Tema 1. Conjuntos y números

Curso Cero MathBridge

Aurora Torrente & Filippo Terragni

Año académico 2020–2021

uc3m | Universidad Carlos III de Madrid

1. Conjuntos

Uno de los conceptos matemáticos fundamentales es el de **conjunto**. Intuitivamente, un conjunto es una colección de objetos denominados *elementos* del conjunto. En concreto, dado un conjunto X y un cierto objeto x, una y sólo una de las siguientes afirmaciones debe ser cierta:

- o bien $x \in X$, es decir el objeto x pertenece al conjunto X;
- o bien no pertenece, $x \notin X$.

Los conjuntos se denotan generalmente utilizando las llaves $\{\,\}$ y pueden ser definidos de varias formas.

- Por extensión, en el caso de que sea posible enumerar todos los elementos del conjunto:
$$X = \{1, 2\} = \{2, 1\} = \{1, 2, 2, 1, 1\}\,.$$
Es importante recordar que los conjuntos no poseen una ordenación privilegiada de sus elementos ni admiten elementos múltiples.

- Por comprensión, en el caso de que su definición se realice atendiendo a la propiedad común que poseen todos los elementos del conjunto:
$$Y = \{y\,,\ \text{donde } y \text{ es una provincia de Andalucía}\}\,.$$
Evidentemente en el ejemplo anterior también podíamos haber definido Y por extensión:
$$Y = \{\text{Almería, Cádiz, Córdoba, Granada, Huelva, Jaén, Málaga, Sevilla}\}.$$

- En la práctica se utilizan notaciones mixtas. Por ejemplo, es habitual introducir el conjunto $\mathbb{N}$ de los números naturales en la forma $\mathbb{N} = \{1, 2, 3, \dots\}$. Sin embargo, la expresión anterior no es una definición de $\mathbb{N}$.

- Lo más habitual es definir un conjunto utilizando otro conocido a través de alguna regla de formación. Por ejemplo, el conjunto C de los cubos se puede escribir de varias formas equivalentes:

$$C = \{n^3 \,:\, n \in \mathbb{N}\} = \{m \in \mathbb{N} \,:\, \exists\, k \in \mathbb{N} \text{ tal que } m = k^3\}\,.$$

  En este ejemplo es evidente que todos los elementos de C son a su vez elementos de $\mathbb{N}$, es decir C es un **subconjunto** de $\mathbb{N}$, en símbolos $C \subset \mathbb{N}$. En la notación anterior, el símbolo $:$ (a veces sustituido por $|$) significa 'donde', 'tal que', mientras que el símbolo $\exists$ significa 'existe'.

El único conjunto que no contiene ningún elemento se llama **conjunto vacío** y normalmente se denota por $\varnothing$. Notése que $\varnothing$ admite infinitas representaciones alternativas, por ejemplo $\varnothing = \{n \in \mathbb{N} \,:\, n^2 = -1\}$.

Recordamos ahora las cuatro operaciones entre conjuntos más elementales.

Unión: $X \cup Y = \{z \,:\, z \in X \text{ ó } z \in Y\} = \{z \,:\, (z \in X) \vee (z \in Y)\}$.

Intersección: $X \cap Y = \{z \,:\, z \in X,\, z \in Y\} = \{z \,:\, (z \in X) \wedge (z \in Y)\}$.

Diferencia: $X \setminus Y = \{z \,:\, z \in X,\, z \notin Y\}$.

Producto Cartesiano: $X \times Y = \{(x, y) \,:\, x \in X,\, y \in Y\}$.

Ejemplo. Sean $X = \{1, 2, a, c\}$, $Y = \{a, b\}$. Entonces se cumplen las igualdades:

$$\begin{aligned} X \cup Y &= \{1, 2, a, b, c\}\,; \\ X \cap Y &= \{a\}\,; \\ X \setminus Y &= \{1, 2, c\}\,; \\ X \times Y &= \{(1, a), (1, b), (2, a), (2, b), (a, a), (a, b), (c, a), (c, b)\}\,. \end{aligned}$$

Es importante subrayar la diferencia entre $\{\,\}$ y $(\,)$. En concreto, $\{1, 2\}$ denota un conjunto y por tanto $\{1, 2\} = \{2, 1\}$. Sin embargo, $(1, 2)$ es un *par ordenado* y por tanto $(1, 2) \neq (2, 1)$.

2. Combinatoria

La combinatoria es una disciplina matemática que (entre otras cosas) se ocupa de desarrollar técnicas que permiten determinar el número de elementos de un conjunto definido por comprensión, sin necesidad de enumerarlos uno a uno.

El número de elementos de un conjunto X se denomina **cardinal** de X y habitualmente se denota mediante $|X|$. Por ejemplo

$$X = \{x \,:\, x \text{ es una provincia de Andalucía}\} \Longrightarrow |X| = 8\,.$$

La mayoría de las técnicas combinatorias elementales se basa en las siguientes dos reglas.

Principio del producto: $|X \times Y| = |X|\,|Y|$.

Principio de la suma: si $X \cap Y = \varnothing$, entonces $|X \cup Y| = |X| + |Y|$.

Ejemplo. Sean

$$\begin{aligned} X &= \{x \mid x \text{ es una provincia de Andalucía}\}, \\ Y &= \{y \mid y \text{ es una provincia de Galicia}\}. \end{aligned}$$

Entonces

$$|X \cup Y| = 12\,, \quad |X \times Y| = 32\,.$$

Muchos problemas pueden ser resueltos utilizando alguna de las siguientes técnicas de recuento, cuyas fórmulas pueden ser deducidas usando el principio del producto.

Permutaciones de n objetos

Los elementos de un conjunto de cardinal n se pueden ordenar de

$$n! \equiv n\,(n-1)\,(n-2)\,\cdots\,2\cdot 1$$

maneras distintas. La fórmula anterior es la definición del *factorial* de un número natural n, que se denota mediante $n!$. Por convenio, $0! = 1$.

Permutaciones con repetición de n objetos

El número de maneras distintas de ordenar n objetos clasificados en k grupos de objetos idénticos entre sí (con n_1 elementos en el primero, n_2 en el segundo, etc.) es

$$\frac{n!}{n_1!\, n_2! \, \cdots \, n_k!}\,, \quad \text{con } n_1 + \cdots + n_k \,=\, n\,.$$

Variaciones de r objetos tomados de entre n

A partir de un conjunto de cardinal n es posible construir un total de

$$V(n,r) \,\equiv\, n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

listas ordenadas formadas por $r \leq n$ elementos distintos.

Variaciones con repetición de r objetos tomados de entre n

Dado un conjunto de cardinal n es posible construir un total de n^r listas ordenadas formadas por $r \leq n$ elementos no necesariamente distintos.

Combinaciones de r objetos tomados de entre n

Dado un conjunto de cardinal n, el número de subconjuntos distintos de $r \le n$ elementos que podemos formar es

$$\binom{n}{r} \equiv \frac{n!}{r!(n-r)!} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}.$$

La fórmula anterior es la definición del *coeficiente binomial* de dos números naturales n y r, con $n \ge r$. Por convenio, $\binom{n}{0} = 1$.

3. Teoría de números

Existen algunos conjuntos de números que es conveniente manejar con soltura. De manera *informal* definimos los siguientes.

Números naturales. $\mathbb{N} = \{1, 2, 3, \ldots\}$

Números enteros. $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

A veces se indica el conjunto de los *enteros no negativos* como

$$\mathbb{Z}_+ = \mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$$

Números racionales. $\mathbb{Q} = \left\{ \frac{p}{q} \ : \ p, q \in \mathbb{Z}\,,\ q \neq 0 \right\}$

Números reales. $\mathbb{R} = \mathbb{Q} \cup \{\,\text{irracionales}\,\}$, donde los números *irracionales* son todos los números que no pertenecen a $\mathbb{Q}$

Se verifica que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. El conjunto $\mathbb{Z}$ de los enteros es *cerrado* bajo las operaciones de suma, diferencia y producto. Es decir, para todo $a, b \in \mathbb{Z}$, $a \pm b \in \mathbb{Z}$ y $a\,b \in \mathbb{Z}$. Además se cumple que:

- 0 es el *elemento neutro* de la suma, esto es $a + 0 = a$ para todo $a \in \mathbb{Z}$.
- 1 es el *elemento neutro* del producto, esto es $a \cdot 1 = a$ para todo $a \in \mathbb{Z}$.
- Para todo $a \in \mathbb{Z}$, existe un único *elemento inverso*, $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$.

Sin embargo, el cociente de dos números enteros puede no ser entero. Por ello debemos definir con cuidado cuándo un número entero divide a otro.

Definición 1 *Dados dos enteros $a \neq 0$ y b, se dice que* ***a* divide a *b*** *si existe $q \in \mathbb{Z}$ tal que $b = a\,q$. En este caso, a es un* **factor** *o* **divisor** *de b, b es un* **múltiplo** *de a, y lo indicamos mediante* $\boldsymbol{a \mid b}$ *(de lo contrario escribimos $a \nmid b$).*

Observamos que:

- Cualquier entero $a \in \mathbb{Z}$ divide a 0, esto es $0 = a \cdot 0$.
- 1 divide a cualquier entero $a \in \mathbb{Z}$, esto es $a = 1 \cdot a$.
- Cualquier entero $a \in \mathbb{Z}$ se divide a sí mismo, esto es $a = a \cdot 1$.

La división usual de dos enteros dando lugar a un *cociente* y un *resto* nos la garantiza el siguiente teorema.

Teorema 1 (divisibilidad) *Sean a, $b \neq 0$ dos enteros. Entonces existen dos enteros únicos q y r tales que*

$$a \;=\; q\,b + r, \quad \text{con} \quad 0 \leq r < |b|\,.$$

Notése lo siguiente.

- Los números a y b se denominan respectivamente **dividendo** y **divisor**.
- El número r se denomina **resto** de la división, esto es $r \;=\; a \bmod b$.
- El número q se denomina **cociente** de la división, esto es

$$q \;=\; a \operatorname{div} b \;=\; \begin{cases} \lfloor a/b \rfloor & \text{si } \; b > 0, \\ \lceil a/b \rceil & \text{si } \; b < 0, \end{cases}$$

  dónde $\lfloor\cdot\rfloor$ y $\lceil\cdot\rceil$ se denominan función suelo y función techo, respectivamente. Puesto que no hemos definido aún el concepto de función, podemos decir que $\lfloor x \rfloor$ es el entero menor que x y más próximo a x, mientras que $\lceil x \rceil$ es el entero mayor que x y más próximo a x, para todo $x \in \mathbb{R}$.

Otros conceptos importantes son los siguientes.

Definición 2 *Dados dos números enteros a, b no nulos, se denomina* **máximo común divisor** *de a y b, denotado por $\operatorname{mcd}(a, b)$, al mayor entero d tal que $d \mid a$ y $d \mid b$.*

Teorema 2 *El máximo común divisor de dos números enteros es único.*

Definición 3 *Dados dos números enteros a, b no nulos, se denomina* **mínimo común múltiplo** *de a y b, denotado por* $\mathrm{mcm}(a, b)$, *al menor número natural m tal que $a \mid m$ y $b \mid m$.*

Una clase muy importante de números naturales son los *números primos*.

Definición 4 *Un número natural $p > 1$ se denomina* **primo** *si los únicos divisores naturales de p son 1 y p. Un número natural $p > 1$ que no sea primo se denomina compuesto.*

Obsérvese que el número natural 1 no es primo. El primer número primo es el 2 y todos los demás números primos son números naturales impares $(3, 5, 7, 11, \ldots)$. Los números primos son muy importantes porque constituyen los 'bloques' fundamentales con que construir los demás números naturales.

Teorema 3 (fundamental de la aritmética) *Todo número natural $n > 1$ se puede descomponer de manera única en factores primos, esto es*

$$n \;=\; p_1^{n_1}\, p_2^{n_2}\, p_3^{n_3} \ldots p_k^{n_k}\,,$$

donde p_i son números primos distintos entre sí y escritos en orden creciente, mientras que los exponentes n_i son números naturales.

En otras palabras, cada número natural (mayor que uno) tiene una descomposición única en números primos. Por ejemplo, $100 = 2^2 \cdot 5^2$. Una vez conocida la descomposición en factores primos de dos números naturales es muy fácil calcular su máximo común divisor y su mínimo común múltiplo, como muestra el siguiente resultado.

Teorema 4 *Si $a, b \in \mathbb{N}$ se factorizan de la forma*

$$\begin{aligned} a &= p_1^{n_1}\, p_2^{n_2} \dots p_k^{n_k}\,, \\ b &= p_1^{m_1}\, p_2^{m_2} \dots p_k^{m_k}\,, \end{aligned}$$

con $n_i, m_i \geq 0$ y donde todos los factores primos p_i de a y b aparecen en ambas factorizaciones, se cumple que

$$\begin{aligned} \operatorname{mcd}(a, b) &= p_1^{\text{mín}(n_1,m_1)}\, p_2^{\text{mín}(n_2,m_2)} \dots p_k^{\text{mín}(n_k,m_k)}\,, \\ \operatorname{mcm}(a, b) &= p_1^{\text{máx}(n_1,m_1)}\, p_2^{\text{máx}(n_2,m_2)} \dots p_k^{\text{máx}(n_k,m_k)}\,. \end{aligned}$$

Un resultado muy importante y conocido desde la antigüedad es que el conjunto de los números primos tiene cardinal infinito.

Teorema 5 (Euclides) *Existen infinitos números primos.*

Es importante no confundir el concepto de número primo con el de números *coprimos* o *primos entre sí*.

Definición 5 *Se dice que dos números enteros a y b son* **coprimos** *o* **primos entre sí** *si $\operatorname{mcd}(a, b) = 1$. Se dice que un conjunto de números enteros $\{a_1, \dots, a_n\}$ es un conjunto de números coprimos si $\operatorname{mcd}(a_1, \dots, a_n) = 1$.*

Ejemplos.

- Los números $25 = 5^2$ y $16 = 2^4$ son coprimos ya que $\operatorname{mcd}(25, 16) = 1$, pero ninguno de ellos es un número primo.
- Los números 5 y 17 son primos y también coprimos.