Preliminares Sobre Estructuras Algebraicas (Resumen)

Índice

En el desarrollo de la asignatura se trabajará, principalmente, con la estructura de espacio vectorial que se extenderá a la noción de espacio euclídeo. El concepto de espacio vectorial se apoya, a su vez, en la estructura de cuerpo. En este resumen se introducen brevemente las estructuras algebraicas básicas que conducen a la noción de cuerpo. Posteriormente, aparecerá la noción de espacio vectorial.

Notación. En lo que sigue, el conjunto vacio se representará como $\emptyset$ y $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ representan los conjuntos de los números naturales, enteros, racionales, reales y complejos, respetivamente. ¡$\mathbb{N}$ contiene al número 0!

También se utilizarán los símbolos de la teoría de conjuntos: $\in, \notin, \subset, \not\subset, \cup, \cap, \setminus$, etc.

1. Algo de conjuntos

Definición. Sean A, B conjuntos. Se define

1. La unión de A con B como el conjunto $A \cup B = \{x \,|\, x \in A \text{ o } x \in B\}$.
2. La intersección de A y B como el conjunto $A \cap B = \{x \,|\, x \in A \text{ y } x \in B\}$.
3. La diferencia de A y B como el conjunto $A \setminus B = \{x \,|\, x \in A \text{ pero } x \notin B\}$.

Definición. Sean $A_1, \ldots, A_n$, conjuntos no vacios. Se define el producto cartesiano de $A_1, \ldots, A_n$ como el conjunto

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \,|\, \text{donde } a_i \in A_i \ \forall i \in \{1, \ldots, n\}\}$$

Observación.

1. A los elementos de $A_1 \times A_2$ se les llama pares, a los de $A_1 \times A_2 \times A_3$ ternas, etc. En general, a los elementos de $A_1 \times \cdots \times A_n$ se les llama n-tuplas.
2. Si $A_1 = A_2 = \cdots = A_n = A$, la notación se simplifica escribiendo A^n.

Ejemplo. Interpretar los siguientes conjuntos $\mathbb{N}^2$, $\mathbb{N}^2 \times \mathbb{Q}^3$.

2. El concepto de grupo

Seguidamente se estudia el concepto de grupo, que permitirá llegar a la noción de cuerpo. Para ello, previamente, se definen las estructuras de grupoide, semigrupo y monoide.

Definición. Sea $A \neq \emptyset$ un conjunto no vacio. Una operación interna en A es una aplicación de $A \times A$ en A. Es decir, una operación interna asigna a cada par de elementos de A un único elemento de A.

Definición. Sea $A \neq \emptyset$ y $\star$ una operación interna en A. Entonces se dice que $(A, \star)$ es un grupoide.

Observación. Si $(A, \star)$ es un grupoide y $x, y \in A$, se escribe $x \star y$ para representar el resultado de la operación de x con y, vía la operación interna $\star$.

Definición. Sea $(A, \star)$ un grupoide. Se dice que

1. $(A, \star)$ es un semigrupo si se cumple la propiedad asociativa. Es decir,

$$\forall x, y, z \in A \text{ se cumple que } (x \star y) \star z = x \star (y \star z).$$

2. $(A, \star)$ es un monoide si es un semigrupo y además existe elemento neutro. Es decir,

$$\exists e \in A \text{ tal que } \forall x \in A \text{ se cumple que } e \star x = x = x \star e.$$

3. $(A, \star)$ es un grupo si es un monoide y además todo elemento tiene elemento inverso. Es decir,

$$\forall x \in A \text{ existe un elemento } y \in A \text{ tal que } x \star y = y \star x = e.$$

   A y se le llama elemento inverso de x y se suele representar como x^{-1}; salvo cuando la operación es la suma en cuyo caso se escribe $-x$ y se llama opuesto de x.

4. $(A, \star)$ es un grupo abeliano (o conmutativo) si es un grupo y se cumple la propiedad conmutativa. Es decir,

$$\forall x, y \in A \text{ se cumple que } x \star y = y \star x.$$

Observación.

1. El elemento neutro, si existe, en único.
2. En un monoide, el elemento inverso, si existe, es único. Esta propiedad no se dá en general en un grupoide no asociativo con elemento neutro (véase Hoja 1 de problemas).

Definición. Un cuerpo es una terna $(\mathbb{K}, +, \cdot)$ donde

(i) $\mathbb{K}$ es un conjunto no vacio,

(ii) $+$ y $\cdot$ son operaciones internas en $\mathbb{K}$, que convenimos en llamar suma y multiplicación respectivamente,

y donde se satisface:

1. $(\mathbb{K}, +)$ es un grupo abeliano.
2. $(\mathbb{K}^*, \cdot)$ es un grupo abeliano, donde $\mathbb{K}^* = \mathbb{K} \setminus \{\text{el elemento neutro de } \mathbb{K} \text{ respecto a la suma}\}$.
3. (Propiedad distributiva) $\forall x, y, z \in \mathbb{K}$ se cumple que $x \cdot (y + z) = x \cdot y + x \cdot z$.

	$\star$	Grupoide	Semigrupo	Monoide	Grupo	Grupo Abel.
$\mathbb{N}$	$+$	x	x	x		
$\mathbb{N}$	$\cdot$	x	x	x		
$\mathbb{Z}$	$+$	x	x	x	x	x
$\mathbb{Z}$	$\cdot$	x	x	x		
Pares	$+$	x	x	x	x	x
Pares	$\cdot$	x	x			
Impares	$+$					
Impares	$\cdot$	x	x	x		
$\mathbb{Q}$	$+$	x	x	x	x	x
$\mathbb{Q}$	$\cdot$	x	x	x		
$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$	$\cdot$	x	x	x	x	x
$\mathbb{R}$	$+$	x	x	x	x	x
$\mathbb{R}$	$\cdot$	x	x	x		
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$	$\cdot$	x	x	x	x	x
$\mathbb{C}$	$+$	x	x	x	x	x
$\mathbb{C}$	$\cdot$	x	x	x		
$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$	$\cdot$	x	x	x	x	x
$\mathbb{Z}[\mathtt{i}]$	$+$	x	x	x	x	x
$\mathbb{Z}[\mathtt{i}]$	$\cdot$	x	x	x		
$\mathbb{Q}(\mathtt{i})$	$+$	x	x	x	x	x
$\mathbb{Q}(\mathtt{i})$	$\cdot$	x	x	x		
$\mathbb{Q}(\mathtt{i})^* = \mathbb{Q}(\mathtt{i}) \setminus \{0\}$	$\cdot$	x	x	x	x	x
$\mathbb{Z}_m$	$+$	x	x	x	x	x
$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]\}$ (p primo)	$\cdot$	x	x	x	x	x

Cuadro 1: Estructura algebraica de los principales conjuntos

Observación. Sea $\mathbb{K}$ un cuerpo. Al elemento neutro respecto de la suma se le llama cero del cuerpo y se representa como 0 o como $0_{\mathbb{K}}$. Al elemento neutro respecto de la multiplicación se le llama uno del cuerpo y se representa como 1 o como $1_{\mathbb{K}}$.

Observación. En un cuerpo $\mathbb{K}$ se verifican las siguientes propiedades básicas:

1. $\forall a \in \mathbb{K}$ se verifica que $a \cdot 0 = 0 \cdot a = 0$.
2. $\forall a, b \in \mathbb{K}$ se verifica que $(-a) \cdot b = -(a \cdot b)$, $a \cdot (-b) = -(a \cdot b)$, $(-a) \cdot (-b) = a \cdot b$.
3. Si $a, b \in \mathbb{K}$ son tal que $a \cdot b = 0$ entonces $a = 0$ o $b = 0$.

Observación. Si en la condición (2) de la definición de cuerpo, en lugar de exigir que $(\mathbb{K}^*, \cdot)$ sea un grupo abeliano, se exige que $(\mathbb{K}, \cdot)$ sea un semigrupo conmutativo (resp. monoide conmutativo) aparece la noción de anillo conmutativo (resp. anillo conmutativo unitario).

Ejemplo. Los cuerpos mas importantes que se utilizarán en la asignatura son:

- El cuerpo de los números racionales $\mathbb{Q}$.
- El cuerpo de los números reales $\mathbb{R}$.
- El cuerpo de los números complejos $\mathbb{C}$.
- El cuerpo de los racionales gaussianos $\mathbb{Q}(i)$ (véase Hoja 1 de problemas).
- El cuerpo finito primo $\mathbb{Z}_p$ (véase siguiente sección).

	Anillo conm.	Anillo conm. unitario	cuerpo
$(\text{Pares}, +, \cdot)$	x		
$(\mathbb{Z}, +, \cdot)$	x	x	
$(\mathbb{Q}, +, \cdot)$	x	x	x
$(\mathbb{R}, +, \cdot)$	x	x	x
$(\mathbb{C}, +, \cdot)$	x	x	x
$(\mathbb{Z}[\mathtt{i}], +, \cdot)$	x	x	
$(\mathbb{Q}(\mathtt{i}), +, \cdot)$	x	x	x
$(\mathbb{Z}_p, +, \cdot)$ (p primo)	x	x	x

Cuadro 2: Estructura algebraica de los principales conjuntos

4. El cuerpo finito primo $\mathbb{Z}_p$

4.1. Conjuntos cocientes

Para introducir el conjunto $\mathbb{Z}_p$, se requiere el concepto de relación de equivalencia que a su vez implica la noción de relación binaria. Informalmente, una relación binaria es un criterio que decide si dos elementos dados de un conjunto están relacionados. Así, si $\mathscr{R}$ es una relación binaria en un conjunto A y $a, b \in A$, se escribe

- $a \mathscr{R} b$ para indicar que a se relaciona con b
- $a \not\mathscr{R} b$ para indicar que a no se relaciona con b

Definición. Un relación binaria $\mathscr{R}$ en un conjunto A es una relación de equivalencia si se cumple que

- [Propiedad reflexiva] Para todo $a \in A$ se verifica que $a \mathscr{R} a$.
- [Propiedad simétrica] Para todo $a, b \in A$, si $a \mathscr{R} b$ entonces $b \mathscr{R} a$.
- [Propiedad transitiva] Para todo $a, b, c \in A$, si $a \mathscr{R} b$ y $b \mathscr{R} c$ entonces $a \mathscr{R} c$.

Definición. Sea $\mathscr{R}$ una relación de equivalencia en A. Para cada elemento $a \in A$, se define la clase de equivalencia de a como el conjunto

$$[a] = \{b \in A \mid a \mathscr{R} b\}.$$

A cualquier elemento en $[a]$ se le llama representante de la clase $[a]$.

Proposición. Sea $A \neq \emptyset$ y $\mathscr{R}$ una relación de equivalencia en A. Se verifica que

1. $\forall\, a \in A$ se cumple que $[a] \neq \emptyset$.
2. $\forall\, a, b \in A$ se cumple que $[a] = [b]$ si y solo si $a \mathscr{R} b$.
3. $\forall\, a, b \in A$, si $[a] \neq [b]$ entonces $[a] \cap [b] = \emptyset$.

Definición. Sea $A \neq \emptyset$ un conjunto no vacio y $\mathscr{R}$ una relación de equivalencia en A. Se define el conjunto cociente de A sobre $\mathscr{R}$ como el conjunto

$$A/\mathscr{R} = \{[a] \mid a \in A\}.$$

4.2. El conjunto cociente $\mathbb{Z}_m$

En lo que sigue sea $m \in \mathbb{N}$, $m \geq 1$, un número natural fijo al que llamaremos módulo. Se considera en $\mathbb{Z}$ la siguiente relación binaria

$$\text{Si } a, b \in \mathbb{Z} \text{ entonces } a \equiv_m b \text{ si y solo si } m \text{ divide a } a - b.$$

La expresión $a \equiv_m b$ se suele leer como a es congruente a b módulo m.

Es sencillo comprobar que $\equiv_m$ es de hecho una relación de equivalencia que genera m clases de equivalencia

$$\begin{array}{ll} [0] = \{km \,|\, k \in \mathbb{Z}\} & \text{múltiplos de } m \\ [1] = \{km + 1 \,|\, k \in \mathbb{Z}\} & (\text{múltiplos de } m) + 1 \\ \vdots & \\ [m-1] = \{km + (m-1) \,|\, k \in \mathbb{Z}\} & (\text{múltiplos de } m) + (m-1) \end{array}$$

Por tanto, el conjunto cociente $\mathbb{Z}/\equiv_m$, que se representa por $\mathbb{Z}_m$, tiene m elementos

$$\mathbb{Z}_m = \{[0], \ldots, [m-1]\}.$$

Observación. En cada clase de equivalencia de $\mathbb{Z}_m$ existe un único representante entre 0 y $m-1$ que llamaremos representante canónico. Para obtenerlo, basta dividir por m cualquier elemento positivo de la clase.

Observación. Sean $[a], [b] \in \mathbb{Z}_m$. Para decidir si $[a] = [b]$, se puede actuar como sigue: (1) determinar los representantes canónicos de $[a]$ y $[b]$ y comprobar si coinciden. (2) comprobar si $a \equiv_m b$, es decir, comprobar si m divide a $a - b$.

4.3. El cuerpo finito primo $\mathbb{Z}_p$

En esta sección, se asume que el módulo es un número primo y para enfatizar este hecho, en lugar de utilizar m, representamos al módulo por p. Por tanto, en lo que sigue, $p \in \mathbb{N}$, p primo.

En $\mathbb{Z}_p$ se consideran las operaciones

$$\begin{array}{ll} \text{Suma} & [a] + [b] = [a + b] \\ \text{Multiplicación} & [a] \cdot [b] = [a \cdot b] \end{array}$$

Teorema. $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.

Cabe indicar que $0_{\mathbb{Z}_p} = [0]$, $1_{\mathbb{Z}_p} = [1]$. Asimismo, para obtener el inverso, respecto al producto, de un elemento en $\mathbb{Z}_p \setminus \{[0]\}$, se puede actuar como sigue:

1. Construir la tabla de multiplicar.
2. Aplicar el Teorema pequeño de Fermat para obtener que si $[a] \neq [0]$ entonces
$$[a]^{-1} = [a^{p-2}]$$
3. Utilizar el algoritmo extendido de Euclídes junto con la igualdad de Bézout (véase pizarra).