Introducción

En la clase de hoy, empezaremos la construcción del conjunto $\mathbb{Z}$ de los números enteros a partir del conjunto $\mathbb{N}$ de los números naturales.

Construcción de $\mathbb{Z}$

Definimos la relación R en $\mathbb{N} \times \mathbb{N}$ por:

$$(m, n)R(p, q) \Leftrightarrow m + q = n + p$$

para todo $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$.

Teorema 1

R es una relación de equivalencia.

Demostración del Teorema 1

Tenemos que demostrar que R es reflexiva, simétrica y transitiva.

R es reflexiva, ya que para todo $(m, n) \in \mathbb{N}^2$, tenemos que $m + n = n + m$, y por tanto $(m, n)R(m, n)$.

R es simétrica, ya que para todo $(m, n) \in \mathbb{N}^2$, tenemos que:

$$(m, n)R(p, q) \Rightarrow m+q = n+p \Rightarrow q+m = p+n \Rightarrow (p, q)R(m, n).$$

R es transitiva. Supongamos que $(m, n)R(p, q)$ y $(p, q)R(r, s)$. Tenemos que demostrar que $(m, n)R(r, s)$. Como $(m, n)R(p, q)$, deducimos que $m + q = n + p$. Y como $(p, q)R(r, s)$, inferimos que $p + s = q + r$. Por tanto,

$$m + q + p + s = n + p + q + r.$$

Demostración del Teorema 1

Asi pues,

$$m + s = n + r.$$

Con lo cual, $(m, n)R(r, s)$. $\square$

Construcción de $\mathbb{Z}$

Definimos:

$$Z = (\mathbb{N} \times \mathbb{N})/R.$$

Hallemos las clases de equivalencia. Si $(m, n) \in \mathbb{N}^2$, tenemos:

$$\begin{array}{rcl} \overline{(m,n)} & = & \{(x,y) \in \mathbb{N}^2 : (m,n)R(x,y)\} \\ & = & \{(x,y) \in \mathbb{N}^2 : m + y = n + x\} \\ & = & \{(x,y) \in \mathbb{N}^2 : x - y = m - n\} \\ & = & \{(x,y) \in \mathbb{N}^2 : x - y = d\} \end{array}$$

siendo $d = m - n$.

Por ejemplo:

$$\overline{(1,1)} = \{(x,y) \in \mathbb{N}^2 : x - y = 0\} = \{(0,0),(1,1),(2,2),\dots\},$$

$$\overline{(2,1)} = \{(x,y) \in \mathbb{N}^2 : x - y = 1\} = \{(1,0),(2,1),(3,2),\dots\},$$

$$\overline{(1,3)} = \{(x,y) \in \mathbb{N}^2 : x - y = -2\} = \{(1,3),(2,4),(3,5),\dots\}.$$

Identificamos un número entero d con la clase de equivalencia $\{(x,y) \in \mathbb{N}^2 : x - y = d\}$. Por ejemplo, $0 = \overline{(1,1)}$, $1 = \overline{(2,1)}$, $-1 = \overline{(1,2)}$, $-3 = \overline{(2,5)}$, $4 = \overline{(4,0)}$.

Teorema 2

$\{\overline{(m,n)} : (m.n) \in \mathbb{N}^2$ tal que $m = 0$ o $n = 0\} =$ $\{\overline{(0,k)} : k \in \mathbb{N} \setminus \{0\}\} \cup \{\overline{(0,0)}\} \cup \{\overline{(k,0)} : k \in \mathbb{N} \setminus \{0\}\}$ es una buena representación de $\mathbb{Z}$.

Para demostrar el teorema 2, tenemos que probar:

(a) $\{\overline{(m,n)} : (m.n) \in \mathbb{N}^2$ tal que $m = 0$ o $n = 0\} = \mathbb{Z}$.

(b) $\{\overline{(m,n)} : (m.n) \in \mathbb{N}^2$ tal que $m = 0$ o $n = 0\}$ no es redundante.

Demostramos (a), probando las dos inclusiones. Como $\{(m,n) : (m.n) \in \mathbb{N}^2$ tal que $n = 0$ o $m = 0\} \subseteq \mathbb{N} \times \mathbb{N}$, tenemos que

$$\{\overline{(m,n)} : (m,n) \in \mathbb{N}^2 \text{ tal que } m = 0 \text{ o } n = 0\} \subseteq \mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R.$$

Demostración del Teorema 2

Demostramos ahora la otra inclusión, es decir:

$$\mathbb{Z} \subseteq \{\overline{(m,n)} : (m.n) \in \mathbb{N}^2 \text{ tal que } m = 0 \text{ o } n = 0\}.$$

Sea $z \in \mathbb{Z}$. Entonces, $z = \overline{(m,n)}$ para algún $(m,n) \in \mathbb{N}^2$.

Si $m \geq n$, tenemos que $m - n \in \mathbb{N}$. Entonces, como $m + 0 = m - n + n = n + (m - n)$, tenemos que $(m,n)R(m-n,0)$ y por tanto

$z = \overline{(m,n)} =$
$\overline{(m-n,0)} \in \{\overline{(m,n)} : (m.n) \in \mathbb{N}^2$ tal que $m = 0$ o $n = 0\}$.

Y si $m < n$, tenemos que $n - m \in \mathbb{N}$. Entonces, como $m + n - m = n + 0$, tenemos que $(m,n)R(0,n-m)$ y por tanto

$z = \overline{(m,n)} = \overline{(0,n-m)} \in \{\overline{(m,n)} : (m,n) \in \mathbb{N}^2$ tal que $m = 0$ o $n = 0\}$.

Demostramos ahora (b). Para ello, vamos a probar que

Si $(m_1,n_1),(m_2,n_2) \in \{(m,n) : (m,n) \in \mathbb{N}^2$ tal que $m = 0$ o $n = 0\}$ y $\overline{(m_1,n_1)} = \overline{(m_2,n_2)}$, entonces $(m_1,n_1) = (m_2,n_2)$.

Demostración del Teorema 2

Sean $(m_1, n_1), (m_2, n_2) \in \{(m, n) : (m.n) \in \mathbb{N}^2$ tal que $m = 0$ o $n = 0\}$ de manera que $\overline{(m_1, n_1)} = \overline{(m_2, n_2)}$. Como $\overline{(m_1, n_1)} = \overline{(m_2, n_2)}$, tenemos que $m_1 + n_2 = n_1 + m_2$. Distinguimos los dos siguientes casos.

Caso 1. $m_1 > 0$

Se sigue que $n_1 = 0$, y por tanto $m_1 + n_2 = m_2$. Entonces, como $m_1 > 0$, tenemos que $m_2 > 0$, y por tanto $n_2 = 0$ y $m_2 = m_1$. Tenemos entonces

$$(m_1, n_1) = (m_1, 0) = (m_2, 0) = (m_2, n_2).$$

Así pues, $(m_1, n_1) = (m_2, n_2)$.

Caso 2. $m_1 = 0$

Por tanto, $n_2 = n_1 + m_2$. Si $n_2 = 0$, tenemos que $n_1 = m_2 = 0$. Por tanto,

$$(m_1, n_1) = (0, 0) = (m_2, n_2).$$

Y si $n_2 > 0$, entonces $m_2 = 0$, con lo cual $n_2 = n_1$. Por tanto,

$$(m_1, n_1) = (0, n_1) = (0, n_2) = (m_2, n_2).$$

Así pues, $(m_1, n_1) = (m_2, n_2)$. $\square$

Sean $a, b \in \mathbb{Z}$. Pongamos $a = \overline{(m,n)}$ y $b = \overline{(p,q)}$. Definimos entonces

$$a + b = \overline{(m,n)} + \overline{(p,q)} = \overline{(m+p, n+q)}.$$

Intuitivamente, la suma se define de esta manera, porque la clase $\overline{(m,n)}$ representa al entero $m-n$, la clase $\overline{(p,q)}$ representa al entero $p-q$ y
$(m-n) + (p-q) = m - n + p - q = (m+p) - (n+q)$.

Por ejemplo:

$$\overline{(0,2)} + \overline{(-2,0)} = \overline{(-2,2)},$$

$$\overline{(2,3)} + \overline{(-1,4)} = \overline{(1,7)},$$

$$\overline{(5,2)} + \overline{(6,-4)} = \overline{(11,-2)}.$$

Definición de la $+$ en $\mathbb{Z}$

Obsérvese que hemos definido la suma de a y b, a partir de un representante de a y de un representante de b. Tenemos que demostrar entonces que la suma está bien definida, en el sentido de que no depende de los representantes elegidos.

Teorema 3

$+$ está bien definida en $\mathbb{Z}$.

Para demostrar este teorema, supongamos que $\overline{(m,n)} = \overline{(m',n')}$ y $\overline{(p,q)} = \overline{(p',q')}$. Tenemos que demostrar que

$$\overline{(m,n)} + \overline{(p,q)} = \overline{(m',n')} + \overline{(p',q')}.$$

Demostración del Teorema 3

Tenemos que

$$\overline{(m,n)} + \overline{(p,q)} = \overline{(m+p, n+q)},$$

$$\overline{(m',n')} + \overline{(p',q')} = \overline{(m'+p', n'+q')}.$$

Entonces, como

$\overline{(m,n)} + \overline{(p,q)} = \overline{(m',n')} + \overline{(p',q')}$
$\Leftrightarrow \overline{(m+p, n+q)} = \overline{(m'+p', n'+q')}$
$\Leftrightarrow m+p+n'+q' = n+q+m'+p'$, vamos a demostrar que

$$(*) \quad m+p+n'+q' = n+q+m'+p'.$$

Tenemos entonces:

$$\overline{(m,n)} = \overline{(m',n')} \Rightarrow m + n' = n + m',$$

$$\overline{(p,q)} = \overline{(p',q')} \Rightarrow p + q' = q + p'.$$

Por tanto,

$$m+p+n'+q' = m+n'+p+q' = n+m'+q+p' = n+q+m'+p',$$

con lo cual se cumple la condición $(*)$. $\square$

Elementos opuestos

Sea $a \in \mathbb{Z}$. Pongamos $a = \overline{(m,n)}$. Definimos entonces el opuesto de a por

$$-a = \overline{(n,m)}.$$

Demostramos que el opuesto de un elemento está bien definido, es decir, si $a = \overline{(m,n)} = \overline{(m',n')}$, entonces $\overline{(n,m)} = \overline{(n',m')}$. Como $\overline{(m,n)} = \overline{(m',n')}$, tenemos que $m + n' = n + m'$. Por tanto, $m' + n = n' + m$. Así pues, $\overline{(n,m)} = \overline{(n',m')}$.

Teorema 4

Para todo $a, b, c \in \mathbb{Z}$ se cumplen las siguientes propiedades:

(1) Propiedad conmutativa:

$a + b = b + a$

(2) Propiedad asociativa:

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

(3) Existencia del elemento neutro:

$a + \overline{(0, 0)} = a$.

(4) Existencia de elementos opuestos:

$a + (-a) = \overline{(0, 0)}$.

(5) Propiedad cancelativa:

Si $a + c = b + c$ entonces $a = b$.

Demostración del Teorema 4

Demostramos el apartado (1). Pongamos $a = \overline{(m,n)}$ y $b = \overline{(r,s)}$. Tenemos:

$$a + b = \overline{(m,n)} + \overline{(r,s)} = \overline{(m+r, n+s)},$$

$$b + a = \overline{(r,s)} + \overline{(m,n)} = \overline{(r+m, s+n)}.$$

Entonces, como $m + r = r + m$ y $n + s = s + n$ por la propiedad conmutativa en $\mathbb{N}$, tenemos que $a + b = b + a$.

Demostración del Teorema 4

Demostramos el apartado (2). Pongamos $a = \overline{(m,n)}$, $b = \overline{(p,q)}$ y $c = \overline{(r,s)}$. Tenemos:

$$a + b = \overline{(m,n)} + \overline{(p,q)} = \overline{(m+p, n+q)},$$

$$(a+b) + c = \overline{(m+p, n+q)} + \overline{(r,s)} = \overline{((m+p)+r, (n+q)+s)}.$$

Por otra parte, tenemos:

$$b + c = \overline{(p,q)} + \overline{(r,s)} = \overline{(p+r, q+s)},$$

$$a + (b+c) = \overline{(m,n)} + \overline{(p+r, q+s)} = \overline{(m+(p+r), n+(q+s))}.$$

Como la suma es asociativa en $\mathbb{N}$, tenemos que
$(m+p)+r = m+(p+r)$ y $(n+q)+s = n+(q+s)$.

Por tanto, $(a+b)+c = a+(b+c)$.

Demostramos el apartado (3). Pongamos $a = \overline{(m,n)}$. Entonces,

$$a + \overline{(0,0)} = \overline{(m,n)} + \overline{(0,0)} = \overline{(m+0,n+0)} = \overline{(m,n)}.$$

Demostramos ahora el apartado (4). Pongamos $a = \overline{(m,n)}$.
Entonces,

$$a + (-a) = \overline{(m,n)} + \overline{(n,m)} = \overline{(m+n,n+m)} = \overline{(0,0)},$$

ya que $(m+n,n+m)R(0,0)$.

Demostramos por último el apartado (5). Supongamos que $a, b, c \in \mathbb{Z}$ tales que $a + c = b + c$. Tenemos que demostrar que $a = b$. Como $a + c = b + c$, tenemos que $(a + c) + -c = (b + c) + -c$. Ahora, por la propiedad asociativa de la suma en $\mathbb{N}$, obtenemos que

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

Por tanto, aplicando el apartado (4), tenemos que $a + \overline{(0,0)} = b + \overline{(0,0)}$. Entonces, aplicando el apartado (3), obtenemos que $a = b$. $\square$