

# Inducción Matemática

(Por Carlos Domingo. Editado por Carmen Rodríguez y Jacinto Dávila)

1. La estructura de un dominio de integridad la poseen los números enteros que fueron los entes matemáticos que primero reconoció la humanidad al formarse la actividad de “contar”.

Definamos pues un conjunto  $Z$  (... -4, -3, -2, -1, 0, 1, 2, 3, ... ) con una operación  $+$  y otra  $\cdot$  (o simplemente indicada con blanco) con las siguientes propiedades [escribirlas para elementos  $a, b, c, d, \dots$  cualesquiera de  $Z$ ]

- 1) Asociativa  $+$   $(a + b) + c =$  \_\_\_\_\_
- 2) Existe el elemento neutro, 0, de  $+$  \_\_\_\_\_
- 3) Existe inverso o elemento simétrico de  $+$  \_\_\_\_\_
- 4) Conmutativa sobre  $+$  \_\_\_\_\_
- 5) Asociativa sobre  $\cdot$  \_\_\_\_\_
- 6) Existe el elemento unitario de  $\cdot$  \_\_\_\_\_
- 7) Conmutativa sobre  $\cdot$  \_\_\_\_\_
- 8) Distributiva a la izquierda \_\_\_\_\_
- 9) Simplificación a la izquierda \_\_\_\_\_
- 10) Cierre de  $+$  y  $\cdot$  (son funciones de  $Z \times Z \rightarrow Z$ ) \_\_\_\_\_

Estas propiedades, que fueron extraídas por la experiencia humana en la práctica de las operaciones  $+$  y  $\cdot$ , pueden considerarse definiciones de esas operaciones y junto con otras tres que veremos pueden tomarse como la definición de números enteros.

11) Entre los elementos de  $Z$  existe una relación de igualdad que es

- reflexiva: Para todo  $a$  en  $Z$ ,  $a =$  \_\_\_\_\_
- recíproca (o simétrica): Para todo  $a$  y  $b$  en  $Z$ ,  $a = b \rightarrow$  \_\_\_\_\_
- transitiva: Para todo  $a, b$  y  $c$  en  $Z$ , \_\_\_\_\_

Los elementos que la cumplen se dicen iguales.

---

2. Con estos axiomas basta para demostrar una serie de propiedades que en álgebra elemental se dan como nuevas. Además las propiedades demostradas valen para cualquier dominio de integridad.

a) Distributividad a la derecha:  $(a + b) c =$  \_\_\_\_\_ (aplicar 7, 8, 7 a cada término)

b) Unicidad del cero. Si para todo  $a$  es:  $a + Z = a$  entonces  $Z = 0$

En particular para  $a = 0$  es:

$0 + Z =$  \_\_\_\_\_ hipótesis

$0 =$  \_\_\_\_\_ simétrica

$0 + Z =$  \_\_\_\_\_ por 2

\_\_\_\_\_ = \_\_\_\_\_ transitiva

c) Para todo  $a, b, c$  en  $\mathbb{Z}$ ,  $a + b = a + c \rightarrow b = c$

Demostración:

$$a' + a = 0$$

$$a + a' = 0, \text{ etc 3 y 4}$$

$$a' + (a + b) = a' + (a + c), \text{ con 10 y la hipótesis asociativa.}$$

En el teorema anterior se basa la simplificación de términos en diferentes miembros.

d) Para todo  $a$  hay un solo  $x$  tal que:  $a + x = 0$ .

Demostración: (las demostraciones de unicidad suelen hacerse por el absurdo). Suponemos que  $x, y$  son dos números diferentes y decimos.

$$a + x = a + y$$

$$\underline{\hspace{2cm}} = \underline{\hspace{2cm}}, \text{ por c)}$$

para concluir que  $\underline{\hspace{2cm}}$  QEPD.

e) Para todo  $a, b$  en  $\mathbb{Z}$ , hay un solo  $x$  tal que:  $a + x = b$ .

Demostración:

Para ver que lo hay, hay que poner:

$$x = -a + b$$

Para ver que es único hagamos:

$$a + x = \underline{\hspace{2cm}} \text{ por c), una vez más.}$$

f) Para todo  $a$  en  $\mathbb{Z}$ , se tiene que  $a \cdot 0 = 0 \cdot a = 0$

Demostración:

$$a \cdot a = a \cdot (a + 0), \text{ por 2 y 10}$$

$$\underline{\hspace{2cm}} = a \cdot a + \underline{\hspace{2cm}}, \text{ por 8}$$

$$a \cdot 0 = \underline{\hspace{2cm}}, \text{ por b) 7}$$

g) Si  $a \cdot u = a$  para todo  $a$ , entonces  $u = 1$  (compárese con b).

Demostración:

En particular poniendo  $a = 1$ :

$$1 \cdot u = \underline{\hspace{2cm}}$$

$$u \cdot 1 = \underline{\hspace{2cm}}, 8$$

$$1 \cdot u = u \cdot 1 = 1 = 1 \cdot 1, \text{ transitiva y 6}$$

$$1 \cdot u = 1 \cdot 1, \text{ transitiva}$$

$$\underline{\hspace{2cm}} = \underline{\hspace{2cm}}, \text{ simplificación}$$

h) Si  $a \cdot b = 0$  o bien  $a = 0$  o bien  $b = 0$ .

Demostración:

Sea  $a \neq 0$  y  $b \neq 0$

$a \neq 0$ , por hipótesis

$a \neq 0$ , f) y transitiva

\_\_\_\_\_ = \_\_\_\_\_, simplificación

i) El inverso del inverso de  $a$  es  $a$ .

$-(-a) = a$

$-a + a = 0$ , por 2

$-a + (-(-a)) = \text{_____}$ , 2 aplicada a  $-a$  ó  $-a$

$-a + a = -a + (-(-a))$ , transitiva

\_\_\_\_\_ = \_\_\_\_\_, simplificación

j)  $(-a)b = -ab$

$(a + (-a))b = \text{_____}$ , por 3 y distributiva

\_\_\_\_\_ = \_\_\_\_\_, por f)

$ab + (-ab) = \text{_____}$ , por 2

$ab + (-a)b = \text{_____}$ , transitiva

\_\_\_\_\_ = \_\_\_\_\_, simplificación

k)  $(-a)(-b) = ab$

$(-a)(-b) = -((-b))$ , por j)

\_\_\_\_\_ =  $-(-\text{_____})$ , por j)

\_\_\_\_\_ = \_\_\_\_\_, por i)

l) desarrollar  $(a+b)(c+d)$


m) desarrollar  $(a-b)(c-d)$ , note que  $(a-b)$  es  $a + (-b)$


### 3. Relaciones de orden

Un dominio de integridad es ordenado si se pueden distinguir en él ciertos elementos llamados positivos  $Z^+ = \{..., a, b, c, ...\}$  tales que:

a)  $a \in Z^+$  tal que  $b \in Z^+ \Rightarrow a + b \in Z^+$

$a \in Z^+$  tal que  $b \in Z^+ \Rightarrow a \cdot b \in Z^+$

b) Tricotomía:  $a$  es positivo,  $a$  es cero o bien  $-a$  es positivo.

12) El conjunto  $Z$  es ordenado. ¿lo será el de los elementos  $(a + b)$ , con  $a, b$  enteros?


13) Se define  $a < b$  si y sólo si  $b - a$  es positivo. También se indica  $b > a$ . Por comodidad se define  $a \leq b$  si  $a < b$  ó  $a = b$ . Se indica también  $b \geq a$ .

a)  $b \in Z^+ \leftrightarrow b > 0$

b)  $a < b \wedge b < c \Rightarrow a < c$ , ley transitiva

c)  $a < b \Rightarrow a + c < b + c$

d)  $a < b \Rightarrow a < b + c$ ,  $c$  positivo

e)  $a > 0 \Rightarrow -a < 0$

---

### 4. Principio del buen ordenamiento (del buen orden)

(Ver también en [http://es.wikipedia.org/wiki/Conjunto\\_bien\\_ordenado](http://es.wikipedia.org/wiki/Conjunto_bien_ordenado))

Un conjunto se dice *ordenado* si entre dos cualesquiera de sus elementos se da la relación  $a < b$  ó bien  $a = b$  ó bien  $b < a$ .

El conjunto de los enteros es ordenado.

Un conjunto se dice bien ordenado si todo subconjunto no vacío del mismo tiene un elemento menor que todos los demás (primer elemento).

Agregamos el axioma:

14) El conjunto de los enteros es bien ordenado.

En un conjunto "parcialmente ordenado" (COPO en Español, POSET en Inglés) para algunos elementos  $a, b$  no se cumple ni  $a < b$ , ni  $a = b$ , ni  $b < a$ .

5. Dar ejemplos de conjuntos ordenados pero no bien ordenados. Dar ejemplos de conjuntos parcialmente ordenados.


6. No hay ningún entero entre 0 y 1.

Demostración:

Sea  $0 < c < 1$

Sea  $C = \{\text{todos los } c \text{ tales que } 0 < c < 1\}$

Sea  $m$  el menor de los  $c$  (axioma 14)

Se tiene que  $0 < m < 1$  y por tanto:

$m \cdot m < m$ . Sin embargo,  $m^2$  es un entero mayor que cero pero menor que \_\_\_\_\_.  
Luego es menor que 1. Luego  $m$  no es el menor de los  $c$ .

Este teorema permite ver el siguiente que es la base del principio de inducción.

7. Si un conjunto  $C$  de enteros positivos contiene al 1 y siempre que contenga al  $n$  contiene también al  $n + 1$ , entonces contiene a los enteros positivos.

Dar un argumento intuitivo y decir por que no es una demostración:


Demostración:

Supongamos un  $C$  tal que  $1 \in C$  y Si  $n \in C \rightarrow n+1 \in C$ .

Sea  $C'$  el conjunto de los enteros que no pertenecen a  $C$ .

Supongamos tal  $C'$  no vacío. Por 14) tiene un primer elemento.

Sea ese elemento  $m$ . ¿Puede ser  $m = 1$ ? \_\_\_\_\_. Es decir, entonces es  $m$  es  $| > 1 | = 1 | < 1 |$   
(tache los que no correspondan, cuando entienda las razones).

Además  $m - 1 \in C$  ¿por qué?


Pero entonces  $m - 1 + 1 \in$  \_\_\_\_\_ por \_\_\_\_\_

Entonces \_\_\_\_\_  $\in C$  contra la hipótesis.

Luego  $C'$  debe ser \_\_\_\_\_

## 8. Principio (teorema) de inducción completa.

Sea  $p$  una proposición significativa para los enteros.

Supongamos que:

- $p$  es verdadera para 1
- Si  $p$  es verdadera para  $k$  lo es para  $k + 1$

Entonces  $p$  es verdadera para todo número.

Demostración: basta repetir el teorema anterior considerando el conjunto  $C$  para el cual  $p$  es verdadera.

---

9. Con el principio de inducción completa se pueden demostrar (o definir) en un número finito de pasos propiedades (o definiciones) que requerirían un número infinito de pasos.

Ejemplo:

a) Demostrar que la distributividad a izquierda (axioma 1-8) vale para cualquier  $n$ . Es decir:

$$a(b_1 + b_2 + b_3 + \dots + b_n) = a b_1 + a b_2 + \dots + a b_n$$

Supongamos que vale para  $k$ :

--

Se demuestra que vale para  $k+1$ , pues suman a ambos miembros  $a b_{(k+1)}$


Además vale para  $k = 1$  pues


Luego:


b) Contraejemplo:

“Todo número es igual al siguiente”. Supongamos que  $k = k + 1$  (vale para  $k$ ).

Sumando 1 a ambos lados de esa expresión tenemos

$$k + 1 = (k + 1) + 1, \text{ es decir, resulta válida para } k + 1.$$

Luego vale para todo número.

¿Qué piensa de esta demostración?


#### 10. Otro enunciado del principio de inducción

Sea  $p$  una proposición referente a los enteros positivos.

Si de la suposición que es  $p$  verdadera para todo  $k < m$  resulta que es válida para  $m$  entonces es  $p$  válida para todo entero positivo.

Demostración:

Sea  $S$  el conjunto de los enteros positivos para los cuales  $p$  es falsa.


#### 11- Definamos la potenciación así

$$a^1 = a$$

$$a^{(m+1)} = a^{(m)}a$$

Demostrar que  $a^{(m)} a^{(n)} = a^{(m + n)}$


fin del documento sobre inducción matemática. Licencia Pendiente.