

Tema 1

I.1. Estructuras Algebraicas

Álgebra. 1º IEC

I. Introducción

I.1. Estructuras Algebraicas

I.1.1. Definición y propiedades

I.1.2. Tipos de estructuras Algebraicas

I.1.2.1. Semigrupo

I.1.2.2. Grupo

I.1.2.3. Anillo

I.1.2.3. Cuerpo

Símbolos Algebraicos

| (a veces se usa :) tal que

$\Rightarrow$ si

$\Leftrightarrow$ si y solo si

$\in$ Pertenece $\notin$ No pertenece

$\forall$ para todo

$\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ Conjuntos Numéricos

$\exists$ existe $\nexists$ no existe

$\exists!$ existe un único

$\subset, \subseteq, \not\subset, \not\subseteq$ Signos de inclusión

$\cup$ Unión (O) $\cap$ Intersección (Y)

$\perp$ Ortogonalidad

X_+, X_-, X^* los positivos, negativos y todos excepto 0

I.1. Estructuras Algebraicas

I.1.1. Definición y propiedades

Conjunto: colección de objetos (o elementos) bien definidos. Se denota con letras mayúsculas y sus elementos por letras minúsculas.

Conjunto vacío $\emptyset$: carece de elementos

Los elementos se pueden denotar: 1) por extensión (ej. $A = \{1,3,5,7\}$); 2) por compresión (ej. $A = \{a \in \mathbb{N} \mid a \text{ es primo} < 10\}$)

Subconjunto: aquel formado tomando ciertos elementos de un conjunto.

$$\forall b \in B \Rightarrow b \in A \quad B = \{b \in B\} \subset A$$

Subconjuntos impropios de A : $\emptyset$ y A .

Subconjuntos propios de A : $B \subset A$ y $B \neq \emptyset$ y $B \neq A$

Una **operación interna** definida en un conjunto $X \neq \emptyset$ es una función binaria $\star$ que a cada par ordenado (x, y) de $X \times X$ le hace corresponder un único elemento de X .

$$\star : X \times X \rightarrow X$$

$$(x, y) \mapsto z = \star(x, y) = x \star y$$

La imagen por la aplicación $\star$ del par (x, y) se denotará por $\star(x, y) = x \star y$ (se lee *x por y*, el resultado de operar *x* con *y*).

Nota: $\star$ operación interna de $X \Rightarrow \forall x, y \in X \exists! x \star y \in X$ (o sea, si $\star$ es una operación interna en X entonces cualesquiera que sean x e y de X existe $x \star y \in X$ y es único).

Nota: Operación externa (para X): $\star : X \times X' \rightarrow X'$ (ej. producto de vector por escalar), o bien $\star : X \times X \rightarrow X'$ (ej., producto escalar de dos vectores)

Conjunto cerrado (o parte estable de un conjunto): Dada una operación interna $\star$ sobre X y sea $X' \subset X$. Decimos que X' es cerrado para la operación $\star$ cuando: $x, y \in X' \Rightarrow x \star y \in X' \quad \forall x, y \in X'$

Ejemplos de operaciones internas

$\star$	a	b
a	a	b
b	b	a

$\perp$	a	b
a	a	a
b	b	b

Estructura algebraica: conjunto formado por elementos y donde hay definidas ciertas operaciones (internas) que satisfacen unas determinadas propiedades. Se llama estructura, y se escribe $(X, \star)$, al conjunto X junto con la operación $\star$.

Nota: Un conjunto X con varias operaciones también forma una estructura algebraica $(X, \star, \dagger, \dots)$.

Posibles propiedades de una operación interna $\star$

Sea X un conjunto no vacío y sea $\star$ una operación interna definida en X .

Asociativa: $(x \star y) \star z = x \star (y \star z) \equiv x \star y \star z \quad \forall x, y, z \in X$

Conmutativa: $(x \star y) = (y \star x) \quad \forall x, y \in X$

Distributiva: Si además de $\star$, X posee otra operación interna $\dagger$, o sea $(X, \star, \dagger)$, se dirá que $\star$ es distributiva respecto de $\dagger$ si:

$$x \star (y \dagger z) = (x \star y) \dagger (x \star z) \quad \forall x, y, z \in X \quad (y \dagger z) \star x = (y \star x) \dagger (z \star x) \quad \forall x, y, z \in X$$

Elemento neutro: Un elemento $e \in X$ es neutro si: $x \star e = e \star x = x \quad \forall x \in X$

Nota: El elemento neutro puede existir o no, pero si $(X, \star)$ tiene elemento neutro e respecto de $\star$, entonces éste es único.

Elemento simétrico: y es un simétrico de x (y se denota por x') si: $x \star x' = x' \star x = e$

Nota: Si un elemento tiene simétrico decimos que es simetrizable. En principio un elemento puede tener más de un simétrico.

Elemento regular o simplificable: $x \in X$ es un elemento regular si $x \star y = x \star z \Rightarrow y = z$ o $y \star x = z \star x \Rightarrow y = z \quad \forall y, z \in X$

Nota: Todo elemento regular posee a lo más un simétrico. El cero no es regular.

I.1.2. Tipos de estructuras Algebraicas

I.1.2.1. Semigrupo

Semigrupo: Estructura algebraica $(X, \star)$ en la que $\star$ es asociativa.

Propiedades: Al ser $\star$ asociativa se cumple:

- Si un elemento $x \in X$ es simetrizable, su simétrico $x' \in X$ es único
- $(x')' = x \quad \forall x \in X$ (x' es el simétrico de $x \Rightarrow x$ es el simétrico de x')
- Si $x, y \in X$ son elementos simetrizables, $x \star y$ también lo es y su simétrico es $(x \star y)' = y' \star x' \quad \forall x, y \in X$
- Todo elemento $x \in X$ simetrizable es regular (lo inverso no es necesariamente cierto)
- Las ecuaciones $a \star x = b$ y $x \star a = b$ (x incógnita) tienen solución única que es $x = a' \star b$ y $x = b \star a'$

I.1.2.2. Grupo

Grupo: $(X, \star)$ es un grupo si $\star$ es asociativa (o sea, es un semigrupo), existe elemento neutro respecto a $\star$ y todo elemento de X tiene simétrico, o sea:

$$\forall x \in X \quad \exists! e \in X \mid e \star x = x \star e = x$$

$$\forall x \in X \quad \exists! x' \in X \mid x \star x' = x' \star x = e$$

Nota: Todos los elementos de X son regulares (al ser simetrizables). Si todos los elementos de un conjunto X son regulares, entonces se dice que se cumple la ley de cancelación o simplificación.

Propiedades adicionales: $(X, \star)$ es un grupo conmutativo o abeliano si además de las propiedades de grupo verifica la propiedad conmutativa: $\forall x, y \in X \quad x \star y = y \star x$

I.1.2.3. Anillo

Anillo: Un anillo $(X, +, \cdot)$ es un conjunto $X \neq \emptyset$ dotado de dos operaciones internas denotadas por $+$ y $\cdot$ tales que:

- $(X, +)$ es un grupo
- $(X, \cdot)$ es un semigrupo
- Propiedad distributiva del producto respecto de la suma: $x \cdot (y + z) = x \cdot y + x \cdot z$
 $(x + y) \cdot z = x \cdot z + y \cdot z \quad \forall x, y, z \in X.$

Propiedades adicionales:

- $(X, +, \cdot)$ es un anillo conmutativo si la operación $\cdot$ es conmutativa $x \cdot y = y \cdot x \quad \forall x, y \in X$
- $(X, +, \cdot)$ es un **anillo con identidad o unitario** si posee elemento neutro respecto de $\cdot$, o sea, $\exists! e \in X \mid x \cdot e = e \cdot x = x \quad \forall x \in X$ (se denomina unidad del anillo y se denota por 1)
- El conjunto formado por los elementos invertibles de X , o sea, $X'^* = \{x \neq 0 \in X \mid \exists x^{-1} \in X\}$ es un grupo respecto de $\cdot$ al que se llama grupo multiplicativo de X .
- **Divisores de cero:** Dos elementos $x, y \in X$ son divisores de cero si y solo si siendo $x \neq 0$ y $y \neq 0 \Rightarrow x \cdot y = 0$ o $y \cdot x = 0$
- $x \in X$ es invertible $\Rightarrow x$ no es divisor de cero
- $x \in (X, +, \cdot)$ es regular si y solo si no es 0 ni divisor de cero. Análogamente x es divisor de cero si y solo si no es regular para el producto.
- $(X, +, \cdot)$ es un **anillo integro** (o anillo de integridad) cuando no tiene divisores de cero, o sea, si $\forall x, y \in X \quad x \cdot y = 0 \Rightarrow x = 0$ o $y = 0$
- $(X, +, \cdot)$ es un **dominio de integridad** si es un anillo de integridad, unitario y conmutativo.

I.1.2.3. Cuerpo

Cuerpo: Un conjunto X dotado de dos operaciones $+$ y $\cdot$ se dirá que es un cuerpo si $(X, +, \cdot)$ es un anillo con identidad y todo elemento distinto de cero tiene inverso respecto al producto, esto es:

- $(X, +)$ es un grupo (o bien $(X, +, \cdot)$ es un anillo)
- $(X^*, \cdot)$ es un grupo
- Propiedad distributiva del producto: $x \cdot (y + z) = x \cdot y + x \cdot z$ $(x + y) \cdot z = x \cdot z + y \cdot z$
 $\forall x, y, z \in X$.

Propiedades:

- Todo cuerpo tiene al menos dos elementos: $\{0, 1\}$
- Si $(X, \cdot)$ es un grupo conmutativo el cuerpo se dirá conmutativo.
- Un cuerpo $(X, +, \cdot)$ es un anillo unitario, y como todo elemento admite inverso, no existen divisores de cero (anillo íntegro). Así, si X es un cuerpo conmutativo, X es un dominio de integridad.

Extensión de $\mathbb{N}$: $(\mathbb{N}, +)$ es un semigrupo. ¿Cómo extenderlo para convertirlo en grupo? $x + n = m \quad m, n \in \mathbb{N}$ no siempre tiene solución en $\mathbb{N}$. Para la que sí la tenga, se añaden las raíces $x = m - n$ a $\mathbb{N}$, obteniendo $\mathbb{Z} = \{m - n \mid m, n \in \mathbb{N}\}$. Siendo así, $(\mathbb{Z}, +)$ es un grupo

Extensión de $\mathbb{Z}$: Un procedimiento para construir a partir de un dominio de integridad $(\mathbb{Z}, +, \cdot)$ un nuevo anillo donde todos sus elementos poseen inverso es resolver la ecuación $x \cdot q = p \quad q \neq 0$ y añadir sus raíces a $\mathbb{Z}$, obteniendo así $\mathbb{Q} = \{p/q \mid q \neq 0, p, q \in \mathbb{Z}\}$. En ese caso se obtiene $(\mathbb{Q}, +, \cdot)$, que es un cuerpo. Los números racionales son pues las raíces de las ecuaciones polinómicas de grado 1.

Extensión de $\mathbb{Q}$: Existen ecuaciones polinómicas de segundo grado que no tienen raíces racionales pero existen cuerpos (extensiones de $\mathbb{Q}$) donde las anteriores ecuaciones tienen solución. El cuerpo óptimo en el que toda ecuación polinómica tiene raíz es $\mathbb{C}$, que se construye en dos etapas: 1) no algebraica ($\mathbb{R}$, completitud); 2) algebraica ($\mathbb{C}$). $\mathbb{C} = \mathbb{R}(\sqrt{-1}) = \{p + q\sqrt{-1} \mid p, q \in \mathbb{R}\}$. Así $(\mathbb{C}, +, \cdot)$ es cerrado.

Teorema fundamental del álgebra: $\mathbb{C}$ es algebraicamente cerrado



