Producto y orden en $\mathbb{Z}$

Ana Ofelia Negrete Fernández

14 de julio de 2021

1. Introducción

El texto de este día cubrirá:

1. Solución de dos ejercicios que se dejaron de tarea en la entrega pasada (revisar link para consultarla).
2. Introducción al producto en $\mathbb{Z}$.
3. Orden en los enteros.

2. Acerca de la existencia del neutro e inverso aditivo en Z

En link, se dejó de tarea demostrar que $(\mathbb{Z}, \widehat{+})$ es un grupo abeliano. Aquéllo salía de la necesidad de mostrar las propiedades con que los números enteros operan bajo la suma, esas mismas que usamos para hacer cuentas básicas. Para hacer tal prueba, era necesario usar una nueva y muy rimbombante definición de entero y otra de suma en los enteros.

Ahora demostraremos que existe un neutro aditivo en $\mathbb{Z}$. Es decir, queremos ver que:

$\exists\ \overline{0} \in \mathbb{Z}\ \forall r \in \mathbb{Z}\ \left(r + \overline{0} = \overline{0}\right)$.

Antes escribir la prueba, sería bueno determinar quién es un buen candidato para ser el neutro aditivo en $\mathbb{Z}$.

Sea $r = [(a, b)]$. La notación $[(a, b)]$ abrevia el hecho de que $a = b + x$, para $a, b, x \in \mathbb{N}$ (ver la entrada de blog anterior).

Queremos sumarle a r algo que lo deje exactamente igual. Como existe el neutro aditivo en $\mathbb{N}$, se antoja que $(a + p) = (b + q) + x$ implique que $p = 0$ y $q = 0$. Así, $[(a + p, b + q)] = [(a + 0, b + 0)] = [(a, b)]\ \widehat{+}\ [(0, 0)]$.

Ahora sí, escribamos bien la demostración.

Dem.- Sea $r = [(a, b)]$, y propongamos $\overline{0} = [(0, 0)]$.

$$\begin{aligned}
[(a,b)]\ \widehat{+}\ [(0,0)] &= [(a+0, b+0)] && \text{(definición de suma en } \mathbb{Z}\text{)} \\
&= [(a,b)] && \text{(neutro aditivo en } \mathbb{N}\text{)}
\end{aligned}$$

□

Usar $[(0, 0)]$ en la demostración anterior se ocurre muy naturalmente. Sin embargo, recordemos que $[(0, 0)]$ se está refiriendo a toda una colección de números; a saber, todos los $a, b \in \mathbb{N}$ para los que en la ecuación $a = b + x$, se cumpla que $x = 0$.

En efecto,

$$\begin{aligned} [(0,0)] &\implies 0 = 0 + x \\ &\implies x = 0 \end{aligned}$$

Luego,

$$\begin{aligned} 0 &= 0 + x \\ k + 0 &= k + 0 + x \\ k &= k + x \qquad\qquad \text{(neutro aditivo en } \mathbb{N}) \end{aligned}$$

Así,

$$0 = k - k = x \qquad \forall k \in \mathbb{N}.$$

Es decir, $[(0,0)] = [(k,k)]$.

Además,

Proposición. El neutro aditivo en $\mathbb{Z}$ es único.

Dem.- Queremos demostrar que sólo hay un neutro aditivo. Podemos entonces suponer que hay otro que es distinto de $\overline{0}$ y ver qué sucede.

Sea $r = [(a,b)] \in \mathbb{Z}$. Y sea $[(e,f)]$ un neutro aditivo en $\mathbb{Z}$. Entonces

$$[(a,b)] \ \widehat{+} \ [(e,f)] = [(a+e, b+f)] = [(a,b)].$$

Como el neutro aditivo es único en $\mathbb{N}$, entonces $a + e = a \implies e = 0$. Y $b + f = b \implies f = 0$.

$$\therefore \ [(e,f)] = [(0,0)].$$

$\square$

Ahora demostraremos que, para cada entero existe su inverso aditivo. Primero se nos tiene que ocurrir a quién proponer como inverso. Muy fácil: ya que la suma de dos números naturales también es un número natural, podemos elegir $k = a + b = b + a$.

Proposición. $\forall \ r \in \mathbb{Z} \ \exists \ -r \in \mathbb{Z} \ \left(\ r \ \widehat{+} \ (-r) = \overline{0} \ \right)$.

Dem.- Sea $r = [(a,b)]$, y propongamos $-r = [(b,a)]$. Entonces,

$$\begin{aligned} [(a,b)] \ \widehat{+} \ [(b,a)] &= [(a+b, b+a)] \\ &= [(k,k)] \\ &= [(0,0)] \end{aligned}$$

$\square$

3. El producto en $\mathbb{Z}$

Mencionábamos en nuestra previa entrada de blog que en $\mathbb{Z}$ hay una suma y un producto, y que $(\mathbb{Z}, \widehat{+}, \star)$ es dominio entero. No habíamos antes dado la definición del producto en $\mathbb{Z}$:

Definición. El **producto** en $\mathbb{Z}$ es la función

$$\star : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$\text{tal que} \qquad [(a,b)] \star [(c,d)] = [(ac+bd, ad+bc)],$$

donde la multiplicación $[(a,b)] \star [(c,d)]$ equivaldrá a que, para $a = b+x$, $c = d+y$, se tendrá que $[(ac+bd, ad+bd)]$ representa a la ecuación con solución xy,

$$ac + bd = ad + bc + xy.$$

Ahora habría que demostrar que el producto en $\mathbb{Z}$ está bien definido; es decir, es el mismo independientemente de los representantes que se elijan para realizar la multiplicación.

Proposición. El producto en $\mathbb{Z}$ está bien definido.

Dem.- Sean $[(a,b)] = [(e,f)]$ y $[(c,d)] = [(g,h)]$, para $[(a,b)], [(c,d)] \in \mathbb{Z}$.

Como $(a,b) \sim (e,f)$, entonces

$$a + f = b + e.$$

También, $(c,d) \sim (g,h)$, implica que

$$c + h = d + g.$$

Usando la definición de producto de dos enteros, se tiene por un lado que

$$[(a,b)] \star [(c,d)] = [(ac+bd, ad+bc)].$$

Por otro lado, tenemos

$$[(e,f)] \star [(g,h)] = [(eg+fh, eh+fg)].$$

Debemos demostrar que $[(ac+bd, ad+bc)] = [(eg+fh, eh+fg)]$. Es decir, que como ambos números serán iguales, estarán en la misma clase de equivalencia, por lo que se cumplirá

$$(ac+bd) + (eh+fg) = (ad+bd) + (eg+fh).$$

La hipótesis es que $(a,b) \sim (e,f)$ y $(c,d) \sim (g,h)$. Así, multipliquemos

$$\begin{aligned}(a+f)(c+h) &= (b+e)(d+g)\\ ac+ah+fc+fh &= bd+bg+ed+eg.\end{aligned}$$

Sumamos $bd + fh$ en ambos lados de la ecuación y usando nuevamente las hipótesis, obtenemos lo que queremos:

$$\begin{aligned}(bd+fh)+ac+ah+fc+fh &= (bd+fh)+bd+bg+ed+eg\\ (ac+bd)+h(a+f)+f(c+h) &= b(d+g)+d(b+e)+(eg+fh)\\ (ac+bd)+h(b+e)+f(d+g) &= b(c+h)+d(a+f)+(eg+fh)\\ (ac+bd+eh+fg)+hb+df &= (bc+ad+eg+fh)+hb+df\\ ac+bd+eh+fg &= bc+ad+eg+fh.\end{aligned}$$

$\square$

Ya que hemos definido el producto en los enteros, se te quedaría de tarea mostrar las propiedades de que éste es asociativo, conmutativo, existe un neutro multiplicativo y se cumplen las leyes distributivas.

4. El orden en $\mathbb{Z}$

En el apartado de números naturales que escribió Roberto, ya se vieron definiciones y resultados para el orden en $\mathbb{N}$. En particular, definimos para a y b naturales,

$$a < b \iff \exists\ k \in \mathbb{N}\backslash\{0\} \text{ tal que } a + k = b. \tag{1}$$

De aquí que, $[(a, b)] \in \mathbb{Z}$ implica que $b < a$. Luego, $[(b, a)] \in \mathbb{Z}$ implica que $a < b$.

Ya sabemos pues, que, si a y b son números naturales, entonces pasa una y sólo una de las siguientes tres opciones:

$$(a < b) \ \vee \ (a = b) \ \vee \ (b < a). \tag{2}$$

De esto que si $a \neq b$, necesariamente se tendrá $[(a, b)] \neq [(b, a)]$. Y si $a = b$, entonces $[(a, b)] = [(0, 0)]$.

Y a partir de esta intuición definiríamos el orden en $\mathbb{Z}$ (que ya sabemos, en $\mathbb{Z}$ debieran figurar números positivos, números negativos y el cero): Primero nos tomamos $a, b \in \mathbb{N}$. Si $a \neq b$, entonces $[(a, b)]$ será positivo o $[(b, a)]$ será positivo (sólo uno de los dos será positivo, y esto es consecuencia de (2)). En otro caso, $a = b$, lo que nos llevará a la clase del $\overline{0} = [(0, 0)]$, necesariamente.

Basta entonces tomar en consideración los puntos anteriores y definir lo que será un número positivo en $\mathbb{Z}$, para determinar lo que será el orden en $\mathbb{Z}$.

Definición. Sea $[(a, b)] \in \mathbb{Z}$. Definimos la clase de los enteros positivos, denotado $\mathbb{Z}^+$, como sigue:

$$[(a, b)] \in \mathbb{Z}^+ \quad \iff \quad a > b.$$

Proposición. Para cada $z \in \mathbb{Z}$ sucede una y sólo una de las siguientes proposiciones:

1. $[(a, b)] \in \mathbb{Z}^+$,
2. $[(a, b)] = [(0, 0)]$,
3. $-[(a, b)] = [(b, a)] \in \mathbb{Z}^+$.

La demostración de este hecho ya la hice en los párrafos anteriores, sólo que de manera un poquito informal. Si no la entendiste, intenta tú mism@ realizarla y escribirla.

Finalmente, definimos el orden en $\mathbb{Z}$ como sigue:

Definición. Definimos la relación binaria $<^*$ en $\mathbb{Z}$ por

$$[(c, d)] <^* [(a, b)] \text{ si y sólo si } [(a, b)] \ \widehat{+} \ (-[(c, d)]) \in \mathbb{Z}^+.$$

5. Ejercicios

1. Demostrar que el producto en $\mathbb{Z}$ es asociativo, conmutativo, existe el neutro multiplicativo, y se cumplen las leyes distributivas.

2. ¿Existe un inverso multiplicativo en $\mathbb{Z}$? Si, No y por qué.
3. Demuestra la tricotomía de $\mathbb{Z}$.