Matemática Discreta I
Clase 1 - Los números enteros

FAMAF / UNC

15 de marzo de 2022

Axiomas de los números enteros

Todos conocemos los *enteros*.

Primero, los “números naturales”

$$1, 2, 3, 4, 5, \ldots$$

Más adelante introducimos el 0 (cero).

Luego, los enteros negativos

$$-1, -2, -3, -4, -5, \ldots$$

- En este curso no nos preocupamos demasiado por el significado lógico y filosófico de estos objetos, pero necesitamos saber las propiedades que se supone que tienen.

- La idea es: si todos parten de las mismas suposiciones entonces todos llegarán a los mismos resultados.
- Estos supuestos son los llamados *axiomas.*
- Aceptamos sin reparo que existe un conjunto de objetos llamados *enteros*.
- El conjunto de enteros se denotará por el símbolo especial $\mathbb{Z}$.
- Las propiedades de $\mathbb{Z}$ serán dadas por una lista de axiomas.
- Un resultado acerca de $\mathbb{Z}$ es válido si se deduce lógicamente de los axiomas.

Empezaremos listando aquellos axiomas que tratan la suma y la multiplicación.

Notación

Sean $a, b \in \mathbb{Z}$ (números enteros)

- $a + b$ denota la suma.
- $a \cdot b$ (o ab o también $a \times b$) el producto de enteros.

El hecho de que $a \cdot b$ y $a + b$ son enteros, es nuestro primer axioma.

En la siguiente lista de axiomas a, b, c denotan enteros arbitrarios, y 0 y 1 denotan enteros especiales que cumplen las propiedades especificadas más abajo.

I1) $a + b$ y $a \cdot b$ pertenecen a $\mathbb{Z}$.

I2) *Conmutatividad.* $a + b = b + a$; $\qquad ab = ba$.

I3) *Asociatividad.* $(a + b) + c = a + (b + c)$; $\qquad (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

I4) *Existencia de elemento neutro.* Existen números $0, 1 \in \mathbb{Z}$ con $0 \neq 1$ tal que $a + 0 = a$; $\qquad a \cdot 1 = a$.

Los axiomas anteriores involucran a la suma y el producto por separado.

El axioma siguiente relaciona el suma y el producto.

I5) *Distributividad.* $a \cdot (b + c) = a \cdot b + a \cdot c$.

También tenemos propiedades de cancelación.

I6) *Existencia del inverso aditivo, también llamado opuesto.* Por cada a en $\mathbb{Z}$ existe un único entero $-a$ en $\mathbb{Z}$ tal que $a + (-a) = 0$.

I7) *Cancelación.* Si a es distinto de 0 y $a \cdot b = a \cdot c$, entonces $b = c$.

- Debido a la ley de asociatividad para la suma axioma (**I3**) $(a+b)+c$ es igual a $a+(b+c)$ y por lo tanto podemos eliminar los paréntesis sin ambigüedad. Es decir, denotamos

$$a+b+c := (a+b)+c = a+(b+c).$$

- De forma análoga, usaremos la notación

$$abc = (ab)c = a(bc).$$

- Debido a la ley de conmutatividad axioma (**I2**), es claro que del axioma (**I4**) se deduce que $0+a=a+0=a$ y $1\cdot a = a\cdot 1 = a$.
- Análogamente, por (**I2**) e (**I6**) obtenemos que $-a+a=a+(-a)=0$.

Una propiedad que debemos mencionar es la siguiente:

Si $a, b, c \in \mathbb{Z}$ y $a = b$, entonces $a + c = b + c$ y $ac = bc$.

Esto se debe a que:

- la suma y el producto son operaciones que devuelven enteros.
- Si $a = b$, entonces el par a, c es igual al par b, c y por lo tanto devuelven la misma suma y el mismo producto.

Esta propiedad *no es un axioma,* sino una mera aplicación de la lógica formal.

Ejemplo

Demostremos que, para todo n entero, el opuesto de $-n$ es n, es decir que

$$-(-n) = n.$$

Demostración

El axioma (**I6**) nos dice que $-(-n)$ es el único número que sumado a $-n$, da cero. Por lo tanto, para demostrar que $-(-n) = n$ basta ver que $(-n) + n = 0$. Esto se cumple puesto que

$$\begin{aligned} (-n) + n &= n + (-n) && \text{axioma } (\mathbf{I2}) \\ &= 0 && \text{axioma } (\mathbf{I6}) \end{aligned}$$

Por lo tanto $(-n) + n = 0$. $\square$

A continuación definimos la resta o sustracción.

Definición

Si $a, b \in \mathbb{Z}$ definimos $a - b$ como la suma de a más el opuesto de b, es decir que $a - b = a + (-b)$ por definición.

Ahora demostremos una propiedad básica de la resta.

Ejemplo

Sean m y n enteros, entonces

$$m - (-n) = m + n.$$

Demostración

Por la definición de sustracción, $m - (-n)$ es la suma $m + (-(-n))$, es decir

$$m - (-n) = m + (-(-n)).$$

Por el ejemplo de la p. **??** sabemos que $-(-n) = n$ y por lo tanto $m - (-n) = m + (-(-n)) = m + n$. □

Ejemplo

Supongamos que existen dos enteros 0 y $0'$ ambos cumpliendo el axioma (**I4**), esto es

$$a + 0 = a, \qquad a + 0' = a$$

para todo a de $\mathbb{Z}$. Entonces $0 = 0'$.

Demostración

$$\begin{aligned} 0 &= 0 + 0' && \text{axioma } (\textbf{I4}) \text{ aplicado a } 0 \text{ y con } 0' \text{ como neutro} \\ &= 0' + 0 && \text{axioma } (\textbf{I2}) \\ &= 0' && \text{axioma } (\textbf{I4}) \text{ aplicado a } 0' \text{ y con } 0 \text{ como neutro.} \end{aligned}$$

□

Observación

Vale el resultado análogo para el producto: el elemento neutro del producto es único.

Ejemplo

Sea $a \in \mathbb{Z}$, entonces

$$a \cdot 0 = 0$$

Demostración

$$\begin{aligned}
a \cdot 0 &= a \cdot (0 + 0) && \text{axioma } (\mathbf{I4}) \\
a \cdot 0 &= a \cdot 0 + a \cdot 0 && \text{axioma } (\mathbf{I5}) \\
a \cdot 0 - a \cdot 0 &= a \cdot 0 + a \cdot 0 - a \cdot 0 && \text{lógica} \\
0 &= a \cdot 0 + 0 && \text{2 veces axioma } (\mathbf{I6}) \\
0 &= a \cdot 0 && \text{axioma } (\mathbf{I4}).
\end{aligned}$$

$\square$

Ejemplo

(Regla de los signos) Veamos que si $a, b \in \mathbb{Z}$ entonces

$$(1) \quad (-a)(-b) = ab, \qquad (2) \quad a(-b) = (-a)b = -(ab).$$

Demostración

(2) Probaremos $a(-b) = -(ab)$.

Para ello, veremos que $a(-b)$ es el inverso aditivo de ab.

Por unicidad del inverso aditivo (axioma **I6**), de deduce que $a(-b) = -(ab)$.

$$
\begin{aligned}
ab + a(-b) &= a(b - b) && \text{axioma } (\mathbf{I5}) \\
&= a \cdot 0 && \text{axioma } (\mathbf{I6}) \\
&= 0 && \text{ejercicio p. } \mathbf{??}.
\end{aligned}
$$

Es complétamente análogo probar $(-a)b = -(ab)$.

(1) Ejercicio.

$\square$