Propiedades del producto en $\mathbb{Z}$.

Ana Ofelia Negrete Fernández

16 de julio de 2021

1. Introducción

En esta entrada de blog demostraremos algunas propiedades del producto en $\mathbb{Z}$.

Recordemos algunas de ellas. El producto en $\mathbb{Z}$:

- Está bien definido.
- Es conmutativo.
- Es asociativo.
- Tiene neutro.
- Los únicos elementos que tienen inverso multiplicativo son 1 y -1.
- El producto se distribuye sobre la suma.
- Se pueden cancelar factores distintos de cero.
- Producto de positivos es positivo.
- La multiplicación por un positivo respeta el orden.
- La multiplicación por un negativo (es decir, el inverso aditico de un positivo) invierte el orden.

Algunas de estas propiedades, como la conmutatividad, asociatividad, existencia del neutro y distributividad, son aquéllas que determinan (junto con las propiedades de la suma) que $(\mathbb{Z}, \widehat{+}, \star)$ sea un anillo conmutativo con unitario. El resto, son propiedades adicionales, pero también relevantes, por lo que sería bueno demostrarlas.

2. Demostración de las propiedades del producto en $\mathbb{Z}$.

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

  Ya se resolvió este inciso cuando se definió el producto en $\mathbb{Z}$.

- **El producto en $\mathbb{Z}$ es conmutativo.** Queremos ver que $r \star s = s \star r \quad \forall\ r, s \in \mathbb{Z}$. Sean $r = [(a, b)]$ y $s = [(c, d)]$.

$$\begin{aligned} [(a,b)] \star [(c,d)] &= [(ac + bd, ad + bc)] && \text{(definición de producto en } \mathbb{Z}) \\ &= [(ca + db, cb + da)] && \text{(conmutatividad en } \mathbb{N}) \\ &= [(c,d)] \star [(a,b)]. && \text{(definición de producto en } \mathbb{Z}) \end{aligned}$$

□

- **El producto en $\mathbb{Z}$ es asociativo.** Queremos ver que $(r \star s) \star t = r \star (s \star t) \quad \forall\ r, s, t \in \mathbb{Z}$. Sean $r = [(a, b)]$, $s = [(c, d)]$ y $t = [(e, f)]$. Usando la definición de producto en $\mathbb{Z}$, y ley distributiva en $\mathbb{N}$ obtenemos lo que queremos:

$$\begin{aligned}(r \star s) \star t &= [(ac+bd, ad+bc)] \star [(e,f)] \\ &= [((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e)] \\ &= [(ace + bde + adf + bcf, acf + bdf + ade + bce)] \\ &= [(b(cf+de) + a(ce+df), a(cf+de) + b(ce+df))] \\ &= [(a,b)] \star [(ce+df, cf+de)] = r \star (s \star t).\end{aligned}$$

□

- **El producto en $\mathbb{Z}$ tiene neutro multiplicativo.** Queremos ver que existe un elemento tal que $r \star \alpha = r \quad \forall\ r \in \mathbb{Z}$. Notamos que $\alpha = [(1,0)]$:

$$\begin{aligned}[(a,b)] &= [(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)] \\ &= [(a,b)] \star [(1,0)].\end{aligned}$$

□

- **Los únicos elementos que tienen inverso multiplicativo son 1 y -1.**

  Antes de comenzar esta demostración valdría la pena ver que en efecto, 1 y -1 tienen inverso multiplicativo:

$$\begin{aligned}1 \star 1 = [(1,0)] \star [(1,0)] &= [(1 \cdot 1 + 0 \cdot 0, 1 \cdot 0 + 0 \cdot 1)] \\ &= [(1,0)] = 1.\end{aligned}$$

  De este modo, 1 es su propio inverso multiplicativo. Análogamente, el -1 es su propio inverso multiplicativo:

$$\begin{aligned}(-1) \star (-1) = [(0,1)] \star [(0,1)] &= [(0 \cdot 0 + 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0)] \\ &= [(1,0)] = 1.\end{aligned}$$

  Ahora sí, veamos que, si $[(a,b)]$ fuera un entero con inverso multiplicativo $[(c,d)]$, necesariamente obtendremos $[(a,b)] = [(c,d)] = 1$, o $[(a,b)] = [(c,d)] = -1$:

$$\begin{aligned}&[(a,b)] \star [(c,d)] \quad = [(1,0)] \\ \implies \quad &[(ac+bd, ad+bc)] = [(1,0)] \\ \implies \quad &\begin{cases} ac + bd = 1 \\ ad + bc = 0. \end{cases}\end{aligned}$$

  De que $ac + bd = 1$, tenemos que $ac = 1 - bd$. Como $ac \in \mathbb{N}$, entonces $bd \in \{0,1\}$, pues sólo así, $1 - bd \in \mathbb{N}$. De esto emergen dos casos:

  a) $\Big(bd = 1 \ \wedge \ ac = 0\Big)$, de donde se obtiene que $bd = 1 \implies b = 1$, $d = 1$. Y $ac = 0 \implies a = 0 \quad$ ó $\quad c = 0$.

  Ya que $b = d = 1$, sustituyendo en $ad + bc = 0$ tenemos que $a \cdot 1 + 1 \cdot c = a + c = 0$. Y como $a = 0$ ó $c = 0$, entonces $0 + c = 0$ ó $a + 0 = 0$. Conclusión, $a = c = 0$. Así, para este inciso, $[(a,b)] = [(c,d)] = [(0,1)] = -1$.

b) $\Big(bd = 0 \ \wedge \ ac = 1\Big)$, de donde se obtiene que $bd = 0 \implies b = 0$ ó $d = 0$. Y $ac = 1 \implies a = 1$, $c = 1$.

Ya que $a = c = 1$, sustituyendo en $ad + bc = 0$ tenemos que $1 \cdot d + b \cdot 1 = d + b = 0$. Y como $b = 0$ ó $d = 0$, entonces $d + 0 = 0$ ó $0 + b = 0$. Conclusión, $d = b = 0$. Así, para este inciso, $[(a, b)] = [(c, d)] = [(1, 0)] = 1$.

□

- **El producto se distribuye sobre la suma.**

  Aquí hay que notar que hay dos leyes distributivas.

  Demostremos que $r \star (s + t) = (r \star s) \ \widehat{+} \ (r \star t) \quad \forall \ r, s, t \in \mathbb{Z}$. Sean $r = [(a, b)]$, $s = [(c, d)]$, $t = [(e, f)]$ enteros cualquiera. Entonces, usando la definición de producto en $\mathbb{Z}$, distributividad y asociatividad en $\mathbb{N}$ y la definición de suma en $\mathbb{Z}$ tenemos que:

$$\begin{aligned} r \star (s \ \widehat{+} \ t) &= [(a, b)] \star [(c + e, d + f)] \\ &= [(a(c + e) + b(d + f), a(d + f) + b(c + e))] \\ &= [(ac + ae + bd + bf, ad + af + bc + be)] \\ &= [((ac + bd) + (ae + bf), (ad + bc) + (af + be))] \\ &= [(ac + bd, ad + bc)] \ \widehat{+} \ [(ae + bf, af + be)] \\ &= (r \star s) \ \widehat{+} \ (r \star t). \end{aligned}$$

□

  Ya que la demostración de la otra ley distributiva es análoga, se deja como tarea moral.

- **Se pueden cancelar factores distintos de cero.**

  Probaremos que $\Big(r \star s = r \star t\Big) \implies s = t \quad \forall \ r, s, t \in \mathbb{Z}$. Sean $r = [(a, b)]$, $s = [(c, d)]$ y $[(e, f)]$. Tenemos que:

$$\begin{aligned} & [(a, b)] \star [(c, d)] && = [(a, b)] \star [(e, f)] \\ \implies \quad & [(ac + bd, ad + bc)] && = [(ae + bf, af + be)] \\ \implies \quad & (ac + bd) + (af + be) && = (ad + bc) + (ae + bf) \\ \implies \quad & a(c + f) + b(d + e) && = a(d + e) + b(c + f) \end{aligned}$$

  Supongamos que $a \neq b$. Entonces $a(c + f) - b(c + f) \in \mathbb{N}$ y $a(d + e) - b(d + e) \in \mathbb{N}$. Así,

$$\begin{aligned} & a(c + f) + b(d + e) && = a(d + e) + b(c + f) \\ \implies \quad & a(c + f) - b(c + f) && = a(d + e) - b(d + e) \\ \implies \quad & (a - b)(c + f) && = (a - b)(d + e) \\ \implies \quad & c + f && = d + e \end{aligned}$$

  De lo último se concluye que $(c, d) \sim (e, f)$. Es decir, $[(c, d)] = [(e, f)]$, que es lo que queríamos.

- **Producto de positivos es positivo.** Sean $r = [(a, b)]$ y $s = [(c, d)]$, con $r, s \in \mathbb{Z}^+$. Queremos ver que $r \star s \in \mathbb{Z}^+$.

  Ya que $r = [(a, b)] \in \mathbb{Z}^+$, entonces $a > b$, de la definición de entero positivo. Asímismo, como $s = [(c, d)] \in \mathbb{Z}^+$, tenemos que $c > d$.

  De este modo, $a > b$ y $c - d > 0$. Por lo tanto, $a(c - d) > b(c - d)$. Así, haciendo multiplicaciones y reagrupando, $ac + bd - (ad + bc) > 0$. Lo que implica $ac + bd > ad + bc$. De lo que finalmente se concluye que $[(ac + bd, ad + bc)] = [(a, b)] \star [(c, d)] \in \mathbb{Z}^+$.

□

- **La multiplicación por un positivo respeta el orden.**

  Este inciso se deja de tarea.

- **La multiplicación por un negativo invierte el orden.**

  Este inciso también queda como ejercicio al lector.