Lectura 1: Los números enteros

1.1. Axiomas de anillo

En esta sección tiene como objetivo describir las propiedades esenciales de un objeto que intuitivamente conocemos bien: Los números enteros. Dicho objeto, por supuesto, lo comprenderemos en el marco de la teoría de conjuntos y será nuestro punto de partida para explicar varias estructuras algebraicas de gran interés en la matemática. Con ese fin, se da una descripción de las propiedades más relevantes que serán presentadas como axiomas, más adelante mostraremos que estos axiomas son en realidad resultado de una construcción fundamental consecuencia de la existencia de los naturales. De momento y para nuestros objetivos, esta descripción tiene poca relevancia.

Comenzamos asumiendo la existencia de un conjunto, $\mathbb{Z}$, al cual denominaremos *el conjunto de los números enteros* sus elementos en consecuencia serán llamados *números enteros*. Junto a este conjunto, asumimos la existencia de dos operaciones, la suma $+$ y el producto $\cdot$, gobernadas por los siguientes axiomas.

Axioma 1.1. La suma $+$ en $\mathbb{Z}$ es conmutativa y asociativa.

Axioma 1.2. Existe un número entero, 0, que satisface para cada entero a,

$$a + 0 = a.$$

Axioma 1.3. Para cada número entero a, existe un único número entero, $-a$ tal que

$$a + (-a) = 0.$$

Axioma 1.4. El producto $\cdot$ en $\mathbb{Z}$ es conmutativo y asociativo.

Axioma 1.5. Existe un número entero, $1 \neq 0$, que satisface para cada entero a,

$$a \cdot 1 = a.$$

Axioma 1.6. Para cualesquiera números enteros a, b y c números enteros, se cumple

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

+	a	b
a	a	b
b	b	a

·	a	b
a	a	a
b	a	b

Figura 1: Tablas para la suma y el producto con dos elementos.

Con algo de perspicacia, podemos ver que los axiomas anteriores parecen no hacer una referencia particular a $\mathbb{Z}$, son sólo propiedades que asumimos para el conjunto que describimos. En realidad esto es así, pero habrá que explicar el lenguaje en que lo haremos.

Definición 1.1. Para un conjunto A, una función $f\colon A \times A \to A$ se dice una *operación binaria* en A. En ese caso se acostumbra escribir afb en lugar de $f(a,b)$.

Eso quiere decir que los símbolos $+$ y $\cdot$ son en realidad funciones $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ o, en otra palabras, operaciones binarias en $\mathbb{Z}$. Estas funciones por supuesto están gobernadas por los axiomas antes descritos. En cierta forma cuando hacemos referencia a $\mathbb{Z}$, no hacemos referencia solamente al conjunto sino a toda una estructura que está compuesta por el conjunto y este par de operaciones binarias. Podemos, dado que $+$ y $\cdot$ son funciones y por tanto conjuntos, decir que *la estructura de los enteros es la triada* $(\mathbb{Z}, +, \cdot)$.

Una vez identificado esto, estamos en posición de generalizarlo. Para un conjunto cualquiera R, los axiomas 1.1, ...,1.5 y 1.6 pueden ser formulados de manera tal, que involucren operaciones binarias en R y no en $\mathbb{Z}$. A pesar de que pueda ser repetitivo, a continuación se provee una definición que expone este hecho.

Definición 1.2. Sea R un conjunto cualquiera y sean $+$ y $\cdot$ operaciones binarias en R. La triada $(R, +, \cdot)$ se dice *un anillo conmutativo* si satisface las siguientes condiciones para cualesquiera elementos x, y y z del conjunto R.

- $x + y = y + x$.
- $x + (y + z) = (x + y) + z$.
- Existe 0_R en R de forma que $x + 0_R = x$.
- Existe un único y en R de forma que $x + y = 0_R$.
- $x \cdot y = y \cdot x$.
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- Existe 1_R en R de forma que $x \cdot 1_R = x$.
- $x \cdot (y + z) = x \cdot y + x \cdot z$.

No debería existir objeción alguna para afirmar que la triada $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo. Pero las propiedades que se le imponen a un anillo parecen forzadas por $\mathbb{Z}$. Para eliminar esta idea del camino, es necesario proveer algunos ejemplos distintos del conjunto de los números enteros.

Consideremos primero el conjunto $R = \{a, b\}$. Podemos definir la suma y el producto de la manera en que queda indicado en la tabla que aparece en la figura 1. En dicha tabla, podemos

notar (con la suficiente paciencia) que las propiedades que exige la definición de anillo quedan satisfechas. En particular tenemos, $0_R = a$ y $1_R = b$. Este ejemplo, aunque rudimentario, muestra que existen estructuras distintas a la de $\mathbb{Z}$ que cumplen con las mismas propiedades. Esto nos lleva a pensar que quizá existan otras más. En el desarrollo del curso, exhibiremos una diversidad considerable de estas estructuras, mientras tanto es deseable que se provea un ejemplo de un anillo con tres elementos (ejercicio 1.1). Esperando encontrarnos convencidos que los enteros son sólo una expresión de un concepto más amplio, consideraremos además otras propiedades y, cuando sea conveniente, las clasificaremos en el lenguaje de anillos introducido por la definición 1.2.

Teorema 1.1. *Para cualesquiera enteros a, b y c, si $a + c = b + c$ entonces $a = b$.*

Demostración. No es realidad difícil de probar, basta notar que

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

y notando que la suma es asociativa,

$$a = b.$$

■

El resultado del teorema anterior se le conoce como *la ley de cancelación para la suma*. Bajo esta ley y como los inversos aditivos existen, es conveniente escribir $a - b$ en lugar de $a + (-b)$; esto con el único objetivo de simplificar la notación. No se pierda de vista que la "resta" no es propiamente una operación sino una consecuencia de la existencia de los inversos aditivos.

Otro punto destacable, resulta la prueba de la ley de cancelación. En ésta, no se usan más que los axiomas que hemos proveído para los enteros, axiomas que resultan equivalentes a la definición de anillo. Con algo de voluntad, es posible concluir que la ley de cancelación para la suma es válida en cualquier anillo conmutativo. Sin embargo, un resultado análogo para el producto es elusivo y requiere de un axioma adicional. Consideremos primero un par de lemas.

Lema 1.2. *Para cualquier número entero a, se tiene $a \cdot 0 = 0$.*

Demostración. Independiente de conocer o no el valor de $a \cdot 0$, sabemos que este es un número. Ahora

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0.$$

Basta entonces sumar el inverso aditivo de $a \cdot 0$ a esta ecuación para obtener $a \cdot 0 = 0$. ■

Lema 1.3. *Para cualesquiera enteros a y b, se tiene*

$$(-a)\dot{b} = a \cdot (-b) = -(a \cdot b)$$

Demostración. Como los inversos son únicos, basta mostrar que

$$a \cdot b + (-a) \cdot b = 0,$$

en efecto

$$a \cdot b + (-a) \cdot b = (a - a) \cdot b = 0 \cdot b = 0.$$

La otra igualdad se prueba por analogía. ■

En este punto se asume que el lector tiene experiencia más que suficiente manipulando axiomas y las pruebas de este par de lemas le deben ser ya conocidas, por ejemplo durante un curso de cálculo donde los números reales han sido propuestos de manera axiomática como tradicionalmente se hace. Esta expectativa se traducirá en el uso de algunas propiedades de los números enteros sin mención alguna de éstas, sin embargo y si uno es lo suficientemente metódico, ninguna de ellas debería presentar un problema ni en su identificación ni en su prueba.

Axioma 1.7. 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.

Teorema 1.4. *Para cualesquiera enteros a, b y $c \neq 0$, si $a \cdot c = b \cdot c$ entonces $a = b$.*

Demostración. Por hipótesis

$$0 = a \cdot c - b \cdot c = a \cdot c + (-b) \cdot c = (a - b) \cdot c.$$

Como $c \neq 0$, entonces por el axioma 1.7, debemos tener que $a - b = 0$ o en otras palabras $a = b$. ■

Es de notarse que esa propiedad adicional descrita por el axioma, nos debe llevar a pensar que no todos los anillos presentan dicha propiedad. Lamentablemente no estamos aún en posición de proveer un ejemplo de esto, pero eso no limita nuestra capacidad discursiva.

Definición 1.3. Sea R un anillo conmutativo. R se dice *un dominio entero* si, $a \cdot b = 0$ implica que $a = 0$ o $b = 0$.

Bajo esta definición, que no es más que una formulación del axioma para un caso más general, podemos afirmar que $\mathbb{Z}$ es un dominio entero.

1.2. Axiomas de orden

Además de las operaciones, de manera intuitiva, sabemos que el conjunto de los enteros contiene un orden. Un orden lo entendemos como una relación, en este caso de $\mathbb{Z}$ en $\mathbb{Z}$. Para describir ese orden, usaremos un par de axiomas, estos axiomas describirán a un subconjunto de $\mathbb{Z}$ que recibe el nombre el *conjunto de los enteros positivos*, usualmente este conjunto se denota $\mathbb{Z}^+$.

Axioma 1.8. Sean a y b números enteros positivos. Entonces $a + b$ y $a \cdot b$ son positivos también.

Axioma 1.9. Sea a un número entero cualquiera. Entonces, es cierto uno y sólo uno de los siguientes enunciados.

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

Este axioma abre la posibilidad de describir *los enteros negativos* como aquellos elementos $a \in \mathbb{Z}$ de forma que $-a \in \mathbb{Z}^+$; el axioma es además es suficiente 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 $a \neq b$. Presentaremos ahora un par de reusltados para mostrar como trabaja el concepto y de paso, mostrar una de las propiedades que verifican que la relación que hemos definido es en verdad un orden parcial.

Teorema 1.5. *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 en

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

por lo que $a \leq c$. ■

Teorema 1.6. *Sean a, b y c números enteros cualquiera. Entonces, si $a \leq b$ y $0 \leq c$ implican $a \cdot c \leq b \cdot c$.*

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 por definición significa que $a \cdot c \leq b \cdot c$. ■

Bajo esta nueva terminología podemos caracterizar al axioma 1.9 como un conocido resultado. La demostración se deja como ejercicio y realizarlo resulta indispensable para la compresión de los conceptos.

Teorema 1.7 (Ley de tricotomía)**.** *Para números enteros a y b, es cierto uno y sólo uno de los siguientes enunciados.*

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

La ley de tricotomía caracteriza al orden como total. Esto quiere decir que cada par de enteros resulta compara a través de $\leq$.

Ahora, los axiomas de $\mathbb{Z}$ garantizan la existencia de al menos dos números enteros disintos: 0 y 1. Es interesante preguntarse, cómo se comparan estos números a través del orden. Debemos primero notar que cualquier entero a, de acuerdo al axioma 1.9 debe ser o 0 o positivo o negativo. Si fuera 0, entonces $a = 0$ y si fuera positivo a^2 será de igual forma positivo de acuerdo al 1.8, si por el contrario fuera negativo, entonces $-a$ será positivo y en consecuencia

$$a^2 = -(-a \cdot a) = (-a) \cdot (-a)$$

de lo que podemos concluir que de nueva cuenta que a^2 será positivo. De esto se puede concluir que $a^2 \geq 0$ donde la posibilidad de igualdad se presenta solamente cuando $a = 0$. En ese caso, como $1 \neq 0$, concluimos que $1^2 > 0$ pero $1 = 1^2$ por lo que $1 > 0$. Podemos entonces notar que

$$0 < 1 < 2 < 3 \ldots$$

lo que nos lleva a concluir una útil idea que puede parecer extraña (o quizá no, depende de la óptica con que se observe):

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

Esto es de gran utilidad pues algunas de las propiedades concidas de $\mathbb{N}$ tendrán repercusión en la estructura de $\mathbb{Z}$ en particular las que involucran enunciados equivalentes a la inducción.

1.3. Inducción en $\mathbb{Z}$

Comenzaremos ahora a ver cuales son las implicaciones de sobre $\mathbb{Z}$ al contener éste a $\mathbb{N}$. Recordemos el principio de inducción:

Principio de inducción. Para una fórmula $\alpha(n)$ acerca de los números naturales, si

- $\alpha(0)$ es cierto y
- $\alpha(n)$ implica $\alpha(n+1)$ para todo natural n,

entonces $\alpha(n)$ es cierto para todo natural n.

Principio de inducción (versión conjuntista)**.** Para un subconjunto $S \subset \mathbb{N}$ si

- $0 \in S$ y
- $n \in S$ implica $n+1 \in S$ para todo natural n,

entonces $S = \mathbb{N}$.

Sabemos que en $\mathbb{N}$ podemos desplazar el caso base hasta algún número n_0 y garantizar que dicha fórmula es cierta para todo $n \geq n_0$. Este hecho es lo que motiva la siguiente formulación del principio de inducción en $\mathbb{Z}$.

Principio de inducción II. Para una fórmula $\alpha(n)$ acerca de los números enteros y un entero n_0 cualquiera, si

- $\alpha(n_0)$ es cierto y
- $\alpha(n)$ implica $\alpha(n+1)$ para todo entero n,

entonces $\alpha(n)$ es cierto para todo entero $n \geq n_0$.

El principio anterior, por supuesto, presenta también una versión conjuntista y logra ampliar a cualquier entero el principio que rige a la inducción. El ejercicio 1.10 pide exactamente esto y resulta ilustrativo realizarlo como prueba a la comprensión del concepto.

Demostración al principio de inducción II. Consideramo primero el subconjunto de $\mathbb{N}$ definido por

$$S = \{r \in \mathbb{N} \mid \alpha(n_0 + r) \text{ es cierto}\},$$

Afirmamos que S abarca todo $\mathbb{N}$. En efecto, $0 \in S$ pues $\alpha(n_0)$ es cierto. Ahora, si $r \in S$ tenemos que $\alpha(n_0 + r)$ es cierto, lo que por hipótesis nos debe llevar a tener $\alpha(n_0 + (r+1))$ también lo es y en consecuencia $r + 1 \in S$. De acuerdo al principio de inducción $S = \mathbb{N}$ como afirmamos.

Una vez establecido esto, basta darnos cuenta que cualquier número $n \geq n_0$ se puede escribir como $n = n_0 + r$ para algún natural r y como $r \in \mathbb{N} = S$ entonces $\alpha(n_0 + r)$ debe ser cierto, o lo que es lo mismo, $\alpha(n)$ debe ser cierto. Esto es precisamente lo que buscábamos. ■

1.4. Buen orden en $\mathbb{Z}$

Ahora analizaremos que consecuencia tiene la validez del principio de buen orden sobre $\mathbb{Z}$. Formulemos su enunciado para comenzar

Principio de buen orden. Cualquier subconjunto $A \neq \varnothing$ de los naturales tiene un mínimo, i.e., un numero $m \in A$ tal que, para todo numero $n \in A$, satisface $m \leq n$.

Lo primero que se debe aclarar es que este principio no es válido en $\mathbb{Z}$. El conjunto $\mathbb{Z}$ mismo es un subconjunto no vacío de enteros que no presenta mínimo. Esto se debe a que $0 < 1$ y en consecuencia $-1 < 0$, así, para cualquier entero a tenemos que

$$a - 1 < a,$$

por lo que asumir que $\mathbb{Z}$ presenta un mínimo, derivará en contradicción. Debemos entonces preguntarnos cuales son las repercusiones entonces, si el principio no es válido en los enteros. Quizá los enteros no estén acotados, pero cualquier conjunto de enteros acotado inferiormente, debe presentar un mínimo.

Teorema 1.8. *Cualquier subconjunto no vacío y acotado inferiormente de enteros tiene un mínimo.*

Demostración. Sea $S \subset \mathbb{Z}$ un conjunto acotado inferiormente, i.e., existe un entero m, de forma que $m \leq n$ para cualquier $n \in S$. Tomemos ahora el subconjunto de números naturales definido por

$$T = \{n - m \mid n \in S\};$$

este conjunto es por hipótesis no vacío y está compuesto exclusivamente por números naturales. En ese caso, por el principio de buen orden T debe tener un mínimo, digamos $n_0 - m$ para algún n_0 miembro de S. El entero n_0 posee la propiedad que buscamos pues este debe satisfacer para cada n en S

$$n_0 - m \leq n - m,$$

o en otras palabras

$$n_0 \leq n.$$

Esto quiere decir que S admite un mínimo como buscábamos. ■

Este teorema tiene una versión superior, la demostración a ese resultado se menciona en el ejercicio 1.11. Para resaltarlo, lo enunciamos a continuación.

Teorema 1.9. *Cualquier subconjunto no vacío y acotado superiormente de enteros tiene un máximo.*

Como puede apreciarse, muchos resultados acerca de los enteros son enteramente ignorados. Esto tiene como único objetivo provocar su exploración. Esto no debe intimidar, muchos de ellos deben parecer lo suficientemente obvios para admitirlos en los posteriores desarrollos. Lo importante, y aquí vale la pena detenernos a ser cuidadosos, es tener una idea clara de como probar esos resultados tan pronto los veamos, esto se alcanza con diligencia por lo que se invita a realizarlo hasta el hartazgo.

Ejercicios

Ejercicio 1.1. Describe dos operaciones sobre el conjunto $R = \{a, b, c\}$ de forma que R junto a esas dos operaciones forme un anillo. Sugerencia: Usa tablas como las que se proveen para el caso de dos elementos.

Ejercicio 1.2. Verifica que el axioma 1.7 garantiza que $\mathbb{Z}$ es una dominio entero.

Ejercicio 1.3. Demuestra la ley de tricotomía (teorema 1.7).

Ejercicio 1.4. Demuestra que la relación $\leq$ definida en $\mathbb{Z}$ es un orden parcial.

Ejercicio 1.5. Demuestra que si $a < b$ entonces $-a > -b$.

Ejercicio 1.6. Demuestra que si $a < b$ y $c > 0$, entonces $ac < bc$.

Ejercicio 1.7. Demuestra que si $a < b$ y $c < 0$ entonces $ac > bc$.

Ejercicio 1.8. Demuestra que si $a > 0$ y $b > 1$ entonces $a < ab$.

Ejercicio 1.9. Recuerda que en los naturales se tiene que $m \leq n$ si y sólo si existe un único natural k de forma que $n = m + k$. Extiende este resultado a los enteros notando que

$$\mathbb{N} = \mathbb{Z}^+ \cup \{0\}.$$

Ejercicio 1.10. Formula el principio de inducción II como un enunciado de conjuntos.

Ejercicio 1.11. Demuestra que cualquier conjunto no vacío y acotado superiormente tiene un máximo.

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.