) = T_{a \cdot b} = T_a \circ T_b = \varphi(a) \circ \varphi(b).$$

Además, φ es un monomorfismo, pues si $T_a = \varphi(a) = \mathrm{Id}_G$ entonces $T_a(g) = T_e(g)$ para todo $g \in G$. En particular, $a = T_a(e) = T_e(e) = e^2 = e$. Es claro que φ es sobreyectiva. Por lo tanto, G es isomorfo a $L(G)$. □

2.6 Clases laterales y clases de congruencia

Sea G un grupo y H un subgrupo de G. Definimos en G la siguiente relación:

$$a \sim b \iff a \cdot b^{-1} \in H.$$

(1) $\sim$ **es reflexiva:** $a \sim a$ ya que $a \cdot a^{-1} = e \in H$.

(2) $\sim$ **es simétrica:** Si $a \sim b$ entonces $a \cdot b^{-1} \in H$. Luego, $b \cdot a^{-1} = (a \cdot b^{-1})^{-1} \in H$. Por lo que $b \sim a$.

(3) $\sim$ **es transitiva:** Supongamos que $a \sim b$ y $b \sim c$. Entonces $a \cdot b^{-1} \in H$ y $b \cdot c^{-1} \in H$. Luego, $a \cdot c^{-1} = (a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$. Por lo tanto, $a \sim c$.

Tenemos que $\sim$ es una relación de equivalencia. A esta relación la llamaremos **congruencia módulo** H. Denotaremos $a \sim b$ por $a \equiv b \pmod{H}$.

Sea $a \in G$. La clase de a respecto a la relación $\sim$ viene dada por $\overline{a} = \{x \in G : a \equiv x \pmod{H}\}$. Si $x \in \overline{a}$, entonces $a \cdot x^{-1} = h$, para algún $h \in H$. De esto se sigue que $x = h \cdot a$ para algún $h \in H$. Entonces $\overline{a} = \{h \cdot a : h \in H\} = H \cdot a$. La clase $\overline{a} = H \cdot a$ se denomina **clase lateral derecha** de H en G. Note que $H \cdot a$ no necesariamente es un subgrupo de G.

Proposición 2.6.1. $\overline{a} = \overline{b}$ o $\overline{a} \cap \overline{b} = \emptyset$.

Al conjunto cociente vía la relación mod H lo denotaremos por G/H.

Ejercicio 2.6.1. Defina de manera análoga las clases laterales izquierdas $a \cdot H$. Describa claramente todo el proceso.

Si G es un grupo abeliano, entonces $H \cdot a = a \cdot H$, para todo $a \in G$. En este caso, denotamos

$$a \sim b \iff a - b \in H.$$

Ejemplo 2.6.1. Sea $G = \mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$ con la suma $+$. Sea $H = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ un subgrupo de G. Note que $H + \overline{1} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ no es un subgrupo de G.

Lema 2.6.1. Existe una correspondencia biyectiva entre dos clases laterales derechas.

Demostración: Sean $H \cdot a = H \cdot b$ dos clases laterales derechas, con $a \neq b$. Definamos $\varphi : H \cdot a \longrightarrow H \cdot b$ por $h \cdot a \mapsto h \cdot b$. Esta función está bien definida, ya que si $h \cdot a = h' \cdot a$ entonces $h = h'$, y así $h \cdot b = h' \cdot b$. Entonces φ es una función, con inversa $\psi : H \cdot b \longrightarrow H \cdot a$ dada por $h \cdot b \mapsto h \cdot a$. Por lo tanto, φ es una correspondencia biyectiva entre $H \cdot a$ y $H \cdot b$. □

Corolario 2.6.1. Todas las clases laterales derechas tienen el mismo número de elementos.

Definición 2.6.1. La cardinalidad de un grupo G, $\text{Card}(G)$, se conoce como el **orden** de G, y se denota por $o(G)$.

Teorema 2.6.1 (Teorema de Lagrange)**.** Si G es un grupo finito y $H \leq G$, entonces $o(H)|o(G)$. Además, si $o(G) = k \cdot o(H)$ entonces k es el mínimo número de clases laterales derechas distintas de H en G.

Demostración: Como G es finito, se sigue inmediatamente que G/H es un conjunto finito. Digamos que $\text{Card}(G/H) = k$ y $G/H = \{H \cdot x_1, \ldots, H \cdot x_k\}$. Sabemos que G puede escribirse como la unión disjunta

$$G = H \cdot x_1 \sqcup \cdots \sqcup H \cdot x_k.$$

Por lo que

$$o(G) = \text{Card}(H \cdot x_1) + \cdots + \text{Card}(H \cdot x_k).$$

Por el lema anterior, tenemos $\text{Card}(H \cdot x_i) = \text{Card}(H) = o(H)$, para todo $1 \leq i \leq k$. Luego, tenemos $o(G) = k \cdot o(H)$, donde k es el número de clases laterales distintas de H en G. □

Corolario 2.6.2. Todo grupo finito de orden primo es cíclico (en particular abeliano).

Demostración: Sea G un grupo finito tal que $o(G) = p$, donde $p \in \mathbb{N}$ es primo. Sea $x \in G \backslash \{e\}$. Consideremos el subgrupo $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$. Por el Teorema de Lagrange, se tiene $o(\langle x \rangle)|p$. Como p es primo, se tiene $o(\langle x \rangle) = 1$ o $0(\langle x \rangle) = p$, es decir $\langle x \rangle = \{e\}$ o $\langle x \rangle = G$. Pero $x \neq e$, por lo que $\langle x \rangle \neq \{e\}$. Por lo tanto, $\langle x \rangle = G$, es decir que G es cíclico. □

Corolario 2.6.3. Si G es un grupo tal que $o(G) \leq 5$, entonces G es abeliano.

Demostración: El caso $o(G) = 1$ es trivial, pues $G = \{e\}$. Si $o(G) = 2, 3, 5$, entonces el resultado se sigue por el corolario anterior. Falta analizar el caso $o(G) = 4$. Si G es cíclico, no hay nada que demostrar. Supongamos entonces que para todo $x \in G \backslash \{e\}$ se tiene $\langle x \rangle \neq G$. Por el Teorema de Lagrange, tenemos que $o(\langle x \rangle) = 2$ pues $\langle x \rangle \neq \{e\}, G$. Entonces $x^2 = e$ para todo $x \neq e$, es decir $x = x^{-1}$. Luego, $x \cdot y = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1} = y \cdot x$ para todo $x, y \in G$. □

Definición 2.6.2. Si $H \leq G$, definimos el **índice de H en G**, denotado por $(G : H)$, como el número de clases laterales derechas diferentes en G/H.

Corolario 2.6.4. Si G es un grupo finito y $H \leq G$, entonces $(G : H) = o(G)/o(H)$.

Ejercicio 2.6.2. Escriba el recíproco del Teorema de Lagrange y halle un contraejemplo para probar que es falso.

Teorema 2.6.2. Si G es un grupo finito conmutativo y $m|o(G)$ entonces existe $H \leq G$ tal que $o(H) = m$.

Definición 2.6.3. Sea G un grupo y $a \in G$. Definimos el **orden** de a como el menor entero positivo n tal que $a^n = e$. Usaremos la notación $n = o(a)$.

Teorema 2.6.3 (Teorema de Cauchy)**.** Si G es un grupo finito y p es un número primo tal que $p|o(G)$, entonces G tiene un elemento de orden p, y por tanto un subgrupo de orden p.

Teorema 2.6.4 (Teorema de Sylow)**.** Si $o(G) = p^n \cdot m$, donde p es primo y $(p, m) = 1$ entonces G tiene subgrupos de orden p, p^2, p^3, $\ldots$, p^n.

Teorema 2.6.5. Si G es cíclico con generador a, entonces $o(G) = o(a)$.

Corolario 2.6.5. Si G es finito y $a \in G$, entonces $o(a)|o(G)$.

Corolario 2.6.6. Si $o(G) = n$ y $a \in G$ entonces $a^n = e$.

Demostración: Como $o(a)|o(G)$, tenemos que existe $k \in \mathbb{Z}$ tal que $n = o(G) = k \cdot o(a)$. Luego, $a^n = a^{k \cdot o(a)} = (a^{o(a)})^k = e^k = e$. □

2.7 Subgrupos normales

Si G es un grupo y $H \leq G$, entonces G/H no es necesariamente un grupo. Por ahora, no tenemos una operación definida para G/H. Sean $Ha, Hb \in G/H$. Lo más natural es definir $G/H \times G/H \longrightarrow G/H$ por

$$Ha * Hb = Ha \cdot b.$$

El problema es que esta operación no necesariamente está bien definida. Supongamos que $a \equiv a' \pmod{H}$ y $b \equiv b' \pmod{H}$. Entonces $a = h \cdot a'$ y $b = k \cdot b'$, donde $h, k \in H$. Tenemos

$$Ha * Hb = Ha \cdot b = H(h \cdot a' \cdot k \cdot b') = H(a' \cdot k \cdot b').$$

El problema en este punto es que a' y k no necesariamente conmutan. En realidad, sólo basta que $a' \cdot k = k' \cdot a'$, donde $k' \in H$.

Definición 2.7.1. Un subgrupo H de un grupo G se dice **normal** si para todo $g \in G$, se tiene

$$gHg^{-1} := \{g \cdot h \cdot g^{-1} : h \in H\} = H.$$

O equivalentemente, si para todo $g \in G$ se tiene $gH = Hg$. Denotaremos esta condición por $H \lhd G$.

Si usamos la definición equivalente, H es normal si $Hg = gH$ para todo $g \in G$, tenemos que dado $h \cdot g \in Hg$, existe $h' \in H$ tal que $h \cdot g = g \cdot h'$, o viceversa. Por lo tanto, si $H \lhd G$ entonces $Ha * Hb = Ha \cdot b$ es una operación binaria bien definida.

Ejemplo 2.7.1.

(1) Si G es un grupo abeliano entonces todo subgrupo de G es normal.

(2) Consideremos el grupo S_3, cuyos elementos son

$$\rho_0 = (1\ 2\ 3),\ \rho_1 = (2\ 3\ 1),\ \rho_2 = (3\ 1\ 2),\ \rho_3 = (1\ 3\ 2),\ \rho_4 = (3\ 2\ 1),\ \rho_5 = (2\ 1\ 3).$$

Note que $H = \{\rho_0, \rho_3\}$ es un subgrupo de S_3. Además, $H\rho_0 = H\rho_3$, $H\rho_1 = H\rho_4 = \{\rho_1, \rho_4\}$ y $H\rho_2 = H\rho_5 = \{\rho_2, \rho_5\}$. Por otro lado, $\rho_1 H = \{\rho_1, \rho_5\} \neq H\rho_1$. Entonces, H no es un subgrupo normal de S_3.

(3) Dado un homomorfismo $f : G \longrightarrow H$, el núcleo $\mathrm{Ker}(f)$ es un subgrupo normal de G. Ya sabemos que $\mathrm{Ker}(f) \leq G$. Ahora, consideremos $g \in G$ y $x \in \mathrm{Ker}(f)$. Tenemos

$$f(g \cdot x \cdot g^{-1}) = f(g) \cdot f(x) \cdot (f(g))^{-1} = f(g) \cdot e_H \cdot (f(g))^{-1} = f(g) \cdot (f(g))^{-1} = e_H.$$

Tenemos $g \cdot \mathrm{Ker}(f) \cdot g^{-1} \subseteq \mathrm{Ker}(f)$. Por otro lado,

$$x = g \cdot (g^{-1} \cdot x \cdot g) \cdot g^{-1} \in g \cdot \mathrm{Ker}(f) \cdot g^{-1}.$$

Tenemos $\mathrm{Ker}(f) \subseteq g \cdot \mathrm{Ker}(f) \cdot g^{-1}$.

(4) Sin embargo, dado un homomorfismo $f : G \longrightarrow H$, la imagen $\mathrm{Im}(f)$ no es necesariamente un subgrupo normal de H. Consideremos el homomorfismo $f : \mathbb{Z}_2 \longrightarrow S_3$ dado por $\overline{0} \mapsto e$ y $\overline{1} \mapsto \rho_3 = (1\ 3\ 2)$. Tenemos que $\mathrm{Im}(f) = \{e, \rho_3\}$ no es un subgrupo normal de S_3, por el ejemplo (2).

Ejercicio 2.7.1. Halle todos los subgrupos de S_3 y diga cuáles son normales.

Ejercicio 2.7.2. Supongamos que H y K son subgrupos de G tal que $K \leq H \leq G$ y supongamos que $(H : K)$ y $(G : H)$ son ambos finitos. Entonces, $(G : K)$ es finito y $(G : K) = (G : H) \cdot (H : K)$.

Ejercicio 2.7.3. Sea G un grupo y sea H un subgrupo de G tal que $(G : H) = 2$, entonces $H \lhd G$.

Teorema 2.7.1. Si H es un subgrupo normal de G entonces $G/H = \{Ha : a \in G\}$ es un grupo dotado con la operación $Ha * Hb = Ha \cdot b$.

Demostración: Es claro que $*$ es asociativa. También es claro que el elemento neutro de G/H viene dado por $e_{G/H} = He = H$, y que el inverso de cada $Ha \in G/H$ está dado por $(Ha)^{-1} = Ha^{-1}$. □

Teorema 2.7.2. Sea G un grupo y $H \lhd G$. Entonces la aplicación $\pi : G \longrightarrow G/H$ dada por $g \mapsto Hg$ es un epimorfismo cuyo núcleo está cado por $\text{Ker}(\pi) = H$.

Demostración: Dados $g, h \in G$, tenemos

$$\pi(g \cdot h) = H(g \cdot h) = Hg \cdot Hh = \pi(g) \cdot \pi(h).$$

Entonces π es un homomorfismo. Es claro que π es sobreyectivo. Ahora sea $h \in H$. Tenemos que $\pi(h) = Hh = H$ pues $h \in H$. Luego $H \subseteq \text{Ker}(\pi)$. Por otra parte, si $\pi(g) = He$, entonces $Hg = He$, por lo que existe $h \in H$ tal que $g = h \cdot e$, es decir $g = h \in H$. Tenemos $\text{Ker}(\pi) \subseteq H$. □

Teorema 2.7.3 (Teorema Fundamental de Homomorfismos)**.** Sea $F : G \longrightarrow H$ un homomorfismo de grupos. Entonces $G/\text{Ker}(f)$ es isomorfo a $\text{Im}(f)$.

Demostración: Por simplificar, usemos la notación $N = \text{Ker}(f)$. Sea $\varphi : G/N \longrightarrow \text{Im}(f)$ la aplicación dada por $\varphi(Ng) = f(g)$. Veamos que φ está bien definida. Supongamos que $Ng = Ng'$, entonces existe $x \in \text{Ker}(f)$ tal que $g = x \cdot g'$. De donde $f(g) = f(x \cdot g') = f(x) \cdot f(g') = e_H \cdot f(g') = f(g')$ y φ está bien definida. Sean $Ng, Ng' \in G/N$, tenemos

$$\varphi(Ng * Ng') = \varphi(Ng \cdot g') = f(g \cdot g^{-1}) = f(g) \cdot f(g') = \varphi(Ng) \cdot \varphi(Ng').$$

Entonces φ es un homomorfismo. Sea $Ng \in \text{Ker}(\varphi)$. Luego, $f(g) = 0$ y por tanto $g \in N$, es decir $Ng = N$ y por tanto φ es un monomorfismo. Es claro que φ es un epimorfismo. Por lo tanto G/N y $\text{Im}(f)$ son isomorfos. □

Corolario 2.7.1. Si G es un grupo finito y $f : G \longrightarrow H$ es un homomorfismo, entonces $o(G) = o(\text{Im}(f)) \cdot o(\text{Ker}(f))$.

Demostración: Por el teorema anterior, $G/\text{Ker}(f) \cong \text{Im}(f)$. Por lo que

$$o(\text{Im}(f)) = (G : \text{Ker}(f)) = o(G)/o(\text{Ker}(f)).$$

De donde se sigue el resultado. □

2.8 Problemas

Problema 2.1. Decida cuáles de los siguientes conjuntos, con las operaciones binarias $*$ definidas, tiene estructura de grupo:

(a) $\mathbb{Z}$, $a * b = a \cdot b$.

(b) $\mathbb{Z}$, $a * b = a - b$.

(c) $\mathbb{R}^+$, $a * b = a \cdot b$.

(d) $\mathbb{Q}$, $a * b = a \cdot b$.

(e) $\mathbb{R}^*$, $a * b = a \cdot b$.

(f) $\mathbb{C}$, $a * b = a + b$.

Problema 2.2. Múestrese que si G es un grupo finito con identidad e y con un número par de elementos, entonces existe $a \neq e$ en G tal que $a * a = e$.

Problema 2.3. Sea S el conjunto de todos los números reales excepto -1. Defínase $*$ en $S \times S$ por $a * b = a + b + a \cdot b$.

(a) Demuestre que $*$ es una operación binaria.

(b) Demuestre que $(S, *)$ es un grupo.

(c) Encuentre la solución de la ecuación $2 * x * 3 = 7$ en S.

Problema 2.4. Sea $\mathbb{R}^*$ el conjunto de todos los números reales menos el cero. Defínase $*$ en $\mathbb{R}^* \times \mathbb{R}^*$ por $a * b = |a| \cdot b$.

(a) Demuestre que $*$ es una operación binaria en $\mathbb{R}^* \times \mathbb{R}^*$.

(b) Demuestre que existe una identidad para $*$ y un inverso derecho para cada elemento en $\mathbb{R}^*$.

(c) Con esta operación binaria, ¿es $\mathbb{R}^*$ un grupo?.

Problema 2.5. Sea $*$ es una operación binaria en un conjunto S. Un elemento x de S es **idempotente** para $*$ si $x * x = x$. Pruébese que un grupo tiene exactamente un idempotente.

Problema 2.6. Demuestre que todo grupo G con identidad e, tal que $x * x = e$ para toda $x \in G$, es abeliano.

Problema 2.7. Pruébese que un conjunto no vacío G, junto con una operación binaria $*$ tal que las ecuaciones $a * x = b$ y $y * a = b$ tienen soluciones en G para todas las $a, b \in G$, es un grupo.

Problema 2.8. Sea G un grupo y $x \in G$. Demuestre que:

(a) $x^m \cdot x^n = x^{m+n}$.

(b) $(x^m)^n = x^{m \cdot n}$.

Problema 2.9. Sea G un grupo. Se dice que G es **cíclico** si existe $x \in G$ tal que $G = \langle x \rangle$. En este caso, al elemento x se le llama **generador** de G. Demuestre:

(a) Todo grupo cíclico es abeliano.

(b) $(\mathbb{Z}, +)$ es un grupo cíclico teniendo a 1 y a -1 como generadores.

(c) $(\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}, +)$ con p primo, es un grupo cíclico, teniendo a $\overline{1}$, $\ldots$, $\overline{p-1}$ como generadores.

Problema 2.10. Sea $G_p = \{m/p^\alpha : m \in \mathbb{Z},\ (p^\alpha, m) = 1 \text{ y } \alpha \in \mathbb{N}\}$ donde p es un número primo fijo. ¿Es $(G_p, +)$ un grupo?. Si $1/p \in (G_p, +)$, calcule el grupo $\langle 1/p \rangle$. Calcule también $\langle 1/p^2 \rangle$, $\langle 1/p^3 \rangle$, $\ldots$, $\langle 1/p^n \rangle$, con $n \in \mathbb{N}$.

Problema 2.11. Cuáles de los siguientes subconjuntos G de $\mathbb{Z}_{13}$ son grupos con la restricción de la operación producto definido en $\mathbb{Z}_{13}$.

(a) $G = \{\overline{1}, \overline{3}, \overline{5}, \overline{6}, \overline{9}, \overline{11}\}$.

(b) $G = \mathbb{Z}_{13}$.

(c) $G = \{\overline{1}, \overline{3}, \overline{5}, \overline{8}, \overline{9}\}$.

Problema 2.12. Sea G un grupo y sean $a, b, c \in G$. Demuestre que la ecuación $x * a * x * b = x * c$ tiene solución única en G.

Problema 2.13. Demuestre que $G = \{z \in \mathbb{C} : |z| = 1\}$ es un grupo abeliano con la operación de multiplicación usual de números complejos.

Problema 2.14. Sea G un grupo y sea $x \in G$. Se define el **centralizador** de x en G, al cual denotaremos por $C_G(x)$, como el conjunto

$$C_g(x) = \{y \in G : y \cdot x = x \cdot y\}.$$

Demuestre que $C_G(x)$ es un subgrupo de G.

Problema 2.15. Sea G un grupo. Se define el **centro** del grupo G como el conjunto

$$Z(G) = \{a \in G : a \cdot x = x \cdot a \text{ para todo } x \in G\}.$$

Demuestre que $Z(G)$ es un subgrupo abeliano de $Z(G)$.

Problema 2.16. Sean H_1, H_2, $\ldots$, H_n, H_{n+1}, $\ldots$ subgrupos de un grupo G, que verifican la siguiente condición de cadena:

$$H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq H_{n+1} \subseteq \cdots$$

Pruebe que $H = \bigcup_{i=1}^{\infty} H_i$ es un subgrupo de G.

Problema 2.17. Sean H y K subgrupos de un grupo abeliano G. Si $S = \{h \cdot k : h \in H,\ k \in K\}$. ¿Será S un subgrupo de G?.

Problema 2.18. Demuestre que un grupo cíclico con un sólo generador puede tener a lo sumo 2 elementos.

Problema 2.19.

(a) Demuestre que si G es un grupo abeliano con identidad e, entonces el conjunto $\{x \in G : x^2 = e\}$ es un subgrupo de G.

(b) Repítase la parte (a) para el conjunto $\{x \in G : x^n = e\}$ donde n es un entero fijo mayor que 0.

Problema 2.20. Demuestre que si $a \in G$ y G es un grupo finito con identidad e, entonces existe $n \in \mathbb{Z}_{\geq 0}$ tal que $a^n = e$.

Problema 2.21. Sea G un grupo y sea a un elemento fijo de G. Pruebe que el conjunto

$$H_a = \{x \in G : x \cdot a = a \cdot x\}$$

es un subgrupo se G.

Problema 2.22. Sea G un grupo y sea $S \subseteq G$. Demuestre que el conjunto

$$H_S = \{x \in G : x \cdot a = a \cdot x \text{ para todo } a \in S\}$$

es un subgrupo se G.

Problema 2.23. Sea H un subgrupo de G. Para $a, b \in G$, sea $a \sim b \iff a \cdot b^{-1} \in H$. Demuestre que $\sim$ es una relación de equivalencia en G.

Problema 2.24. Muestre mediante un ejemplo la posibilidad de que la ecuación cuadrática $x^2 = e$ tenga más de dos soluciones en algún grupo G con identidad e.

CAPÍTULO 3

ANILLOS

3.1 El concepto de Anillo. Ejemplos

Comencemos este capítulo con la definición de anillo.

Definición 3.1.1. Sea A un conjunto no vacío y sean $+, \cdot : A \times A \longrightarrow A$ dos operaciones binarias sobre A. Decimos que el triple $(A, +, \cdots)$ es un **anillo** si se satisfacen las siguientes condiciones:

(1) $a + (b + c) = (a + b) + c$, para todo $a, b, c \in A$.

(2) $a + b = b + a$, para todo $a, b \in A$.

(3) Existe un elemento $0 \in A$ tal que $a + 0 = a$, para todo $a \in A$.

(4) Para cada $a \in A$, existe $-a \in A$ tal que $a + (-a) = 0$. Llamaremos a $-a$ el **inverso aditivo** de a.

(5) $\cdot$ **es asociativa:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in A$.

(6) $\cdot$ **es distributiva respecto a la suma** $+$**:** $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$, para todo $a, b, c \in A$.

Note que si $(A, +, \cdot)$ es un anillo, entonces $(A, +)$ es un grupo abeliano.

Si además la operación $\cdot$ es conmutativa, diremos que A es un **anillo conmutativo**. Si existe $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in A$, diremos que A es un **anillo con identidad** (1 es la **identidad** de A).

Ejemplo 3.1.1.

(1) $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con identidad.

(2) $(\mathbb{Z}, +, \cdots)$ con la suma usual $+$, y el producto $a \cdot b = 0$ para todo $a, b \in \mathbb{Z}$, es un anillo conmutativo, pero sin identidad.

(3) $(\mathbb{R}, +, \cdots)$ es también un anillo conmutativo con identidad.

(4) $(M_2(\mathbb{R}), +, \cdots)$ es un anillo con identidad, no conmutativo.

(5) $\mathbb{R}[x] = \{a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n : n \in \mathbb{Z}_{\geq 0}$ y $a_i \in \mathbb{R}$ para todo $0 \leq i \leq n\}$ es un anillo conmutativo. En general, si A es un anillo entonces $A[x]$ también lo es.

(6) $C[0,1] = \{f : [0,1] \longrightarrow \mathbb{R} \ / \ f \text{ es continua}\}$, con las operaciones

$$(f+g)(x) = f(x) + g(x) \text{ y } (f \cdot g)(x) = f(x) \cdot g(x),$$

es un anillo conmutativo cuya identidad es la función constantemente igual a 1.

Ejercicio 3.1.1. En todo anillo A se verifican la siguientes proposiciones:

(1) 0 es el único elemento de A tal que $a + 0 = a$, para todo $a \in A$.

(2) El inverso aditivo de cada $a \in A$ es único.

(3) $a \cdot 0 = 0 \cdot a = 0$, para todo $a \in A$.

(4) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$, para todo $a, b \in A$.

(5) $(-a) \cdot (-b) = a \cdot b$, para todo $a, b \in A$.

(6) $-(-a) = a$, para todo $a \in A$.

(7) Si A posee identidad 1, entonces ésta es única.

(8) Si A posee identidad 1, entonces $(-1) \cdot a = -a$, para todo $a \in A$.

(9) $(a+b)^2$ no es necesariamente igual a $a^2 + 2a \cdot b + b^2$. ¿Bajo cuáles condiciones se cumple la igualdad?.

Definición 3.1.2. Decimos que $a \in A$ es un **divisor de cero** si $a \neq 0$ y si existe $b \neq 0$ tal que $a \cdot b = 0$.

Un anillo conmutativo que no tiene divisores de cero se conoce como **dominio de integridad**.

Si A es un anillo con identidad 1, decimos que $a \in A$ es una **unidad** si existe $b \in A$ tal que $a \cdot b = b \cdot a = 1$. Al tal b se le llama **inverso** de a y se le denota por $b = a^{-1}$. Al conjunto de todas las unidades de A lo denotaremos por A^*.

Ejemplo 3.1.2.

(1) $M_n(\mathbb{R})$ es un anillo conmutativo con divisores de cero.

(2) 1 y -1 son las únicas unidades de $(\mathbb{Z}, +, \cdot)$.

3.2 Subanillos e ideales

Definición 3.2.1. Si A es un anillo, un subconjunto no vacío B de A se denomina **subanillo** de A si B, dotado con las mismas operaciones de A restringidas en B, es un anillo. Denotaremos esta condición por $B \leq A$.

Teorema 3.2.1. B es un subanillo de A si, y sólo si, $B \subseteq A$, $B \neq \emptyset$ y B es cerrado bajo diferencias y productos, es decir para todo $x, y \in B$:

(1) $x - y \in B$.

(2) $x \cdot y \in B$.

Demostración: La primera implicación es trivial. Supongamos ahora que B es un subconjunto no vacío de A que satisface (1) y (2). Como $B \neq \emptyset$, existe $b \in B$. Luego, $0 = b - b \in B$, de donde B posee el elemento neutro de A. Si $x \in B$, entonces $-x = 0 - x \in B$. Ahora, si $x, y \in B$ tenemos $x + y = x - (-y) \in B$, pues $-y \in B$. De esto se sigue el resultado. □

Note que si A es un anillo y $B \subseteq A$, entonces $B \leq A$ si, y sólo si,

(1) $(B, +)$ es un subgrupo de $(A, +)$.

(2) $a \cdot b \in B$ para todo $a, b \in B$.

Definición 3.2.2. Sea A un anillo e $I \subseteq A$ un subconjunto no vacío. Decimos que I es un **ideal** de A si:

(1) $a - b \in I$ para todo $a, b \in I$.

(2) Si $x \in I$ y $a \in A$, entonces $x \cdot a, a \cdot x \in I$.

La condición (1) exige que $(I, +|_{I \times I})$ es un subgrupo de $(A, +)$. La condición (2) implica que $a, b \in I \implies a \cdot b \in I$. Por lo tanto, todo ideal I de A es un subanillo de A. Sin embargo, no todo subanillo $B \leq A$ es un ideal de A. Por ejemplo, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, más no un ideal, pues $1 \in \mathbb{Z}$, $1/2 \in \mathbb{Q}$ y sin embargo $1 \cdot 1/2 = 1/2 \notin \mathbb{Z}$.

Ejemplo 3.2.1.

(1) Fijemos $k \in \mathbb{Z}$. Luego $k \cdot \mathbb{Z} = \{n \cdot k : n \in \mathbb{Z}\}$ es un ideal de $\mathbb{Z}$.

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

Ejercicio 3.2.1. Si I es un ideal de un anillo A con identidad 1, y si $1 \in I$, entonces $I = A$.

Teorema 3.2.2. Sea J un conjunto y $\{I_j\}_{j \in J}$ una familia de ideales de A indexada por J. Entonces $\bigcap_{j \in J} I_j$ es un ideal de A.

En cualquier anillo A se puede considerar la intersección de todos los ideales de A, pues al menos $\{0\}$ y el propio A son ideales de A.

3.3 Ideales principales y maximales

Resulta interesante preguntarse qué sucede con la unión de ideales de un anillo A, ¿será ésta también un ideal de A?.

Ejemplo 3.3.1. Consideremos el anillo $(\mathbb{Z}, +, \cdot)$ y considere los ideales $I_1 = 2 \cdot \mathbb{Z}$ y $I_2 = 3 \cdot \mathbb{Z}$. Es claro que $2, 3 \in I_1 \cup I_2$. Sin embargo, $3 - 2 = 1 \notin I_1 \cup I_2$, por lo que $I_1 \cup I_2$ no es un ideal de $\mathbb{Z}$.

Ejercicio 3.3.1. Construya un ejemplo concreto en el cual la unión de ideales es un ideal. Justifique por qué.

Definición 3.3.1. Sea A un anillo y $X \subseteq A$ un subconjunto de A. Llamamos **ideal generado** por X al menor ideal de A que contiene a X, y lo denotaremos por $\langle X \rangle$.

Si $X = \{a\}$, al ideal $\langle \{a\} \rangle$, al que denotaremos $\langle a \rangle$ para simplificar, lo llamaremos **ideal principal generado** por a.

Ejemplo 3.3.2. Sea A una matriz cuadrada con coeficientes reales. El conjunto $H = \{p(x) \in \mathbb{R}[x] : p(A) = 0\}$ es un ideal de $\mathbb{R}[x]$. En efecto, si $p(x) \in H$ y $g(x) \in \mathbb{R}[x]$, entonces $(p \cdot g)(A) = p(A) \cdot g(A) = 0 \cdot g(A) = 0$.

Teorema 3.3.1. Sea A un anillo conmutativo con identidad, entonces el ideal principal generado por $x \in A$, $\langle x \rangle$ está dado por $\{a \cdot x : a \in A\}$.

Demostración: Sea $I = \{a \cdot x : a \in A\}$. Note que $I \neq \emptyset$ ya que $x = 1 \cdot x \in I$. Sean $u = a \cdot x$ y $v = b \cdot x$ en I. Tenemos

$$u - v = a \cdot x - b \cdot x = (a - b) \cdot x \in I,$$

porque $\cdot$ se distribuye respecto a la suma de A. Ahora supongamos que $u = a \cdot x \in I$ y que $b \in A$. Tenemos

$$u \cdot b = (a \cdot x) \cdot b = a \cdot (x \cdot b) = a \cdot (b \cdot x) = (a \cdot b) \cdot x \in I,$$

por la propiedad asociativa de $\cdot$ y porque A es un anillo conmutativo. De forma análoga, se prueba que $b \cdot u \in I$. Por lo tanto, I es un ideal de A.

Ahora, si J es un ideal de A tal que $x \in J$, entonces es fácil ver que $I \subseteq J$. Por lo tanto, I es el menor ideal de A que contiene a $\{x\}$, es decir $I = \langle x \rangle$. □

Teorema 3.3.2.

(1) Todos los ideales de $\mathbb{Z}$ son principales.

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

Demostración: Sólo probaremos (1). Sea I un ideal de $\mathbb{Z}$. Si $I = \langle 0 \rangle$ no hay nada que demostrar. Entonces podemos suponer que I es un ideal no nulo. Sea $x \in I$ distinto de cero. Podemos suponer que $x > 0$, pues si $x < 0$ entonces $-x = -1 \cdot x \in I$ y $-x > 0$. Asumamos que x es el menor entero positivo de I. Sea $y \in I$. Entonces por el algoritmo de la división, existe $q \in \mathbb{Z}$ y $0 \leq r < x$ tal que $y = q \cdot x + r$. Como I es un ideal, se tiene $q \cdot x \in I$ y por tanto $r = y - q \cdot x \in I$. Como $0 \leq r < x$ y x es el menor entero positivo de I, se sigue que $r = 0$ y por tanto $y = q \cdot x \in \langle x \rangle$. La otra contención es clara. Por lo tanto, $I = \langle x \rangle$. □

Ejercicio 3.3.2. Demostrar la parte (2) del teorema anterior.

Ejemplo 3.3.3. Considere el anillo $\mathbb{Z}[x]$ y sea I el ideal generado por $\{2, x\}$. Veamos que I no es un ideal principal de $\mathbb{Z}[x]$. Supongamos lo contrario. Sea $p(x) \in \mathbb{Z}[x]$ su único generador. Como $2 \in I$ tenemos $2 = p(x) \cdot q(x)$, para algún $q(x) \in \mathbb{Z}[x]$. Luego, $p(x)$ debe ser un polinomio constante. Por otra parte, como $x \in I$ se tiene $p(x)|x$. De esto se sigue que $p(x) = 1$ y por tanto $I = \mathbb{Z}[x]$, obteniendo así una contradicción.

Definición 3.3.2. Sea A un anillo. Decimos que un ideal $\mathcal{M}$ de A es **maximal** si:

(1) $\mathcal{M} \neq A$.

(2) Para todo ideal I de A, $\mathcal{M} \subsetneq I \subseteq A \Longrightarrow I = A$.

En otras palabras, un ideal maximal es aquél que no está contenido en otro ideal no trivial.

Ejemplo 3.3.4.

(1) El ideal $3 \cdot \mathbb{Z}$ de $\mathbb{Z}$ es maximal.

(2) El ideal $\langle x^2 + 1 \rangle$ de $\mathbb{Q}[x]$ es maximal.

(3) El ideal $4 \cdot \mathbb{Z}$ de $\mathbb{Z}$ no es maximal, pues $4 \cdot \mathbb{Z} \subseteq 2 \cdot \mathbb{Z} \subseteq \mathbb{Z}$.

Teorema 3.3.3.

(1) Si $\mathcal{M}$ es un ideal de $\mathbb{Z}$ entonces $\mathcal{M}$ es maximal si, y sólo si, $\mathcal{M} = p \cdot \mathbb{Z}$ para algún número primo $p \in \mathbb{Z}$.

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

Demostración: Sólo probaremos (1). Supongamos que $\mathcal{M}$ es un ideal maximal. Como todo ideal de $\mathbb{Z}$ es principal, se tiene que $\mathcal{M} = k\mathbb{Z}$, para algún $k \in \mathbb{Z}$. Supongamos que k no es primo, entonces $k = p \cdot q$ donde $p \neq \pm 1$ y $q \neq \pm$. Tenemos que $p \cdot \mathbb{Z}$ es un ideal de $\mathbb{Z}$ tal que $\mathcal{M} \subsetneq p \cdot \mathbb{Z} \subsetneq \mathbb{Z}$. Luego, $\mathcal{M}$ no es maximal, obteniendo una contradicción. Por lo tanto, k es primo.

Ahora supongamos que $\mathcal{M} = p \cdot \mathbb{Z}$, donde $p \in \mathbb{Z}$ es un número primo. Sea $I = q \cdot \mathbb{Z}$ otro ideal tal que $\mathcal{M} \subsetneq I$. Entonces $q|p$ y luego $q = \pm 1$, porque p es primo. De donde $q \cdot \mathbb{Z} = \mathbb{Z}$ y $\mathcal{M}$ es maximal. □

Ejercicio 3.3.3. Demuestre la parte (2) del teorema anterior.

Ejemplo 3.3.5. $\langle x^2 - 1 \rangle$ no es un ideal maximal de $\mathbb{Q}[x]$, pues $\langle x^2 - 1 \rangle \subseteq \langle x - 1 \rangle$.

3.4 Anillo cociente

Sea A un anillo y sea I in ideal de A. Definimos en A la relación

$$a \sim b \Longleftrightarrow a - b \in I.$$

Proposición 3.4.1. La relación $\sim$ es una relación de equivalencia.

Proposición 3.4.2. Si $a_1 \sim b_1$ y $a_2 \sim b_2$ entonces:

(1) $-a_1 \sim -b_1$.

(2) $a_1 + a_2 \sim b_1 + b_2$.

(3) $a_1 \cdot a_2 \sim b_1 \cdot b_2$.

Demostración:

(1) Como $a_1 - b_1 \in I$, tenemos $-a_1 - (-b_1) = -(a_1 - b_1) \in I$ y por tanto $-a_1 \sim -b_1$.

(2) Supongamos $a_1 - b_1, a_2 - b_2 \in I$. Luego $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in I$ y por ende $a_1 + a_2 \sim b_1 + b_2$.

□

Ejercicio 3.4.1. Probar la parte (3) de la proposición anterior.

Denotaremos por $\overline{a} := \{b \in A : a \sim b\}$ la clase de equivalencia de $a \in A$. Como $\overline{a} = \{a + x : x \in I\}$, también se suele usar la notación $\overline{a} = a + I$. Por la proposición anterior, tenemos que las operaciones

$$(1) \quad (a + I) + (b + I) = (a + b) + I$$
$$(2) \quad (a + I) \cdot (b + I) = (a \cdot b) + I$$

están bien definidas.

Teorema 3.4.1. Sea A/I el conjunto de todas las clases de equivalencia con respecto a la relación $\sim$. Entonces $(A/I, +, \cdot)$, donde $+$ y $\cdot$ son las operaciones definidas por (1) y (2), respectivamente, es un anillo, denominado **anillo cociente**. Más aún, si A es conmutativo (resp. con identidad $1 \in A$), entonces A/I también es conmutativo (resp. A/I también posee elemento identidad $1 + I \in A/I$).

Ejercicio 3.4.2. Demostrar el teorema anterior.

3.5 Homomorfismos de anillos

Definición 3.5.1. Sean A y B dos anillos y sea $f : A \longrightarrow B$ una función. Diremos que f es un **homomorfismo de anillos** si para todo $x, y \in A$, se tiene:

(1) $f(x + y) = f(x) + f(y)$, y

(2) $f(x \cdot y) = f(x) \cdot f(y)$.

Teorema 3.5.1. Si $f : A \longrightarrow B$ es un homomorfismo de anillos, entonces:

(1) $f(0) = 0$.

(2) $f(-a) = -f(a)$.

Ejemplo 3.5.1. Los siguientes son ejemplos de homomorfismos de anillos:

(1) $f : A \longrightarrow A$ dado por $a \mapsto a$ (**homomorfismo identidad**).

(2) $f : A \longrightarrow A$ dado por $a \mapsto 0$ (**homomorfismo cero**).

(3) $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ dado por $a \mapsto \overline{a}$ (**proyección canónica**).

(4) $f : \mathbb{Z} \longrightarrow \mathbb{Q}[x]$ dado por $k \mapsto k$ (**inclusión**).

(5) $f : \mathbb{C} \longrightarrow M_2(\mathbb{R})$ dado por $a + i \cdot b \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

Ejemplo 3.5.2. La función $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $a \mapsto a + 1$ no es un homomorfismo, pues $f(0) = 1 \neq 0$.

Definición 3.5.2. Sea $f : A \longrightarrow B$ un homomorfismo de anillos. Entonces f se dice ser:

(1) un **monomorfismo** si f es una función inyectiva;

(2) un **epimorfismo** si f es una función sobreyectiva;

(3) un **isomorfismo** si f es una función biyectiva;

(4) un **automorfismo** si f es un isimorfismo y si $A = B$.

Definición 3.5.3. Sea $f : A \longrightarrow B$ un homomorfismo de anillos. Los conjuntos $\text{Ker}(f) := \{a \in A : f(a) = 0\}$ y $\text{Im}(f) := \{f(a) : a \in A\}$ se denominan **núcleo** e **imagen** de f, respectivamente.

Teorema 3.5.2. Si $f : A \longrightarrow B$ es un homomorfismo de anillos, entonces:

(1) $\text{Ker}(f)$ es un ideal de A.

(2) $\text{Im}(f)$ es un subanillo de B.

Demostración:

(1) Note que $0 \in \text{Ker}(f)$, entonces $\text{Ker}(f) \neq \emptyset$. Sean $a, b \in \text{Ker}(f)$, entonces $f(a - b) = f(a) - f(b) = 0 - 0 = 0$ y por ende $a - b \in \text{Ker}(f)$. Ahora, supongamos que $a \in A$ y $b \in \text{Ker}(f)$, entonces $f(a \cdot b) = f(a) \cdot f(b) = f(a) \cdot 0 = 0$ y $f(b \cdot a) = f(b) \cdot f(a) = 0 \cdot f(a) = 0$. Por lo que $a \cdot b, b \cdot a \in \text{Ker}(f)$. Por lo tanto, $\text{Ker}(f)$ es un ideal de A.

(2) Note que $0 = f(0) \in \text{Im}(f)$, de donde $\text{Im}(f) \neq \emptyset$. Sean $f(a), f(b) \in \text{Im}(f)$. Se tiene $f(a) - f(b) = f(a - b) \in \text{Im}(f)$ y $f(a) \cdot f(b) = f(a \cdot b) \in \text{Im}(f)$. Por lo tanto, $\text{Im}(f)$ es un subanillo de B.

□

Ejemplo 3.5.3. La función $f : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ dada por $n \mapsto (n, n)$ es un homomorfismo de anillos cuya imagen $\text{Im}(f)$ no es un ideal de $\mathbb{Z} \times \mathbb{Z}$, pues $(1, 0) \cdot (2, 2) = (2, 0) \notin \text{Im}(f)$.

Teorema 3.5.3. Sea $f : A \longrightarrow B$ un homomorfismo de anillos, entonces f in inyectivo si, y sólo si, $\text{Ker}(f) = \{0\}$.

Teorema 3.5.4. Sea I un ideal de A, entonces la función $\pi : A \longrightarrow A/I$ dada por $a \mapsto a + I$ es un homomorfismo (llamado **homomorfismo canónico**), y además $\mathrm{Ker}(\pi) = I$.

Demostración: Sean $a + I, b + I \in A/I$. Tenemos

$$\pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b),$$
$$\pi(a \cdot b) = (a \cdot b) + I = (a + I) \cdot (b + I) = \pi(a) \cdot \pi(b).$$

Ahora sea $a \in \mathrm{Ker}(\pi)$. Luego $a + I = 0 + I$, es decir $a \in I$. Por otro lado, si $a \in I$ es claro que $\pi(a) = a + I = 0 + I$, es decir $a \in \mathrm{Ker}(\pi)$. □

Teorema 3.5.5 (Primer Teorema Fundamental de Homomorfismos de Anillos)**.** Sea $f : A \longrightarrow B$ un epimorfismo. Entonces la aplicación $\varphi : A/\mathrm{Ker}(f) \longrightarrow B$ dada por $a + \mathrm{Ker}(f) \mapsto f(a)$ es un isomorfismo de anillos.

Demostración: Primero veamos que φ está bien definida. Supongamos que $a + \mathrm{Ker}(f) = b + \mathrm{Ker}(f)$. Entonces $a - b \in \mathrm{Ker}(f)$. Luego

$$\varphi(a + \mathrm{Ker}(f)) - \varphi(b + \mathrm{Ker}(f)) = \varphi((a - b) + \mathrm{Ker}(f)) = f(a - b) = 0.$$

Por lo que φ está bien definida.

Veamos que φ es un homomorfismo de anillos. Sean $a + \mathrm{Ker}(f), b + \mathrm{Ker}(f) \in A/\mathrm{Ker}(f)$. Tenemos

$$\begin{aligned}\varphi((a + \mathrm{Ker}(f)) + (b + \mathrm{Ker}(f))) &= \varphi((a + b) + \mathrm{Ker}(f)) = f(a + b) = f(a) + f(b)\\ &= \varphi(a + \mathrm{Ker}(f)) + \varphi(b + \mathrm{Ker}(f)),\\ \varphi((a + \mathrm{Ker}(f)) \cdot (b + \mathrm{Ker}(f))) &= \varphi((a \cdot b) + \mathrm{Ker}(f)) = f(a \cdot b) = f(a) \cdot f(b)\\ &= \varphi(a + \mathrm{Ker}(f)) \cdot \varphi(b + \mathrm{Ker}(f)).\end{aligned}$$

Sea $a + \mathrm{Ker}(f) \in \mathrm{Ker}(\varphi)$. Entonces $0 = \varphi(a + \mathrm{Ker}(f)) = f(a)$. Luego $a \in \mathrm{Ker}(f)$ y así $a + \mathrm{Ker}(f) = 0 + \mathrm{Ker}(f)$. Por lo que φ es injectivo.

Ahora sea $b \in B$. Como f es un epimorfismo, existe $a \in A$ tal que $b = f(a) = \varphi(a + \mathrm{Ker}(f))$. Por lo que φ es también un epimorfismo. □

Ejemplo 3.5.4. Sea A el anillo de todas las funciones de $\mathbb{R}$ en $\mathbb{R}$, con las operaciones usuales. Sea $I = \{f \in A : f(0) = 0\}$. Es fácil ver que I es un ideal de A. Si definimos $h : A \longrightarrow \mathbb{R}$ por $h(f) = f(0)$, tenemos que h es un epimorfismo de anillos tal que $\mathrm{Ker}(h) = I$. Por el teorema anterior, se tiene $A/I \cong \mathbb{R}$.

3.6 Problemas

Problema 3.1. Demostrar las siguientes proposiciones.

(a) $A = \{n + m \cdot \sqrt{3} : n, m \in \mathbb{Z}\}$ es un anillo.

(b) $B = \{a + b \cdot \sqrt{3} : a, b \in \mathbb{Q}\}$ es un anillo, donde todo elemento no nulo de B es una unidad.

(c) $C = \{a + b \cdot \sqrt[4]{3} : a, b \in \mathbb{Q}\}$ no es un anillo.

(d) $D = \{a + b \cdot \sqrt[3]{3} + c \cdot \sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$ es un anillo tal que sus elementos no nulos son unidades.

Problema 3.2. Sean $R_1, \ldots, R_n$ anillos. Demostrar que el conjunto

$$R_1 \oplus \cdots \oplus R_n = \{(a_1, \ldots, a_n) : a_1 \in R_1, \ldots, a_n \in R_n\},$$

equipado con las operaciones

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n),$$

es un anillo.

Problema 3.3. El conjunto $\{0, 2, 4, 6, 8\}$, equipado con la suma y el producto módulo 10, es un anilllo. ¿Cuál es la identidad multiplicativa?. ¿Cuáles son los elementos invertibles?.

Problema 3.4. Sea R un anillo. Se define el **centro** de R como el conjunto $Z(R) = \{x \in R : x \cdot y = y \cdot x \text{ para todo } y \in R\}$. Demuestre que $Z(R)$ es un subanillo conmutativo de R.

Problema 3.5. Calcule en centro del anillo $M_n(\mathbb{R})$.

Problema 3.6. Sea R un anillo conmutativo. Demostrar que las siguientes proposiciones son equivalentes:

(a) Los únicos ideales de R son $\{0\}$ y R.

(b) Todo homomorfismo de anillos $f : R \longrightarrow A$, donde $A \neq \{0\}$, es inyectivo.

Problema 3.7. Sea R un anillo y sea S un subanillo con identidad de R. Si I es un ideal de R, demuestre que:

(a) $S \cap I$ es un ideal de S.

(b) $S + I = \{s + i : s \in S, i \in I\}$ es un subanillo con identidad de R.

(c) $S/(S \cap I)$ es isomorfo a $(S + I)/I$.

Problema 3.8. Se define la **característica** de un anillo R como el menor entero positivo n tal que $1+\cdots+1 = 0$ (n veces). Si no existe tal entero n, diremos que R tiene característica cero. Si R es un anillo de característica n e I es un ideal de R, ¿cuál puede ser la característica de R/I?.

Problema 3.9. Recordemos que un elemento e de un anillo R se llama **idempotente** si $e^2 = e$. Sea R un anillo en el que todo elemento de R es idempotente. Demostrar que R es conmutativo y de característica 2.

Problema 3.10. Un elemento a de un anillo R se llama **nilpotente** si existe un entero $n \geq 1$ tal que $a^n = 0$. Demostrar que si a es nilpotente, entonces $1 - a$ es una unidad.

Problema 3.11. Sea R un anillo conmutativo y denotemos por $N(R)$ el conjunto formado por todos los elementos nilpotentes de R. A $N(R)$ se le conoce como el **nilradical** de R. Probar que $N(R)$ es un ideal de R. Calcule el nilradical de $\mathbb{Z}_n$.

CAPÍTULO 4

CUERPOS

4.1 El concepto de Cuerpo. Ejemplos

Consideremos el anillo $\mathbb{Z}_{10}$ y el subanillo $A = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\} \subseteq \mathbb{Z}_{10}$. Hay dos cosas interesantes sobre A. La primera es que A posee elemento identidad, a saber $1 = \overline{6}$. La otra es que $(\overline{2})^{-1} = \overline{8} \in A$, $(\overline{3})^{-1} = \overline{2} \in A$, $(\overline{4})^{-1} = \overline{4} \in A$, $(\overline{6})^{-1} = \overline{6} \in A$. No todo elemento de $\mathbb{Z}_{10}$ posee inverso multiplicativo. El elemento $\overline{2} \in A$ posee inverso multiplicativo, pero éste no está en A.

Definición 4.1.1. Un anillo conmutativo A con elemento identidad es un **cuerpo** si todos sus elementos distintos de cero poseen inverso multiplicativo.

Ejemplo 4.1.1. Los siguientes son ejemplos de cuerpos:

(1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(2) $\mathbb{Q}(\sqrt{2}) = \{a + b \cdot \sqrt{2} : a, b \in \mathbb{Q}\}$, donde $1 = 1 + 0 \cdot \sqrt{2}$ y $(a + b \cdot \sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \cdot \sqrt{2}$. Note que $a^2 - 2b^2 \neq 0$ para todo $a, b \in \mathbb{Q}$.

(3) $\mathbb{Z}_n$, donde $n \in \mathbb{Z}$ es un número primo.

Observacicón 4.1.1.

(1) En un cuerpo no pueden haber divisores de cero. Todo cuerpo es un dominio de integridad. En efecto, supongamos que en un cuerpo A que existen $a, b \neq 0$ tales que $a \cdot b = 0$. Entonces $b = a^{-1} \cdot (a \cdot b) = 0$, obteniendo una contradicción.

(2) Un cuerpo sólo tiene ideales triviales. En efecto, supongamos que en un cuerpo K existe un ideal no trivial $I \neq \{0\}$. Sea $a \in I$. Luego $1 = a^{-1} \cdot a \in I$, de donde $I = K$. ¿Si un anillo sólo posee ideales triviales, entonces es un cuerpo?.

Ejercicio 4.1.1 (Conjetura de Contreras)**.** Sea $\varphi : A \longrightarrow B$ un homomorfismo de anillos. Si I es un ideal bilateral de A, entonces $\varphi(I)$ es un ideal bilateral de B.

Ejercicio 4.1.2. Demuestre que si A es un cuerpo entonces para cada $a \in A$ se tiene que $a^{-1} \in A$ es único.

4.2 Cuerpo cociente

En $\mathcal{Z} \times (\mathbb{Z}\backslash\{0\})$ definimos la relación $(a,b) \sim (c,d) \Longrightarrow a \cdot d = b \cdot c$. Demostrar que $\sim$ es una relación de equivalencia es fácil. A la clase de (a,b) la denotaremos por a/b.

De manera similar, si D es un dominio de integridad, sobre $D \times (D\backslash\{0\})$ definimos la relación de equivalencia

$$(a,b) \sim (c,d) \Longrightarrow a \cdot d = b \cdot c.$$

Denotaremos por $D/\sim$ al conjunto de clases de equivalencia, y por a/b a la clase de (a,b). Luego

$$\frac{a}{b} = \{(c,d) \in D \times (D\backslash\{0\}) : a \cdot d = b \cdot c\}.$$

Teorema 4.2.1. Sea D un dominio de integridad. Sobre el conjunto $F = D/\sim$ definimos las operaciones

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot b}{c \cdot d}.$$

Entonces $(F, +, \cdot)$ es un cuerpo.

Demostración: Primero veamos que las operaciones están bien definidas. Comencemos suponiendo que $(a,b) \sim (a',b')$ y $(c,d) \sim (c',d')$. Entonces $a \cdot b' = a' \cdot b$ y $c \cdot d' = c' \cdot d$. Luego

$$a \cdot b' + c \cdot d' = a' \cdot b + c' \cdot d,$$
$$a \cdot b' \cdot d \cdot d' = a' \cdot b \cdot d \cdot d',$$
$$c \cdot d' \cdot b \cdot b' = c' \cdot d \cdot b \cdot b'.$$

De donde

$$a \cdot b' \cdot d \cdot d' + c \cdot d' \cdot b \cdot b' = a' \cdot b \cdot d \cdot d' + c' \cdot d \cdot b \cdot b'$$
$$(a \cdot d + c \cdot b) \cdot b' \cdot d' = (a' \cdot d' + c' \cdot b') \cdot b \cdot d.$$

Lo último implica que $\frac{a \cdot d + c \cdot b}{b \cdot d} = \frac{a' \cdot d' + c' \cdot b'}{b' \cdot d'}$.

De las mismas relaciones anteriores, se tiene que

$$(a \cdot b') \cdot (c \cdot d') = (a' \cdot b) \cdot (c' \cdot d)$$
$$(a \cdot c) \cdot (b' \cdot d') = (a' \cdot c') \cdot (b \cdot d).$$

De donde $\frac{a \cdot c}{b \cdot d} = \frac{a' \cdot c'}{b' \cdot d'}$.

Note que $b \cdot d \neq 0$, porque D es un dominio entero.

Por lo tanto, la suma y producto de clases de equivalencia está bien definido.

(1) Asociatividad de la suma: Sean $a/b, c/d, e/f \in F$. Tenemos

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} &= \frac{a\cdot d+b\cdot c}{b\cdot d}+\frac{e}{f}=\frac{(a\cdot d+b\cdot c)\cdot f+(b\cdot d)\cdot e}{(b\cdot d)\cdot f}\\ &= \frac{(a\cdot d)\cdot f+(b\cdot c)\cdot f+(b\cdot d)\cdot e}{(b\cdot d)\cdot f}=\frac{(a\cdot d)\cdot f+b\cdot(c\cdot f)+b\cdot(d\cdot e)}{b\cdot(d\cdot f)}\\ &= \frac{a\cdot(d\cdot f)+b\cdot(c\cdot f+d\cdot e)}{b\cdot(d\cdot f)}=\frac{a}{b}+\frac{c\cdot f+d\cdot e}{d\cdot f}\\ &= \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right).\end{aligned}$$

(2) Conmutatividad de la suma: Sea $a/b, c/d \in F$. Tenemos

$$\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+b\cdot c}{b\cdot d}=\frac{c\cdot b+d\cdot a}{d\cdot b}=\frac{c}{d}+\frac{a}{b}.$$

(3) El neutro aditivo en F está dado por $0/1$:

$$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+0\cdot b}{b\cdot 1}=\frac{a+0}{b}=\frac{a}{b},\ \text{para todo } \frac{a}{b}\in F.$$

(4) El inverso aditivo de $a/b \in F$ viene dado por $(-a)/b$. En efecto

$$\frac{a}{b}+\frac{(-a)}{b}=\frac{a\cdot b+(-a)\cdot b}{b\cdot b}=\frac{a\cdot b-a\cdot b}{b\cdot b}=\frac{0}{b\cdot b}=\frac{0}{1}.$$

(5) Asociatividad del producto: Sean $a/b, c/d, e/f \in F$. Tenemos

$$\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{c\cdot e}{d\cdot f}=\frac{a\cdot(c\cdot e)}{b\cdot(d\cdot f)}=\frac{(a\cdot c)\cdot e}{(b\cdot d)\cdot f}=\frac{a\cdot c}{b\cdot d}\cdot\frac{e}{f}=\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}.$$

(6) Conmutatividad del producto: Sean $a/b, c/d \in F$. Tenemos

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}=\frac{c\cdot a}{d\cdot b}=\frac{c}{d}\cdot\frac{a}{b}.$$

(7) El elemento identidad viene dado por $1/1 \in F$. En efecto, sea $a/b \in F$. Tenemos

$$\frac{a}{b}\cdot\frac{1}{1}=\frac{a\cdot 1}{b\cdot 1}=\frac{a}{b}.$$

(8) Cada $a/b \in F$ no nulo ($a \neq 0$) posee inverso multiplicativo dado por $b\cdot a$. En efecto,

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{a\cdot b}{b\cdot a}=\frac{a\cdot b}{a\cdot b}=\frac{1}{1}.$$

□

Definición 4.2.1. El cuerpo $F = D/\sim$ se conoce como **cuerpo de fracciones** o **cuerpo cociente** de D.

La función $D \longrightarrow D/\sim$ dada por $a \mapsto a/1$ es un monomorfismo. Por lo tanto, todo dominio entero puede **sumergirse** en un cuerpo.

Ejemplo 4.2.1. ¿Cuál será el cuerpo de cocientes de $\mathbb{Q}[x]$?

Sean $p(x) = a_n \cdot x^n + \cdots a_1 \cdot x + a_0$ y $q(x) = b_m \cdot x^m + \cdots + b_1 \cdot x + b_0$ en $\mathbb{Q}[x]$, no nulos. Luego, $a_n, b_m \neq 0$. Entonces $p(x) \cdot q(x) \neq 0$ porque $a_n \cdot b_m \neq 0$. El cuerpo de fracciones $\mathbb{Q}[x]/\sim$ está dado por el conjunto de las funciones racionales, es decir las funciones de la forma $\frac{p(x)}{q(x)}$, donde $p(x) \in \mathbb{Q}[x]$ y $q(x) \in \mathbb{Q}[x]\backslash\{0\}$.

4.3 Característica de un polinomio

Definición 4.3.1. Se dice que un cuerpo $\mathbb{K}$ posee **característica** n si n es el menor entero positivo tan que $x + \cdots + x = 0$ (n veces), para todo $x \in \mathbb{K}$. Si no existe tal n, se dice que $\mathbb{K}$ es de característica cero.

Ejercicio 4.3.1. Dé un ejemplo de un cuerpo distinto de $\mathbb{Z}_p$ (p primo) con característica distinta de cero, si es que existe.

Teorema 4.3.1. La característica de un cuerpo es o cero o un número primo.

Demostración: Supongamos que un cuerpo $\mathbb{K}$ tiene característica $m \neq 0$. Sabemos que $m \cdot x = 0$, para todo $x \in \mathbb{K}$. Supongamos que m no es primo, entonces $m = n \cdot q$, para algún $n, q \in \mathbb{Z}$ entre 0 y m. Tenemos

$$0 = m \cdot 1 = (n \cdot q) \cdot 1 = (n \cdot 1) \cdot (q \cdot 1).$$

Como $\mathbb{K}$ es un dominio de integridad, se tiene $n \cdot 1 = 0$ o $q \cdot 1 = 0$, obteniendo así una contradicción. □

Teorema 4.3.2. Sea $\mathbb{K}$ un cuerpo y sea I un ideal de $\mathbb{K}$. Entonces $I = \{0\}$ o $I = \mathbb{K}$.

Teorema 4.3.3. Si R es un dominio de integridad con identidad y los únicos ideales de R son R y $\{0\}$, entonces R es un cuerpo.

Demostración: Sea $a \neq 0$ en R. Es fácil ver que $R \cdot a = \{r \cdot a : r \in R\}$ es un ideal de R. Luego, $R \cdot a = \{0\}$ o $R \cdot a = R$. Como $a = 1 \cdot a \in R \cdot a$, se tiene que $R \cdot a \neq \{0\}$. Entonces $R \cdot a = R$. Por ende $1 \in R \cdot a$, de donde existe $b \in R$ tal que $a \cdot b = b \cdot a = 1$. Se sigue que R es un cuerpo. □

CAPÍTULO 5

ANILLOS DE POLINOMIOS

5.1 Elementos algebraicos y trascendentes sobre un anillo

Sea R un anillo y

$$R[x] = \{\sum_{r=0}^{n} a_r \cdot x^r : a_r \in R \text{ y } n \in \mathbb{N}\}$$

el anillo de polinomios sobre R. A cada elemento de $R[x]$ se denomina **polinomio**.

Pregunta: ¿Existe $a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n = 0$ si algún $a_i \neq 0$?.

Definición 5.1.1. Sea A un anillo y sea $u \notin A$. Sea $B = A[u]$. Decimos que u es **algebraico** sobre A si existe alguna expresión de la forma $a_0 + a_1 \cdot u + \cdots + a_n \cdot u^n = 0$ con algún $a_i \neq 0$.

Por ejemplo, i es algebraico sobre $\mathbb{R}$ porque $x^2 + 1 = 0$ en i.

Definición 5.1.2. Si u no es algebraico sobre A, decimos que u es **trascendente**.

Proposición 5.1.1. Sea A un anillo conmutativo con identidad. Entonces existen elementos trascendentes sobre A.

Demostración: Sea

$$B = \{(a_0, a_1, \dots) : a_i \in A \text{ y } a_i = 0 \text{ salvo para un número finito de índices } i\}$$

el conjunto de todas las sucesiones infinitas de elementos de A cuyos elementos son casi todos cero. Note que para cada $(a_i)_{i\geq 0} \in B$ existe $n \in \mathbb{N}$ tal que $a_{n+1} = a_{n+2} = \cdots = 0$.

En B vamos a definir las siguientes operaciones de suma y producto:

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots),$$
$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots), \text{ donde } c_i = \sum_{k=0}^{i} a_k \cdot b_{i-k}.$$

Note que la suma y el producto de dos elementos en B está de nuevo en B. Tenemos que $(B, +, \cdot)$ es un anillo conmutativo con identidad $1 = (1, 0, \dots)$. El anillo A puede sumergirse en B, pues la función $\varphi : A \longrightarrow B$ dada por $a \mapsto (a, 0, \dots)$ es un monomorfismo. Podemos ver a B como una extensión de A. Sean:

$$\begin{aligned} x &= (0, 1, 0, \dots), \\ x^2 &= (0, 0, 1, 0, \dots), \\ x^3 &= (0, 0, 0, 1, 0, \dots), \\ &\vdots \end{aligned}$$

Sea $b = (b_0, b_1, \dots) \in B$. Tenemos

$$\begin{aligned} b &= (b_0, 0, \dots) + (0, b_1, \dots) + \cdots \\ &= b_0 \cdot (1, 0, \dots) + b_1 \cdot (0, 1, \dots) + \cdots \\ &= b_0 + b_1 \cdot x + \cdots + b_n \cdot x^n, \text{ para algún } n \in \mathbb{N}. \end{aligned}$$

Denotaremos $B = A[x]$. Tomamos B y contruímos $B[y]$ para obtener $R[x, y]$. Note que $B[y] = R[x][y] = R[x, y]$. En general

$$R[x_1, x_2, \dots, x_m] = R[x_1, x_2, \dots, x_{m-1}][x_m].$$

Veamos que x es trascendente. Supongamos que $a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n = 0$. Entonces $(a_0, a_1, \dots, a_n, 0, \dots) = 0$ y por lo tanto $a_i = 0$ para todo $i \in \mathbb{Z}_{\geq 0}$. Por lo tanto, x es trascendente. □

Ejercicio 5.1.1. Si A es un anillo conmutativo con identidad y x es trascendente sobre A, entonces existe un homomorfismo de anillos $\varphi : A[x] \longrightarrow A[u]$. Más aún, si u es trascendente sobre A, entonces φ es un isomorfismo.

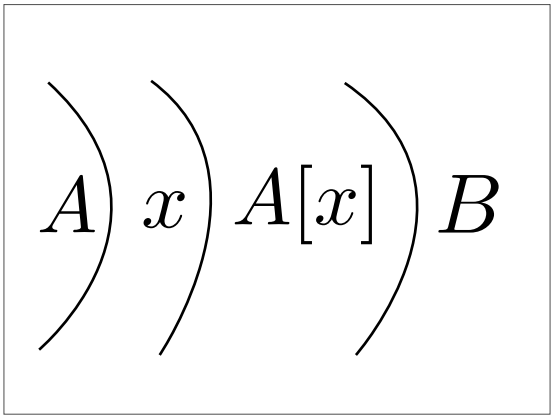
Lema 5.1.1. Si x es trascendente sobre un anillo R y si $a_0 + a_1 \cdot x + \cdots + a_N \cdot x^N = b_0 + b_1 \cdot x + \cdots + b_M \cdot x^M$, entonces $N = M$ y $a_j = b_j$ para todo j.

Demostración: Supongamos que $M > N$. Entonces $\sum_{k=0}^{N}(a_k - b_k) \cdot x^k + \sum_{k=N+1}^{M} b_k x^k = 0$. Como x es trascendente, $a_k - b_k = 0$ para todo $0 \leq k \leq N$, y $b_k = 0$ para todo $N + 1 \leq k \leq M$. De aquí se deduce que $N = M$ y que $a_i = b_i$ para todo i. □

5.2 Polinomios de varias variables

Sea A un anillo y considere al anillo de polinomios $A[x]$. Queremos construir $A[x, y]$. Sea

$$B = \{\sum_{j=0}^{n} a_j \cdot y^j : a_j \in A[x], \ n \in \mathbb{N}\}.$$



Si x es trascendente sobre sobre A y y es trascendente sobre $A[x]$, se dice que x y y son **algebraicamente independientes**.

¿Cómo son los elementos de $A[x][y] = A[x, y]$. Tenemos

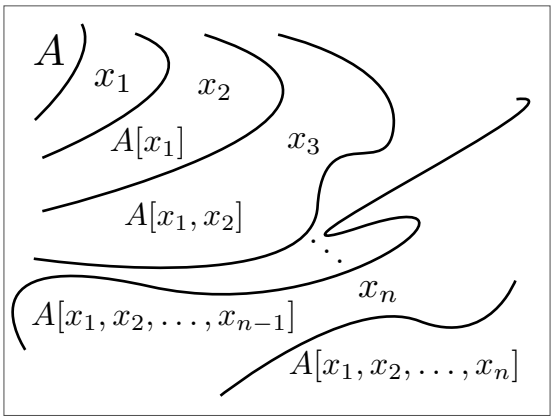
$$A[x, y] = \{\sum_{i,k} a_{ik} \cdot x^i \cdot x^k \,:\, a_{ik} \in A \text{ y } i, k \in \mathbb{Z}_{\geq 0}\}.$$

Si ya construímos $A[x_1, x_2, \ldots, x_{n-1}]$, podemos construir

$$B = \left\{ \sum_{\alpha_1,\ldots,\alpha_n} a_{(\alpha_1,\ldots,\alpha_n)} \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n} \,:\, a_{(\alpha_1,\ldots,\alpha_n)} \in A \right\},$$

donde

$$B = A[x_1, \ldots, x_n] = A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n].$$



Definición 5.2.1. $x_1, \ldots, x_n$ son **algebraicamente independientes** si $\sum a_{(\alpha_1,\ldots,\alpha_n)} \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n} = 0$ implica que $a_{(\alpha_1,\ldots,\alpha_n)} = 0$ para todo $(\alpha_1, \ldots, \alpha_n)$ en $(\mathbb{Z}_{\geq 0})^n$.

Proposición 5.2.1. Sean $x_1, \ldots, x_n$ algebraicamente independientes, tales que x_n es trascendente sobre $A[x_1, \ldots, x_{n-1}]$, x_{n-1} es trascendente sobre $A[x_1, \ldots, x_{n-2}]$, $\ldots$, x_2 es trascendente sobre $A[x_1]$, y x_1 es trascendente sobre A, donde A es un anillo conmutativo con elemento identidad. Entonces

$$\sum_{(j_1,\ldots,j_n)} a_{(j_1,\ldots,j_n)} \cdot x_1^{j_1} \cdots x_n^{j_n} = 0 \Longrightarrow a_{(j_1,\ldots,j_n)} = 0 \text{ para todo } (j_1, \ldots, j_n) \in (\mathbb{Z}_{\geq 0})^n.$$

Demostración: Por inducción sobre n. Para $n = 1$, si $\sum a_{j_i} \cdot x_1^{j_1} = 0$ entonces $j_1 = 0$ para todo $j_1 \in \mathbb{Z}_{\geq 0}$, porque x_1 es trascendente sobre A. Ahora supongamos que el resultado se cumple para $n-1$. Supongamos $\sum_{(j_1,\ldots,j_n)} a_{(j_1,\ldots,j_n)} \cdot x_1^{j_1} \cdots x_n^{j_n} = 0$. Escribamos $\sum_{(j_1,\ldots,j_n)} a_{(j_1,\ldots,j_n)} \cdot x_1^{j_1} \cdots x_n^{j_n} = \sum b_j \cdot x_n^j$, donde $b_j \in A[x_1, \ldots, x_{n-1}]$. Como x_n es trascendente sobre $A[x_1, \ldots, x_{n-1}]$, se tiene $b_j = 0$ para todo b_j en la expresión anterior. Usando la hipótesis inductiva, se sigue que $a_{(j_1,\ldots,j_n)} = 0$ para todo $(j_1, \ldots, j_n) \in (\mathbb{Z}_{\geq 0})^n$. □

5.3 Anillos euclidianos

Definición 5.3.1. Sea R un dominio de integridad. Decimos que R es un **anillo euclidiano** si para todo $a \neq 0$ en R existe un entero no negativo $d(a)$ tal que:

(1) Para cualesquiera $a, b \in R$, ambos distintos de cero, $d(a) \leq d(a \cdot b)$.

(2) Para cada $a, b \in R$, ambos distintos de cero, existen $t, r \in R$ tales que $a = t \cdot b + r$ donde $r = 0$ o $d(r) < d(b)$.

Ejercicio 5.3.1.

(1) Si R es un dominio de integridad y x es trascendente sobre R, demuestre que $R[x]$ es un dominio de integridad.

(2) Generalice el resultado anterior a $R[x_1, \ldots, x_n]$ con $x_1, \ldots, x_n$ algebraicamente independientes sobre R.

(3) Si F es un cuerpo, entonces $F[x]$ es un dominio de integridad euclídeo.

(4) Si F es un cuerpo e I es un ideal de $F[x]$, demuestre que I es un ideal principal.

Definición 5.3.2. Sea $p(x) \in R[x]$, donde x es trascendente sobre R. Decimos que $c \in R$ es una **raíz** o **cero** de $p(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ si $\varphi(p(x)) = 0$, donde $\varphi : R[x] \longrightarrow R[c]$ es el homomorfismo de evaluación $\varphi(p(x)) = a_0 + a_1 \cdot c + \cdots + a_n \cdot c^n$. Note que x tiene que ser trascendente para que φ esté bien definido.

Ejercicio 5.3.2. Demuestre las siguientes proposiciones:

(1) Si F es un cuerpo y $p(x) \in F[x]$, entonces $c \in F$ es raíz de $p(x)$ si, y sólo si, $x - c$ divide a $p(x)$.

(2) Si F es un cuerpo, $p(x) \in F[x]$, entonces el número de raíces distintas de $p(x)$ es menor o igual que el grado de $p(x)$.

(3) Si F es un cuerpo finito y $p(x) \in F[x]$, entonces existe $c \in F$ tal que $p(c) \neq 0$.

(4) Si F es un cuerpo finito, entonces existe $p(x) \in F[x]$ tal que $p(c) = 0$ para todo $c \in F$.

Ejercicio 5.3.3. Dados dos polinomios $p(x), q(x) \in F[x]$, demuestre que existe $d(x) \in F[x]$ que satisface:

(1) $d(x)|p(x)$ y $d(x)|q(x)$.

(2) Si existe $r(x)$ tal que $r(x)|p(x)$ y $r(x)|q(x)$, entonces $r(x)|d(x)$.

Pruebe que $d(x) = \lambda(x) \cdot p(x) + \beta(x) \cdot q(x)$, para algunos $\lambda(x), \beta(x) \in F[x]$.

Ejercicio 5.3.4. Sean F y K cuerpos, con $F \subseteq K$. Supongamos que $f(x), g(x) \in F[x]$ son primos relativos en $F[x]$. Demuestre que son primos relativos en $K[x]$. ¿Se puede afirmar algo en caso contrario?.

BIBLIOGRAFÍA

[1] Herstein, I. N. *Topics in Algebra*. Second Edition. John Wiley & Sons, Inc. (1975).

[2] Fraleigh, J. B. *A First Course in Abstract Algebra*. Seventh Edition. Pearson. (2002).