Tema 1: Fundamentos.

1. Nociones básicas de la Teoría de Conjuntos.

Definición. Un **conjunto** es una colección de objetos. A los objetos de un conjunto se les llama **elementos** del conjunto.

Se denominará **conjunto vacío** al conjunto que no tiene elementos y se denotará por $\emptyset$.

Normalmente, emplearemos letras mayúsculas (A, B, ...) para denotar los conjuntos y usaremos letras minúsculas (a, b, c, ...) para los elementos de un conjunto. Para indicar que un elemento a está en un conjunto A escribiremos $a \in A$, que se lee "*a pertenece a A*". En caso contrario escribiremos $a \notin A$, que se lee "*a no pertenece a A*".

Existen dos formas de definir un conjunto:

i) **Por extensión**: En este caso se indican todos elementos que forman el conjunto escritos entre los símbolos { y } y separados por ",". Por ejemplo, $A = \{1, 2, 3\}$ significa que el conjunto A está formado por los elementos 1, 2 y 3.

ii) **Por comprensión**: Se señalan la(s) propiedad(es) que caracteriza(n) los elementos del conjunto. En este caso escribiremos el conjunto de la siguiente manera: $\{x \mid p(x)\}$, donde $p(x)$ es la propiedad que debe verificar el elemento x para pertenecer al conjunto. Por ejemplo, $B = \{x \mid x \text{ es un número natural y } x \leq 3\}$ (observar que el conjunto B coincide con el conjunto A del apartado i)).

Si A y B son dos conjuntos tales que cada elemento de B pertenece a A, se dice que B está contenido en A y se escribe $B \subseteq A$ (ó $B \subset A$). Es decir,

$$B \subseteq A \qquad \Longleftrightarrow \qquad \forall b \in B, b \in A.$$

En caso contrario, esto es, si existe al menos un elemento de B que no está en A, se dice que B no está contenido en A y se expresa mediante $B \not\subseteq A$ (ó $B \not\subset A$). Esto es,

$$B \not\subseteq A \qquad \Longleftrightarrow \qquad \exists b \in B \text{ tal que } b \notin A.$$

Si B es un conjunto tal que $B \subseteq A$, se dice que B es un **subconjunto** de A.

Si $B \subseteq A$ y $B \neq A$, escribiremos $B \underset{\neq}{\subset} A$, cuando queramos destacar que $B \neq A$ y se dirá que B es un **subconjunto propio** de A. Es evidente que

$$B \underset{\neq}{\subset} A \Longleftrightarrow \forall b \in B, b \in A \text{ y } \exists a \in A \text{ tal que } a \notin B.$$

Ejemplos.

1. $\emptyset$, que representa el **conjunto vacío**, está contenido en cualquier conjunto A.
2. Si A es un conjunto, entonces $A \subseteq A$.
3. Sean $A = \{1, -1, -3, 5\}$ y $\mathbb{Z} = \{x \mid x \text{ es un número entero}\}$. Entonces, $A \underset{\neq}{\subset} \mathbb{Z}$.
4. Sean $A = \{1, 2, 3, -\sqrt{2}, \sqrt{5}\}$ y $B = \mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z} \text{ y } b \neq 0\}$. Entonces, $A \not\subset B$.
5. Si $\mathbb{N}$ denota el conjunto de los números naturales y $\mathbb{Q}$ el conjunto de los números racionales, se tiene $\mathbb{N} \underset{\neq}{\subset} \mathbb{Q}$.
6. Si $A = \{n \in \mathbb{N} | n \text{ es primo}\}$ denota el conjunto de los números primos y $\mathbb{Z}$ el conjunto de los números enteros, se tiene $A \underset{\neq}{\subset} \mathbb{Z}$.

Definición. Sea A un conjunto. Se llama **conjunto de las partes de** A ó **booleano** de A, y se denota por $\mathfrak{P}(A)$, al conjunto formado por todos los subconjuntos de A (incluyendo el conjunto vacío y el propio A), esto es,

$$\mathfrak{P}(A) = \{B | B \subseteq A\}.$$

Definición. Sea A un conjunto. Se llama **cardinal de** A al número de elementos de A. Normalmente, se suele denotar el cardinal de A por $|A|$ ó por $\#A$.

Definición. Un conjunto A se dice que es **finito** si tiene un número finito de elementos, esto si, si $|A| < \infty$.

Para denotar una **familia de conjuntos** indicada por I escribiremos $\{A_i \mid i \in I\}$ o $\{A_i\}_{i \in I}$ donde I es un conjunto de índices no vacío.

Definición. Sean A y B dos conjuntos. La **intersección** de los conjuntos A y B es el conjunto denotado por $A \cap B$ formado por los elementos que pertenecen simultáneamente a A y B, esto es,

$$A \cap B = \{x \mid x \in A \ \wedge x \in B\}.$$

Cuando $A \cap B = \emptyset$, se suele decir que los conjuntos A y B son **disjuntos**.

Si $\{A_i\}_{i \in I}$ es una familia de conjuntos, la intersección de ellos es un conjunto denotado por $\bigcap_{i \in I} A_i$ y cuyos elementos son:

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \forall i \in I\}.$$

Diremos que la familia $\{A_i\}_{i \in I}$ es **disjunta** cuando se verifique la siguiente condición:

$$\forall i, j \in I, \ i \neq j, \quad A_i \cap A_j = \emptyset.$$

Definición. Sean A y B dos conjuntos. La **unión** de los conjuntos A y B, denotado por $A \cup B$, es el conjunto formado por los elementos que pertenecen a A ó a B, esto es,

$$A \cup B = \{x \mid x \in A \ \vee x \in B\}.$$

Si A y B son disjuntos, se dirá que la unión de A y B es disjunta y se denotará por $A \dot{\cup} B$.

Si $\{A_i\}_{i \in I}$ es una familia de conjuntos, la unión de ellos se denota por $\bigcup_{i \in I} A_i$ y tiene por elementos:

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I \text{ tal que } x \in A_i\}.$$

Al igual que antes, si la familia $\{A_i\}_{i \in I}$ es disjunta, diremos que la unión de ella es disjunta y lo denotaremos por $\dot{\bigcup}_{i \in I} A_i$.

Ejemplos.

1. Consideremos la familia $\{A_n\}_{n \in \mathbb{N}}$, donde $A_n = [n, n+1)$ para cada $n \in \mathbb{N}$. Entonces,

$$\bigcup_{n \in \mathbb{N}} = [1, +\infty).$$

Además, la familia anterior es disjunta ya que $A_n \cap A_m = \emptyset$ si $n \neq m$.

2. Consideremos la familia $\{A_n\}_{n\in\mathbb{N}}$, donde $A_n = (n, n+1)$ para cada $n \in \mathbb{N}$. Entonces,

$$\bigcup_{n\in\mathbb{N}} = (1, +\infty) - \mathbb{N}.$$

Además, la familia anterior es disjunta ya que $A_n \cap A_m = \emptyset$ si $n \neq m$.

3. Consideremos la familia $\{A_n\}_{n\in\mathbb{N}}$, donde $A_n = [n, n+1]$ para cada $n \in \mathbb{N}$. Entonces,

$$\bigcup_{n\in\mathbb{N}} = [1, +\infty).$$

Además, la familia anterior no es disjunta ya que para cada $n \in \mathbb{N}$, $A_n \cap A_{n+1} = \{n+1\}$.

Definición. Sean A y B dos conjuntos. Se llama **diferencia** de los conjuntos A y B, y se denota por $A - B$, al conjunto formado por los elementos de A que no pertenecen a B, esto es,

$$A - B = \{x \in A \mid x \notin B\}.$$

Definición. Sean A y B dos conjuntos. Se llama **producto cartesiano** de los conjuntos A y B, y se denota $A \times B$, al conjunto formado por todos los pares (a, b) con $a \in A$ y $b \in B$, es decir,

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

En relación al producto cartesiano destacamos:

1.- El par (a, b) es un par ordenado, esto es, siempre se debe verificarse que $a \in A$ y $b \in B$.

2.- Si $(a_1, b_1), (a_2, b_2) \in A \times B$, entonces $(a_1, b_1) = (a_2, b_2)$ si y sólo si $a_1 = a_2$ y $b_1 = b_2$.

3.- Si $|A| = n$ y $|B| = m$, entonces $|A \times B| = n \times m$.

4.- Si $A \neq B$, entonces $A \times B \neq B \times A$.

Del mismo modo que hemos definido el producto cartesiano de dos conjuntos, podemos definir el producto cartesiano de k conjuntos $A_1, A_2, \ldots A_k$ de la manera siguiente:

$$A_1 \times A_2 \times \ldots \times A_k = \{(a_1, a_2, \ldots, a_k) \mid \forall i \in \{1, 2, \ldots k\}, \ a_i \in A_i\}.$$

Definición. Sean A un conjunto y $\{A_i\}_{i\in I}$ una familia disjunta de subconjuntos de A. Diremos que $\{A_i\}_{i\in I}$ es una **partición** de A si $A = \dot{\bigcup}_{i\in I} A_i$.

Ejemplo.

1. Si $A = \{1, 2, 3, 4\}$, entonces $\{\{1\}, \{2, 3\}, \{4\}\}$ es una partición de A.

2. Aplicaciones.

Definición. Sean A y B dos conjuntos. Una **aplicación** ó **función** de A en B es una regla que a cada $a \in A$ le hace corresponder un único elemento de B.

Normalmente, se suele denotar una aplicación de A en B por $f : A \to B$. En tal caso, a A se le llama **dominio** de la aplicación y a B **codominio** ó **conjunto final**.

Si $a \in A$ y $f : A \to B$ es una aplicación, se denota por $f(a)$ el elemento de B que le hace corresponder la aplicación f al elemento a. A $f(a)$ se le llama **imagen de** a por la aplicación f.

Ejemplos.

1. **Aplicación identidad**: Si A es un conjunto, se define la aplicación identidad mediante:
$$\begin{array}{rccc} 1_A : & A & \longrightarrow & A \\ & a & \to & 1_A(a) = a. \end{array}$$
A veces denotaremos la aplicación identidad por id_A.

2. **Aplicación inclusión**. Si $A \subseteq B$, se define la aplicación inclusión de la manera que sigue:
$$\begin{array}{rccc} i_A : & A & \longrightarrow & B \\ & a & \to & i_A(a) = a. \end{array}$$
Como se observa, si $A = B$, entonces la aplicación inclusión coincide con la aplicación identidad.

3. **Aplicación constante**. Si A y B son dos conjuntos y $b_0 \in B$ un elemento fijo de B, entonces:
$$\begin{array}{rccc} c_{b_0} : & A & \longrightarrow & B \\ & a & \to & c_{b_0}(a) = b_0. \end{array}$$

4. Sean $S \subseteq A$ y $f : A \longrightarrow B$ una aplicación. Se llama **restricción** de f a S a la siguiente aplicación:
$$\begin{array}{rccc} f_{|S} : & S & \longrightarrow & B \\ & s & \to & f_{|S}(s) = f(s). \end{array}$$

5. Sean $S \subseteq A$ y $f : S \longrightarrow B$ una aplicación. Se llama **extensión** de f a A a la cualquier aplicación $g : A \longrightarrow B$ tal que $g_{|S} = f$.

6. Sean $A_1, ..., A_k$ conjuntos no vacíos. Consideremos su producto cartesiano $A_1 \times ... \times A_k$, que será también no vacío. Para cada $i \in \{1, 2, \ldots, k\}$, la **proyección i-ésima** es la aplicación denotada por p_i que está definida de la manera siguiente:

$$\begin{array}{rccc} p_i: & A_1 \times ... \times A_k & \longrightarrow & A_i, \\ & (a_1, ..., a_k) & \to & p_i((a_1, ..., a_k)) = a_i. \end{array}$$

Definición. Sean $f : A \to B$ una aplicación y $S \subseteq A$. Entonces, la **imagen del subconjunto** S, que denotaremos por $f(S)$, es el subconjunto de B cuyos elementos son imágenes de elementos de S, esto es,

$$f(S) = \{f(a) | \ \ a \in S\}.$$

Observar que si $f : A \to B$ una aplicación, se puede tomar como subconjunto S de A el propio A. En tal caso, $f(A) = \{f(a) \mid a \in A\}$ recibe el nombre de **imagen** de A por la aplicación f. A veces, también se suele denotar la imagen de A por la aplicación f mediante Imf.

Si $f : A \to B$ es una aplicación de A en B y $b \in B$, entonces se llama **antiimagen** de b a un elemento $a \in A$ tal que $f(a) = b$. De la definición de aplicación, se deduce que si $f : A \to B$ es una aplicación, entonces cada elemento de A tiene una única imagen, pero no todo elemento de B tiene que tener antiimagen e incluso un mismo elemento de B puede tener más de una antiimagen. Por ello, en lo que sigue,

$$f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}.$$

A veces, para simplificar notación, escribiremos $f^{-1}(b)$ en vez de $f^{-1}(\{b\})$.

Del mismo modo, si $f : A \to B$ es una aplicación y $T \subseteq B$, el subconjunto de A formado por las antiimagenes de los elementos de T se denota por

$$f^{-1}(T) = \{a \in A | f(a) \in T\}$$

y se llama **imagen inversa del subconjunto** T. Obviamente, puede suceder que $f^{-1}(T) = \emptyset$.

Ejemplos.

1. Sea $f : \mathbb{R} \to \mathbb{R}$ la aplicación definida por $f(x) = x^2$. Si tomamos como subconjunto de $\mathbb{R}$, $S = \{0, 1, -1, 2\} \subseteq \mathbb{R}$, entonces $f(S) = \{0, 1, 4\}$. Fácilmente se comprueba que la imagen inversa de $T = \{x \in \mathbb{R} \mid -2 \leq x \leq -1\}$ es vacía, esto es, $f^{-1}(T) = \emptyset$. En cambio, si se elige $T = \{0, 1, -1, 2\} \subseteq \mathbb{R}$, entonces $f^{-1}(T) = \{0, 1, -1, \sqrt{2}, -\sqrt{2}\}$.

2. En el ejemplo anterior, $Imf = \{f(a) \ \mid \ a \in A\} = \{a^2 \ \mid \ a \in \mathbb{R}\} = \mathbb{R}^+ = [0, +\infty)$.

Definición. Sean $f : A \to B$ y $g : C \to D$ dos aplicaciones. Se dice que f y g son **iguales** cuando $A = C$, $B = D$ y $f(a) = g(a) \ \ \forall a \in A$.

Definición. Una aplicación $f : A \longrightarrow B$ se dice que es **inyectiva** si dados dos elementos cualesquiera distintos de A sus imágenes son diferentes. Es decir,

$$\forall a, a' \in A, \ a \neq a' \Rightarrow f(a) \neq f(a').$$

Equivalentemente, podemos expresar la condición de ser inyectiva mediante

$$\forall a, a' \in A, \ f(a) = f(a') \Rightarrow a = a'.$$

Definición. Una aplicación $f : A \longrightarrow B$ es **suprayectiva** si $f(A) = B$. Esto es,

$$\forall b \in B \ \ \exists a \in A \ \mid \ f(a) = b.$$

Definición. Una aplicación $f : A \longrightarrow B$ se llama **biyectiva** si es suprayectiva e inyectiva. Esto es,

$$\forall b \in B \ \ \exists! a \in A \ \mid \ f(a) = b.$$

Ejemplos.

1. Sea
$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & [0, +\infty) \\ & x & \to & x^2. \end{array}$$
Claramente, la aplicación anterior es suprayectiva y no es inyectiva.

2. Sea
$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \to & 2n. \end{array}$$
La aplicación anterior es inyectiva pero no suprayectiva.

3. Para cualquier conjunto A la aplicación identidad 1_A es biyectiva.

Definición. Sean $f : A \longrightarrow B$ y $g : C \longrightarrow D$ dos aplicaciones tales que $B \subseteq C$. Llamamos **composición de f y g**, a la aplicación denotada por $g \circ f$ y definida mediante

$$\begin{array}{rccc} g \circ f: & A & \longrightarrow & D \\ & a & \to & g(f(a)) \end{array}$$

Esto es, $(g \circ f)(a) = g(f(a)), \ \ \forall a \in A$.

Ejemplo.

1. Sean $f : \mathbb{R} \longrightarrow \mathbb{R}$ y $g : \mathbb{R} \longrightarrow \mathbb{R}$ dos aplicaciones definidas por $f(x) = x^2, \quad \forall x \in \mathbb{R}$ y $g(x) = x + 1, \quad \forall x \in \mathbb{R}$. Entonces, $(g \circ f)(x) = x^2 + 1, \quad \forall x \in \mathbb{R}$ y $(f \circ g)(x) = (x + 1)^2, \quad \forall x \in \mathbb{R}$.

Como se puede observar en el ejemplo anterior, en general, $f \circ g$ no coincide con $g \circ f$.

Definición. Sea $f : A \longrightarrow B$ una aplicación biyectiva. Se llama **función inversa de** f, y se denota por f^{-1}, a la aplicación $f^{-1} : B \longrightarrow A$ definida por

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

Ejemplo.

1. Sea
$$\begin{array}{rccc} f: & [0,+\infty) & \longrightarrow & [0,+\infty) \\ & x & \to & x^2 \end{array}$$
La función f es biyectiva y su función inversa es:
$$\begin{array}{rccc} f^{-1}: & [0,+\infty) & \longrightarrow & [0,+\infty) \\ & x & \to & \sqrt{x} \end{array}$$

A pesar de utilizar la misma notación, no se debe confundir la antiimagen de un elemento b (que es un subconjunto de A cuyos elementos tienen por imagen a b) con la imagen del elemento b por la aplicación f^{-1}. La primera se puede calcular simepre y la segunda sólo si f es biyectiva. Es fácil demostrar que

Proposición 2.1. *Sea $f : A \longrightarrow B$ una aplicación biyectiva. Entonces,*

i) $f \circ f^{-1} = 1_B$

ii) $f^{-1} \circ f = 1_A$

iii) f^{-1} *es biyectiva y* $(f^{-1})^{-1} = f$.

Proposición 2.2. *Sea $f : A \longrightarrow B$ una aplicación biyectiva y sea $g : B \longrightarrow A$. Entonces son equivalentes:*

(i) $g = f^{-1}$.

(ii) $f \circ g = 1_B$ *y* $g \circ f = 1_A$.

3. Relaciones de equivalencia.

Definición. Sea A un conjunto. Una **relación binaria** $\sim$ definida sobre A es una regla que nos indica si dados dos elementos a y b pertenecientes a A están o no relacionados.

Si $\sim$ es una relación definida sobre A y $a, b \in A$ están relacionados, entonces escribiremos $a \sim b$. En caso contrario, aparecerá $a \not\sim b$.

Definición. Sea A un conjunto. Una **relación de equivalencia** definida en A es una relación binaria de A que verifica las tres propiedades siguientes:

i) Reflexiva: $a \sim a \quad \forall a \in A$.

ii) Simétrica: $a \sim b \Leftrightarrow b \sim a \quad a, b \in A$.

iii) Transitiva: $a \sim b \;\; y \;\; b \sim c \Rightarrow a \sim c \quad a, b, c \in A$.

Ejemplos.

1. En un conjunto A definimos la relación:

$$a \sim b \quad \Leftrightarrow a = b.$$

Fácilmente se comprueba que es de equivalencia.

2. En $A = \mathbb{Z}$ se define la siguiente relación:

$$a \sim b \Leftrightarrow a - b \text{ es un número par.}$$

Claramente, $\sim$ es una relación de equivalencia.

3. En $A = \mathbb{Z}$ se define la siguiente relación:

$$a \sim b \Leftrightarrow a < b.$$

La relación binaria anterior no es de equivalencia porque no se cumple la propiedad simétrica ni la propiedad reflexiva.

4. En $A = \mathbb{Z}$ se define la siguiente relación:

$$a \sim b \Leftrightarrow a \geq b.$$

La relación binaria anterior no es de equivalencia porque no se cumple la propiedad simétrica.

Definición. Sean A un conjunto y $\sim$ una relación de equivalencia sobre A. Para cada $a \in A$ se llama **clase de equivalencia de** a, y se denotará por $\overline{a}$ o por $[a]$, al siguiente conjunto:

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

Como se observa, $\overline{a}$ es un subconjunto no vacío de A ya que $a \in \overline{a}$.

Es fácil demostrar que:

Teorema 3.1. *Sea A un conjunto, $a, b \in A$ y $\sim$ una relación de equivalencia sobre A. Entonces, la intersección de dos clases de equivalencia es no vacía si y sólo si ambas clases coinciden, esto es,*

$$[a] \cap [b] \neq \emptyset \Longleftrightarrow [a] = [b].$$

Definición. Sea A un conjunto y $\sim$ una relación de equivalencia en A. Un **sistema completo de representantes de la relación** $\sim$ es un subconjunto $X \subseteq A$ tal que cualquier elemento de A está relacionado con exactamente un elemento de X.

Dado un conjunto A y $\sim$ una relación de equivalencia sobre A, al conjunto $A/\sim$ formado por las clases de equivalencia se le llama **conjunto cociente**, esto es

$$A/\sim = \overline{A} = \{\overline{a} \mid a \in A\}.$$

Claramente, al unir todas las clases de equivalencia se obtiene A. Por consiguiente, de esta observación y del teorema anterior deducimos:

Teorema 3.2. *Sea A un conjunto y $\sim$ una relación de equivalencia definida en A. Entonces, el conjunto cociente $\overline{A}$ es una partición de A.*

Ejemplos.

1. Si definimos en una conjunto A la relación $\sim$ mediante $\forall a, b \in A$, $a \sim b$ si y sólo si $a = b$, se verifica que

   $$\overline{a} = \{b \in A \mid a \sim b\} = \{b \in A \mid a = b\} = \{a\}$$

   y que

   $$A/\sim = \overline{A} = \{\{a\} \mid a \in A\} = A.$$

2. En $A = \mathbb{Z}$ definimos la relación $\forall a, b \in \mathbb{Z}$, $a \sim b$ si y sólo si $a - b$ es un número par. Entonces, si a es un número par,

   $$\overline{a} = \{x \in \mathbb{Z} \mid a - x \text{ es par}\} = \{x \in \mathbb{Z} \mid x \text{ es par}\} = \overline{2} = \overline{4} = \dots.$$

En cambio, si $b \in \mathbb{Z}$ es impar,

$$\overline{b} = \{x \in \mathbb{Z} \mid b - x \text{ es par}\} = \{x \in \mathbb{Z} \mid x \text{ es impar}\} = \overline{1} = \overline{3} = ...$$

Por consiguiente, el conjunto cociente sólo tiene dos clases de equivalencia distintas y viene dado por

$$\overline{\mathbb{Z}} = \{\overline{1}, \overline{2}\}.$$

Un sistema completo de representantes de esta relación estará formado por dos números enteros tales que uno es par y el otro es impar. Por ejemplo, son sistemas completos de representantes los conjuntos $\{1, 2\}$, $\{0, -7\}$, ó $\{-4, -57\}$ pero no es sistema completo de representantes los conjuntos $\{1, -5\}$, $\{-4, 2\}$, $\{0, 1, 2\}$ ó $\{1\}$.

3. Sea $A = \mathbb{R}^2 - \{(0, 0)\}$. Definimos en A la siguiente relación:

   $\forall (x_1, y_1), (x_2, y_2) \in A, \ \ (x_1, y_1) \sim (x_2, y_2) \Longleftrightarrow \exists \lambda \in \mathbb{R} - \{0\} \ \mid \ x_1 = \lambda x_2 \ \text{ y } \ y_1 = \lambda y_2$

   Es inmediato comprobar que la relación anterior es de equivalencia. Además, si $(x_1, y_1) \in A$, entonces

$$\begin{aligned} \overline{(x_1, y_1)} &= \{(x_2, y_2) \ \mid \ (x_1, y_1) \sim (x_2, y_2)\} \\ &= \{(x_2, y_2) \ \mid \ \exists \lambda \in \mathbb{R} - \{0\} \ \text{ tal que } \ x_2 = \lambda x_1 \ \ \wedge \ \ y_2 = \lambda y_1\} \\ &= \{(\lambda x_1, \lambda y_1) \ \mid \ \lambda \in \mathbb{R} - \{0\}\}. \end{aligned}$$

   Por ejemplo, $\overline{(1, 0)} = \{(\lambda, 0) \ \mid \ \lambda \in \mathbb{R} - \{0\}\}$. Esto es, la clase de equivalencia del elemento (x_1, y_1) es el conjunto de puntos de A que se encuentran sobre la recta que pasa por (x_1, y_1) y el origen $(0, 0)$. Obviamente, el $(0, 0)$ no está en la clase de equivalencia del elemento (x_1, y_1) porque no pertenece al conjunto A. Por consiguiente, el conjunto cociente estará definido por

$$= \{\overline{(x, y)} | (x, y) \in A\},$$

   esto es el conjunto formado por las rectas que pasan por el origen (quitando el origen). A este conjunto cociente se suele denotar por $hbox\mathbf{P}^1(\mathbb{R})$ y se le llama el **espacio proyectivo de dimensión 1**.

4. Leyes de composición internas.

Definición. Sea A un conjunto no vacío. Una **ley de composición interna sobre A,** o una **operación (interna)** de A es una aplicación:

$$\begin{array}{rccc} f: & A \times A & \longrightarrow & A \\ & (a, b) & \to & f(a, b). \end{array}$$

Nota: Generalemente, en lugar de escribir $f(a, b)$, escribiremos el resultado de la operación del siguiente modo: $a * b, a \ o \ b, a \cdot b, ...$ y a la operación la denominaremos por el símbolo utilizado: $*, o, \cdot, ...$

Definición. Un **sistema algebraico** es un conjunto A no vacío con una o varias operaciones internas sobre él.

Ejemplos.

1. Sea $A = \{0, 1\}$. En A podemos definir dos operaciones: $*$ y $\circ$ de la manera siguiente:

$$\begin{array}{ll} 0 * 0 = 0 & 0 \circ 0 = 0 \\ 0 * 1 = 0 & 0 \circ 1 = 1 \\ 1 * 0 = 0 & 1 \circ 0 = 1 \\ 1 * 1 = 1 & 1 \circ 1 = 0 \end{array}$$

   Como se observa, en un conjunto se pueden definir más de una operación.

2. Sea $A = \mathbb{Z}$. Definimos

$$a * b = \sqrt{a \cdot b}, \forall a, b \in \mathbb{Z},$$

   no es una operación de $\mathbb{Z}$ porque $\sqrt{a \cdot b}$ no pertenece siempre a $\mathbb{Z}$. En cambio,

$$a * b = -2, \forall a, b \in \mathbb{Z},$$

   sí es una operación de $\mathbb{Z}$.

3. Sea $A = \mathbb{N}$. Entonces, $a * b = a^b, \forall a, b \in A$, es una operación en $\mathbb{N}$ pero si tomamos $A = \mathbb{Z}$, no lo es.

4. Sea $\mathbb{F} = \{f : A \to B \mid f \text{ aplicación}\}$.

   a) $f+g$, donde $(f+g)(x) = f(x)+g(x)$, $\forall x \in \mathbb{R}$, $\forall f, g \in \mathbb{F}$, suma usual de funciones, es una operación en $\mathbb{F}$.

   b) $f \cdot g$, donde $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in \mathbb{R}$, $\forall f, g \in \mathbb{F}$, producto usual de funciones, es una operación en $\mathbb{F}$.

   c) Si $A = B$, entonces $f \circ g$, donde $(f \circ g)(x) = f(g(x))$, $\forall x \in \mathbb{R}$, $\forall f, g \in \mathbb{F}$, composición usual de funciones, es una operación en $\mathbb{F}$.

5. Sea A un conjunto y $\mathfrak{P}(A)$ su booleano. Entonces, la unión, intersección y diferencia de dos elementos de $\mathfrak{P}(A)$ son operaciones de $\mathfrak{P}(A)$.

Sea $(A, *)$ un sistema algebraico. Entonces, $*$ puede verificar las siguientes propiedades:

(i) **Asociativa**: $\forall a, b, c \in A$, $(a * b) * c = a * (b * c)$.

(ii) **Conmutativa**: $\forall a, b \in A$, $a * b = b * a$.

(iii) **Existencia de elemento neutro o identidad**: $\exists e \in A$ tal que $\forall a \in A$, $a * e = a = e * a$.

(iv) **Existencia de elemento opuesto o inverso**: $\forall a \in A$, $\exists a^{'} \in A$, tal que $a * a^{'} = e = a^{'} * a$, donde e es el elemento neutro de $*$.

Normalmente, se suele denotar el inverso de a por a^{-1}, si la operación es denotada por $\cdot$ y por $-a$, si la operación es denotada por $+$. También se suele denotar por 1 el elemento neutro, si es que hay, cuando la operación se denota por $\cdot$ y por 0, si la operación es denotada por $+$.

Definición. Sean $(A, *)$ un sistema algebraico y $a \in A$. Se dice que a es **inversible** si a tiene elemento inverso.

Ejemplos.

1) En $(\mathbb{R}, +)$, donde $+$ denota la suma de números reales, se verifican las propiedades asociativa y conmutativa, el número 0 es el elemento neutro y cada $x \in \mathbb{R}$ tiene inverso: $-x$.

2) En $(\mathbb{R}, .)$, donde $.$ denota el producto de números reales, se verifican las propiedades asociativa y conmutativa, el número 1 es el elemento neutro y cada $x \in \mathbb{R} - \{0\}$ tiene inverso: $\frac{1}{x}$. Pero $\cdot$ no verifica la propiedad de "existencia de elemento inverso" porque el 0 no tiene inverso para esta operación.

Observamos que si $*$ una operación asociativa en A, entonces para $a_1, ..., a_n \in A$ arbitrarios todas las expresiones que resultan de intercalar paréntesis en $a_1 * ... * a_n$ dan el mismo valor. Esto es, si $*$ es asociativa podemos intercalar paréntesis donde queramos sin que se altere el resultado. Por este motivo, denotaremos al resultado de estas expresiones por $a_1 * ... * a_n$.

Es fácil demostrar

Teorema 4.1. *Sea $(A, *)$ un sistema algebraico. Si existe un elemento neutro, entonces éste es único.*

Teorema 4.2. *Sea $(A, *)$ un sistema algebraico con elemento neutro e. Si $*$ es asociativa y $a \in A$ es inversible, entonces el elemento inverso de a es único.*

Destacamos que el resultado anterior deja de ser cierto si $*$ no es asociativa. Por ejemplo, si consideremos la siguiente operación en $\mathbb{R}$:

$$x * y = x^2y^2 + x + y \quad \forall x, y \in \mathbb{R},$$

resulta que $*$ es una operación conmutativa con elemento neutro el 0. Si tomamos ahora el elemento $x = -1$, se sigue que $x' = \frac{-1 \pm \sqrt{1+4}}{2} = \frac{-1 \pm \sqrt{5}}{2} \in \mathbb{R}$ son elementos inversos de $x = -1$.

5. Estructuras algebraicas básicas.

Dependiendo de las propiedades que verifique una operación interna, al sistema algebraico $(A, *)$ le daremos distintos nombres:

Definición. Sea $(A, *)$ un sistema algebraico. Se dice que $(A, *)$ es un **semigrupo** si $*$ verifica la propiedad asociativa.

Un semigrupo $(A, *)$ se dice que es **conmutativo**, si $*$ es conmutativa.

Un semigrupo $(A, *)$ se dice que es **monoide** si $*$ tiene elemento neutro.

Un monoide $(A, *)$ se dice que es un **grupo**, si todo elemento de A es inversible, esto es si $*$ verifica la existencia de elemento inverso.

Un grupo $(A, *)$ se dice que es **abeliano**, si $*$ es conmutativa.

Ejemplos.

1. $(\mathbb{Z}, +)$ y $(\mathbb{Q}, +)$ son grupos abelianos.

2. $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ y $(\mathbb{R}, \cdot)$ son monoides pero no grupos ya que no todo elemento de $\mathbb{Z}$, $\mathbb{Q}$ ó $\mathbb{R}$ tiene inverso en $\mathbb{Z}$, $\mathbb{Q}$ ó $\mathbb{R}$, respectivamente.

3. Sea $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ el conjunto formado por las matrices de orden 2×2 con entradas en $\mathbb{R}$, esto es,
$$Mat_2(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \;\mid\; a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{R} \right\}$$
En este conjunto definimos las dos operaciones siguientes: $+$ y $\cdot$.
$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix},$$
$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}.$$
Es fácil probar que $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), +)$ es un grupo abeliano y que $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), \cdot)$ es un monoide. De forma análoga se pueden definir operaciones $+$ y $\cdot$ en $\mathrm{Mat}_{n\times n}$ conjunto formado por las matrices de orden n por n.

Definición. Sea $(R, +, \cdot)$ un sistema algebraico. Se dice que $(R, +, \cdot)$ es un **anillo** si se verifican las siguientes condiciones:

i) $(R, +)$ es un grupo abeliano.

ii) $(R, \cdot)$ es un semigrupo.

iii) Propiedades distributivas:

$$\begin{array}{l} x \cdot (y+z) = x \cdot y + x \cdot z \quad \forall x, y, z \in R \\ (y+z) \cdot x = y \cdot x + z \cdot x \quad \forall x, y, z \in R \end{array}.$$

Definición. Sea $(R, +, \cdot)$ un anillo. Se dice que es **conmutativo** cuando $\cdot$ es conmutativa.

Definición. Sea $(R, +, \cdot)$ un anillo. Se dice que es un **anillo con identidad** ó **unitario**, si $\cdot$ posee elemento neutro. Al elemento neutro para $\cdot$ se le llama **elemento identidad**.

Ejemplos.

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son anillos unitarios conmutativos.
2. $(\mathbb{N}, +, \cdot)$ no es un anillo porque, $(\mathbb{N}, +)$ no es un grupo.
3. Sea $R = \{2n \mid n \in \mathbb{Z}\}$, con las operaciones suma y producto usuales. Entonces, $(R, +, \cdot)$ es un anillo conmutativo.
4. $(\mathrm{Mat}_{n\times n}(\mathbb{R}), +, \cdot)$ es un anillo unitario.

Definición. Sea $(R, +, \cdot)$ un sistema algebraico. Se dice que $(R, +, \cdot)$ es un **cuerpo** si se verifican las siguientes propiedades:

i) $(R, +, \cdot)$ es un anillo conmutativo y unitario.

ii) Todos los elementos de $R - \{0\}$ son inversibles para $\cdot$.

Ejemplos.

1. $(\mathbb{Z}, +, .)$ no es un cuerpo porque no todos los elementos de $\mathbb{Z} - \{0\}$ son inversibles.
2. $(\mathbb{R}, +, .)$ es un cuerpo.
3. $(Mat_{n\times n}(\mathbb{R}), +, .)$ no es un cuerpo ya que la operación $\cdot$ no es conmutativa y además no todos los elementos de $Mat_{n\times n}(\mathbb{R}) - \{0\}$ tienen inverso.

6. El anillo de polinomios $K[x]$.

Dado un cuerpo K, se llama **polinomio en la indeterminada x con coeficientes en el cuerpo** K a $p(x) = \sum_{i=0}^{m} a_i x^i$, siendo $a_i \in K, i = 0, \ldots, m, m \in \mathbb{N} \cup \{0\}$.

Por convenio, $x^0 = 1$ y si $a_i = 0$, entonces $a_i x^i = 0$. Esto nos permite denotar al polinomio $p(x) = \sum_{i=0}^{m} a_i x^i = a_m x^m + \ldots + a_0$ por $p(x) = \sum a_i x^i$, entendiendo que $a_i = 0$ si $i > m$.

Dos polinomios $p(x) = \sum a_i x^i$ y $q(x) = \sum b_i x^i$ son iguales si $a_i = b_i$, para todo i.

Definición. Sea $p(x) = \sum a_i x^i \neq 0$ un polinomio en x con coeficientes en el cuerpo K. Se llama **grado del polinomio** $p(x)$ y de denota por deg(p), al mayor exponente m al que aparece elevado la varible x, siendo $a_m \neq 0$, esto es,

$$\deg(\mathrm{p}) = \max\{\mathrm{i} \in \mathbb{N} \cup \{0\} \mid \mathrm{a_i} \neq 0\}.$$

Si $p(x) = 0$, entonces el grado de p es $-\infty$.

Obviamente, si $p(x) = \sum a_i x^i \neq 0$ es un polinomio de grado m, entonces $a_j = 0$, si $j > m$.

Definición. Sea $p(x) = \sum a_i x^i$ un polinomio de grado m. Se llama **coeficiente director** de $p(x)$ al coeficiente a_m. Si el coeficiente director de $p(x)$ es 1, se dice que $p(x)$ es un **polinomio mónico**.

El conjunto de todos los polinomios en x con coeficientes en K se denota por:

$$K[x] = \{\sum_{i=0}^{m} a_i x^i \mid a_i \in K, i = 0, \ldots, m, m \in \mathbb{N} \cup \{0\}\},$$

En $K[x]$ se definen dos operaciones: la suma y el producto de polinomios.

Definición. Sean $p(x) = \sum a_i x^i$ y $q(x) = \sum b_i x^i$ dos polinomios de $K[x]$. Se llama **suma de los polinomios** $p(x)$ **y** $q(x)$, y se denota por $p(x) + q(x)$ al polinomio

$$p(x) + q(x) = \sum (a_i + b_i) x^i.$$

Es fácil ver que $(K[x], +)$ tiene estructura de grupo abeliano siendo 0 el elemento neutro del mismo y dado $p(x) = \sum a_i x^i$, su elemento opuesto es $-p(x) = \sum (-a_i) x^i$.

Definición. Sean $p(x) = \sum a_i x^i$ y $q(x) = \sum b_i x^i$ dos polinomios de $K[x]$. Se llama **producto de los polinomios** $p(x)$ **y** $q(x)$, y se denota por $p(x) \cdot q(x)$ al polinomio

$$p(x) \cdot q(x) = \sum c_i x^i,$$

donde $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, para todo i.

Se puede demostrar que $(K[x], \cdot)$ es un semigrupo conmutativo con elemento identidad, siendo éste 1. Además, $(K[x], +, \cdot)$ tiene estructura de anillo conmutativo con elemento identidad, que recibe el nombre de **anillo de los polinomios con coeficientes en** K **en la indeterminada** x.

Por otro lado, sabemos que dados $p(x), q(x) \in K[x]$, siendo $q(x) \neq 0$, existen unos únicos polinomios $c(x)$ y $r(x)$ tales que $p(x) = q(x)c(x) + r(x)$ y $deg(r) < deg(q)$. A $r(x)$ se le llama **resto de la división de** $p(x)$ **entre** $q(x)$ y a $c(x)$ **cociente de la división de** $p(x)$ **entre** $q(x)$.

Definición. Sean $p(x), q(x) \in K[x]$, siendo $q(x) \neq 0$. Se dice que $q(x)$ divide a $p(x)$ si $r(x) = 0$, siendo $r(x)$ el resto de la división de $p(x)$ entre $q(x)$.

Si $r(x) \neq 0$, entonces se dice que $q(x)$ no divide a $p(x)$.

Por ltimo, otro concepto que utilizaremos es el de raíz de un polinomio. Si $p(x) \in K[x]$ y $\alpha \in K$, entonces se dice que α es una **raíz** de $p(x)$ de multiplicidad m si $(x-\alpha)^m$ divide a $p(x)$ y $(x-\alpha)^{m+1}$ no divide a $p(x)$.

Lo anterior equivale a decir que $p(x) = (x-\alpha)^m q(x)$, siendo $q(\alpha) \neq 0_K$.

Se puede demostrar que

Proposición 6.1. *Sea $p(x) \in K[x]$ un polinomio de grado n. Entonces, $p(x)$ tiene a lo más n raíces en K.*

En los ejemplos utilizaremos frecuentemente el cuerpo $K = \mathbb{Q}$, esto es, trabajaremos con los polinomios en la indeterminada x con coeficientes racionales. Para stos, existe una forma sencilla de localizar sus raíces racionales, basandonos en el siguiente resultado que busca las posibles raíces racionales de un polinomio con coeficientes enteros:

Proposición 6.2. *Sea $p(x) = \sum a_i x^i \in \mathbb{Z}[x]$ un polinomio de grado m. Entonces, las raíces racionales de $p(x)$ son de la forma a/b, con a, b primos entre sí, a divisor de a_0 y b divisor de a_m.*

Obviamente, la condición expresada en la Proposición anterior es una condición necesaria pero no suficiente. Es decir, las raíces racionales satisfacen la tesis de la proposición, pero no todos los números racionales a/b que la satisfagan han de ser raíces del polinomio. Entre los valores a/b que cumplen la tesis, localizaremos las raíces seleccionando aquellos tales que $p(\frac{a}{b}) = 0$.

A partir del estudio de las raíces racionales de un polinomio con coeficientes enteros, se puede calcular las raíces racionales de un polinomio con coeficientes racionales. En

efecto, si $p(x) = \sum a_i x^i \in \mathbb{Q}[x]$, entonces los coeficientes de este polinomio son de la forma $a_i = \frac{b_i}{c_i}$, siendo $b_i, c_i \in \mathbb{Z}$. Entonces, el polinomio $q(x) = \sum e_i x^i$, donde $e_i = \frac{a_i c}{c_i}$, siendo c el mínimo común múltiplo de los c_i. Entonces, $q(x) \in \mathbb{Z}[x]$ tiene las mismas raíces que $p(x)$ y las raíces de $q(x)$ se pueden calcular por el método descrito en el resultado anterior.