TEMAS DE MATEMÁTICAS
(Oposiciones de Secundaria)

TEMA 11

<u>CONCEPTOS BASICOS DE LA TEORIA DE CONJUNTOS. ESTRUCTURAS ALGEBRAICAS.</u>

TEMA 11

CONCEPTOS BASICOS DE LA TEORIA DE CONJUNTOS. ESTRUCTURAS ALGEBRAICAS.

1. INTRODUCCIÓN.

El precursor de la teoría de conjuntos fue George Cantor (1845-1918). La desarrolló como una rama autónoma de la matemática y le dio el nombre de Mengenlehre (teoría de conjuntos).

Cantor definió conjunto como “una colección de objetos determinados y perfectamente diferenciables en nuestra contemplación o en nuestro pensamiento, que constituyen una totalidad”.

Esta intuitiva definición de Cantor dio lugar a la aparición de paradojas, que fueron solucionadas por Poincaré. Este puso en evidencia que la raíz de las paradojas que se plantearon estaba en el hecho de que se definía un objeto en términos de una clase de objetos que incluía al propio objeto definido.

Una paradoja famosa, planteada por Bertrand Russell fue: “Un barbero ha de afeitar a todos aquellos y sólo a aquellos habitantes del pueblo que no se afeitan a si mismos ¿Ha de afeitarse el barbero a si mismo o no?”. Cualquiera que sea la respuesta se llega a una contradicción.

2. CONJUNTOS.

Los conjuntos están formados por colecciones de objetos, atendiendo a la definición de Cantor, y a los objetos los llamo elementos.

Notación. Nombraremos a los conjuntos mediante letras mayúsculas y a los elementos con minúsculas. Indicaremos que un elemento a esta o pertenece a un conjunto C y mediante $a \in C$, y su negación se representa por $a \notin C$.

OBS Un conjunto queda completamente definido cuando se conocen todos sus elementos. Y se pueden conocer de dos maneras diferentes:

1) Por extensión, cuando se enumeran todos sus elementos. Por ejemplo

$$A = \{a, b, c\}.$$

2) Por Compresión, cuando se da una propiedad que define inequívocamente a los elementos del conjunto. Por ejemplo:

$$A = \{\sqcap \in \mathbb{N} / \sqcap \bmod 2 = 0\}$$

DEF Se define el conjunto vacío, $\varnothing$, como un conjunto sin elementos. $\varnothing = \{\}$

DEF Diremos que el conjunto A está incluido en B, o A es subconjunto de B, si todo elementos de A está en B. Lo denotaremos por $A \subset B$. Es decir:

$$A \subset B \Leftrightarrow \{\forall x \in A \Rightarrow x \in B\}$$

Todo conjunto A tiene dos subconjuntos especiales que llamaremos impropios. Son el conjunto vacío, Ø, y el propio conjunto.

DEF Diremos que B es un subconjunto propio de A si no es vacío $B \subset A$ y $B \neq A$.

PROP Sean A, B y C conjuntos. Se verifican las siguientes propiedades:

1) $A \subset A$
2) $A \subset B$ y $B \subset A \Leftrightarrow A = B$
3) $A \subset B$ y $B \subset C \Rightarrow A \subset C$

Dem.

La demostración es inmediata a partir de la definición.

La propiedad uno recibe el nombre de Reflexiva y la tres de transitiva. La segunda se llama antisimétrica y se utiliza para demostrar la igualdad entre dos conjuntos.

DEF Llamaremos conjunto de las partes de A, siendo A un conjunto, al conjunto que tiene por elementos todos los subconjuntos de A, y se denota por P(A). Entonces

$$B \in P(A) \Leftrightarrow B \subset A$$

2.1. Operaciones con conjuntos.

Sea u un conjunto, que llamaremos universal. Consideraremos P(u).

2.1.1. Intersección.

DEF Sean A y B dos conjuntos tales que A, B ∈ P(u). Definimos la intersección de A y B como el conjunto formado por los elementos comunes a A y B. Se representa por U.

$$AUB = \{x^{\in u} / x \in A \text{ y } x \in B\}$$

PROP La operación de intersección definida anteriormente, verifica las siguientes propiedades ∀A, B, C ∈ P(u).

1) Idempotente: $A \cap A = A$

2) Conmutativa: $A \cap B = B \cap A$

3) Asociativa: $(A \cap B) \cap C = A \cap (B \cap C)$

4) Elemento Neutro U: $A \cap U = A$

5) Elemento Absorbente Ø: $A \cap Ø = Ø$

DEF Dados A y B que pertenecen a P(u), diremos que son disjuntos si su intersección es vacía. Es decir, A y B son disjuntos si $A \cap B = \emptyset$.

2.1.2. Unión.

DEF Sean A y B dos conjuntos tales que $A, B \in P(U)$. Definimos la unión de A y B como el conjunto formado por los elementos que pertenecen al menos a uno de los dos conjuntos. Se representa por $\cup$.

$$A \cup B = \{x \in U / x \in A \text{ ó } x \in B\}$$

PROP La operación de unión definida anteriormente verifica las siguientes propiedades $\forall A, B, C \in P(U)$:

1) Idempotente: $A \cup A = A$

2) Conmutativa: $A \cup B = B \cup A$

3) Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$

4) Elemento neutro, $\emptyset$: $A \cup \emptyset = A$

5) Elemento Absorbente, U: $A \cup U = U$

2.1.3. Complementación.

DEF Sea $A \in P(U)$. Llamaremos complemento de A respecto de U, y lo denotaremos por $\overline{A}$ o A^c, al conjunto

$$A^c = \{x \in U / x \notin A\}$$

PROP La operación de complementación definida anteriormente verifica las siguientes propiedades

$$\forall A, B, C \in P(U).$$

1) $A \cup A^c = U$ y $A \cap A^c = \emptyset$

2) $\emptyset^c = U$ y $U^c = \emptyset$

3) $(A^c)^c = A$

4) $A \subset B \Rightarrow B^c \subset A^c$

5) Leyes de Morgan: $(A \cup B)^c = A^c \cup B^c$ y $(A \cap B)^c = A^c \cap B^c$

2.1.4. Diferencia.

DEF Sean A y B dos conjuntos tales que $A, B \in P(U)$. Definimos la diferencia de A menos B al conjunto formado por los elementos de A que no están en B.

$$A - B = \{x \in A / x \notin B\}$$

DEF Sean A y B dos conjuntos tales que A, B $\in$ P(U). Definimos la diferencia simétrica de A y B al conjunto formado por los elementos que pertenecen a A o a B pero no a ambos. Se representa por Δ

$$A \Delta B = \{x \in A \cup B / \ x \notin A \cap B\}$$

PROP $A \Delta B = (A - B) \cup (B - A)$

2.2. Algebra de Boole de las partes de un conjunto.

PROP Se verifica:

1) Leyes de Absorción: $\forall A, B \in P(U)$

   a) $A \cup (A \cap B) = A$
   b) $A \cap (A \cup B) = A$

2) Propiedades distributivas: $\forall A, B, C \in P(U)$

   a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

DEF El conjunto P(U) con las operaciones de unión e intersección tiene estructura de Algebra de Boole.

3. PRODUCTO CARTESIANO DE CONJUNTOS.

DEF Definimos par ordenado como el objeto matemático formado por dos elementos u objetos en un orden determinado. Se denota por (a, b). Los elementos a y b reciben el nombre de componentes o coordenadas del par (a, b).

$$(a, b) = (x, y) \Leftrightarrow a = x \quad y \quad b = y$$

Podemos generalizar la definición anterior a n elementos.

DEF Definimos la □- tupla ordenada por $(x_1, x_2, \ldots, x_n)$ siendo $x_1, x_2, \ldots x_n$ □ elementos u objetos en un orden determinado.

DEF Sean A y B dos conjuntos cualesquiera. Llamaremos Producto Cartesiano de A y B, y se representa por AxB, al conjunto formado por todos los pares ordenados (a, b) tales que $a \in A$ y $b \in B$.

$$AxB = \{(a, b) / \ a \in A \text{ y } b \in B\}$$

Se puede observar fácilmente que si el conjunto A tiene n elementos y el conjunto B tiene m elementos, entonces el conjunto AxB tendrá n x m elementos.

Igualmente, podemos generalizar la definición de producto cartesiano a n conjuntos.

DEF Sean $A_1, A_2, \ldots A_n$ n conjuntos cualesquiera. Llamaremos producto cartesiano de $A_1, A_2, \ldots A_n$, y se representa por $A_1 \text{x } A_2 \text{x} \ldots \text{x} A_n$, al conjunto formado por todas las n-tuplas $(x_1, x_2, \ldots, x_n)$ tales que

$$x_1 \in A_1,\ x_2 \in A_2, \ldots x_n \in A_n.$$

$$A_1 \text{x} A_2 \text{x} \ldots \text{x} A_n = \{(x_1, x_2, \ldots x_n) / x_i \in A_i \quad \forall_{i:\, 1,\ldots,n}\}$$

Para poder representar el producto cartesiano de dos conjuntos tenemos dos posibles formas:

1) Mediante un diagrama cartesiano. Son análogos a los utilizados para representar las coordenadas del plano cartesiano, con la diferencia de que ahora solo utilizamos el 1^{er} cuadrante.

2) Mediante un diagrama sagital. Se representan los conjuntos por medio de diagramas de Venn y se unen a los elementos del primer conjunto con los del segundo conjunto mediante flechas.

PROP $A \text{ x } B = \emptyset \Leftrightarrow A = \emptyset$ ó $B = \emptyset$

Dem.

Si $A \text{ x } B = \emptyset \Leftrightarrow$ No existe ningún par ordenado $(a, b) \in A \text{ x } B \Leftrightarrow A = \emptyset$ ó $B = \emptyset$

PROP $A \text{ x } B \subset A' \text{ x } B' \Leftrightarrow A \subset A'$ y $B \subset B'$

Dem.

Sean $a \in A$ y $b \in B \Rightarrow (a, b) \in A \text{ x } B \Rightarrow$ Por hipótesis $(a, b) \in A' \text{ x } B' \Rightarrow$

$\Rightarrow a \in A'$ y $b \in B'$

Luego $A \subset A'$ y $B \subset B'$

Sea $(a, b) \in A \text{ x } B \Rightarrow a \in A$ y $b \in B \Rightarrow$ Por hipótesis $a \in A'$ y $b \in B' \Rightarrow (a, b) \in A' \text{ x } B'$

Luego $A \text{ x } B \subset A' \text{ x } B'$

PROP Propiedad distributiva del producto cartesiano respecto de la intersección:

1) $A\text{x} (B \cap C) = (A\text{x}B) \cap (A\text{x}C)$

2) $(BnC) \text{ x } A = (B\text{x}A) \cap (C\text{x}A)$

Dem.

1) El conjunto $A\text{x}(B \cap C)$ está formado por

$Ax\ (B\cap c) = \{(a, x)/a\in A \text{ y } x\in B\cap C\}$

y $\{(a, x)/a\in A \text{ y } x\in BnC\} = \{(a, x)/a\in B \text{ y } x\in C\} =$

$= \{(a, x)/(a\in A \text{ y } x\in B) \text{ y } (a\in A \text{ y } x\in C)\} =$

$= \{(a, c)/a\in A \text{ y } x\in B\} \cap \{(a, x)/ a\in A \text{ y } x\in C\} =$

$= (AxB) \cap (AxC)$

Luego $Ax\ (B\cap C) = (AxB) \cap (AxC)$

2) Análogo al anterior.

PROP Propiedad distributiva del producto cartesiano respecto de la unión.

1) $Ax\ (B\cup C) = (AxB) \cup (AxC)$

2) $(B\cup C)\ xA = (BxA) \cup (CxA)$

<u>Dem.</u>

2) $(B\cup C)\ xA = \{(x, a)/ x\in B\cup C \text{ y } a\in A\} = \{(x, a)/(x\in B \text{ ó } x\in C) \text{ y } a\in A\} =$

$= \{(x, a)/(x\in B \text{ y } a\in A) \text{ ó } (x\in C \text{ y } a\in A)\} = \{(x, a)/x\in B \text{ y } a\in A\} \cup \{x, a)/ x\in C \text{ y }$

$a\in A\} = (BxA) \cup (CxA)$

1) Análogo al anterior.

PROP Propiedades distributiva del producto cartesiano respecto de la diferencia.

1) $Ax\ (B - C) = (AxB) - (AxC)$
2) $(B - C)\ xA = (BxA) - (CxA)$

<u>Dem.</u>

1) $Ax\ (B - C) = \{(a, x) / a\in A \text{ y } x\in (B - C)\} = \{(a, x) / a\in A \text{ y } (x\in B \text{ y } x\notin C)\} =$

$= \{(a, x) / (a\in A \text{ y } x\in B) \text{ y } (a\in A \text{ y } x\notin C)\} = (AxB) - (AxC)$j

2) Análogo al caso anterior.

<u>4. CORRESPONDENCIAS Y RELACIONES ENTRE CONJUNTOS.</u>

<u>4.1. Correspondencias.</u>

DEF Llamaremos Grafo, G, a todo conjunto compuesto por pares ordenados.

Según la definición, dados A y B conjuntos, un grafo es cualquier subconjunto de AxB.

DEF Sean A y B dos conjuntos. Un subconjunto G de AxB, $G \subset AxB$ llamado grafo, define una correspondencia entre A y B. El conjunto G recibe el nombre de grafo de al correspondencia. La correspondencia se denota por la terna (A, B, G).

Dada la correspondencia (A, B, G), podemos definir:

1) El conjunto $\{a \in A \ / \ \exists b \in B \text{ con } (a, b) \in G\}$, subconjunto de A, recibe el nombre de Dominio de la Correspondencia. Se denota por Dom (A, B, G).

2) El conjunto $\{b \in B \ / \ \exists a \in A \text{ con } (a, b) \in G\}$, subconjunto de B, recibe el nombre de Imagen de Correspondencia. Se denota por Im (A, B, G).

3) Dado $a \in A$, el conjunto $\{b \in B \ / \ (a, b) \in G\}$ recibe el nombre de imagen de a. Se denota por Im (a).

La correspondencia (A, B, G) se suele denotar por f, escribiéndose $f: A \rightarrow B$, donde para cada $(a, b) \in G$, b se puede escribir como $b = f(a)$.

DEF Dada la correspondencia (A, B, G) definimos la correspondencia inversa como (B, A, G^{-1}) siendo $G^{-1} = \{(b, a) \ / \ (a, b) \in G\}$. También se suele denotar por f^{-1}.

Es claro que el conjunto $\text{Dom}(f) = \text{Im}(f^{-1})$ y que $\text{Im}(f) = \text{Dom}(f^{-1})$ por la propia definición del conjunto G^{-1}.

4.2. Relaciones.

DEF Sean A y B dos conjuntos. Llamaremos relación entre $a \in A$ y $b \in B$, y se denota por aRb, a toda propiedad definida sobre AxB.

Toda relación lleva asociado un subconjunto $G \subset AxB$ siendo
$G = \{(a, b) \in AxB \ / \ aRb\}$.

DEF El conjunto G asociado a una relación R entre A y B recibe el nombre de Gráfica de la Relación.

DEF Llamaremos Relación Binaria al caso particular de una relación entre elementos del mismo conjunto, (caso A = B).

Una relación binaria definida sobre A puede verificar las siguientes propiedades:

1) Reflexiva: $\forall a \in A$ se verifica $(a, a) \in G$ ó aRa.

2) Simétrica: $\forall (a, b) \in G \Rightarrow (b, a) \in G$ $(\forall aRb \Rightarrow bRa)$.

3) Antisimétrica: Si $(a, b) \in G$ y $(b, a) \in G \Rightarrow a = b$ $(aRb \text{ y } bRa \Rightarrow a = b)$.

4) Transitiva: Si $(a, b)\in G$ y $(b, c)\in G \Rightarrow (a, c)\in G$.

5) Convexa: $\forall a, b\in A \quad (a, b)\in G$ ó $(b, a)\in G$.

4.2.1. Relaciones de Equivalencia.

DEF Una Relación de Equivalencia es una Relación binaria que verifica las propiedades reflexiva, simétrica y transitiva.

DEF Sea A un conjunto y R una relación de equivalencia definida en A. Para cada $a\in A$ definimos la clase de equivalencia de a como el conjunto de elementos $x\in A$ tales que aRx. Se representa por [a].

$$[a] = \{x\in A \ / \ aRx\}$$

PROP Sea A un conjunto y R una relación de equivalencia definida en A. Si a y a´ son elementos de A, son equivalentes:

1) aRa´
2) $a\in [a´]$
3) $[a] = [a´]$

Dem.

1) $\Leftrightarrow$ 2) Es cierta por definición de clase de equivalencia.

2) $\Leftrightarrow$ 3)
$$\left.\begin{array}{l}\text{Sea } x\in [a] \Rightarrow xRa \\ \text{Por hipótesis } a\in [a´] \Rightarrow aRa´\end{array}\right\} \Rightarrow xRa´ \Rightarrow x\in [a´]$$

Luego $[a´] \subset [a]$

$$\left.\begin{array}{l}Si \quad x\in [a´] \Rightarrow xRa´ \\ Por\ hipótesis\ aRa´ \Rightarrow a´Ra\end{array}\right\} \Rightarrow xRa \Rightarrow x\in [a]$$

Luego $[a´]\subset[a]$

Como $[a]\subset[a´]$ y $[a´]\subset[a] \Rightarrow [a] = [a´]$

3) $\Rightarrow$ 2)

Como $a\in [a]$ y por hipótesis $[a] = [a´] \Rightarrow a\in [a´]$

COROLARIO. Dos clases de equivalencia o son iguales o son distintas.

Dem.

Sean [a] y [b] dos clases de equivalencia con $a\in [a]$ y $b\in [b]$.

Si [a] ∩ [b] ≠ Ø, sea $x\in [a]\cap[b] \Rightarrow$ $\left.\begin{cases} x\in [a] \Rightarrow [x]=[a] \\ x\in [b] \Rightarrow [x]=[b] \end{cases}\right\} \Rightarrow [a]=[b]$

DEF El conjunto formado por todas las clases de equivalencia que resultan de una relación de equivalencia R sobre el conjunto A, se llama Conjunto Cociente de A por la relación de equivalencia R, y se representa por A/R.

COROLARIO. La igualdad $\bigcup_{[a]\in A/R} [a] = A$ es cierta

Dem.

Como $[a]=\{a'\in A / aRa'\} \Rightarrow [a]\subset A \Rightarrow \bigcup_{[a]\in A/R} [a]\subset A$

Para cada $x\in A$ se verifica que $x\in [x] \Rightarrow x\in \bigcup_{[a]\in A/R} [a] \Rightarrow A\subset \bigcup_{[a]\in A/R} [a]$

Luego se da la igualdad.

4.2.2. Relaciones de Orden.

DEF Una Relación de Preorden es una relación binaria que verifica las propiedades Reflexiva y Transitiva.

DEF Una Relación de Orden es una relación binaria que verifica las propiedades Reflexiva, Antisimétrica y Transitiva.

DEF Una Relación de Orden Total es una Relación de Orden que además verifica la propiedad Conexa.

Las relaciones de orden se suelen denotar por el símbolo ≤.

DEF Un elemento $a\in A$ diremos que es mínimo si $a \leq x \ \forall x\in A$. Es máximo si $x \leq a \ \forall x\in A$.

DEF Un elemento $a\in A$ diremos que es minimal si no existe $x \neq a$ tal que $x \leq a$. Diremos que es maximal si no existe $x \neq a$ tal que $a \leq x$.

OBS Elemento mínimo, si existe, es único. Para que exista, debe ser comparable con todos, y ser el más pequeño. En cambio, elemento minimal es el más pequeño de todos con los que se puede comparar. Puede haber más de uno.

DEF Llamaremos Cadena a toda parte totalmente ordenada de un conjunto con una Relación de Orden.

Si la relación definida en el conjunto A es de orden total, existe una única cadena y la representación se puede realizar en línea recta (por ejemplo $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ó $\mathbb{R}$).

5. APLICACIONES ENTRE CONJUNTOS.

DEF Sea f una correspondencia entre los conjuntos A y B ($f: A \to B$). Diremos que f es una aplicación de A en B si verifica que para cada $a \in A$ existe un único $b \in B$ tal que $f(a) = b$.

Por tanto, si f es una aplicación, para cada $a \in A$ el conjunto Im(a) tiene un único elemento.

DEF Sea $f: A \to B$ una aplicación y $A' \subset A$ un subconjunto. La aplicación $f': A \to B$ definida por $f'(x) = f(x)$ recibe el nombre de Restricción de f a A´, y se denota por $f' = f|_{A'}$.

DEF Dos aplicaciones $f: A \to B$ y $g: C \to D$ son iguales si $A = C$, $B = D$ y $\forall a \in A$ $f(a) = g(a)$. Se denota por $f = g$.

DEF Diremos que la aplicación $f: A \to B$ es constante si $\forall a \in A$ se verifica que $f(a) = b$, para un cierto $b \in B$.

PROP Si f es una aplicación constante, el conjunto Dom(f) está formado por un solo elemento.

Dem.

Inmediata.

Una aplicación importante es la aplicación identidad. Es una aplicación de un conjunto en si mismo, $f: A \to A$, donde a cada elemento le hace corresponder como imagen él mismo, $f(x) = x \forall x \in A$. Se representa por I_A.

DEF Sean A y B dos conjuntos y $f: A \to B$ una aplicación:

1) Diremos que f es inyectiva si de $f(a) = f(a')$ con $a, a' \in A$ se deduce $a = a'$.

2) Diremos que f es suprayectiva si $\forall b \in B$ $\exists a \in A$ tal que $f(a) = b$. El elemento $a \in A$ no tiene porqué ser único.

3) Diremos que f es biyectiva si es simultáneamente inyectiva y suprayectiva.

A la vista de al definición podemos decir que una aplicación $f: A \to B$ es inyectiva si elementos distintos de A tienen imágenes distintas en B. Y es suprayectiva si todo elemento de B es imagen de alguno de A.

PROP Sean A y B dos conjuntos y f una aplicación de A en B biyectiva. La correspondencia inversa, f^{1}, es una aplicación de B en A.

Dem.

Como f es biyectiva, en particular es suprayectiva. Entonces,

$\forall b \in B \ \exists a \in A$ / f(a) = b. Y $f^{-1}(b) = a$.

Si $\exists a' \in A$ / $f^{-1}(b) = a'$ tenemos:

$$\left.\begin{array}{l} 1)\ f^{-1}(b) = a \Rightarrow f(a) = b \\ 2)\ f^{-1}(b) = a' \Rightarrow f(a') = b \end{array}\right\} \Rightarrow f(a) = f'(a')$$ y como f es inyectiva a = a´.

Luego a cada elemento $b \in B$ le corresponde un único elemento $a \in A$ tal que $f^{-1}(b) = a$, que es la definición de aplicación para f^{-1}.

PROP Sea f: A $\rightarrow$ B una aplicación biyectiva. La aplicación inversa f^{-1}: B $\rightarrow$ A es también biyectiva, y $(f^{-1})^{-1} = f$.

DEF Sean A, B, C y D conjuntos, f: A $\rightarrow$ B y g: C $\rightarrow$ D aplicaciones y $\mathrm{Imf} \subset C$. Llamaremos Aplicación Compuesta de f y g a h: A $\rightarrow$ D definida por $\forall x \in A$ h(x) = g(f(x)). Se denota por h = g ó f.

PROP Sean A, B, C y D conjuntos de f: A $\rightarrow$ B, g: B $\rightarrow$ C y h: C $\rightarrow$ D aplicaciones. Se verifica la propiedad asociativa para la operación de composición de aplicaciones. ho(g o f) = (h o g)of

Dem.

$\forall x \in A$ $\quad (h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$

$\quad ((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))$

Luego $h \circ (g \circ f) = (h \circ g) \circ f$

Si la aplicación f está definida de A en su mismo, f: A $\rightarrow$ A, entonces $f \circ f = f^2$ y $F^n = f^{n-1} \circ f$.

PROP Sean A y B dos conjuntos y f: A $\rightarrow$ B y g: B $\rightarrow$ A dos aplicaciones. Se verifican las siguientes propiedades:

1) $I_B \circ f = f \circ I_A = f$

2) f es biyectiva $\Rightarrow f^{-1} \circ f = I_A$ y $f \circ f^{-1} = I_B$

3) $g \circ f = I_A \Rightarrow$ f es inyectiva y g suprayectiva.

4) $g \circ f = I_A$ y $f \circ g = I_B \Rightarrow$ f y g son biyectivas con $g = f^{-1}$.

Dem.

1) $(I_B \circ f)(x) = I_B(f(x)) = f(x) = f(I_A(x)) = (f \circ I_A)(x) \quad \forall x \in A$

2) $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = I_A(x) \qquad \forall x \in A$

Como f es biyectiva $(f^{-1})^{-1} = f \Rightarrow f \circ f^{-1} = (f^{-1})^{-1} \circ f^{-1} = I_B$ aplicando lo demostrado en este mismo apartado.

3) Sean $a, a' \in A$ con $f(a) = f(a') \Rightarrow g(f(a)) = g(f(a')) \Rightarrow (g \circ f)(a) = (g \circ f)(a') \Rightarrow$

$\Rightarrow I_A(a) = I_A(a') \Rightarrow a = a' \Rightarrow$ f es inyectiva.

Dado $a \in A \Rightarrow f(a) = b$ para algún $b \in B \Rightarrow g(f(a)) = g(b) \Rightarrow (g \circ f)(a) = g(b) \Rightarrow$

$\Rightarrow I_A(a) = g(b) \Rightarrow g(b) = a \Rightarrow$ g es suprayectiva.

4) Como $g \circ f = I_A \Rightarrow$ f es inyectiva y g suprayectiva.

Como $f \circ g = I_B \Rightarrow$ g es inyectiva y f suprayectiva.

Luego f y g son biyectivas siendo

$$f^{-1} = f^{-1} \circ I_B = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = I_A \circ g = g$$

COROLARIO. Sea A, B y C conjuntos con $f: A \rightarrow B$, $g: B \rightarrow C$ aplicaciones biyectivas. Entonces $g \circ f$ es biyectiva y verifica $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

<u>Dem</u>.

$(g \circ f) \circ (f^{-1} \circ g^{-1}) = ((g \circ f) \circ f^{-1}) \circ g^{-1} = g \circ I_B \circ g^{-1} = g \circ g^{-1} = I_C$

$(f^{-1} \circ g^{-1}) \circ (g \circ f) = ((f^{-1} \circ g^{-1}) \circ g) \circ f = f^{-1} \circ I_B \circ f = f^{-1} \circ f = I_A$

Por el apartado 4) de la proposición anterior $g \circ f$ es biyectiva y $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

6. LEYES DE COMPOSICIÓN.

DEF Llamamos operación entre los conjuntos A y B con valores en C a toda aplicación de AxB en C.

DEF Llamamos operación interna, o ley de composición interna, definida en A a toda aplicación de AxA en A.

DEF Llamamos operación externa, o ley de composición externa, definida sobre A por la derecha a toda aplicación de AxB en A. Será por la izquierda si la aplicación es de BxA en A. El conjunto B recibe el nombre de dominio de operadores.

6.1. Leyes de Composición Interna.

Una operación interna definida sobre A, por definición, hace corresponder a cada par de elementos de A, es decir, un elemento de AxA, un único elemento de A.

Si $(x, y) \in AxA$, su imagen por la aplicación que define la operación externa se suele indicar mediante alguno de los siguientes símbolos:

$$x \cdot y, \quad x + y, \quad x \perp y, \quad x \circ y, \text{ etc.}$$

Si se escribe $x + y$ la operación interna recibe el nombre de "suma", y se lee "x mas y".

Si se escribe $x \cdot y$ la operación interna recibe el nombre de "producto", y se lee " x por y" ó " x multiplicado por y".

Veamos las propiedades que puede verificar una ley de composición interna.

Sea S una operación interna sobre A.

1) Diremos que S verifica la propiedad asociativa en A si

$$\forall x, y, z \in A \quad (xSy)Sz = xS(ySz)$$

2) Diremos que S es conmutativa si

$$\forall x, y \in A \qquad xSy = ySx$$

3) Diremos que S admite Elemento Neutro o Unidad si

$$\exists e \in A \quad \text{tal que} \quad \forall x \in A \quad eSx = xSe = x$$

4) Diremos que S admite elemento Simétrico si $\forall x \in A$

Por la izquierda $\quad \exists x' \in A \quad$ tal que $\quad x'Sx = e$

Por la derecha $\quad \exists x' \in A \quad$ tal que $\quad xSx' = e$

5) Diremos que S admite Elemento regular o Simplificable si $\forall x, y \in A$

r es Regular por la izquierda en A si $rSx = rSy \Rightarrow x = y$

r es Regular por la derecha en A si $xSr = ySr \Rightarrow x = y$

r es regular si y solo si lo es por ambos lados.

6) Diremos que S admite la propiedad idempotente si

$$\forall x \in A \qquad xSx = x$$

7) Diremos que S admite la propiedad distributiva respecto de otra operación interna T de A si:

Por la derecha: $(xTx)Sz = (xSz)T(ySz)$

Por la izquierda: $xS(yTz) = (xSy)T(xSz)$

Notación Dado un conjunto A con una operación interna S, se denotará por (A, S).

Como ejemplos tenemos $(\mathbb{N}, +)$ ó $(\mathbb{R}, +)$ ó $(\mathbb{Z}, \cdot)$.

6. 2. Leyes de Composición Externa.

Según la definición, en el conjunto A hay definida una operación externa si tenemos un conjunto B que será el dominio de operadores y una aplicación de AxB (o BxA) en A.

Los elementos del dominio de operadores se suelen denotar mediante letras griegas.

Veamos algunas de las propiedades que puede verificar una ley de composición externa, que denotaremos por T.

1) Conmutativa.

$$\forall \alpha \in B \quad \forall x \in A \qquad \alpha Tx = xT\alpha$$

2) Pseudoasociativa.

$$\forall \boldsymbol{a}, \boldsymbol{b} \in B \quad \forall x \in A \begin{cases} \boldsymbol{a}T(\boldsymbol{b}Tx) = (\boldsymbol{a}R\boldsymbol{b})Tx \\ (xT\boldsymbol{a})T\boldsymbol{b} = xT(\boldsymbol{a}R\boldsymbol{b}) \end{cases}$$

siendo R una operación interna en B.

3) Elemento Unidad.

$$\exists \sqcup \in B \quad \forall x \in A \qquad \sqcup Tx = x = xT\sqcup$$

4) Distributiva respecto de S, operación interna en A.

$$\forall \boldsymbol{a} \in B \text{ y } \forall x, y \in A \begin{array}{l} \text{Por la izquierda} \quad \boldsymbol{a}T(xSy) = (\boldsymbol{a}Tx)S(\boldsymbol{a}Ty) \\ \text{Por la derecha} \quad (xSy)T\boldsymbol{a} = (xT\boldsymbol{a})S(yT\boldsymbol{a}) \end{array}$$

5) Distributiva la operación interna R de B respecto de T.

$$\forall \boldsymbol{a}, \boldsymbol{b} \in B \quad \forall x \in A \begin{cases} \text{Por la izquierda} \quad (\boldsymbol{a}R\boldsymbol{b})Tx = (\boldsymbol{a}Tx)S(\boldsymbol{b}Tx) \\ \text{Por la derecha} \quad xT(\boldsymbol{a}R\boldsymbol{b}) = (xT\boldsymbol{a})S(xT\boldsymbol{b}) \end{cases}$$

7. ESTRUCTURAS ALGEBRAICAS.

7.1. Estructuras Algebraicas con una operación interna.

A lo largo de este punto vamos a denotar la operación interna mediante el símbolo $*$. Entonces, el par (A, $*$) denota al conjunto A con la operación interna $*$.

DEF El par (A, $*$) es un Semigrupo si la operación interna es asociativa en A.

DEF El par (A, $*$) es un Semigrupo Conmutativo si además verifica la propiedad Conmutativa.

DEF Diremos que (A, $*$) es un Monoide si es un semigrupo con elemento neutro.

Ejemplos:

1) ($\mathbb{N}^*$, +) es un semigrupo conmutativo.

2) $(\mathbb{N}, \cdot)$ es un Monoide.

DEF Diremos que $(G, *)$ es un grupo si se cumplen las propiedades asociativa, existencia de elemento neutro y existencia de elemento simétrico. Si además se verifica la propiedad conmutativa, diremos que es un grupo abeliano o conmutativo.

PROP En un grupo $(G, *)$ el elemento neutro es único.

Dem.

Sabemos que $e \in G$ es el elemento neutro.

Sea $e' \in G$ un elemento tal que $e' * x = x * e' = x \quad \forall x \in G$

Entonces se da que $e' = e' * e = e$ y por tanto el neutro es único.

PROP Cada elemento de G admite un único inverso.

Dem.

$\forall x \in G$ sabemos que $\exists x^{-1} \in G \ / \ x * x^{-1} = e = x^{-1} * x$

Sea $x'^{-1} \in G$ otro inverso de x.

$X'^{-1} = x'^{-1} * e = x'^{-1} * (x * x^{-1}) = (x'^{-1} * x) * x^{-1} = e * x^{-1} = x^{-1}$

Por tanto el inverso es único.

PROP Dado $(G, *)$ un grupo y $x, y, z \in G$ elementos cualesquiera, se verifica:

1) Si $x * y = e \Rightarrow x = y^{-1}$, $y = x^{-1}$

2) Si $x * y = x * z \Rightarrow y = z$

3) Si para algún $y \in G$ $x * y = y \Rightarrow x = e$ (análogamente $y * x = y$)

4) $(x * y)^{-1} = y^{-1} * x^{-1}$

Dem.

1) $x * y = e \Rightarrow (x * y) * y^{-1} = e * y^{-1} \Rightarrow x * (y * y^{-1}) = y^{-1} \Rightarrow x * e = y^{-1} \Rightarrow x = y^{-1}$

$x * y = e \Rightarrow x^{-1} * (x * y) = x^{-1} * e \Rightarrow (x^{-1} * x) * y = x^{-1} \Rightarrow e * y = x^{-1} \Rightarrow y = x^{-1}$

2) $x * y = x * z \Rightarrow x^{-1} * (x * y) = x^{-1} * (x * z) \Rightarrow (x^{-1} * x) * y = (x^{-1} * x) * z \Rightarrow e * y = e * z \Rightarrow$

$\Rightarrow y = z$

3) $x * y = y \Rightarrow (x * y) * y^{-1} = y * y^{-1} \Rightarrow x * (y * y^{-1}) = e \Rightarrow x * e = e \rightarrow x = e$

4) $(x*y)*(y^{-1}*x^{-1}) = (x*(y*y^{-1}))*x^{-1} = (x*e)*x^{-1} = x*x^{-1} = e$

Aplicando 1) $y^{-1}*x^{-1} = (x*y)^{-1}$

COROLARIO $\forall x \in G$ con (g, $*$) grupo, se verifica $(x^{-1})^{-1} = x$

Dem.

Tomando $y = x^{-1}$ y aplicando el apartado 1) de la proposición anterior se obtiene.

DEF Llamaremos Orden del Grupo (G, $*$) al número de elementos de G, en caso de que sea finito.

DEF Sea (G, $*$) un grupo y HCG un subconjunto no vacío. Diremos que (H, $*$) es un Subgrupo de (G, $*$) si

1) $\forall x, y \in H \Rightarrow x*y \in H$
2) $e \in H$
3) $\forall x \in H \quad \exists x^{-1} \in H$

PROP Sea (G, $*$) un grupo y HCG un subgrupo no vacío. (H, $*$) es un subgrupo de (g, $*$) si y solo si $\forall x, y \in H \quad x*y^{-1} \in H$.

Dem.

"$\Rightarrow$"

Como (H, $*$) es subgrupo $\Rightarrow \forall x, y \in H \quad x, y^{-1} \in H \Rightarrow x*y^{-1} \in H$.

"$\Leftarrow$"

Sea $x \in H$. Entonces por hipótesis $x*x^{-1} \in H \Rightarrow e \in H$.

Sea $x \in H$ y $e \in H$ por hipótesis $e*x^{-1} \in H \Rightarrow x^{-1} \in H$

Sea $x, y \in H \Rightarrow$ por lo anterior $y^{-1} \in H \Rightarrow$ Aplicando la hipótesis $x*(y^{-1})^{-1} \in H \Rightarrow$
$\Rightarrow x*y \in H$.

Como (H, $*$`) verifica las tres condiciones $\Rightarrow$ (H, $*$) es subgrupo de (G, $*$).

7.2. Estructuras Algebraicas con dos operaciones internas.

A lo largo de este punto vamos a denotar las dos operaciones internes mediante símbolos $*$ y $\circ$.

7.2.1. Anillos.

DEF La terna (A, $*$, $\circ$) es un Semianillo si se verifican

1) (A, $*$) es un semigrupo conmutativo con neutro.

2) $(A, \circ)$ es un semigrupo.
3) La operación $\circ$ es distributiva respecto de la operación $*$.

DEF $(A, *, \circ)$ es un Semianillo conmutativo si $(A, *, \circ)$ es un semianillo y $(A, \circ)$ es un semigrupo conmutativo.

DEF $(A, *, \circ)$ es un Semianillo con elemento unidad si $(A, *, \circ)$ es un Semianillo y $(A, \circ)$ es un semigrupo con elemento neutro.

Ejemplo.

$(\mathbb{N}, +, \cdot)$es un semianillo conmutativo con elemento unidad.

DEF Llamamos Anillo a la terna $(A, *, \circ)$ verificando:

1) $(A, *)$ es un grupo conmutativo.
2) $(A, \circ)$ es un semigrupo.
3) La operación $\circ$ es distributiva respecto de la suma.

Si además, la operación $\circ$ es conmutativa, el anillo es Conmutativo; si la operación $\circ$ tiene elemento neutro, es un anillo unidad; y si verifica ambas, es un anillo conmutativo con elemento unidad.

Ejemplo:

Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con la suma y el producto forman Anillos Conmutativos con elemento Unidad.

PROP Sea $(A, +, \cdot)$ un anillo. $\forall x, y, z \in A$ se verifican las siguientes propiedades:

1) $O \cdot x = x \cdot O = O$

2) $(-x) \cdot y = x \cdot (-y) = -(xy)$

3) $(-x) \cdot (-y) = xy$

4) $x \cdot (y - z) = xy - xz$ y $(x - y) \cdot z = x \cdot z - y \cdot z$

<u>Dem</u>.

1) $x \cdot O = x \cdot (O + O) = x \cdot O + x \cdot O \Rightarrow x \cdot O = O$

$O \cdot x = (O + O) \cdot x = O \cdot x + O \cdot x \Rightarrow O \cdot x = O$

2) $(-x) \cdot y + x \cdot y = (-x + x) \cdot y = O \cdot y = O \Rightarrow (-x) \cdot y = -(xy)$

$x \cdot y + x \cdot (-y) = x \cdot (y - y) = x \cdot O = O \Rightarrow x \cdot (-y) = -(xy)$

3) $(-x) \cdot (-y) = -(x \cdot (-y)) = -(-(x \cdot y)) = x \cdot y$

4) $x \cdot (y - z) = x \cdot (y + (-z)) = x \cdot y + x \cdot (-z) = x \cdot y + (-x \cdot z) = x \cdot z - y \cdot z$

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

DEF Diremos que $a, b \in A$, con $(A, *, \circ)$ anillos, son Divisores de Cero si $a \neq e_0$, $b \neq e_0$ y $a \circ b = e_0$ (con e_0 es neutro de la operación $\circ$.

OBS Si utilizamos las operaciones habituales de suma y producto (al igual que en la proposición anterior), la definición dice que las divisiones de cero son aquellas que verifican $a \neq 0$, $b \neq o$ y $a \cdot b = 0$.

DEF $(A, *, \circ)$ es un Dominio de integridad si es un Anillo conmutativo con elemento unidad y no posee divisores de cero.

DEF Sea $(A, *, \circ)$ un Anillo y SCA un subconjunto no vacío. Diremos que $(S, *, \circ)$ es un Subanillo de $(A, *, \circ)$ si

1) $(S, *)$ es un subgrupo de $(A, *)$
2) $\forall x, y \in S$ se cumple que $x \circ y \in S$.

Si además, $(A, *, \circ)$ es un Anillo con unidad, $(S, *, \circ)$ lo será si $e_0 \in S$-

Ejemplos:

$(\mathbb{Z}, +, \cdot)$ es un subanillo conmutativo con unidad de $(\mathbb{Q}, +, \cdot)$.

DEF Diremos que un subconjunto no vacío $I \subset A$, con $(A, *, \circ)$ anillo, es un Ideal de A si cumple

1) $(I, *)$ es un subgrupo de $(A, *)$

2A) $\forall x \in I$ y $\forall a \in A$ $a \circ x \in I$

2B) $\forall x \in I$ y $\forall a \in A$ $x \circ a \in I$

Si sólo verifica 1 y 2A diremos que es ideal por la izquierda y si sólo verifica 1 y 2B será ideal por la derecha.

Ejemplo:

Todos los ideales de $\mathbb{Z}$ son los conjuntos $I = (a)$ con $(a) = \{a \cdot n \,/\, n \in \mathbb{Z}\}$

PROP Sea $(A, *, \circ)$ un anillo. Todo ideal I del anillo es un subanillo.

Dem.

Inmediatamente a partir de ambas definiciones.

OBS El recíproco de la proposición anterior no es cierto.

DEF Sea $(A, *, \circ)$ un anillo y $B\subset a$ un subconjunto. Llamamos ideal engendrado por el subconjunto B al menor ideal que contiene a B.

DEF Diremos que un ideal I es principal si es un ideal engendrado por un subconjunto con un solo elemento.

DEF Un Anillo $(A, *, \circ)$ es Principal si es un dominio de integridad y todos sus ideales son principales.

DEF Sea $(A, *, \circ)$ un anillo conmutativo e I un ideal de A. Diremos que I es Ideal Maximal si $I \neq A$ y no está contenido estrictamente en un ideal propio.

DEF Sea $(A, *, \circ)$ un anillo conmutativo e I un ideal de A con $I \neq A$. Diremos que I es un ideal primo si la relación $x\circ y\in I$ implica que $x\in I \quad \circ \quad y\in I$.

7.2.2. Cuerpos.

DEF Diremos que un anillo $(K, *, \circ)$ es un Cuerpo si todo elemento no nulo de K admite inverso para la operación $\circ$. El Cuerpo es conmutativo si la operación $\circ$ es conmutativa.

También podemos prescindir de la noción de Anillo y dar como definición de Cuerpo la siguiente.

DEF Diremos que la terna $(K, *, \circ)$ es un Cuerpo si se verifica:

1) $(K, *)$ es un grupo conmutativo.

2) $(K - \{\circ\}, \circ)$ es un grupo.

3) La operación $\circ$ es distributiva respecto de $*$.

Si además $(K - \{\circ\}, \circ)$ es conmutativo, diremos que $(K, *, \circ)$ es un Cuerpo Conmutativo.

DEF Un subconjunto $K_0\subset K$ con $(K, *, \circ)$ es un subcuerpo si $(K_0, *, \circ)$ es un cuerpo.

7.2.3. Retículo.

DEF Llamaremos Retículo a la terna $(A, *, \circ)$ verificando:

1) Las dos operaciones internas son asociativas.
2) Las dos operaciones internas son conmutativas.
3) Las dos operaciones internas son idempotentes.
4) Las dos operaciones internas son absorbentes.

OBS Para que una operación interna sea idempotente debe verificar que $\forall a\in A$

$a*a = a$ ó $a\circ a = a$.

Para que $*$ y $\circ$ sean absorbentes (verifiquen la propiedad de absorción) debe cumplirse que $\forall a, b\in A$ $(a*b)\circ a = a$ y $(a\circ b)*a = a$

Ejemplo:

Dado un conjunto U, tenemos que $(P(U), \cup, \cap)$ es un retículo.

DEF La terna $(A, *, \circ)$ es un retículo distributivo cuando, además de ser retículo, ambas operaciones internas verifican la propiedad distributiva de una respecto a la otra.

DEF Llamaremos Elemento Infinito del retículo $(A, *, \circ)$ y lo representaremos por i, al elemento neutro de al operación $*$.

DEF Llamaremos Elemento Universal del retículo $(A, *, \circ)$, y lo representaremos por u, al elemento neutro de la operación $\circ$.

PROP Sea $(A, *, \circ)$ un retículo con elemento ínfimo y elemento universal. Dado $a\in A$ se verifica

1) $a\circ i = i$
2) $a*u = u$

Dem.

Como i es el elemento neutro de $*$ se verifica $\forall a\in A$ $a*i = a$
Por la propiedad de absorción

$$(i*a)\circ i = i \Rightarrow a\circ i = i$$

Como u es el elemento neutro de $\circ$ se verifica $\forall a\in A$ $a\circ u = a$
Por la propiedad de absorción

$$(u\circ a)*u = u \Rightarrow a*u = u$$

DEF Diremos que $(A, *, \circ)$ es un retículo Complementario si es un retículo con elementos ínfimo y universal y además verifica:

$$\forall a\in A \quad \exists a^c\in A \,/\, a*a^c = u \quad y \quad a\circ a^c = i$$

7.3. Estructuras Algebraicas con una operación interna y otra externa.

En este punto vamos a denotar por $\bullet$ a la operación externa, teniendo como subíndice el conjunto sobre el que está definida.

7.3.1. Módulos.

DEF Sea $(A, *, \circ)$ un anillo conmutativo con unidad y M un conjunto sobre el que hay definida una operación interna, $*_M$, y una operación externa $\bullet_A$, con dominio de operadores A. Diremos que $(M, *_M, \bullet_A)$ es un A-Módulo si verifica

1) (M, $*_M$) es un grupo conmutativo.

2) La Ley externa verifica la propiedad distributiva (por ambos lados) respecto de $*_M$, la propiedad pseudoasociativa y existe elemento unidad.

Si además, la operación externa es conmutativa, diremos que (M, $*_M$, $\bullet_A$) es un A-Módulo Conmutativo.

DEF Si (M, $*_M$, $\bullet_A$) es un A-Módulo y $S \subset M$ es no vacío, diremos que S es un submódulo de M si S, con las operaciones de M restringidas, es un A-Módulo.

7.3.2. Espacios Vectoriales.

DEF Sea (M, $*_M$, $\bullet_A$) un A-Módulo. Diremos que es un Espacio Vectorial si el dominio de operadores A tiene estructura del Cuerpo.

Una definición alternativa sin que aparezca el concepto de Módulo sería:

DEF La terna (V, $*_V$, $\bullet_K$) es un K-Espacio Vectorial si verifica:

1) (K, $*_{K)}$, $\circ$) es un cuerpo.

2) (V, $*_V$) es un grupo conmutativo.

3) La ley externa verifica la propiedad distributiva (por ambos lados) respecto de $*_V$, la propiedad pseudoasociativa y existe elemento unidad.

DEF Si (V, $*_V$, $\bullet_K$) es un K-espacio vectorial y $W \subset V$ es no vacío, diremos que W es un subespacio vectorial de V si W, con las operaciones de V restringidas, es un K-espacio vectorial.

PROP W es un Subespacio vectorial de (V, $*_{V)}$, $\bullet_K$) si y solo si verifica:

1) $\forall x,\ y \in W \Rightarrow x *_V y \in W$

2) $\forall \alpha \in K\ \ \forall x \in W \Rightarrow \alpha \bullet_K x \in W$