1. Campos

Definición 1 (producto cartesiano de conjuntos)**.** Sean A y B dos conjuntos. Se define el producto cartesiano de A y B como

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

Observación 2. Observemos que el orden en que aparecen los conjuntos es importante, puesto que los elemenetos del producto cartesiano son **parejas ordenadas**.

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

Si $A_1, \ldots, A_n$ son conjuntos, entonces se define el producto cartesiano de $A_1, \ldots, A_n$ como:

$$A_1 \times \ldots \times A_n := \{(a_1, \ldots, a_n) \mid a_i \in A_i \ \forall i = 1, \ldots, n\},$$

donde cada elemento $(a_1, \ldots, a_n)$ ordenado se llama n-ada, n-tupla, etc.

Ejemplo 3. Si consideramos el producto cartesiano $\mathbb{Z} \times \mathbb{R}$, podemos decir que $(2, \pi) \in \mathbb{Z} \times \mathbb{R}$, pero $(\pi, 2) \notin \mathbb{Z} \times \mathbb{R}$.

Si $1 \leqslant j \leqslant n$, A_j se llama el **factor** j**-ésimo** del producto cartesiano $A_1 \times \ldots \times A_n$. Si $(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$, entonces a_j es la j**-ésima coordenada** o j**-ésima entrada** de $(a_1, \ldots, a_n)$. Cuando $A_1 = A_2 = \ldots = A_n = A$, se escribe A^n en lugar de $\underbrace{A_1 \times \ldots \times A_n}_{n \text{ veces}}$. En particular, $\mathbb{R}^n = \{(a_1 \ldots, a_n) \mid a_i \in \mathbb{R} \ \forall i = 1, \ldots, n\}$.

Ejemplo 4.

$$\begin{aligned} \mathbb{R}^1 &= \mathbb{R} && \text{recta numérica de dimensión 1.} \\ \mathbb{R}^2 &= \mathbb{R} \times \mathbb{R} && \text{plano euclideano de dimensión 2.} \\ \mathbb{R}^3 &= \mathbb{R} \times \mathbb{R} \times \mathbb{R} && \text{espacio euclideano de dimensión 3.} \end{aligned}$$

Observación 5. Los conjuntos mencionados antes se supone que son no vacíos. Notemos que $A \times \emptyset = \emptyset$ pues $(a, b) \in A \times \emptyset$ si y sólo si $a \in A$ y $b \in \emptyset$, lo cual es una contradicción.

Definición 6 (operación binaria en un conjunto)**.** Sea A un conjunto no vacío. Una operación binaria en A es una función $f : A \times A \to A$.

Nota: Supongamos que f es una operación binaria sobre A, entonces

$$\begin{aligned} f : A \times A &\to A \\ (a, b) &\mapsto f(a, b). \end{aligned}$$

La imagen de (a, b) bajo f tendría que escribirse como $f((a, b))$ pero para no abusar de la notación escribimos $f(a, b)$.

Ejemplo 7. La suma usual de números enteros se puede representar como una operación binaria en los enteros:

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto +(a, b) := a + b. \end{aligned}$$

Observe que en la expresión $+(a, b) = a+b$, el símbolo $+$ sirve para denotar dos conceptos diferentes: el símbolo $+$ que aparece en $+(a, b)$ es el nombre de la función, como bien podría ser $f(a, b)$, siendo f el nombre, mientras que en la expresión $a + b$, el símbolo $+$ se usa como el operador usual suma.

Ejemplo 8. Sea la operación:

$$\begin{aligned} * : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto *(a, b) := |a|b. \end{aligned}$$

En este ejemplo, la operación binaria sobre los enteros, $*$, consiste en tomar el valor absoluto del primer entero y multiplicarlo por el segundo entero. De esta forma podemos construir nuestras propias operaciones binarias.

Ejemplo 9. Consideremos la función $\circ$ definida como sigue:

$$\begin{aligned} \circ : \mathbb{N} \times \mathbb{N} &\to \mathbb{Q} \\ (a, b) &= \circ(a, b) := \frac{a}{b}. \end{aligned}$$

La función $\circ$ no es una operación binaria sobre los naturales, observemos por ejemplo que

$$\begin{aligned} \circ\,(1, 2) &= \frac{1}{2} \\ \circ\,(5, 3) &= \frac{5}{3}. \end{aligned}$$

Al considerar operaciones binarias sobre un conjunto, queremos garantizar que la operación debe ser **cerrada**. Esto significa que al tomar dos elementos de cierto conjunto A, el resultado de operarlos, según la regla de la operación definida, debe ser también un elemento de A.

Supóngase que $A \neq \emptyset$ y f es una operación binaria sobre A. Si $a, b \in A \Rightarrow f(a, b) \in A$. Escribimos:

$$a + b = f(a, b).$$

$a + b$ es sólo notación, no quiere decir la suma de a con b como se conoce. Al ser pura notación, igual se podría escribir $a * b$, $a \triangle b$ u otro símbolo para evitar la notación de función $f(a, b)$. Bajo la notación anterior, decimos que f es:

1. **asociativa** si $\forall a, b, c \in A \Rightarrow a + (b + c) = (a + b) + c$, o con notación funcional:
$$f\big(a, f(b, c)\big) = f\big(f(a, b), c\big),$$

2. **conmutativa** si $\forall a, b \in A \Rightarrow a + b = b + a$, o con notación funcional:
$$f(a, b) = f(b, a),$$

3. decimos que A tiene **elemento neutro** o **elemento identidad** si existe un elemento $e \in A$ tal que
$$a + e = a = e + a, \forall a \in A.$$
Nota: Si A posee identidad e, entonces ésta es única. En efecto, supóngase que $e' \in A$ es también identidad de A. Entonces $e' = e' + e = e$,

4. supóngase que A tiene identidad e. Sea $a \in A$. Decimos que a es **invertible** o que tiene **inverso** si existe $b \in A$ tal que
$$a + b = e = b + a;$$
si esto ocurre, entonces b se llama **el inverso de** a y se le denota por $-a$.

   Nota: Supongamos que la operación es asociativa. Si a es invertible, su inverso es único. Pues si b y c son inversos de a, entonces
$$\begin{aligned} b &= b + e \\ &= b + (a + c) \\ &= (b + a) + c \\ &= e + c \\ &= c, \end{aligned}$$

5. se define $\forall a, b \in A$, cuando A tenga identidad y exista el inverso de b,
$$a - b := a + (-b).$$

Ejemplo 10. Retomemos el ejemplo 8, en el cual la operación $*$ actúa sobre los enteros según la regla $*(a, b) = |a|b$. También puede escribirse como:
$$a * b = |a|b.$$

Mostremos que esta operación es asociativa: sean $a, b, c \in \mathbb{Z}$, entonces

$$\begin{aligned} a * (b * c) &= |a|(|b|c) \\ &= (|a||b|)c \\ &= |ab|c \\ &= ||a|\ b|c \\ &= (a * b) * c. \end{aligned}$$

Se puede ver fácilmente que esta operación no es conmutativa. Por ejemplo, tómense $a = 1$ y $b = -1$.

Definición 11 (campo o cuerpo)**.** Sea F un conjunto no vacío, y $+, \cdot$ dos operaciones binarias sobre F. Decimos que F es campo (o cuerpo) si:

1. $+$ es asociativa,
2. $+$ es conmutativa,
3. $+$ tiene elemento identidad, denotada por 0,
4. cada elemento de F tiene inverso con respecto a $+$,
5. $\cdot$ es asociativa,
6. $\cdot$ es conmutativa,
7. $\cdot$ tiene elemento identidad, denotada por 1, con $1 \neq 0$,
8. cada elemento de F distinto de 0 tiene inverso con respecto a $\cdot$,
9. $\cdot$ es distributiva con respecto a $+$: $\forall a, b, c \in F \quad a \cdot (b + c) = a \cdot b + a \cdot c$

NOTA: Si F es un campo, a los elementos de F se les llama **escalares** por su conexión con los espacios vectoriales.

Proposición 12 (leyes de cancelación)**.** *Sea F un campo. Entonces, en F se cumplen las leyes de la cancelación, es decir, $\forall a, b, c \in F$ se tiene que:*

i) $a + b = a + c \Rightarrow b = c$,

ii) $a \neq 0$ *y* $a \cdot b = a \cdot c \Rightarrow b = c$.

Demostración:

i)

$$
\begin{aligned}
b = b + 0 = b + (a + (-a)) &\\
&= (b + a) + (-a)\\
&= (a + b) + (-a)\\
&= (a + c) + (-a)\\
&= (c + a) + (-a)\\
&= c + (a + (-a))\\
&= c + 0\\
&= c.
\end{aligned}
$$

ii)

$$
\begin{aligned}
b = b \cdot 1 = b \cdot (a \cdot a^{-1}) &\\
&= (b \cdot a) \cdot a^{-1}\\
&= (a \cdot b) \cdot a^{-1}\\
&= (a \cdot c) \cdot a^{-1}\\
&= (c \cdot a) \cdot a^{-1}\\
&= c \cdot (a \cdot a^{-1})\\
&= c \cdot 1\\
&= c.
\end{aligned}
$$

Para el producto hemos usado la notación a^{-1} para indicar el inverso de a.

En realidad las cadenas de igualdad son una demostración incompleta. Se sugiere al lector completar la demostración anotando a la derecha de cada cadena de igualdad qué propiedad de la definición 11 justifica cada paso. $\square$

Corolario 13. *Sea F un campo y $a, b \in F$. Entonces:*

i) $a \cdot 0 = 0$,

ii) $a \cdot b = 0 \Rightarrow a = 0$ *o* $b = 0$.

Demostración:

i) Al emplear las propiedades de las operaciones de campo y el inciso $i)$ de la proposición 12 se tiene que

$$\begin{aligned} a \cdot 0 + 0 &= a \cdot 0 = a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0 \\ &\Rightarrow a \cdot 0 = 0. \end{aligned}$$

ii) Supóngase que $a \neq 0$, entonces, de las propiedades de las operaciones de campo y del inciso $ii)$ de la proposición 12 se tiene que

$$\begin{aligned} b = 1 \cdot b =&(a \cdot a^{-1}) \cdot b = (a^{-1} \cdot a) \cdot b \\ &= a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0. \end{aligned}$$

□

Observación 14. Se puede verificar que $\mathbb{Z}$ no es un campo. Sí lo son $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$. Denotaremos por $\mathbb{K}$ a $\mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$.

Ejemplo 15. Denotemos por $\mathbb{R}[x]$ al conjunto de polinomios con coeficientes reales en la variable x. Afirmamos que $\mathbb{R}[x]$ no es campo. Veamos que los polinomios no son invertibles bajo el producto usual. Sea $f(x) = -x + 1 \in \mathbb{R}[x]$. Entonces $\nexists g(x) \in \mathbb{R}[x]$ tal que $g(x)f(x) = 1$. De lo contrario, entonces

$$g(x) = \frac{1}{f(x)} = \frac{1}{-x+1} = 1 + x + x^2 + \ldots \notin \mathbb{R}[x].$$

Recordemos que un polinomio debe tener la forma $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. $\mathbb{R}[x]$ no tiene estructura de campo pero sí de anillo, se conoce como **anillo de polinomios**.

Por otro lado, se denota con $\mathbb{R}(x)$ al conjunto de funciones racionales con coeficientes en $\mathbb{R}$ en la variable x y se define como

$$\mathbb{R}(x) := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{R}[x] \text{ y } g(x) \neq 0 \right\}.$$

$R(x)$ con las operaciones usuales de suma y producto es un campo.

Ejemplo 16.

$$\mathbb{Q}(\sqrt{2}) := \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\} \subseteq \mathbb{R}$$

con las operaciones usuales de suma y producto en $\mathbb{R}$ es un campo.

Ejemplo 17. Sea $\mathbb{F}_2 := \{0, 1\}$ con las siguientes operaciones:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

es un campo.

Observación 18. Si F es un campo, entonces estamos suponiendo que $1 \neq 0$. Si $1 = 0$, entonces $\forall a \in F$ se tiene que

$$a = a \cdot 1 = a \cdot 0 = 0.$$

Por tanto, se tendría que $F = \{0\}$.

Definición 19 (subcampo)**.** Si F es un campo y K es un subconjunto de F tal que, con las operaciones de suma y producto de F, hacen de K un campo, entonces decimos que K es un subcampo de F.

Notamos que, por ejemplo, $\mathbb{Q}$ es un subcampo de $\mathbb{R}$ y $\mathbb{R}$ es un subcampo de $\mathbb{C}$. Pero también $\mathbb{Q}$ es un subcampo de $\mathbb{C}$.