Lectura 0: Construcción de los números enteros

0.1. Los enteros como conjuntos

La historia cuenta que el matemático Prusiano Leopold Kronecker afirmó:

«Los números enteros fueron hechos por dios, todo lo demás es obra del hombre».

Esta postura logró influenciar el desarrollo de la matemática hasta nuestros días y jugó un importante rol en el establecimiento de los fundamentos para toda la matemática. Sin embargo, el desarrollo de la teoría de conjuntos, impuso un ligero cambio sobre este postulado, de alguna forma podríamos afirmar que los sucesores de Kronecker reformaron su posición para establecer lo siguiente:

«Los números naturales fueron hechos por dios, todo lo demás es obra del hombre».

En esta sección exploraremos el argumento que usaron éstos para garantizar que son sólo los naturales los únicos números que necesitamos conocer para construir todos los otros, en particular como podemos extender bajo algunas construcciones sobre la teoría de conjuntos, los números naturales y así encontrar un conjunto que presenta todas las características que reconocemos de los enteros. Asumiremos para conseguir esto, la existencia de los números naturales y su principales propiedades.

Comencemos explorando una de las deficiencias que conocemos de los números naturales:

La existencia de inversos para la suma. Sabemos que para cualesquiera dos números naturales m y n, si $m \leq n$ podemos encontrar un tercer número natural k que resulta el único que satisface $m + k = n$; este número era el candidato ideal para darle sentido a la expresión $n - m$. Lo anterior afirma que la existencia de la "resta" de dos naturales está condicionada a la pareja de elementos que tomamos y como éstos se comparan. Por ejemplo, como $3 > 1$ y $1 + 2 = 3$, la expresión $3 - 1$ equivale al número 2; basta invertir la operación para notar que $1 - 3$ carece en absoluto de sentido al ser imposible encontrar un número natural k de forma que $3 + k = 1$. ¿Cómo podemos resolver esto?

El problema reside en identificar que la operación que intentamos "extender" involucra siempre un par de números y el orden en que éstos se presenten es relevante. Podemos entonces pensar en escribir $1 - 3$ como la pareja ordenada $(1, 3)$, consiguiendo remover la ambigüedad que existe en la expresión original. Tenemos que notar que hemos conseguido aproximar una operación que no conocemos como parejas ordenadas y que, como es el caso en las parejas ordenadas, $(1, 3)$ y $(3, 1)$ son objetos distintos y representan expresiones distintas. De esta forma representaremos "la diferencia de dos naturales" como un elemento de $\mathbb{N} \times \mathbb{N}$. Debemos ahora considerar si esto es suficiente.

A pesar de lo sencillo que pueda parecernos lo anterior, contiene una propiedad indeseable, en general las diferencias están representadas por más de una pareja. Por ejemplo, $(3, 1)$ debería

resultar ser igual a $(2,0)$ o $(4,2)$ pero todas las parejas mencionadas son distintas. No debemos caer derrotados todavía, estas parejas guardan una poderosa relación. Comencemos preguntando sobre los casos en los que la diferencia tiene sentido en los naturales, para esto supongamos $n \leq m$, entonces la diferencia está representada por la pareja (m,n), si cualquier otra pareja (a,b) con $b \leq a$ representa a la misma diferencia, debemos tener

$$m - n = a - b.$$

Esta es precisamente la propiedad que buscamos para asociar parejas, sin embargo tiene la peculiaridad que depende de la existencia de la diferencia en los naturales. De nueva cuenta no todo está perdido, observemos que la expresión que hemos encontrado puede ser reescrita como

$$m + b = a + n,$$

de hecho es posible probar que son equivalentes (ejercicio). Esta segunda expresión no parece depender de alguna propiedad en particular de las parejas involucradas, por ejemplo $(1,3)$ y $(2,4)$ representarían la misma diferencia en el sentido que satisfacen la igualdad anterior. De hecho, esta interpretación no ofrece resistencia alguna: Son parejas ordenadas de naturales que satisfacen una igualdad que involucra solamente a la suma. Esta idea general es la que detona la construcción de un sistema de números más amplio. Comenzaremos precisando las ideas contenidas en estos párrafos.

Definición 0.1. Sean (m,n) y (a,b) parejas de números naturales, i.e., elementos del conjunto $\mathbb{N} \times \mathbb{N}$. Diremos que (m,n) es equivalente con (a,b), en símbolos escribiremos $(m,n) \sim (a,b)$, si

$$m + b = n + a.$$

No es una coincidencia que se llamará equivalente a relación involucrada, de hecho el nombre sugiere un resultado que debe parecer natural. La prueba del siguiente teorema se deja como ejercicio.

Teorema 0.1. *La relación $\sim$ es de equivalencia en $\mathbb{N} \times \mathbb{N}$.*

Como discutimos en los párrafos anteriores, el conjunto $\mathbb{N} \times \mathbb{N}$ contiene muchos más elementos de los que necesitamos, sin embargo, hemos logrado definir una relación de equivalencia lo que nos permitirá reducir el conjunto en cuestión a la medida adecuada usando sus clases de equivalencia. Como exploración podemos preguntarnos acerca de la clase de equivalencia de $(3,0)$. Para calcularla debemos encontrar todas las parejas (m,n) relacionadas con este elemento, i.e., $(3,0) \sim (m,n)$. En otras palabras

$$3 + n = m,$$

por lo que la clase de equivalencia resulta simplemente ser

$$[(3,0)] = \{(3,0),(4,1),(5,2),\ldots,(k+3,k),\ldots\}.$$

De igual forma podemos encontrar la clase de equivalencia de la pareja $(1,2)$ la cual debe estar formada por todos los elementos (m,n) tales que $m+1 = n$; en otras palabras

$$[(1,2)] = \{(0,1),(1,2),\ldots,(k,k+1),\ldots\}.$$

Estos ejemplos (y algunos ejercicios disponibles) ponen de manifiesto algo que no parece evidente a simple vista. En cada clase de equivalencia parece existir un elemento que la describe de manera muy natural, aquel que incluye al menos un cero en alguno de sus componentes. Esto es precisamente lo que afirma el siguiente teorema.

Teorema 0.2. *Cada clase de equivalencia $[(m,n)]$ contiene al menos un elemento tiene una coordenada cero. En otras palabras, para cada pareja (m,n) existe un natural k de forma que $(m,n) \sim (k,0)$ o $(m,n) \sim (0,k)$.*

Demostración. Sabemos que en los naturales podemos tener solamente dos casos separados: o $m \leq n$ o $n < m$. Supongamos entonces que $m \leq n$, en ese caso debe existir k de forma que $m + k = n$ de forma que podemos simplemente escribir

$$m + k = n + 0,$$

lo que por definición implica que $(m,n) \sim (0,k)$. Por otro lado si suponemos que $n < m$ eso implica que existe un natural k distinto de 0 de forma que $n + k = m$ por lo que podemos escribir

$$m + 0 = n + k$$

por lo que $(m,n) \sim (k,0)$. Esto es precisamente lo que deseamos probar. ■

El resultado anterior aunque en apariencia inocente, es de vital importancia, pues nos permite proveer una lista de todas las clases de equivalencia al todas contener al menos un elemento con algún componente 0. De esta forma, las clases de equivalencia que buscamos se pueden listar como

$$\ldots, [(0,2)], [(0,1)], [(0,0)], [(1,0)], [(2,0)], \ldots$$

Uno puede notar que así escritos, estos conjuntos tiene un increíble parecido con el concepto intuitivo que tenemos de números enteros enteros. Esto es precisamente lo que nos lleva a la siguiente definición.

Definición 0.2. Definimos *el conjunto de los números enteros* como $\mathbb{N} \times \mathbb{N}/\sim$ que representamos simbólicamente por $\mathbb{Z}$[1]. De manera concreta

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$$

Haremos una digresión para ilustrar ahora la forma en que indicaremos los elementos de $\mathbb{Z}$ para la cual interpretaremos de manera gráfica sus elementos. De hecho, no es difícil ver que cada clase de equivalencia se puede representar como una función lineal con pendiente uno. Esto quiere decir que cada una de las clases de equivalencia son lineas paralelas entre si. Cada una de estás lineas tiene una posición "natural" que nos permite identificarla bajo nuestra versión intuitiva de un número entero se tratara. Los detalles de esto desarrollan en los ejercicios y la representación que se comenta se puede encontrar en la figura 1.

En consideración de lo anterior, debemos notar que los números naturales son objetos completamente distintos a los números enteros y sin embargo podemos asociar a cada natural un entero a través de la interpretación que hemos proveído. Por ejemplo, hemos propuesto que la pareja $(3,0)$ representaría a la diferencia $3 - 0$ que sabemos se trata simplemente del número natural 3, no parece entonces fuera de lugar asociar la clase de equivalencia $[(3,0)]$ al número 3, de alguna forma representan el mismo concepto, sin embargo se trata de objetos distintos. Antes de realizar este paso, debemos comprobar que los números enteros cumplen con las propiedades que buscamos por lo que será necesario realizar una distinción temporal entre ambos.

[1]Del alemán « Zahlen». Kronecker afirmó, en alemán original, «Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk» en referencia a este conjunto.

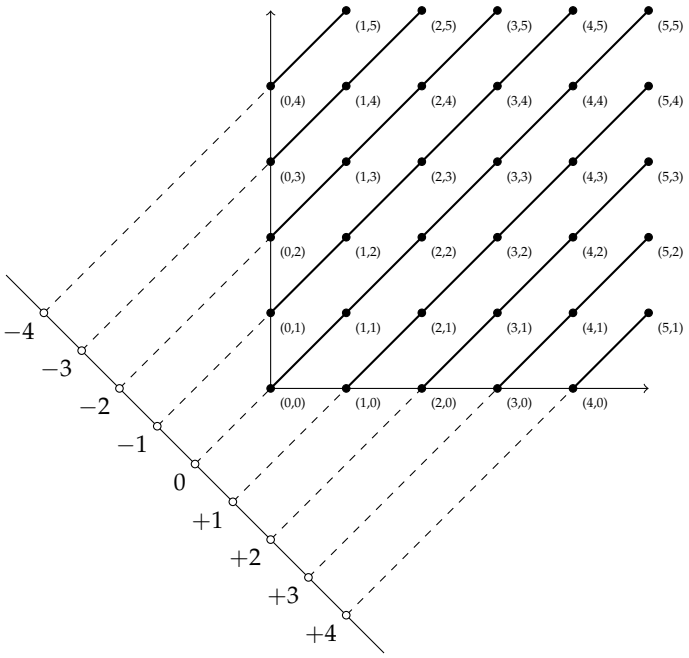

Figura 1: Representación gráfica de $\mathbb{N} \times \mathbb{N}$ que difiere de la interpretación tradicional tomando los ejes invertidos. Las clases de equivalencia están representadas por lineas que unen los elementos que pertenecen a una misma clase. Dichas lineas corresponden a su vez a le definición que hemos dado del conjunto $\mathbb{Z}$, que en esta figura se interpreta de la forma común.

Volvamos ahora un poco sobre nuestros pasos con el objeto de explorar como es que los enteros deben sumarse y multiplicarse. Hasta ahora hemos interpretado un entero como un conjunto de parejas de naturales, comenzando esta exploración pensando en diferencias. Pensemos entonces en dos diferencias $m - n$ y $a - b$ nuestro objetivo es mostrar como debería ser la suma de estas de manera intuitiva, bajo esta suma deberíamos tener por supuesto la siguiente propiedad:

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

Este hecho se puede probar como un sencillo resultado en $\mathbb{N}$ cuando las diferencias involucradas tienen sentido (ejercicio).

Lo anterior muestra que podemos interpretar la suma de diferencias como otra diferencia, al menos esto es lo que esperaríamos de una definición adecuada. Volvemos entonces a nuestra interpretación como parejas de naturales y usamos la sugerencia del párrafo anterior para deshacernos de la condición que $\mathbb{N}$ nos impone para considerar la suma.

Definición 0.3. Para dos parejas de naturales (m, n) y (a, b) definimos

$$(m, n) + (a, b) = (m + a, b + n).$$

Hagamos ahora un análisis similar para el producto. Tomemos para esto dos diferencias $m - n$ y $a - b$, de manera intuitiva podemos observar que

$$(m - n) \cdot (a - b) = (m \cdot a + n \cdot b) - (m \cdot b + n \cdot a).$$

No debe ser sorprendente que lo anterior se pueda probar como resultado en $\mathbb{N}$ cuando las diferencias involucradas tienen sentido.

Es notable que el producto de diferencias se pueda interpretar como otra diferencia. La expresión en el párrafo anterior es precisamente la motivación requerida que nos permite dar una interpretación del producto cuando tratamos las diferencias como parejas ordenadas.

Definición 0.4. Para dos parejas de naturales (m, n) y (a, b) definimos

$$(m, n) \cdot (a, b) = (m \cdot a + n \cdot b, m \cdot b + n \cdot a).$$

En la definiciones 0.3 y 0.4 hemos introducido operaciones en el conjunto $\mathbb{N} \times \mathbb{N}$, argumentando que nuestra interpretación de las diferencias descansaba en parejas de naturales, sin embargo hemos definido el conjunto de los números enteros como un conjunto cociente de $\mathbb{N} \times \mathbb{N}$ por lo que nuestro objetivo de definir la suma y el producto sobre $\mathbb{Z}$ no ha sido alcanzado y *a priori* no parece posible ajustar las operaciones definidas. En realidad, no es difícil inducir la suma y el producto en $\mathbb{Z}$ a través de la suma y el producto definidos en $\mathbb{N} \times \mathbb{N}$ pero para conseguirlo será necesario hacer una pequeña digresión y presentar el concepto de *operación compatible*.

0.2. Operaciones compatibles

El concepto de operación es probablemente el primero de naturaleza algebraica con el que nos enfrentaremos es importar notar que de manera intuitiva podría parecernos que no necesitamos definirlo, pero al interpretar todo en términos de conjuntos es importante proveer de una definición en este marco.

Definición 0.5. Sea A un conjunto cualquiera. A una función $f : A \times A \to A$ se le llama operación en A. Convencionalmente se escribe afb en lugar de $f(a, b)$.

Como ejemplos de la anterior definición, podemos pensar a la suma y al producto definidas en la sección anterior como funciones:

$$+, \cdot : (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{N} \times \mathbb{N}$$

y en consecuencia serán operaciones en $\mathbb{N} \times \mathbb{N}$.

Lo que realmente necesitamos es estudiar bajo que condiciones una operación puede inducir otra en el conjunto cociente cuando una relación de equivalencia está involucrada. Debemos entonces formular el concepto de operación compatible en donde *la operación respete la equivalencia*. En otras palabras, cuando *es equivalente operar sobre elementos equivalentes*.

Definición 0.6. Sea A un conjunto y sea $\sim$ una relación de equivalencia en A. Una operación f en A se dice *compatible con* $\sim$ si, para cualesquiera x, x', y y y' en A, $x \sim x'$ y $y \sim y'$ implica

$$f(x, y) \sim f(x', y').$$

La siguiente proposición es sólo una reinterpretación de la definición anterior pero ilustra cual es la importancia de una operación compatible.

Proposición 0.3. *Sea A un conjunto, $\sim$ una relación de equivalencia en A y f una operación compatible con $\sim$. Entonces, existe una función $\bar{f}\colon A/\sim \times A/\sim \to A/\sim$ de forma que para cada para de elementos x y y del conjunto A,*

$$\bar{f}([x], [y]) = [f(x, y)].$$

Demostración. Usaremos el hecho que una función es de manera última una relación, definiremos entonces $\bar{f}$ primero como una relación y mostraremos después que posee la propiedad que define a las funciones. Proponemos entonces

$$\bar{f} = \left\{(([x], [y]), [z]) \mid \text{Existen } x' \in [x] \text{ y } y' \in [y] \text{ tales que } f(x', y') \in [z]\right\}.$$

No debemos perder de vista que los elementos de las parejas que componen a $\bar{f}$ son clases de equivalencia; este hecho lo usaremos para probar que $\bar{f}$ es en realidad una función.

Supongamos

$$(([x], [y]), [z]) \in \bar{f} \quad \text{y} \quad (([x], [y]), [z']) \in \bar{f}.$$

Bajo estas hipótesis y siguiendo la definición de $\bar{f}$, podemos entonces encontrar x_1 y x_2 en $[x]$ y, y_1 y y_2 en $[y]$ de forma que $f(x_1, y_1) \in [z]$ y $f(x_2, y_2) \in [z']$. Esto significa que $x_1 \sim x$ y $x_2 \sim x$ y al ser la relación de equivalencia, debemos tener $x_1 \sim x_2$ y de igual forma podemos concluir que $y_1 \sim y_2$, ahora al f es una operación compatible con la relación, debemos tener que

$$f(x_1, y_1) \sim f(x_2, y_2),$$

pero $f(x_1, y_1) \sim z$ y también $f(x_2, y_2) \sim z'$ de lo que debemos concluir que $z \sim z'$ y en consecuencia $[z] = [z']$. Concluimos entonces que $\bar{f}$ es una función como deseábamos.

Para probar la identidad que distingue a la función debemos notar que

$$z \in \bar{f}([x], [y])$$

si existen $x' \sim x$ y $y' \sim y$ de forma que $z = f(x', y')$. Como $x \sim x$ y $y \sim y$ debemos entonces concluir que

$$f(x, y) \in \bar{f}([x], [y])$$

por lo que podemos concluir que

$$\bar{f}([x], [y]) = [f(x, y)]$$

para cualesquiera x y y elementos de A. Esta identidad es la que buscábamos. ■

Definición 0.7. A la función $\bar{f}$ de la proposición anterior se le denomina *la operación inducida por f en $A/\sim$.*

La proposición anterior debe usarse de manera directa. En cuanto se prueba que una operación es compatible con una relación de equivalencia, se puede inducir una operación en el conjunto cociente con la propiedad indicada. En muchas ocasiones, este procedimiento se simplifica y se define directamente la operación sobre el conjunto cociente usando algún representante de la clase de equivalencia, en ese caso, cuando la operación es compatible se dice que *la operación está bien definida*. Gracias a esta proposición estamos ahora en la antesala de definir las operaciones para los enteros la cual será resultado directo del siguiente teorema.

Teorema 0.4. *Consideramos $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$, entonces*

1. *La operación $+$ en $\mathbb{N} \times \mathbb{N}$ es compatible con $\sim$.*
2. *La operación $\cdot$ en $\mathbb{N} \times \mathbb{N}$ es compatible con $\sim$.*

Demostración. Para mostrar que las operaciones son compatibles, supongamos para esto cuatro parejas de naturales de forma que $(m, n) \sim (m', n')$ y $(a, b) \sim (a', b')$. Mostraremos primero que

$$(m + a, n + b) \sim (m' + a', n' + b');$$

en efecto, basta notar que

$$m + n' = m' + n$$

y

$$a + b' = a' + b,$$

lo cual implica a su vez

$$\begin{aligned}(m + a) + (n' + b') &= (m + n') + (a + b') \\ &= (m' + n) + (a' + b) \\ &= (m' + a') + (n + b),\end{aligned}$$

lo cual implica precisamente que $(m + a, n + b) \sim (m' + a', n' + b')$. O en otras palabras

$$(m, n) + (a, b) \sim (m', n') + (a', b')$$

lo cual indica que la operación $+$ es compatible con $\sim$, lo que prueba 1.

Para probar necesitamos un poco de paciencia para notar lo siguiente:

$$\begin{aligned}
&m \cdot a + n' \cdot a + m' \cdot b + n \cdot b + m' \cdot a + m' \cdot b' + n' \cdot a' + n' \cdot b \\
&= a \cdot (m + n') + b \cdot (m' + n) + m' \cdot (a + b') + n' \cdot (a' + b) \\
&= a \cdot (m' + n) + b \cdot (m + n') + m' \cdot (a' + b) + n' \cdot (a + b') \\
&= m' \cdot a + n \cdot a + m \cdot b + n' \cdot b + m' \cdot a' + m' \cdot b + n' \cdot a + n' + b',
\end{aligned}$$

Usando la ley de simplificación en $\mathbb{N}$, de lo anterior se desprende que

$$m \cdot a + n \cdot b + m' \cdot b' + n' \cdot a' = m' \cdot a' + n' \cdot b' + m \cdot b + n \cdot a,$$

lo que implica precisamente que

$$(m \cdot a + n \cdot b, m \cdot b + n \cdot a) \sim (m' \cdot a' + n' \cdot b', m' \cdot b' + n' \cdot a')$$

o en otras palabras

$$(m, n) \cdot (a, b) \sim (m', n') \cdot (a', b'),$$

lo que indica que el producto es compatible con $\sim$, probando 2. ■

Concluimos esta sección haciendo énfasis en el objetivo original para el que iniciamos la digresión: Existen dos operaciones en $\mathbb{Z}$, $\oplus$ y $\odot$, que satisfacen

$$[(m, n)] \oplus [(a, b)] = [(m + a, n + b)]$$

y

$$[(m, n)] \odot [(a, b)] = [(m \cdot a + n \cdot b, m \cdot b + n \cdot a)],$$

donde $\oplus$ y $\odot$ son las operaciones inducidas por $+$ y $\cdot$, respectivamente, en $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$.

0.3. Aritmética en $\mathbb{Z}$

Conocemos ahora que $\mathbb{Z}$ tiene asociadas dos operaciones y a pesar que nos hemos esmerado en notar cuan diferentes son estas de las asociadas a $\mathbb{N}$, en el fondo se trata de las mismas operaciones. Es por eso que siempre que no exista ambigüedad escribiremos $+$ en lugar de $\oplus$ y $\cdot$ en lugar de $\odot$. Hagamos esto patente a través de forzar su definición.

Definición 0.8. Para elementos $[(m, n)]$ y $[(a, b)]$ de $\mathbb{Z}$ definimos *la suma* entre estos como

$$[(m, n)] + [(a, b)] = [(m + a, n + b)]$$

y el producto como

$$[(m, n)] \cdot [(a, b)] = [(m \cdot a + n \cdot b, m \cdot b + n \cdot a)].$$

Es importante notar que las operaciones a la izquierda de las igualdades anteriores se realizan entre números enteros mientras las que aparecen a la derecha de las igualdad se realizan entre naturales. ¿Por qué entonces las mezclamos? Existe una sencilla identificación del conjunto $\mathbb{N}$ en $\mathbb{Z}$ que además respeta las operaciones, a decir

$$k \mapsto [(k, 0)].$$

El ejercicio muestra en que sentido esta función respeta las operaciones de $\mathbb{N}$ y es la causa por lo que podemos decidir nombrarlas de la misma manera. No sólo eso, a partir de ahora usaremos la siguiente convención: si un natural k aparece en un enunciado que involucre elementos de $\mathbb{Z}$ se deberá entender su elemento asociado en $\mathbb{Z}$, i.e., el número entero $[(k,0)]$. Una vez establecido esto, podemos presentar los algunos resultados notables de los cuales algunos se presentan sin demostración considerando que éstas se realizaran como ejercicios. Como una nota de advertencia, los siguientes resultados se presentan sin ninguna referencia a la peculiar forma en que el conjunto $\mathbb{Z}$ ha sido construido y servirán como bloque fundamental para derivar cualquier resultado conocido acerca de los enteros.

Teorema 0.5. *La suma $+$ en $\mathbb{Z}$ es conmutativa y asociativa.*

Teorema 0.6. *El número entero 0 satisface para cada entero a*

$$a + 0 = a$$

Demostración. Basta seguir la convención que hemos propuesto. Sea $[(m,n)]$ un elemento de $\mathbb{Z}$ entonces

$$[(m,n)] + [(0,0)] = [(m+0, n+0)] = [(m,n)]$$

y como 0 se debe interpretar como $[(0,0)]$ el resultado que buscamos sigue. ■

Teorema 0.7. *Para cada número entero a existe otro entero b tal que*

$$a + b = 0$$

Demostración. De nueva cuenta usaremos nuestra convención, además de notar que $[(k,k)] = [(0,0)]$. En ese caso, para cualquier elemento $[(m,n)]$ de $\mathbb{Z}$ tenemos que

$$[(m,n)] + [(n,m)] = [(m+n, m+n)] = [(0,0)],$$

lo cual afirma el resultado. ■

Teorema 0.8. *El producto $\cdot$ en $\mathbb{Z}$ es conmutativo y asociativo.*

Teorema 0.9. *El número entero 1 satisface para cada entero a*

$$a \cdot 1 = a$$

Demostración. De nueva cuenta será necesario usar nuestra convención para interpretar el enunciado. Sea $[(m.n)]$ un elemento de $\mathbb{Z}$, entonces

$$[(m,n)] \cdot [(1,0)] = [(m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1)] = [(m,n)].$$

Por convención 1 se debe interpretar como $[(1,0)]$ por lo que el resultado sigue. ■

Teorema 0.10. *Sean a, b y c números enteros. Entonces,*

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

Demostración. La prueba del resultado, descansa sobre el hecho que la multiplicación es distributiva sobre la suma respecto en las operaciones definidas en $\mathbb{N} \times \mathbb{N}$. En efecto,

$$\begin{aligned}
&(a,b)\cdot((m_1,n_1)+(m_2,n_2)) = (a,b)\cdot(m_1+m_2,n_1+n_2)\\
&= (a\cdot(m_1+m_2)+b\cdot(n_1+n_2), a\cdot(n_1+n_2)+b\cdot(m_1+m_2))\\
&= ((a\cdot m_1+b\cdot n_1)+(a\cdot m_2+b\cdot n_2), (a\cdot n_1+b\cdot m_1)+(a\cdot n_2+b\cdot m_2))\\
&= (a\cdot m_1+b\cdot n_1, a\cdot n_1+b\cdot m_1)+(a\cdot m_2+b\cdot n_2, a\cdot n_2+b\cdot m_2)\\
&= (a,b)\cdot(m_1,n_1)+(a,b)\cdot(m_2,n_2).
\end{aligned}$$

Según las definiciones de la suma y producto en $\mathbb{Z}$, lo anterior implica que

$$\begin{aligned}
[(a,b)]\cdot([(m_1,n_1)]+[(m_2,n_2)]) &= [(a,b)\cdot((m_1,n_1)+(m_2,n_2))]\\
&= [(a,b)\cdot(m_1,n_1)+(a,b)\cdot(m_2,n_2)]\\
&= [(a,b)]\cdot[(m_1,n_1)]+[(a,b)]\cdot[(m_2,n_2)]
\end{aligned}$$

Lo anterior es lo que se buscaba probar. ■

Teorema 0.11. *Sean a y b números enteros. Entonces, si a y b son ambos distintos de 0, el producto $a \cdot b$ es también distinto de 0.*

Demostración. Sabemos que cualquier número entero se puede representar por parejas de la forma $(0,k)$ o $(k,0)$ para algún natural k. En ese caso examinaremos todos los casos posibles: Sean k_1 y k_2 números naturales distintos de 0, entonces el producto de dos enteros puede ser de las siguientes cuatro formas.

1. $[(k_1,0)]\cdot[(k_2,0)]$.
2. $[(k_1,0)]\cdot[(0,k_2)]$.
3. $[(0,k_1)]\cdot[(k_2,0)]$.
4. $[(0,k_1)]\cdot[(0,k_2)]$.

Para el primer caso, notamos que $(k_1,0)\cdot(k_2,0) = (k_1\cdot k_2,0)$ y como $k_1\cdot k_2 \neq 0$ pues ambos números asumen distinto de cero, entonces el producto resulta: $[(k_1\cdot k_2,0)] \neq [(0,0)]$ que es lo que buscamos probar. El cuarto caso resulta muy similar.

Para el segundo caso basta notar $(k_1,0)\cdot(0,k_2) = (0,k_1\cdot k_2)$ y de nueva cuenta $k_1\cdot k_2 \neq 0$ por lo que el producto satisface: $[(0,k_1\cdot k_2)] \neq [(0,0)]$ que es lo que buscamos probar. El tercer caso resulta muy similar.

Si estamos convencidos que los casos comentados son los únicos posibles y que todos derivan en que el producto es distinto de 0, entonces la prueba está completa. ■

Los teoremas anteriores constituyen una base mínima pero suficiente para probar muchos de los resultados que conocemos acerca de los números enteros. Muchos de estos junto a sus pruebas, deben ser ya conocidas cuando se lean estas notas, en ese caso el lector no debe encontrar dificultad en proveer estos resultados olvidándose por completo del significado de $\mathbb{Z}$ en la teoría de conjuntos y preocupándose únicamente por su naturaleza operativa que los anteriores teoremas indican. Consideremos por ejemplo el siguiente teorema

Teorema 0.12. *Sean a, b y c enteros cualquiera. Entonces, $a + c = b + c$ implica que $a = b$.*

Demostración. De acuerdo con el teorema 0.7, existen un número entero d de forma que $c + d = 0$. En ese caso,

$$(a + c) + d = (b + c) + d,$$
$$a + (c + d) = b + (c + d),$$
$$a + 0 = b + 0,$$

y finalmente,

$$a = b.$$

■

Es notable que el teorema anterior no requiera en absoluto de la definición que hemos dado de $\mathbb{Z}$. Sólo dependemos de sus operaciones, las cuales permiten de igual forma derivar un corolario.

Corolario 0.13. *Si $c + a = c + b$, entonces $a = b$.*

Demostración. Basta simplemente notar

$$a + c = c + a = c + b = b + c$$

por lo que el teorema anterior implica que

$$a = b.$$

■

El teorema 0.12 y su corolario llevan un nombre particular: *leyes de cancelación de la suma*. Estas leyes nos dejan hablar sin dificultad alguna de la unicidad de los inversos.

Teorema 0.14. *Para cada número entero a existe uno y sólo un entero b de forma que*

$$a + b = 0.$$

Demostración. El teorema 0.7 implica la existencia de al menos un número entero b con la característica que buscamos. Supongamos entonces algún otro número c de forma que $a + c = 0$, en ese caso

$$a + b = 0 = a + c$$

lo que, bajo las leyes de cancelación, implica que $b = c$, de lo que sigue el resultado. ■

El teorema anterior afirma que hay un sólo número con una determinada propiedad. Lo que nos permite asignarle cierta notación.

Definición 0.9. Para un número entero a, denotaremos por $-a$ como el único número entero de forma que $a + (-a) = 0$. Además, para otro entero b, definimos

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

Es importante remarcar una vez más que los teoremas y la discusión que siguió de ellos, no utiliza en absoluto la interpretación que dimos de $\mathbb{Z}$, podemos sin embargo, conectar el resultado de vuelta. Al analizar la prueba del teorema 0.7 podemos calcular el inverso para la suma para un entero $a = [(m, n)]$, observando simplemente que

$$[(m, n)] + [(n, m)] = [(0, 0)]$$

por lo que

$$-a = [(n, m)].$$

Esto quiere decir que para calcular el inverso sobre una clase de equivalencia de una pareja, basta tomar un representante, intercambiar las coordenadas y volver a calcular su clase de equivalencia. Como los inversos son únicos, no importa que clase de equivalencia resulte, sólo basta seguir el procedimiento anterior para obtenerlo.

Algunos resultado inmediatos se presentaran en forma de ejercicios, es importante realizar una gran cantidad de estos, muchos de los métodos que se usan para encontrar las pruebas son tan generales, que son idénticas a los resultados presentados en otros cursos de naturaleza completamente distinta.

0.4. Orden en $\mathbb{Z}$

Para introducir un orden en el conjunto debemos recordar que en una sección anterior se logro mostrar a $\mathbb{Z}$ como una lista de la siguiente forma:

$$\ldots, [(0, 2)], [(0, 1)], [(0, 0)], [(1, 0)], [(2, 0)], \ldots.$$

Lo anterior sugiere una forma muy natural de introducir el orden en los enteros realizando una partición entre los números adelante de $[(0, 0)]$ y los números antes. Se trata entonces de distinguir a «los enteros positivos» de los «negativos». La siguiente definición muestra esta distinción.

Definición 0.10. Designaremos como *el conjunto de los enteros positivos* al conjunto

$$\mathbb{Z}^+ = \{[(k, 0)] \mid k \in \mathbb{N}\backslash\{0\}\}.$$

El conjunto en cuestión no es otro que la lista a la derecha del cero entero; quizá resulte más claro escribir el conjunto como lista para verificar la identificación anterior:

$$\mathbb{Z}^+ = \{[(1, 0)], [(2, 0)], [(3, 0)], \ldots\}.$$

Si recordamos la convención que se realizó en la construcción de los enteros, podemos interpretar el conjunto anterior simplemente como

$$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$$

sin olvidarnos que los símbolos contenidos dentro los paréntesis no indican números naturales, sino las clases de equivalencia asociadas a natural. Aunque de momento no haremos uso de esta notación es importante usar este hecho. Presentamos ahora algunos de los resultados que nos servirán para construir un orden en $\mathbb{Z}$.

Teorema 0.15. *Sean a y b números enteros positivos. Entonces $a + b$ y $a \cdot b$ son positivos también.*

Demostración. Al ser los números positivos, deben existir naturales k_1 y k_2 distintos de 0 de forma que $a = [(k_1, 0)]$ y $b = [(k_2, 0)]$. En ese caso

$$a + b = [(k_1, 0)] + [(k_2, 0)] = [(k_1 + k_2, 0)] \in \mathbb{Z}^+$$

y también

$$a \cdot b = [(k_1, 0)] \cdot [(k_2, 0)] = [(k_1 \cdot k_2, 0)] \in \mathbb{Z}^+,$$

lo que implica el resultado que buscamos. ■

Teorema 0.16. *Sea a un número entero cualquiera. Entonces, es cierto uno y sólo uno de los siguiente enunciados.*

1. $a = 0$.
2. *a es un entero positivo.*
3. *$-a$ es un entero positivo.*

Demostración. El resultado es en realidad una interpretación del teorema 0.2. Este afirma que existe un número natural k de forma que tenemos dos posibilidades $a = [(k, 0)]$ o $a = [(0, k)]$. Si $a \neq 0$, entonces $k \neq 0$ lo que implica en el primer caso que $a \in \mathbb{Z}^+$, mientras en el segundo $-a = -[(0, k)] = [(k, 0)] \in \mathbb{Z}^+$. Esto es precisamente lo que afirma el enunciado que buscamos probar. ■

Este par de teorema son suficientes para definir un orden en $\mathbb{Z}$ caracterizado de la siguiente forma: Diremos que $a \leq b$ si $b - a \in \mathbb{Z}^+$. Afirmaremos de manera complementaria que $a < b$ si $a \leq b$ pero $a \neq b$. Bajo esta nueva terminología podemos caracterizar al teorema 0.16 como un conocido resultado. La demostración se deja como ejercicio y realizarlo resulta indispensable.

Corolario 0.17. *Para números enteros a y b, es cierto uno y sólo uno de los siguientes enunciado.*

1. $a = b$.
2. $a < b$.
3. $b < a$.

Existen por supuesto resultados muy sencillos de probar acerca del orden de $\mathbb{Z}$ ilustremos esto con un par de teoremas.

Teorema 0.18. *Sean a, b y c números enteros cualquiera. Entonces, si $a \leq b$ y $b \leq c$ entonces $a \leq c$.*

Demostración. Como hipótesis tenemos dos hechos: $a \leq b$ y $b \leq c$. El primero se traduce como $b - a \in \mathbb{Z}^+$ y el segundo $c - b \in \mathbb{Z}^+$. Esto deriva inmediatamente que

$$c - a = (c - b) + (b - a) \in \mathbb{Z}^+,$$

por lo que $a \leq c$ que es lo que deseamos concluir. ■

Debido al resultado anterior, se dice que el orden en los enteros es *transitivo*. Las otras dos propiedades importantes que definen a un orden son la antisimetría y reflexividad. Estas se probarán en los ejercicios.

Teorema 0.19. *Sean a, b y c números enteros cualquiera. Entonces, si $a \leq b$ y $0 \leq c$ entonces $a \cdot c \leq b \cdot c$*

Demostración. Por hipótesis, $b - a \in \mathbb{Z}^+$ y además $c \in \mathbb{Z}^+$ por lo que

$$b \cdot c - a \cdot c = b \cdot c + (-a) \cdot c = (b - a) \cdot c \in \mathbb{Z}^+.$$

Lo anterior implica que $a \cdot c \leq b \cdot c$. ■

De nueva cuenta debemos notar que las pruebas de estos últimos teoremas no dependen de los conceptos intrínsecos que se utilizaron para construir $\mathbb{Z}$. De hecho, hemos llegado al climax de este desarrollo, pues podemos abandonar la construcción que hemos dado y concentrarnos completamente en las propiedades puramente operativas de $\mathbb{Z}$. De hecho, los teoremas 0.5, 0.6, 0.7, 0.8, 0.9, 0.10, 0.15 y 0.16 aparecen como axiomas de los enteros en textos como [CLRT90]. En la siguiente estableceremos algunas convenciones que nos permitirán obtener un concepto de números enteros que empate con nuestra intuición.

0.5. Anillos

Hemos sentado las bases de los número enteros: Propuesto un conjunto, dos operaciones y un orden. Esta estructura resulta un caso particular de un fenómeno mas general que en matemáticas se denomina «anillo». En esta sección presentaremos una terminología para clasificar $\mathbb{Z}$ como un fenómeno mucho más general.

Definición 0.11. Sea R un conjunto y sean $+$ y $\cdot$ operaciones en A. A la terna $(A, +, \cdot)$ se denomina un *anillo conmutativo con elemento unitario* o simplemente *anillo*,si satisface las siguientes propiedades para cualesquiera x, y y z elementos de A:

1. $x + y = y + x$.
2. $(x + y) + z = x + (y + z)$
3. Existe un elemento 0 en A de forma que $x + 0 = x$.
4. Existe un elemento x^* en A de forma que $x + x^* = 0$.
5. $x \cdot y = y \cdot x$.
6. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
7. Existe un elemento 1 en A de forma que $x \cdot 1 = x$.
8. $x \cdot (y + x) = x \cdot y + x \cdot z$.

En general, no se escribe un anillo como una terna sino sólo se menciona el conjunto base mencionando que es un anillo y dejando implícitas las operaciones. Por ejemplo, los teoremas 0.5, 0.6, 0.7, 0.8, 0.9 y 0.10 exhiben a la terna $(\mathbb{Z}, +, \cdot)$ como un anillo conmutativo con unidad, este hecho se puede presentar bajo la anterior convención de la siguiente manera.

Teorema 0.20. *El conjunto $\mathbb{Z}$ es un anillo conmutativo con unidad.*

El conjunto $\mathbb{Z}$ sin embargo presenta algunas otras propiedades. Por ejemplo el teorema 0.11 muestra una propiedad que hemos enunciado como elemental pero que no aparece en la lista anterior.

Definición 0.12. Sea R un anillo conmutativo con elemento unitario. Al anillo A se le denomina un *dominio entero* si satisface lo siguiente Para cualesquiera $x \neq 0$ y $y \neq 0$, debemos tener que $x \cdot y \neq 0$.

Bajo la anterior definición, el teorema 0.11 se puede interpretar de la siguiente manera.

Corolario 0.21. *El conjunto $\mathbb{Z}$ es un dominio entero.*

Ahora, el anillo $\mathbb{Z}$, no sólo presenta operaciones sino también un orden y este orden es susceptible de ser caracterizado en términos de su estructura. De hecho, $\mathbb{Z}$ estas propiedades del orden son un fenómeno general en anillos.

Definición 0.13. Sea R un anillo conmutativo con elemento unitario y sea $\leq$ un orden en A. Decimos que A es un *anillo ordenado* si el $\leq$ es total y satisface para todo x, y y z en R las siguientes propiedades:

1. Si $x \leq y$, entonces $x + z \leq y + z$.
2. Si $0 \leq a$ y $0 \leq b$, entonces $0 \leq a \cdot b$.

El teorema 0.18 junto a los ejercicios muestra que la relación definida para $\mathbb{Z}$ es un orden. El corolario 0.17 muestra que ese orden es total, mientras que los teoremas 0.19 y 0.15 garantizan las propiedades 1 y 2 de la definición anterior respectivamente. En conjunto, estos resultado garantizan el siguiente teorema.

Teorema 0.22. *El conjunto $\mathbb{Z}$ es un anillo ordenado.*

Estas caracterizaciones afirman que $\mathbb{Z}$ es precisamente un caso particular de un caso mucho más general. Estas definiciones a pesar de ser introducidas en la discusión de los enteros, resulta importante recordarlas pues la estructura de anillo aparecerá en incontables ocasiones en el futuro y en realidad forman parte un extenso completamente ajeno al curso denominado «Teoría de Anillos».

Para terminar esta sección, estableceremos una convención acerca de la relación que guardan $\mathbb{N}$ y $\mathbb{Z}$. El conjunto $\mathbb{N}$ se ha usado para construir $\mathbb{Z}$ sin embargo, es destacable que dentro de $\mathbb{Z}$ exista un subconjunto que guarda por completo las propiedades que de $\mathbb{N}$, a decir el conjunto

$$[(0,0)], [(1,0)], [(2,0)], \ldots$$

Denominemos a este conjunto por un momento $\mathbb{N}^*$. Desde el punto de vista de conjunto estos conjuntos son el mismo al existir una función biyectiva de $\mathbb{N}$ en $\mathbb{N}^*$ definida por

$$f(k) = [(k,0)].$$

Esta misma función guarda tres importantes propiedades, que se prueban en los ejercicios, las cuales son:

1. $f(a+b) = f(a) + f(b)$.
2. $f(a \cdot b) = f(a) \cdot f(b)$.
3. $a \leq b$ si y sólo si $f(a) \leq f(b)$.

Éstas son en realidad las propiedades que definen a $\mathbb{N}$ por lo que la función f dada, las logra transferir a $\mathbb{N}^*$. Esto quiere decir que cualquier resultado que se realice en $\mathbb{N}$ puede ser afirmado de igual forma en $\mathbb{N}^*$ y viceversa por lo que la distinción entre los dos conjuntos se vuelve completamente innecesaria. Esto nos permite afirmar, abusando de la notación, que la siguiente contención de conjuntos es cierta

$$\mathbb{N} \subset \mathbb{Z}.$$

Para fines prácticos esto es realmente lo que deseamos alcanzar, en este punto será conveniente olvidarnos de la elaborada construcción que presentamos y limitarnos a operar $\mathbb{Z}$ con los axiomas de anillo y considerando $\mathbb{N}$ como un subconjunto de éstos.

Ejercicios

Ejercicio 0.1. Probar que la relación $\sim$ es de equivalencia si está definida en $\mathbb{N} \times \mathbb{N}$ por:

$$(m, n) \sim (a, b) \text{ si y sólo } m + b = n + a.$$

Ejercicio 0.2. Encuentra las siguientes clases de equivalencia de la relación del ejercicio anterior.

1. $[(5, 4)]$.
2. $[(3, 3)]$.
3. $[(2, 4)]$.
4. $[(3, 5)]$.

Ejercicio 0.3. Usando las clases de equivalencia del ejercicio anterior, encuentra las parejas de la forma $(0, k)$ o $(k, 0)$ que garantiza el teorema 0.2 son representantes de éstas.

Ejercicio 0.4. Muestra que cada clase de equivalencia $[(m, n)]$ define una función i.e., prueba que el subconjunto $[(m, n)]$ de $\mathbb{N} \times \mathbb{N}$ tiene la propiedad de función.

Ejercicio 0.5. Muestra que como función cada clase de equivalencia puede escribirse como

$$f(x) = x + k$$

para algún k en los números naturales.

Para los ejercicios 0.6, 0.7 y 0.8, recuerda que en $\mathbb{N}$, si $m \leq n$ entonces $k = m - n$ es el único número natural tal que $m = n + k$. De otra forma, los resultados carecen de sentido.

Ejercicio 0.6. Sean a, b, m y n números naturales. Si $a \leq b$ y $m \leq n$ demuestra que

$$a - b = m - n \text{ si y sólo si } a + n = b + m.$$

Ejercicio 0.7. Sean a, b, m y n números naturales. Si $a \leq b$ y $m \leq n$ demuestra que

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

Ejercicio 0.8. Sean a, b, m y n números naturales. Si $a \leq b$ y $m \leq n$ demuestra que

$$(m - n) \cdot (a - b) = (m \cdot a + n \cdot b) - (m \cdot b + n \cdot a).$$

Los siguientes ejercicios son la muestra de las leyes operativas para lo que hemos construido como $\mathbb{Z}$. Debe notarse, que si los teoremas base se toman como axiomas, es posible olvidarse por completo de la construcción que se ha presentado en está sección. Las pruebas que se requieren en estos resultados, tienen todos este espíritu.

Ejercicio 0.9. Para enteros a y b, si $a + b = a$ demuestra que $b = 0$.

Ejercicio 0.10. Para un entero a, muestra que

$$-(-a) = a.$$

Ejercicio 0.11. Para enteros a y b, muestra que

$$(-a) \cdot b = -(a \cdot b) \text{ y } (-a)(-b) = ab.$$

Ejercicio 0.12. Para enteros a y b, prueba que

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

Ejercicio 0.13. Demuestra que si $a + b = c$, entonces $a = c - b$ para enteros a, b y c.

Ejercicio 0.14. Este ejercicio complementa el teorema 0.18 para afirmar que la relación $\leq$ definida en $\mathbb{Z}$ es un orden. Demuestra que para cualesquiera enteros a y b,

1. $a \leq a$.
2. $a \leq b$ y $b \leq a$ implican $a = b$.

Ejercicio 0.15. Demuestra el teorema 0.17.

Ejercicio 0.16. Demuestra que para enteros a y b, tenemos que

$$0 \leq a^2 + b^2$$

Ejercicio 0.17. Para enteros a, b y c tales que $b < a$ y $0 < c$, demuestra que

$$b \cdot c < a \cdot c.$$

Ejercicio 0.18. Para enteros a y b de forma que $b > 1$, demuestra que $a \cdot > a$.

Por último mostraremos todas las propiedades que harán posible identificar $\mathbb{N}$ como un subconjunto de $\mathbb{Z}$.

Ejercicio 0.19. Considera la función $f\colon \mathbb{N} \to \mathbb{Z}$ definida por $f(k) = [(k, 0)]$. Muestra que

1. f es inyectiva.
2. $f(k + k') = f(k) + f(k')$.
3. $f(k \cdot k') = f(k) \cdot f(k')$.
4. $k \leq k'$ implica $f(k) \leq f(k')$.

Referencias

[CLRT90] Cárdenas, Humberto, Luis, Emilio, Raggi, Francisco y Tomás, Francisco: *Álgebra Superior*. Editorial Trillas, 1990.

Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentalo. El único objectivo real al que sirven, es preparar el curso de Álgebra Superior II impartido en la carrera de Actuaría de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.