Introducción

En la clase de hoy, continuaremos con la construcción del conjunto $\mathbb{Z}$ de los números enteros a partir del conjunto $\mathbb{N}$ de los números naturales, que iniciamos en la última clase.

Empezaremos recordando brevemente los conceptos y resultados que vimos en la última clase.

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.

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

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 $\mathbb{Z}$.

Definición de la $+$ en $\mathbb{Z}$

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

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

Teorema 3

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

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 $a = b$.

Definición del producto en $\mathbb{Z}$

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

$$a \cdot b = \overline{(m,n)} \cdot \overline{(p,q)} = \overline{(mp+nq, mq+np)}.$$

Intuitivamente, el producto 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 $(m-n)\cdot(p-q) = (mp+nq) - (mq+np)$, que representa a $\overline{(mp+nq, mq+np)}$.

Por ejemplo, $\overline{(0,3)} \cdot \overline{(4,0)} = \overline{(0\cdot 4 + 3\cdot 0, 0\cdot 0 + 3\cdot 4)} = \overline{(0,12)}$.

Definición del producto en $\mathbb{Z}$

Al igual que con la suma, debemos demostrar que el producto en $\mathbb{Z}$ está bien definido, en el sentido de que no depende de los representantes elegidos.

Teorema 5

$\cdot$ 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

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

Es decir, tenemos que demostrar la siguiente condición:

$$(*) \quad \overline{(mp+nq, mq+np)} = \overline{(m'p'+n'q', m'q'+n'p')}.$$

Demostración del Teorema 5

Como $\overline{(m,n)} = \overline{(m',n')}$, tenemos:

(1) $m + n' = n + m'$.

Y como $\overline{(p,q)} = \overline{(p',q')}$, tenemos:

(2) $p + q' = q + p'$.

Demostración del Teorema 5

Multiplicando por p los dos lados de (1), obtenemos:

(3) $pm + pn' = pm' + pn$.

Y multiplicando por q los dos lados de (1), obtenemos:

(4) $nq + m'q = n'q + mq$.

Ahora, multiplicando por m' los dos lados de (2), obtenemos:

(5) $pm' + q'm' = p'm' + qm'$.

Y multiplicando por n' los dos lados de (2), obtenemos:

(6) $qn' + p'n' = n'q' + n'p$.

Ahora, sumando las partes izquierdas de las condiciones (3)-(6) por un lado, y sumando las partes derechas de (3)-(6), obtenemos:

$pm + pn' + nq + m'q + pm' + q'm' + qn' + p'n' =$
$pm' + pn + n'q + mq + p'm' + qm' + n'q' + n'p.$

Entonces, simplificando esta igualdad, obtenemos que

$$pm + nq + q'm' + p'n' = pn + mq + p'm' + n'q'.$$

Por tanto,

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

Así pues, se cumple la condición $(*)$. $\square$

Propiedades básicas del $\cdot$ en $\mathbb{Z}$

Teorema 6

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

(1) Propiedad conmutativa:

$a \cdot b = b \cdot a$

(2) Propiedad asociativa:

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(3) Existencia del elemento neutro:

$a \cdot \overline{(1,0)} = a$.

(4) Propiedad distributiva:

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

(5) Propiedad cancelativa:

Si $a \cdot c = b \cdot c$ y $c \neq \overline{(0,0)}$, entonces $a = b$.

(6) No hay divisores de cero:

Si $a \cdot b = \overline{(0,0)}$, entonces $a = \overline{(0,0)}$ o $b = \overline{(0,0)}$.

Los apartados (1)-(3) se demuestran de manera análoga a los apartados (1)-(3) del Teorema 4. Demostramos entonces los apartados (4)-(6).

Demostramos (4). Pongamos $a = \overline{(m,n)}$, $b = \overline{(p,q)}$ y $c = \overline{(r,s)}$. Tenemos:

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

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

Por otra parte, tenemos:

$$a \cdot b = \overline{(m,n)} \cdot \overline{(p,q)} = \overline{(mp+nq, mq+np)},$$

$$a \cdot c = \overline{(m,n)} \cdot \overline{(r,s)} = \overline{(mr+ns, ms+nr)},$$

$a \cdot b + a \cdot c = \overline{(mp+nq, mq+np)} + \overline{(mr+ns, ms+nr)} = \overline{(mp+nq+mr+ns, mq+np+ms+nr)}$.

Es decir,

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

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

Demostración del Teorema 6

Demostramos (5). Pongamos $a = \overline{(m,n)}$, $b = \overline{(p,q)}$ y $c = \overline{(r,s)}$. Tenemos:

$$a \cdot c = \overline{(m,n)} \cdot \overline{(r,s)} = \overline{(mr+ns, ms+nr)},$$

$$b \cdot c = \overline{(p,q)} \cdot \overline{(r,s)} = \overline{(pr+qs, ps+qr)}.$$

Entonces, como $a \cdot c = b \cdot c$, tenemos que $mr + ns + ps + qr = ms + nr + pr + qs$. Es decir,

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

Por tanto, $(m+q)(r-s) = (n+p)(r-s)$. Ahora, aplicando la propiedad cancelativa del producto en $\mathbb{N}$, deducimos que $m+q = n+p$. Por tanto, $\overline{(m,n)} = \overline{(p,q)}$, con lo cual $a = b$.

Demostramos ahora (6). Pongamos $a = \overline{(m,n)}$ y $b = \overline{(p,q)}$. Tenemos:

$$a \cdot b = \overline{(m,n)} \cdot \overline{(p,q)} = \overline{(mp+nq, mq+np)}.$$

Entonces, como $a \cdot b = \overline{(0,0)}$, tenemos que $mp + nq = mq + np$. Si $p = q$, tenemos que $b = \overline{(p,p)} = \overline{(0,0)}$, ya que $(p,p)R(0,0)$.

Supongamos entonces que $p \neq q$. Si $q > p$, tenemos que $q - p > 0$. Entonces, como $mp + nq = mq + np$, tenemos que $m(q-p) = n(q-p)$. Ahora, por la propiedad cancelativa del producto en $\mathbb{N}$, deducimos que $m = n$, y por tanto $a = \overline{(m,n)} = \overline{(m,m)} = \overline{(0,0)}$. Y si $p > q$, procediendo de forma análoga, deducimos también que $a = \overline{(0,0)}$. $\square$

Definición del orden en $\mathbb{Z}$

Sean $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$. Definimos entonces

$$\overline{(a,b)} \leq \overline{(c,d)} \Leftrightarrow a+d \leq b+c.$$

Intuitivamente, el orden se define de esta manera, porque la clase $\overline{(a,b)}$ representa al entero $a-b$, la clase $\overline{(c,d)}$ representa al entero $c-d$ y tenemos que $a-b \leq c-d \Leftrightarrow a+d \leq b+c$.

En el siguiente teorema, demostramos que el orden está bien definido, es decir, no depende de los representantes elegidos.

Teorema 7

$\leq$ está bien definido en $\mathbb{Z}$.

Supongamos que $\overline{(a,b)} = \overline{(a',b')}$ y $\overline{(c,d)} = \overline{(c',d')}$. Y supongamos que $\overline{(a,b)} \leq \overline{(c,d)}$. Tenemos que demostrar que $\overline{(a',b')} \leq \overline{(c',d')}$.

Tenemos:

$$\overline{(a,b)} = \overline{(a',b')} \Rightarrow a + b' = b + a',$$

$$\overline{(c,d)} = \overline{(c',d')} \Rightarrow c + d' = d + c'.$$

Entonces:

$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a + d \leq b + c \Rightarrow$
$a + d + b + a' + c + d' \leq b + c + a + b' + d + c'$

Observamos que a, b, c y d aparecen en los dos lados de la última desigualdad, y por tanto se pueden eliminar.

Por consiguiente, tenemos que $a' + d' \leq b' + c'$. Así pues, $\overline{(a',b')} \leq \overline{(c',d')}$. $\square$

El orden en $\mathbb{Z}$

Teorema 8

$\leq$ es un orden total en $\mathbb{Z}$.

$\leq$ es reflexiva, ya que para todo $\overline{(a,b)} \in \mathbb{Z}$, $a+b=b+a$, y por tanto $\overline{(a,b)} \leq \overline{(a,b)}$.

$\leq$ es antisimétrica. Para demostrarlo, supongamos que $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$ tales que $\overline{(a,b)} \leq \overline{(c,d)}$ y $\overline{(c,d)} \leq \overline{(a,b)}$. Tenemos que probar que $\overline{(a,b)} = \overline{(c,d)}$.Tenemos entonces:

$$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a+d \leq b+c,$$

$$\overline{(c,d)} \leq \overline{(a,b)} \Rightarrow c+b \leq d+a.$$

Como la relación de orden en $\mathbb{N}$ es antisimétrica, deducimos que $a+d=b+c$, y por tanto $\overline{(a,b)} = \overline{(c,d)}$.

$\leq$ es transitiva. Para demostrarlo, supongamos que $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{Z}$ tales que $\overline{(a,b)} \leq \overline{(c,d)}$ y $\overline{(c,d)} \leq \overline{(e,f)}$. Tenemos que probar que $\overline{(a,b)} \leq \overline{(e,f)}$.Tenemos entonces:

$$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a+d \leq b+c.$$

$$\overline{(c,d)} \leq \overline{(e,f)} \Rightarrow c+f \leq d+e.$$

Por tanto,

$$a+d+c+f \leq b+c+d+e.$$

Simplificando esta desigualdad, obtenemos que $a+f \leq b+e$, con lo cual tenemos que $\overline{(a,b)} \leq \overline{(e,f)}$.

El orden en $\mathbb{Z}$

$\leq$ es total. Para demostrarlo, supongamos que $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$. Tenemos que demostrar que $\overline{(a,b)} \leq \overline{(c,d)}$ o $\overline{(c,d)} \leq \overline{(a,b)}$. Como sabemos que el orden en $\mathbb{N}$ es total, tenemos que $a+d \leq b+c$ o $b+c \leq a+d$.

Si $a+d \leq b+c$, entonces $\overline{(a,b)} \leq \overline{(c,d)}$. Y si $b+c \leq a+d$, entonces $\overline{(c,d)} \leq \overline{(a,b)}$.

Por tanto, $\leq$ es total. $\square$

A continuación, vamos a demostrar que dentro de $\mathbb{Z}$ tenemos una copia de $\mathbb{N}$ que se comporta correctament con la suma, el producto, los elementos neutros de la suma y el producto y también con el orden.

Una copia de $\mathbb{N}$ en $\mathbb{Z}$

Teorema 9

Sea $\sigma : \mathbb{N} \longrightarrow \mathbb{Z}$ definida por $\sigma(n) = \overline{(n, 0)}$ para todo $n \in \mathbb{N}$. Se tiene entonces:

(1) σ es una aplicación inyectiva de $\mathbb{N}$ en $\mathbb{Z}$.

(2) σ preserva la suma, es decir, $\sigma(m + n) = \sigma(m) + \sigma(n)$ para todo $m, n \in \mathbb{N}$.

(3) σ preserva el producto, es decir, $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$ para todo $m, n \in \mathbb{N}$.

(4) $\sigma(0) = \overline{(0, 0)}$.

(5) $\sigma(1) = \overline{(1, 0)}$.

(6) Para todo $m, n \in \mathbb{N}$,

$$m \leq n \Leftrightarrow \sigma(m) \leq \sigma(n).$$

Demostramos el apartado (1). Es claro que σ es una aplicación, porque está definida para todo elemento de $\mathbb{N}$. Para probar que σ es inyectiva, supongamos que m y n son números naturales distintos. Por tanto $m + 0 \neq n + 0$, con lo cual $(m, 0) \not R (n, 0)$.Tenemos entonces:

$$\sigma(m) = \overline{(m, 0)} \neq \overline{(n, 0)} = \sigma(n).$$

Demostramos (2). Para todo $m, n \in \mathbb{N}$ tenemos:

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

Demostramos (3). Para todo $m, n \in \mathbb{N}$ tenemos:
$\sigma(mn) = \overline{(mn, 0)} = \overline{(mn + 0 \cdot 0, m \cdot 0 + 0 \cdot n)} = \overline{(m, 0)} \cdot \overline{(n, 0)} = \sigma(m) \cdot \sigma(n).$

Los apartados (4) y (5) son inmediatos, por la definición de σ.

Demostramos entonces el apartado (6). Para todo $m, n \in \mathbb{N}$ tenemos:

$$\sigma(m) \leq \sigma(n) \Leftrightarrow \overline{(m,0)} \leq \overline{(n,0)} \Leftrightarrow m+0 \leq n+0 \Leftrightarrow m \leq n.$$

Por tanto,

$$m \leq n \Leftrightarrow \sigma(m) \leq \sigma(n). \quad \square$$