Semana 5: Números enteros

1. Axiomas de anillo

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 5.1. La suma + en \mathbb{Z} es conmutativa y asociativa, i.e., para cualesquiera enteros a, b y c, tenemos

$$a + b = b + a$$

y

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

Axioma 5.2. Existe un número entero, 0, que satisface para cada entero a,

$$a + 0 = a$$
.

Axioma 5.3. Para cada número entero a, existe un único número entero, -a tal que

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

Axioma 5.4. El producto \cdot en \mathbb{Z} es conmutativo y asociativo, i.e., para cualesquiera enteros a, b y c, tenemos

$$a \cdot b = b \cdot a$$

y

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

Axioma 5.5. Existe un número entero, $1 \neq 0$, que satisface para cada entero a,

$$a \cdot 1 = a$$
.

Axioma 5.6. Para cualesquiera números enteros a, b y c números enteros, se cumple

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

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 5.1. Para un conjunto A, una función $f: A \times A \to A$ 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 $5.1, \ldots, 5.6$ 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 5.2. 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 $x + y = 0_R$.
- $\mathbf{x} \cdot \mathbf{y} = \mathbf{y} \cdot \mathbf{x}.$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z.$
- 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} , +, ·) 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 $\{0,1\}$. Podemos definir la suma y el producto utilizando las operaciones usadas para el dominio booleano como

$$a + b = (a \lor b) \land (\neg a \land b)$$
 y $a \cdot b = a \land b$

Estas operaciones aparecen descritas por completo 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, $0_R = 0$ y $1_R = 1$. Este ejemplo, aunque rudimentario, muestra que existen estructuras distintas a la de \mathbb{Z} que cumplen con las mismas propiedades. Esto abre la puerta para admitir que existen estructuras distintas a los enteros que también resultan anillos, por ejemplo se puede obtener un anillo con tres elementos usando el conjunto $\{0,1,2\}$ observando con detalle el caso de un anillo con dos elementos (ejercicio 5.1).

Vamos ahora a mostrar una serie de resultados que los enteros satisfacen. Una lectura correcta y detenida de ellos, debería revelar que pueden verificados usando las mismas pruebas para un anillo cualquiera.

Figura 1: Operaciones para un anillo con dos elementos

Teorema 5.1. 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.

Lema 5.2. 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 5.3. 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 5.7. 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 5.4. 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 5.7, debemos tener que a - b = 0 o en otras palabras a = b.

Es de notarse que esa propiedad adicional descrita por el axioma 5.7 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 5.3. Sea $(R, +, \cdot)$ un anillo conmutativo. R se dice *un dominio entero* si y sólo 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 $(\mathbb{Z}, +, \cdot)$ es un dominio entero.

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. 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 denotado como $\mathbb Z^+$, del cual sus elementos son nombrados *enteros positivos*.

Axioma 5.8. Sean $a \ y \ b$ números enteros positivos. Entonces, $a + b \ y \ a \cdot b$ son positivos también.

Axioma 5.9. 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 suficiente para definir un orden en \mathbb{Z} caracterizado de la siguiente forma: Diremos que $a \le b$ si $b - a \in \mathbb{Z}^+$. Afirmaremos de manera complementaria que a < b si $a \le b$ pero $a \ne b$.

Teorema 5.5. *Sean a y b enteros cualesquiera. Si a* \leq *b, entonces* $-b \leq -a$.

Demostración. Es una simple observación, si $a \le b$ entonces b - a es positivo, pero

$$-a - (-b) = b - a$$

por lo que -a - (-b) a de ser también positivo y en consecuencia $-b \le -a$.

Teorema 5.6. Sean a, b y c números enteros cualquiera. Si $a \le b$ y $b \le c$ entonces $a \le c$.

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

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

lo anterior es suficiente para observar que $a \le c$ por la definición que hemos dado.

Teorema 5.7. Sean a, b y c números enteros cualquiera. Si $a \le b$ y $0 \le c$, se tiene $a \cdot c \le b \cdot c$.

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 5.9 como un conocido resultado. La demostración se deja como ejercicio y realizarlo resulta indispensable para la compresión de los conceptos.

Teorema 5.8 (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 se puede compara utilizando la relación ≤resulta compara a través del axioma 5.8.

Ahora, los axiomas de \mathbb{Z} garantizan la existencia de al menos dos números enteros distintos: 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 5.9 debe ser a=0 o $a\in\mathbb{Z}^+$ o $a\in\mathbb{Z}^-$. Si fuera a=0, entonces $a^2=0$; si fuera positivo, entonces a^2 sería de igual forma positivo; y si fuera negativo, entonces -a será positivo y

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

por lo que a^2 sería positivo. Con lo anterior podemos concluir que a^2 es siempre positivo o nulo, en otras palabras para cualquier entero a, se tiene que $a^2 \ge 0$, donde la posibilidad de igualdad se presenta solamente cuando a=0. En ese caso, como $1\ne 0$, concluimos que $1^2>0$ pero $1=1^2$ por lo que 1>0. Podemos entonces notar que

$$0 < 1 < 2 < 3 \dots$$

Además, junto al teorema 5.5, lo anterior nos permite concluir que

$$\cdots - 3 < -2 < -1 < 0.$$

Es esta precisamente la descripción del orden en los enteros la que hemos desarrollado intuitivamente durante nuestra vida.

3. Inducción

Al describir al conjunto $\mathbb Z$ estamos de paso describiendo también al conjunto de los naturales y estamos asumiendo que

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

Quizá la propiedad más importante de IN es el principio de inducción para el cual se asumirá cierta experiencia de parte del estudiante. Aquí se presentará como un axioma y aunque nos parezca una presentación es importante sentirnos cómodos con el concepto si hemos de continuar con el curso. Si por alguna razón parece confusa, será mejor no avanzar hasta alcanzar un mínimo de comodidad con ella.

Axioma 5.10 (Principio de inducción). Sea $\alpha(n)$ un enunciado acerca de los números naturales que satisface:

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

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

Ejemplo. Para cualquier número natural n se tiene que

$$0+1+\cdots+n=\frac{n(n+1)}{2}.$$

Para demostrar esto, usaremos el principio de inducción. Por supuesto, el resultado es válido para n = 0. Ahora, supongamos que el resultado es válido para algún número n, i.e.,

$$0+1+\cdots+n=\frac{n(n+1)}{2},$$

deseamos mostrar que el resultado será igualmente válido para n + 1. Entonces,

$$0+1+\dots+n+(n+1) = \frac{n(n+1)}{2} + n+1$$

$$= \frac{n(n+1)+2n+2}{2}$$

$$= \frac{n^2+3n+2}{2}$$

$$= \frac{(n+1)(n+2)}{2}.$$

Que es precisamente lo que deseábamos. Por el principio de inducción el resultado sigue.

Resulta interesante, explorar la implicación del principio de inducción sobre subconjuntos de \mathbb{N} . De alguna forma, la teoría de conjuntos es un intento por intercambiar enunciados lógicos por objetos que es posible describir con más precisión.

Teorema 5.9 (Inducción para conjuntos). *Sea* $S \subseteq \mathbb{N}$ *un conjunto que satisface:*

- 1. $0 \in S$.
- 2. $n \in S$ implica $n + 1 \in S$ para todo natural n.

Entonces, $S = \mathbb{N}$.

Demostración. Como $S \subseteq \mathbb{N}$ basta con proba que $\mathbb{N} \subseteq S$ lo cual conseguiremos usando el principio de inducción. Tomemos el enunciado para números naturales $\alpha(n)$ como «n pertenece a S». Por hipótesis, $0 \in S$ por lo que $\alpha(0)$ es cierto. Supongamos ahora que $\alpha(n)$ es cierto, esto quiere decir que $n \in S$, por hipótesis, lo anterior implica que n + 1 pertenece a S o lo que es lo mismo $\alpha(n + 1)$ es cierto. Esto indica que $\alpha(n)$ implica $\alpha(n + 1)$. Luego, por el principio de inducción, $\alpha(n)$ es cierto para todo natural. En otras palabras, para todo natural n, se tiene $n \in S$. ■

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} .

Teorema 5.10. Sean $\alpha(n)$ una fórmula acerca de los números enteros y un entero n_0 que satisfacen:

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

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

Demostración. Consideramos primero el subconjunto de N definido por

$$S = \{ m \in \mathbb{N} \mid \alpha(n_0 + m) \},$$

Afirmamos que S abarca todo \mathbb{N} . En efecto, $0 \in S$ pues $\alpha(n_0)$ es cierto. Ahora, si $m \in S$ tenemos que $\alpha(n_0 + m)$ es cierto, lo que por hipótesis nos debe llevar a tener $\alpha(n_0 + (m+1))$ también lo es y en consecuencia $m+1 \in S$. De acuerdo al principio de inducción para conjuntos descrito en el teorema 5.9, debemos tener que $S = \mathbb{N}$ como afirmamos.

Una vez establecido esto, basta darnos cuenta que cualquier entero n tenemos que $n \ge n_0$ si y sólo si podemos expresar $n = n_0 + m$ para algún natural m. Como $S = \mathbb{N}$ podemos afirmar que $\alpha(n_0 + m)$ debe ser cierto para todo natural m, o lo que es lo mismo, $\alpha(n)$ para cualquier debe ser cierto para cualquier $n \ge n_0$.

El principio anterior, por supuesto, presenta también una versión para conjuntos y logra ampliar a cualquier entero el principio que rige a la inducción. El ejercicio 5.10 pide exactamente esto y resulta ilustrativo realizarlo como prueba a la comprensión del concepto.

Teorema 5.11. *Sea* $\alpha(n)$ *un enunciado acerca de los números naturales que satisface:*

- 1. $\alpha(0)$ es cierto.
- 2. Si $\alpha(k)$ es cierto para todo $k \leq n$, entonces es cierto también $\alpha(n+1)$.

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

Demostración. Para mostrarlo, usaremos el enunciado $\beta(n)$ acerca de los números naturales definido como « $\alpha(k)$ *es cierto para todo* $k \le n$ ». Por hipótesis, es inmediato que $\beta(0)$ es cierto. Supongamos entonces que $\beta(n)$ es cierto. En ese caso, $\alpha(k)$ es cierto para $k \le n$ y por la forma en que hemos tomado al enunciado α , debe ser igualmente cierto $\alpha(n+1)$. Esto implica que $\alpha(k)$ es cierto siempre que $\alpha(n+1)$ es cierto y por el principio de inducción $\alpha(n)$ debe ser cierto para todo natural $\alpha(n)$.

Basta observar que si $\beta(n)$ es cierto, en particular $\alpha(n)$ es también cierto; luego, como $\beta(n)$ es cierto para todo natural, también lo debe ser $\alpha(n)$.

Este último resultado se denomina *el principio de inducción completa* que, aunque puede parecer diferente al principio de inducción, es una consecuencia de éste como muestra el teorema. Este principio se puede igualmente formular en una versión de conjuntos y es un buen ejercicio encontrar el enunciado y proveer una demostración.

4. Buen orden

Ahora analizaremos una consecuencia importante del principio de inducción sobre $\mathbb N$ y el impacto que tiene en $\mathbb Z$.

Teorema 5.12 (Principio de buen orden). Cualquier subconjunto $A \neq \emptyset$ de los naturales tiene un mínimo, i.e., un numero $m \in A$ tal que, para todo numero $n \in A$, satisface $m \le n$.

Demostración. Deseamos probar que A tiene un elemento mínimo y para mostrarlo procederemos por contraposición. Supongamos para esto que A no tiene un elemento mínimo. Definimos entonces el conjunto

$$S = \{ m \in \mathbb{N} \mid k \notin A \} .$$

En ese caso, $0 \in S$ pues si no estuviera, entonces sería parte de A por lo que A tendría un mínimo. Supongamos ahora que los números $0,1,\ldots,m$ pertenecen a S, entonces el número m+1 no puede ser un elemento de A, pues si lo hiciera, este deberá ser el mínimo del conjunto. Por lo tanto $m+1 \in S$. Por el principio de inducción completa $S=\mathbb{N}$ por lo que $A=\varnothing$. Podemos entonces concluir que si un subconjunto de los naturales no posee un mínimo éste debe ser el conjunto vacío, o en otras palabras, un conjunto no vacío tiene un elemento mínimo. Esto último es el principio de buena ordenación.

Lo primero que se debe aclarar es que este principio no es válido en \mathbb{Z} . El conjunto \mathbb{Z}^- es un subconjunto no vacío de enteros que no presenta mínimo. Esto se debe a que, para cualquier entero a, se tiene que

$$a - 1 < a$$
,

por lo que asumir que \mathbb{Z}^- presenta un mínimo, derivará en contradicción. Aunque el principio no es válido, se puede dar un resultado similar que sí lo es.

Teorema 5.13. Cualquier subconjunto no vacío y acotado inferiormente de enteros tiene un mínimo.

Demostración. Sea $S \subseteq \mathbb{Z}$ un conjunto acotado inferiormente, i.e., existe un entero m, de forma que $m \le n$ 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 $n \in S$,

$$n_0 - m < n - m$$

o en otras palabras

$$n_0 \leq n$$
.

Esto quiere decir que S admite a n_0 como un mínimo.

Este teorema tiene una versión para cotas superiores, la demostración a ese resultado se menciona en el ejercicio 5.11. Para resaltarlo, lo enunciamos a continuación.

Teorema 5.14. 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.

Ejercicios

Ejercicio 5.1. Describe dos operaciones sobre el conjunto $A = \{0, 1, 2\}$ de forma que A junto a esas dos operaciones forme un anillo. Sugerencia: Usa tablas como las que se proveen para el caso de dos elementos.

Ejercicio 5.2. Verifica que el axioma 5.7 garantiza que Z es una dominio entero.

Ejercicio 5.3. Demuestra la ley de tricotomía (teorema 5.8).

Ejercicio 5.4. Demuestra que si a < b y c > 0, entonces ac < bc.

Ejercicio 5.5. Demuestra que si a < b y c < 0 entonces ac > bc.

Ejercicio 5.6. Demuestra que si a > 0 y b > 1 entonces a < ab.

Ejercicio 5.7. Demuestra para todo natural $n \ge 1$ que

$$1^3 + 3^3 + \dots + (2n-1)^3 = n^2(2n^2 - 1).$$

Ejercicio 5.8. Usando inducción, demuestra para todo natural n > 3 que $2^n < n!$.

Ejercicio 5.9. Suponga se conocen los axiomas 5.1, 5.2 y 5.3 de los números enteros pero no se ha hablado de la multiplicación. Se puede definir la multiplicación de manera recursiva en los naturales como sigue:

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

Usando inducción, demuestra que

$$n \cdot (m+k) = n \cdot m + n \cdot k.$$

Ejercicio 5.10. Formula el principio de inducción completa como un enunciado de conjuntos.

Ejercicio 5.11. Demuestra que cualquier conjunto de enteros no vacío y acotado superiormente tiene un máximo.

Para entregar: Ejercicio 5.11

Referencias

- [Chi95] Childs, Lindsay N.: A concrete introduction to higher algebra. Springer, 2ª edición, 1995.
- [CLRT90] Cárdenas, Humberto, Luis, Emilio, Raggi, Francisco y Tomás, Francisco: Álgebra Superior. Editorial Trillas, 1990.
- [Spi12] Spivak, Michael: *Cálculo Infinitesimal*. Editorial Reverté, 3ª edición, 2012.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.