2. Estructuras Algebraicas

2.1. Conjuntos

Un conjunto es una reunión en un todo de determinados objetos bien definidos y diferentes entre sí. Llamamos elementos a los objetos que lo forman.
Requisitos:

- No ambigüedad.
- Elementos diferentes.
- El propio conjunto no puede ser un elemento.

Definiciones:

- Por extensión. $A = \{a, b, c, d\}$
- Por comprensión. $B = \{x \in \mathbb{N} \mid x \text{ es primo } \}$

Si a es un elemento del conjunto A, decimos que a pertenece a A y lo denotamos por $a \in A$.
En caso contrario lo denotamos por $a \notin A$.
Definimos el conjunto vacío como el conjunto carente de elementos.

$$\varnothing = \{\}$$

Decimos que $A = B$ si tienen exactamente los mismos elementos, es decir, si:

$$x \in A \text{ si y sólo si } x \in B$$

Decimos que A es un subconjunto de B o que A está incluido en B, $A \subseteq B$, si se satisface que

$$x \in A \text{ implica que } x \in B$$

Para todo conjunto A se cumple $\varnothing \subseteq A$ y $A \subseteq A$. Al resto de los subconjuntos los llamamos subconjuntos propios.

Lema 1 *Dados dos conjuntos A y B, $A = B$ si y sólo si $A \subseteq B$ y $B \subseteq A$.*

Diremos que A está contenido estrictamente en B si $A \subseteq B$ y $A \neq B$ y lo denotamos por

$$A \subset B$$

Trabajaremos siempre dentro de un conjunto mayor al que llamaremos universo o conjunto universal.
Dado un conjunto A, llamaremos partes de A, $\wp(A)$, al conjunto de todos los subconjuntos de A.
Llamamos cardinal de A al número de elementos que lo forman y lo denotamos por $|A|$.

Lema 2 *Dado un conjunto A, si $|A| = n$, entonces $|\wp(A)| = 2^n$.*

2.1.1. Operaciones con conjuntos

Sea $\mathcal{U}$ el universo y $A, B \subseteq \mathcal{U}$.
Llamamos complementario de A al conjunto

$$\overline{A} = \{x \in \mathcal{U} \mid x \notin A\}$$

Definimos la unión y la intersección respectivamente como

$$A \cup B = \{x \in \mathcal{U} \mid x \in A \text{ o } x \in B\} \qquad A \cap B = \{x \in \mathcal{U} \mid x \in A \text{ y } x \in B\}$$

Decimos que A y B son disjuntos si $A \cap B = \varnothing$.

2.1.1. Operaciones con conjuntos

Sea $\mathcal{U}$ el universo y $A, B \subseteq \mathcal{U}$.
Llamamos complementario de A al conjunto

$$\overline{A} = \{x \in \mathcal{U} \mid x \notin A\}$$

Definimos la unión y la intersección respectivamente como

$$A \cup B = \{x \in \mathcal{U} \mid x \in A \text{ o } x \in B\} \qquad A \cap B = \{x \in \mathcal{U} \mid x \in A \text{ y } x \in B\}$$

Decimos que A y B son disjuntos si $A \cap B = \varnothing$.

Dada una familia de conjuntos, $\{A_i\}_{i \in I}$, definimos su unión y su intersección resp. como

$$\bigcup_{i \in I} A_i = \{x \in \mathcal{U} \mid \text{ existe } i \in I \text{ con } x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x \in \mathcal{U} \mid x \in A_i \text{ para todo } i \in I\}$$

Otras Operaciones:

Diferencia: $A \smallsetminus B = \{x \in \mathcal{U} \mid x \in A \text{ y } x \notin B\} = A \cap \overline{B}$

Diferencia simétrica:

$$A \Delta B = \{x \in \mathcal{U} \mid x \in A \text{ o } x \in B \text{ pero } x \notin A \cap B\} = (A \cup B) \smallsetminus (A \cap B)$$

Propiedades:

Doble complemen.	$\overline{\overline{A}} = A$	
Conmutativa	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Asociativa	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Idempotencia	$A \cup A = A$	$A \cap A = A$
Absorción	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Neutralidad	$A \cup \varnothing = A$	$A \cap \mathcal{U} = A$
Dominación	$A \cup \mathcal{U} = \mathcal{U}$	$A \cap \varnothing = \varnothing$
Inversas	$A \cup \overline{A} = \mathcal{U}$	$A \cap \overline{A} = \varnothing$
de Morgan	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$

Propiedades Distributivas

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Principio de Inclusión-Exclusion

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

2.1.2. Producto Cartesiano

Sea $\mathcal{U}$ el universo y $A, B \subseteq \mathcal{U}$. Llamamos par ordenado a las listas del tipo (a, b) con $a \in A$ y $b \in B$. Además convenimos que

$$(a, b) = (a', b') \text{ si y sólo si } a = a' \text{ y } b = b'$$

Se define el producto cartesiano de A por B como el conjunto de todos los pares ordenados y lo denotamos por $A \times B$, es decir,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

La relacione existente entre los cardinales de estos conjuntos es la siguiente:

$$|A \times B| = |A|\ |B|$$

2.2. Relaciones

Llamamos relación binaria de A en B a cualquier subconjunto de $A \times B$. Al conjunto A lo llamamos conjunto inicial y al conjunto B conjunto final.
Sea $\mathcal{R} \subseteq A \times B$. Si $(a, b) \in \mathcal{R}$ lo representamos por $a\mathcal{R}b$ y en caso contrario por $a \not\mathcal{R} b$.
Se definen los conjuntos dominio e imagen de una relación $\mathcal{R} \subseteq A \times B$ como

$$\mathcal{D}om(\mathcal{R}) = \{x \in A \mid \text{ existe } b \in B \text{ con } x\mathcal{R}b\}$$

$$\mathcal{I}m(\mathcal{R}) = \{x \in B \mid \text{ existe } a \in A \text{ con } a\mathcal{R}x\}$$

2.2.1. Relaciones Internas

Decimos que una relación es interna en un conjunto A si cumple $\mathcal{R} \subseteq A \times A$

Para cada conjunto A se define la relación identidad en A como

$$a \, \mathcal{I}_A b \quad \text{si y solo si} \quad a = b$$

Propiedades que pueden presentar las Relaciones Internas:

- Reflexiva: Para todo $a \in A$ se tiene $a\mathcal{R}a$
- Antirreflexiva: Para todo $a \in A$ se tiene $a \not\mathcal{R} a$
- Simétrica: Para todo $a, b \in A$, si $a\mathcal{R}b$ entonces $b\mathcal{R}a$
- Antisimétrica: Para todo $a, b \in A$, si $a\mathcal{R}b$ y $b\mathcal{R}a$ entonces $a = b$
- Transitiva: Para todo $a, b, c \in A$, si $a\mathcal{R}b$ y $b\mathcal{R}c$ entonces $a\mathcal{R}c$

2.2.2. Relaciones de Orden

Sea $\mathcal{R}$ una relación interna en A.

Decimos que $\mathcal{R}$ es de orden si es reflexiva, antisimétrica y transitiva.

Decimos que dos elementos $a, b \in A$ son comparables si $a\mathcal{R}b$ o $b\mathcal{R}a$.

Una relación de orden es total si todos los elementos son comparables entre sí; en otro caso decimos que es parcial.

Ejemplo 3 *Definimos en $\mathbb{N}$ la relación "ser divisor de" como*

$$a \textit{ es divisor de } b \textit{ si y solo si existe } m \in \mathbb{N} \textit{ tal que } am = b$$

- *¿Es una relación de orden?*

2.2.2. Relaciones de Orden

Sea $\mathcal{R}$ una relación interna en A.

Decimos que $\mathcal{R}$ es de orden si es reflexiva, antisimétrica y transitiva.

Decimos que dos elementos $a, b \in A$ son comparables si $a\mathcal{R}b$ o $b\mathcal{R}a$.

Una relación de orden es total si todos los elementos son comparables entre sí; en otro caso decimos que es parcial.

Ejemplo 3 *Definimos en $\mathbb{N}$ la relación "ser divisor de" como*

$$a \text{ es divisor de } b \text{ si y solo si existe } m \in \mathbb{N} \text{ tal que } am = b$$

- *¿Es una relación de orden?*
- *¿Es total o parcial?*

2.2.2. Relaciones de Orden

Sea $\mathcal{R}$ una relación interna en A.

Decimos que $\mathcal{R}$ es de orden si es reflexiva, antisimétrica y transitiva.

Decimos que dos elementos $a, b \in A$ son comparables si $a\mathcal{R}b$ o $b\mathcal{R}a$.

Una relación de orden es total si todos los elementos son comparables entre sí; en otro caso decimos que es parcial.

Ejemplo 3 *Definimos en $\mathbb{N}$ la relación "ser divisor de" como*

$$a \text{ es divisor de } b \text{ si y solo si existe } m \in \mathbb{N} \text{ tal que } am = b$$

- *¿Es una relación de orden?*
- *¿Es total o parcial?*
- *Si la definimos en $\mathbb{Z}$, ¿es de orden?*

2.2.2. Relaciones de Orden

Sea $\mathcal{R}$ una relación interna en A.

Decimos que $\mathcal{R}$ es de orden si es reflexiva, antisimétrica y transitiva.

Decimos que dos elementos $a, b \in A$ son comparables si $a\mathcal{R}b$ o $b\mathcal{R}a$.

Una relación de orden es total si todos los elementos son comparables entre sí; en otro caso decimos que es parcial.

Ejemplo 3 *Definimos en $\mathbb{N}$ la relación "ser divisor de" como*

$$a \textit{ es divisor de } b \textit{ si y solo si existe } m \in \mathbb{N} \textit{ tal que } am = b$$

- *¿Es una relación de orden?*
- *¿Es total o parcial?*
- *Si la definimos en $\mathbb{Z}$, ¿es de orden?*
- *¿Y si lo hacemos en $\mathbb{R}$?*

2.2.3. Relaciones de Equivalencia

Una relación interna se dice que es de equivalencia si es reflexiva, simétrica y transitiva.

Dado un conjunto $A \neq \varnothing$, decimos que una familia de subconjuntos no vacíos de A, $\{A_i\}_{i\in I}$, es una partición de A si satisfacen las dos condiciones siguientes:

1. $\bigcup_{i\in I} A_i = A$
2. Para todo $i, j \in I$ con $i \neq j$ se tiene que $A_i \cap A_j = \varnothing$

Sea $\mathcal{R}$ una relación de equivalencia en A y $a \in A$. Llamamos clase de equivalencia de a al conjunto

$$[a] = \{x \in A \mid a\mathcal{R}x\}$$

Teorema 4 *Sea $\mathcal{R} \subseteq A \times A$ una relación de equivalencia y $a, b \in A$.*

1. $a \in [a]$
2. *Si $a\mathcal{R}b$ entonces $[a] = [b]$*
3. *Si $[a] \neq [b]$ entonces $[a] \cap [b] = \varnothing$*

Corolario 5 *Las clases de equivalencia de una relación de equivalencia $\mathcal{R}$ en A forman una partición de A.*

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\textit{mod } m)} b \textit{ si y solo si } m \textit{ es divisor de } b - a$$

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\textit{mod } m)} b \textit{ si y solo si } m \textit{ es divisor de } b - a$$

- *Prueba que $\equiv_{(\textit{mod } 2)}$ es una relación de equivalencia.*

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\textit{mod } m)} b \textit{ si y solo si } m \textit{ es divisor de } b - a$$

- *Prueba que $\equiv_{(\textit{mod } 2)}$ es una relación de equivalencia.*
- *Calcula $[0]$.*

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\textit{mod } m)} b \textit{ si y solo si } m \textit{ es divisor de } b - a$$

- *Prueba que $\equiv_{(\textit{mod } 2)}$ es una relación de equivalencia.*
- *Calcula $[0]$.*
- *Calcula $[1]$.*

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\textit{mod}\ m)} b \textit{ si y solo si } m \textit{ es divisor de } b - a$$

- *Prueba que $\equiv_{(\textit{mod}\ 2)}$ es una relación de equivalencia.*
- *Calcula $[0]$.*
- *Calcula $[1]$.*
- *Determina $\mathbb{Z}/_{\equiv_{(\textit{mod}\ 2)}}$.*

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\textit{mod}\ m)} b \text{ si y solo si } m \text{ es divisor de } b - a$$

- *Prueba que $\equiv_{(\textit{mod}\ 2)}$ es una relación de equivalencia.*
- *Calcula $[0]$.*
- *Calcula $[1]$.*
- *Determina $\mathbb{Z}/_{\equiv_{(\textit{mod}\ 2)}}$.*

Generalizando tenemos que $\mathbb{Z}_m = \mathbb{Z}/_{\equiv_{(\textit{mod}\ m)}} = \{[0], [1], \ldots [m-1]\}$.

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\textit{mod } m)} b \textit{ si y solo si } m \textit{ es divisor de } b - a$$

- *Prueba que $\equiv_{(\textit{mod } 2)}$ es una relación de equivalencia.*
- *Calcula $[0]$.*
- *Calcula $[1]$.*
- *Determina $\mathbb{Z}/_{\equiv_{(\textit{mod } 2)}}$.*

Generalizando tenemos que $\mathbb{Z}_m = \mathbb{Z}/_{\equiv_{(\textit{mod } m)}} = \{[0], [1], \ldots [m-1]\}$.

- *¿A qué clase pertenece 19 en $\mathbb{Z}_5$?*

Llamamos conjunto cociente de A con la relación $\mathcal{R}$ al conjunto formado por las clases de equivalencias y lo denotamos por $A/_{\mathcal{R}}$

Ejemplo 6 *Dado un $m \in \mathbb{Z}$, consideremos en $\mathbb{Z}$ la relación*

$$a \equiv_{(\mathit{mod}\ m)} b \text{ si y solo si } m \text{ es divisor de } b - a$$

- *Prueba que $\equiv_{(\mathit{mod}\ 2)}$ es una relación de equivalencia.*
- *Calcula $[0]$.*
- *Calcula $[1]$.*
- *Determina $\mathbb{Z}/_{\equiv_{(\mathit{mod}\ 2)}}$.*

Generalizando tenemos que $\mathbb{Z}_m = \mathbb{Z}/_{\equiv_{(\mathit{mod}\ m)}} = \{[0], [1], \ldots [m-1]\}$.

- *¿A qué clase pertenece 19 en $\mathbb{Z}_5$?*
- *Si $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ y $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$, ¿es cierto que $\mathbb{Z}_4 \subseteq \mathbb{Z}_5$?*

2.3. Funciones

Decimos que una relación $f \subseteq A \times B$ es una función o aplicación si satisface las dos condiciones siguientes:

1. $\mathcal{D}om(f) = A$
2. Si $(a,b) \in f$ y $(a,c) \in f$ entonces $b = c$

NOTACIÓN:
Escribiremos $f : A \to B$ y $f(a) = b$
y diremos que b es imagen de a o que a es origen de b.

EJEMPLOS: $I_{\mathbb{N}}$ e $I_{\mathbb{R}}$.

Sea $f : A \to B$ una aplicación, $X \subseteq A$ y $Y \subseteq B$.
Llamamos imagen de X al conjunto

$$f(X) = \{f(x) \mid x \in X\}$$

y preimagen o imagen inversa de Y al conjunto

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$$

2.3.1. Tipos de Funciones

Sea $f : A \to B$ una función.

- Decimos que f es inyectiva si $f(x) = f(x')$ implica que $x = x'$
- Decimos que f es sobreyectiva si $\mathcal{I}m(f) = B$
- Decimos que f es biyectiva si es inyectiva y sobreyectiva.

2.3.2. Composición de Funciones y Función Inversa

Dadas dos funciones $f : A \to B$ y $g : B \to C$ se define f compuesto con g como la función

$$g \circ f : A \to C \qquad (g \circ f)(x) = g(f(x))$$

Diremos que f es inversible si la relación f^{-1} es una función.

Teorema 7 *Una función es inversible si y solo si es biyectiva.*

Teorema 8 *Sea $f : A \to B$ una función inversible. f^{-1} es la única función que cumple*

$$f^{-1} \circ f = I_A \qquad f \circ f^{-1} = I_B$$