1

NÚMEROS ENTEROS

1.1 ARITMÉTICA

Todo lector de este apunte conoce los *enteros*. En una etapa muy temprana de nuestras vidas conocemos los números enteros positivos o "números naturales"

$$1, 2, 3, 4, 5, \ldots$$

Más adelante introducimos el 0 (cero), y los enteros negativos

$$-1, -2, -3, -4, -5, \ldots$$

En este curso no nos preocupamos demasiado por el significado lógico y filosófico de estos objetos, pero necesitamos saber las propiedades que se supone que tienen. Si todos parten de las mismas suposiciones entonces todos llegarán a los mismos resultados. Estos supuestos son los llamados axiomas.

El punto de vista adoptado en este apunte es el señalado antes. Aceptamos sin reparo que existe un conjunto de objetos llamados *enteros* conteniendo los enteros positivos y los negativos, y el cero, familiares en nuestra temprana educación y experiencia. El conjunto de enteros se denotará por el símbolo especial $\mathbb{Z}$. Las propiedades de $\mathbb{Z}$ serán dadas por una lista de axiomas, a partir de las cuales seremos capaces de deducir todos los resultados sobre números enteros que necesitaremos en las cuestiones subsiguientes. Empezaremos listando aquellos axiomas que tratan la suma y la multiplicación.

Adoptaremos las notaciones usuales $a + b$ para la suma de dos enteros a y b, y $a \cdot b$ (frecuentemente ab o también $a \times b$) para su producto. Pensamos en $+$ y $\cdot$ como *operaciones* que a un par de enteros a y b les hacen corresponder un entero $a + b$ y otro $a \cdot b$. El hecho de que $a \cdot b$ y $a + b$ son enteros, y no algún objeto extraño como elefantes, es nuestra primera suposición, el axioma **I1**.

En la siguiente lista de axiomas a, b, c denotan enteros arbitrarios, y 0 y 1 denotan enteros especiales que cumplen las propiedades especificadas más abajo.

I1) $a + b$ y $a \cdot b$ pertenecen a $\mathbb{Z}$.

I2) *Conmutatividad.* $a + b = b + a; \qquad ab = ba.$

I3) *Asociatividad.* $(a + b) + c = a + (b + c); \qquad (a \cdot b) \cdot c = a \cdot (b \cdot c).$

I4) *Existencia de elemento neutro.* Existen números $0, 1 \in \mathbb{Z}$ con $0 \neq 1$ tal que $a + 0 = a; \qquad a \cdot 1 = a.$

I5) *Distributividad.* $a \cdot (b + c) = a \cdot b + a \cdot c.$

I6) *Existencia del inverso aditivo, también llamado opuesto.* Por cada a en $\mathbb{Z}$ existe un único entero $-a$ en $\mathbb{Z}$ tal que $a + (-a) = 0.$

I7) *Cancelación.* Si $a \neq 0$ y $a \cdot b = a \cdot c$, entonces $b = c.$

Debido a la ley de asociatividad para la suma, axioma **I3**, $(a + b) + c$ es igual a $a + (b + c)$ y por lo tanto podemos eliminar los paréntesis sin ambigüedad. Es decir, denotamos

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

De forma análoga, usaremos la notación

$$abc = (ab)c = a(bc).$$

Debido a la ley de conmutatividad, axioma **I2**, es claro que del axioma **I4** se deduce que $0 + a = a + 0 = a$ y $1 \cdot a = a \cdot 1 = a$. Análogamente, por **I2** e **I6** obtenemos que $-a + a = a + (-a) = 0.$

Una propiedad que debemos mencionar es la siguiente: si $a, b, c \in \mathbb{Z}$ y $a = b$, entonces $a + c = b + c$ y $ac = bc$. Esto se debe a que la suma y el producto son operaciones que, como acabamos de decir, toman un par de enteros y devuelven otro entero. Si $a = b$, entonces el par a, c es igual al par b, c y por lo tanto devuelven la misma suma y el mismo producto. Esta propiedad no es un axioma, sino una mera aplicación de la lógica formal.

Todos los axiomas corresponden a propiedades familiares de los enteros que aprendemos en distintos niveles de nuestra educación matemática. De ellas pueden deducirse la mayoría de las reglas aritméticas comunes de los enteros como en el siguiente ejemplo.

Ejemplo 1.1.1. Demostremos que, para todo n entero, el opuesto de $-n$ es n, es decir que

$$-(-n) = n.$$

Demostración. El axioma **I6** nos dice que $-(-n)$ es el único número que sumado a $-n$, da cero. Por lo tanto, para demostrar que $-(-n) = n$ basta ver que $(-n) + n = 0$. Esto se cumple puesto que

$$\begin{aligned} (-n) + n &= n + (-n) && \text{(axioma I2)} \\ &= 0 && \text{(axioma I6)} \end{aligned}$$

Por lo tanto $(-n) + n = 0$. □

Como ya dijimos, los números enteros vienen provistos con dos operaciones fundamentales, la suma y la multiplicación. A continuación definimos la resta o sustracción.

Definición 1.1.2. Si $a, b \in \mathbb{Z}$ definimos $a - b$ como la suma de a más el opuesto de b, es decir que $a - b = a + (-b)$ por definición.

Ahora demostremos una propiedad básica de la resta.

Ejemplo. Demostremos que para dos enteros m y n cualesquiera

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

Demostración. Por la definición de sustracción, $m - (-n)$ es la suma $m + (-(-n))$, es decir

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

Por el ejemplo 1.1.1 sabemos que $-(-n) = n$ y por lo tanto $m - (-n) = m + (-(-n)) = m + n$. □

Tanto formalismo, como el usado en las demostraciones realizadas en el ejemplo anterior, puede ser tedioso, pero nos permite comenzar a comprender la estructura de una demostración formal.

Proposición 1.1.3. *Supongamos que existen dos enteros 0 y $0'$ ambos cumpliendo el axioma **I4**, esto es*

$$a + 0 = a, \qquad a + 0' = a$$

para todo a de $\mathbb{Z}$. Entonces $0 = 0'$.

Demostración.

$$\begin{aligned} 0 &= 0 + 0' && \text{(axioma \textbf{I4} aplicado a } 0 \text{ y con } 0' \text{ como neutro)} \\ &= 0' + 0 && \text{(axioma \textbf{I2})} \\ &= 0' && \text{(axioma \textbf{I4} aplicado a } 0' \text{ y con } 0 \text{ como neutro).} \end{aligned}$$

□

El resultado anterior nos demuestra que hay un único elemento elemento que cumple el axioma **I4** en lo que respecta a la suma. A este elemento lo denotamos 0 y lo denominamos el *elemento neutro de la suma*. Lo mismo podemos probar con el elemento neutro respecto al producto (ver ejercicio 3), es decir hay un único elemento, denotado 1, que satisface el axioma **I4** en lo que se refiere al producto. A este elemento lo llamamos el *elemento neutro del producto*.

Proposición 1.1.4 (Regla de los signos)**.** *Veamos que si* $a, b \in \mathbb{Z}$ *entonces*

$$(-a)(-b) = ab, \qquad a(-b) = (-a)b = -(ab).$$

Demostración. Veremos que $a(-b) = -(ab)$. Los otros casos se dejan como ejercicio para el lector.

Una forma de demostrar este caso es observando que $-(ab)$ es el inverso aditivo de ab y comprobando que $a(-b)$ es también inverso aditivo de ab.

$$\begin{aligned} ab + a(-b) &= a(b-b) && \text{axioma I5} \\ &= a \cdot 0 && \text{axioma I4} \\ &= 0 && \text{ejercicio 4.} \end{aligned}$$

Es decir $a(-b)$ es el inverso aditivo de ab, luego por la unicidad del inverso aditivo axioma I6, $a(-b) = -(ab)$. □

Algunos resultados similares pueden encontrarse en los siguientes ejercicios. Como aún no tenemos todos los axiomas correspondientes a los enteros, los resultados no son particularmente interesantes, pero lo que importa es recordar que pueden ser probados sobre la base única de los axiomas.

§ *Ejercicios*

1) Demostrar la regla $(a+b)c = ac + bc$, explicando cada paso.

2) Como siempre x^2 denota $x \cdot x$. Demostrar que dados dos enteros a y b tal que $a + b \neq 0$, entonces existe un único c tal que $(a+b)c = a^2 - b^2$.

3) Probar que hay un único elemento neutro del producto.

4) La siguiente es una demostración de la fórmula $0x = 0$ usando solo los axiomas planteados antes. Escribir la demostración completa, explicando que axioma es usado en cada paso.

$$\begin{aligned} 0x &= (0+0)x && \text{(axioma .....)} \\ &= 0x + 0x. && \text{(axioma .....)} \end{aligned}$$

Luego $0x = 0x + 0x$. Sumando $-0x$ a ambos miembros de la igualdad, obtenemos

$$\begin{aligned} 0x + (-0x) &= 0x + 0x + (-0x) && \text{(usando lógica formal)} \\ 0 &= 0x + 0 && \text{(axioma ..... dos veces)} \\ 0 &= 0x. && \text{(axioma .....)} \end{aligned}$$

1.2 ORDENANDO LOS ENTEROS

El orden natural de los enteros es tan importante como sus propiedades aritméticas. Desde el comienzo aprendemos los números en el orden $1, 2, 3, 4, 5$, y el hecho de que 4 es "mayor" que 3 se convierte en algo de importancia práctica para nosotros. Expresamos esta idea formalmente diciendo que existe una relación que indicamos "$<$" ($a < b$ se lee: a es menor que b).

Solo cuatro axiomas se necesitan para especificar las propiedades básicas del símbolo $<$, y ellos son listados en lo que sigue. La numeración de los axiomas se continúa de la sección 1.1. Como antes, a, b y c denotan enteros arbitrarios.

I8) *Ley de tricotomía.* Vale una y sólo una de las relaciones siguientes:

$$a < b, \qquad a = b, \qquad b < a.$$

I9) *Ley transitiva.* Si $a < b$ y $b < c$, entonces $a < c$.

I10) *Compatibilidad de la suma con el orden.* Si $a < b$, entonces $a + c < b + c$.

I11) *Compatibilidad del producto con el orden.* Si $a < b$ y $0 < c$, entonces $ac < bc$.

Esta claro que podemos definir los otros símbolos de orden $>$, $\leqslant$ y $\geqslant$, en términos de los símbolos $<$ e $=$. Diremos que $m > n$, o que m es mayor que n, si $n < m$, diremos que $m \leqslant n$ si $m < n$ o $m = n$. Finalmente, diremos que $m \geqslant n$ si $m > n$ o $m = n$. Es importante notar que el axioma **I11** tiene una versión valedera para estos nuevos símbolos.

a) **($>$)** Si $a > b$ y $c > 0$, entonces $ac > bc$.

b) **($\leqslant$)** Si $a \leqslant b$ y $0 \leqslant c$, entonces $ac \leqslant bc$.

c) **($\geqslant$)** Si $a \geqslant b$ y $c \geqslant 0$, entonces $ac \geqslant bc$.

Usando las definiciones de $\geqslant$, $<$, $>$ y el axioma **I11** original es muy sencillo demostrar estas variantes. Por otro lado,

Proposición 1.2.1. *Sean* $a, b, c \in \mathbb{Z}$.

a) Si $c < 0$, *entonces* $0 < -c$.

b) Si $a < b$ *y* $c < 0$, *entonces* $ac > bc$.

Demostración (*).

a) Sumando $-c$ a ambos miembros de la desigualdad $c < 0$, obtenemos $c + (-c) < 0 + (-c)$ (compatibilidad de la suma con la relación de orden).

Por los axiomas de inverso aditivo y elemento neutro, la expresión se reduce a $0 < -c$.

b) Como $a < b$, si sumamos a ambos miembros de la desigualdad $-a - b$, por la compatibilidad de la suma con $<$, obtenemos $a - a - b < b - a - b$ y por la aplicación reiterada de los axiomas de inverso aditivo y elemento neutro obtenemos $-b < -a$. Por a) sabemos que $0 < -c$, por lo tanto, por **I11**, $(-b)(-c) < (-a)(-c)$. Aplicando la regla de los signos obtenemos $bc < ac$ y por lo tanto $ac > bc$.

□

Ya hemos usado (en axiomas **I4** e **I7**) el símbolo $\neq$ que denota "*no* es igual a " o bien "es distinto a". En general, cuando tachamos un símbolo, estamos indicando la negación de la relación que define. Por ejemplo, $a \not< b$ denota "a *no* es menor que b".

Observación. Demostremos que $a \not< b$ es equivalente a $a \geqslant b$: por la ley de tricotomía axioma **I8** tenemos que solo vale una y solo una de las siguientes afirmaciones

$$a < b, \qquad a = b, \qquad b < a.$$

Como $a \not< b$, entonces vale una de las dos afirmaciones siguientes, $a = b$ o $b < a$, es decir vale que $a \geqslant b$. De forma análoga se prueba que $a \leqslant b$ si y sólo si $a > b$, $a \not> b$ si y sólo si $a \leqslant b$ y $a \ngeqslant b$ si y sólo si $a < b$.

Ejemplo 1.2.2. Demostremos las siguiente propiedades de $\leqslant$. Sean a, b y c enteros arbitrarios, entonces

O1) *Reflexividad.* $a \leqslant a$.

O2) *Antisimetría.* Si $a \leqslant b$ y $b \leqslant a$, entonces $a = b$.

O3) *Transitividad.* Si $a \leqslant b$ y $b \leqslant c$, entonces $a \leqslant c$.

Demostración.

(**O1**) Como $a = a$, tenemos entonces que $a \leqslant a$ (por definición de $\leqslant$).

(**O2**) Como $a \leqslant b$, tenemos que $a < b$ o bien $a = b$ (por tricotomía no pueden valer ambas). Si ocurriera que $a < b$, por la observación anterior, tendríamos que $a \ngeqslant b$, es decir $b \nleqslant a$, lo cual es absurdo pues una de nuestras hipótesis es, justamente, lo contrario: $b \leqslant a$. Es decir, la única posibilidad que queda es que $a = b$.

(**O3**) Como $a \leqslant b$, entonces $a < b$ o bien $a = b$. Como $b \leqslant c$, entonces $b < c$ o bien $b = c$. Para hacer la demostración, debemos pensar en todas las posibles combinaciones de estas afirmaciones:

- $a < b$ y $b < c$. Es este caso, por **I9**, $a < c$. Luego $a \leqslant c$.
- $a < b$ y $b = c$. Luego $a < c$ y eso implica que $a \leqslant c$.
- $a = b$ y $b < c$. Luego $a < c$ y eso implica que $a \leqslant c$.
- $a = b$ y $b = c$. Es claro entonces que $a = c$, lo cual implica que $a \leqslant c$.

□

Una relación que satisfaga las tres propiedades anteriores (reflexividad, antisimetría y transitividad) es llamada *una relación de orden*. Observar que $<$ *no* es una relación de orden, en el sentido de la definición anterior.

A primera vista podría parecer que ya tenemos todas las propiedades que necesitamos de $\mathbb{Z}$, pero, sorprendentemente, aún falta un axioma de vital importancia. Supongamos que X es un subconjunto de $\mathbb{Z}$; entonces diremos que el entero b es una *cota inferior* de X si

$$b \leqslant x \qquad \text{para todo } \ x \in X.$$

Algunos subconjuntos no tienen cotas inferiores: por ejemplo, el conjunto de los enteros negativos $-1, -2, -3, \ldots$, claramente no tiene cota inferior. Por otro lado, el conjunto S denotado por los números resaltados en la Fig. 1 tiene muchas cotas inferiores. Una mirada rápida nos dice que -9 por ejemplo es una cota inferior, mientras que una inspección más minuciosa revela que -7 es la "mejor" cota inferior, pues en realidad pertenece a S. En general, una cota inferior de un conjunto X que es a su vez es un elemento de X, es conocido como el *mínimo* de X.

$$-10, -9, -8, \mathbf{-7}, \mathbf{-6}, -5, -4, \mathbf{-3}, -2, -1, 0, \mathbf{1}, \mathbf{2}, \mathbf{3}, 4, 5, 6, 7, 8, 9, 10$$

Figura 1: El mínimo de S es -7.

Nuestro último axioma para $\mathbb{Z}$ afirma algo que es (aparentemente) una propiedad obvia.

I12) Si X es un subconjunto de $\mathbb{Z}$ que no es vacío y tiene una cota inferior, entonces X tiene un mínimo.

El axioma **I12** es conocido como el *axioma de buena ordenación* o *axioma del buen orden* o *principio de buena ordenación*. Una buena forma de entender su significado es considerar X un conjunto de enteros acotado inferiormente y un juego en el cual dos personas eligen alternativamente un elemento de X, sujetos a la regla de que cada número debe ser estrictamente menor que el anterior. El axioma nos dice que cuando los números son enteros, el juego terminará; además el final se producirá cuando uno de los jugadores tenga el buen sentido de elegir el mínimo. Esta propiedad aparentemente

obvia *no* se mantiene necesariamente cuando tratamos con números que no son enteros, pues X puede no tener un mínimo aunque tenga una cota inferior. Por ejemplo supongamos que X es el conjunto de fracciones $3/2, 4/3, 5/4, \ldots$ teniendo por forma general $(n+1)/n$, $n \geqslant 2$. Este conjunto tiene una cota inferior (1, por ejemplo) pero no tiene mínimo y por lo tanto los jugadores podrían seguir jugando para siempre, eligiendo fracciones más y más cercanas a 1.

El axioma del buen orden nos da una justificación firme para nuestro intuitivo dibujo de los enteros: un conjunto de puntos regularmente espaciados sobre una linea recta, que se extiende indefinidamente en ambas direcciones como en la Fig. 2. En particular dice que no podemos acercarnos más y más a un entero sin alcanzarlo, de forma que el dibujo de la Fig. 3 no es correcto.

Figura 2: El dibujo correcto de $\mathbb{Z}$.

Figura 3: El dibujo incorrecto de $\mathbb{Z}$.

El hecho de que haya espacios vacíos entre los enteros nos lleva a decir que el conjunto $\mathbb{Z}$ es *discreto* y es esta propiedad la que da origen al nombre "matemática discreta". En cálculo y análisis, los procesos de límite son de fundamental importancia, y es preciso usar aquellos sistemas numéricos que son *continuos*, en vez de los discretos.

El siguiente resultado es obvio, pero debe ser demostrado. Sin embargo, la demostración es bastante compleja y sólo se da por completitud.

Proposición 1.2.3. 1 *es el menor entero mayor que* 0.

Demostración (*). Primero debemos probar que $0 < 1$. Ahora bien, como $0 \neq 1$ (por axioma **I4**), por la ley de tricotomía (axioma **I8**), debe ocurrir que $0 < 1$ o $1 < 0$. Supongamos que $1 < 0$, luego por proposición 1.2.1, $1 \cdot 1 > 1 \cdot 0$. Como 1 es elemento neutro de la multiplicación, obtenemos $1 > 0$, que contradice nuestra suposición. Esta contradicción vino de suponer que $1 < 0$. Por lo tanto, $0 < 1$.

Probaremos ahora que no existe a entero tal que $0 < a < 1$ y lo haremos por el absurdo: supongamos que existe $a \in \mathbb{Z}$ tal que $0 < a < 1$ y sea

$$X = \{a \in \mathbb{Z} : 0 < a < 1\}.$$

La suposición que hicimos implica que X es no vacío. Dado que todos los elementos de X son positivos, X es un subconjunto de $\mathbb{Z}$ acotado inferiormente (0 es cota inferior). Por el axioma del buen orden (axioma **I12**) resulta que X tiene un elemento mínimo, que llamaremos a_0, y cumple

$$0 < a_0 < 1.$$

Usamos ahora la compatibilidad del producto con la relación de orden (**I11**): por un lado multiplicamos por a_0 la desigualdad $0 < a_0$ y obtenemos $0 < a_0^2$, y por otro lado multiplicamos por a_0 la desigualdad $a_0 < 1$ y obtenemos $a_0^2 < a_0$. Es decir

$$0 < a_0^2 < a_0 < 1.$$

La desigualdad $0 < a_0^2 < 1$ dice que $a_0^2 \in X$ pero la desigualdad $a_0^2 < a_0$ dice que a_0 no es el mínimo elemento de X, lo cual es una contradicción pues dijimos que a_0 es el mínimo elemento de X. El absurdo vino de suponer que existe $a \in \mathbb{Z}$ tal que $0 < a < 1$. □

§ *Ejercicios*

1) Sean $a, b \in \mathbb{Z}$ tal que $a, b \neq 0$. Probar que $ab \neq 0$. (Ayuda: considerar primero el caso $a > 0$ y $b > 0$).

2) Demostrar que $\geqslant$ es una relación de orden.

3) Demostrar que dados cualesquiera $a, b, c \in \mathbb{Z}$ vale que si $a < b$ y $0 \leqslant c$, entonces $ac \leqslant bc$.

4) Demostrar que si $a \leqslant b$ y $c \leqslant 0$, entonces $bc \leqslant ac$.

5) Demostrar que $0 \leqslant x^2$ para todo x en $\mathbb{Z}$.

6) Deducir de la proposición 1.2.3 que $n + 1$ es el menor entero mayor que n para todo n en $\mathbb{Z}$.

7) Demostrar que si un conjunto X tiene mínimo, este es único. Dicho más formalmente: demostrar que si existen $c, c' \in X$ tal que $c \leqslant x$ y $c' \leqslant x$ para todo $x \in X$, entonces $c = c'$.

8) En cada uno de los siguientes casos decir si el conjunto X tiene o no una cota inferior, y si la tiene, encontrar el mínimo.

   (1) $X = \{x \in \mathbb{Z} | x^2 \leqslant 16\}$.

   (2) $X = \{x \in \mathbb{Z} | x = 2y \text{ para algún } y \in \mathbb{Z}\}$.

   (3) $X = \{x \in \mathbb{Z} | x \leqslant 100\, x\}$.

9) Un subconjunto Y de Z se dice que tiene una *cota superior* c si $c \geqslant y$ para todo $y \in Y$. Una cota superior que además es un elemento de Y

es llamada el *máximo* de Y. Usar el axioma **I12** para demostrar que si Y es no vacío y tiene una cota superior, entonces tiene máximo. [Ayuda: aplicar el axioma al conjunto cuyos elementos son $-y$ ($y \in Y$).]

10) Los enteros n que satisfacen $1 \leqslant n \leqslant 25$ están acomodados en forma arbitraria en un arreglo cuadrado de cinco filas y cinco columnas. Se selecciona el máximo de cada fila, y se denota s al mínimo entre ellos. De manera similar, el mínimo de cada columna es seleccionado y t denota al máximo entre ellos. Demostrar que $s \geqslant t$ y de un ejemplo en el cual $s \neq t$.

1.3 DEFINICIONES RECURSIVAS

Sea $\mathbb{N}$ el conjuntos de enteros positivos, esto es

$$\mathbb{N} = \{n \in \mathbb{Z} | n \geqslant 1\},$$

y denotemos $\mathbb{N}_0$ el conjunto $\mathbb{N} \cup \{0\}$, esto es

$$\mathbb{N}_0 = \{n \in \mathbb{Z} | n \geqslant 0\}.$$

$\mathbb{N}$ es llamado el conjunto de *números naturales*. Si X es un subconjunto de $\mathbb{N}$ (o de $\mathbb{N}_0$) entonces automáticamente tiene una cota inferior, pues cada elemento x de X satisface $x \geqslant 1$ (o $x \geqslant 0$). Así, en este caso el axioma del buen orden toma la forma

si X es un subconjunto no vacío de $\mathbb{N}$ o $\mathbb{N}_0$ entonces X tiene un mínimo.

Esta la forma más usada en la práctica.

Nuestro primer uso del axioma del buen orden será para justificar un procedimiento muy usual. Frecuentemente encontramos una expresión de la forma u_n, donde n indica cualquier entero positivo: por ejemplo, podríamos tener $u_n = 3n + 2$, o $u_n = (n + 1)(n + 2)(n + 3)$. En estos ejemplos u_n es dado por una fórmula explícita o *cerrada* y no existe dificultad en calcular u_n cuando se nos da un valor específico para n. Sin embargo en muchos casos el valor de u_n viene dado por los valores anteriores y no conocemos una fórmula cerrada; es más, nuestro problema puede ser encontrarla. En estos casos pueden darnos ciertos valores de u_n para enteros positivos n pequeños, y una relación entre el u_n general y algunos de los u_r con $r < n$. Por ejemplo, supongamos nos es dado

$$u_1 = 1, \qquad u_2 = 2, \qquad u_n = u_{n-1} + u_{n-2}, \qquad n \geqslant 3.$$

Para calcular los valores de u_n para todo n de $\mathbb{N}$ podemos proceder como sigue:

$$\begin{aligned} u_3 &= u_2 + u_1 = 2 + 1 = 3, \\ u_4 &= u_3 + u_2 = 3 + 2 = 5, \\ u_5 &= u_4 + u_3 = 5 + 3 = 8, \end{aligned}$$

y así siguiendo. Éste es un ejemplo de una *definición recursiva*. Es "obvio" que el método dará un valor único de u_n para todo entero positivo n. Pero hablando estrictamente necesitamos el axioma del buen orden para justificar la conclusión a través de las siguientes líneas.

Supongamos que existe un entero positivo n para el cual u_n no está definido de manera única. Entonces por el axioma del buen orden existe un entero positivo mínimo m con esta propiedad. Como u_1 y u_2 están explícitamente definidos, m no es 1 o 2 y la ecuación $u_m = u_{m-1} + u_{m-2}$ es aplicable. Por la definición de m, u_{m-1} y u_{m-2} están definidos de manera única, y la ecuación nos da un valor único para u_m , contrariamente a la hipótesis. La contradicción surge de suponer que no está bien definido para algún n, y por lo tanto esta suposición debe ser falsa.

El lector no debe desanimarse por el uso de argumentos tan retorcidos para establecer algo que es "obviamente" verdadero. En primer lugar, no debemos usar resultados ilegítimamente (sin demostrarlos), y en segundo lugar, el hecho de que el resultado sea "obvio" simplemente indica que estamos trabajando con la correcta representación mental de $\mathbb{N}$ y $\mathbb{Z}$. Una vez que hemos establecido esa representación sobre bases firmes podemos empezar a extendernos y obtener resultados que no sean tan "obvios".

El método de definición recursiva aparecerá bastante seguido en el resto del apunte. Existen otras formas de este procedimiento que se "esconden" por su notación. ¿Qué significan las siguientes expresiones?

$$\sum_{r=1}^{n} 2r-1, \qquad 1+3+5+\cdots+(2n-1).$$

Claramente no basta decir que uno significa lo mismo que el otro, porque cada uno contiene un misterioso símbolo, $\sum$ y $\cdots$, respectivamente. Lo que deberíamos decir es que cada uno de ellos es equivalente a la expresión s_n, dada por la siguiente definición recursiva:

$$s_1 = 1, \qquad s_n = s_{n-1} + (2n-1), \qquad n \geqslant 2.$$

Esto hace ver claro que ambos símbolos misteriosos son, en realidad, una forma de acortar una definición recursiva, y que por lo tanto son expresiones definidas para todo n en $\mathbb{N}$.

Ideas similares pueden aplicarse a la definición de productos tal como $n!$ (que se lee n *factorial*). Si decimos que

$$n! = 1 \cdot 2 \cdot 3 \cdots n,$$

el significado es bastante claro para cualquiera. Pero para precisar debemos usar las definiciones recursivas.

Definición 1.3.1. Sea $n \in \mathbb{N}$ sean a_i para $1 \leqslant i \leqslant n$, una secuencia de números (enteros, reales, etc.). Entonces $\sum_{i=1}^{n} a_i$ denota la función recursiva definida

$$\sum_{i=1}^{1} a_i = a_1, \qquad \sum_{i=1}^{n} a_i = \sum_{i=1}^{n-1} a_i + a_n \quad (n \geqslant 2).$$

En este caso decimos que $\sum_{i=1}^{n} a_i$ es la *sumatoria* de los a_i de $i = 1$ a n. El símbolo $\prod_{i=1}^{n} a_i$ denota la función recursiva definida

$$\prod_{i=1}^{1} a_i = a_1, \qquad \prod_{i=1}^{n} a_i = \prod_{i=1}^{n-1} a_i \cdot a_n \quad (n \geqslant 2).$$

En este caso decimos que $\prod_{i=1}^{n} a_i$ es la *productoria* de los a_i de $i = 1$ a n.

En el caso de $n!$ se puede o bien definir como $\prod_{i=1}^{n} i$, o bien como

$$1! = 1, \qquad n! = n \cdot (n-1)! \quad (n \geqslant 2).$$

Otro caso que debemos mencionar es el de la definición de "n-ésima potencia": sea x un número, si $n \in \mathbb{N}$ definimos

$$x^1 = x, \qquad x^n = x \cdot x^{n-1} \quad (n \geqslant 2).$$

Por completitud, definimos $x^0 = 1$.

§ *Ejercicios*

1) En el caso siguiente calcule (donde sea posible) los valores de u_1, u_2, u_3 y u_4 dados por las ecuaciones. Si no puede calcular los valores explicar porque la definición no esta bien.

   a) $u_1 = 1, \quad u_2 = 1, \quad u_n = u_{n-1} + 2u_{n-2}, \quad n \geqslant 3.$

   b) $u_1 = 1, \quad u_n = u_{n-1} + 2u_{n-2}, \quad n \geqslant 2.$

   c) $u_1 = 0, \quad u_n = nu_{n-1}, \quad n \geqslant 2.$

2) Sea u_n definido por las ecuaciones

   $$u_1 = 2, \qquad u_n = 2^{u_{n-1}}, \qquad n \geqslant 2.$$

   ¿Cuál es el primer valor de n para el cual no se puede calcular u_n usando una calculadora de bolsillo o de su celular?

3) Escribir fórmulas explícitas para las expresiones u_n definidas por las siguientes ecuaciones.

   a) $u_1 = 1, \quad u_n = u_{n-1} + 3, \quad n \geqslant 2.$

   b) $u_1 = 1, \quad u_n = n^2 u_{n-1}, \quad n \geqslant 2.$

1.4 EL PRINCIPIO DE INDUCCIÓN

Supongamos que nos piden que demostremos el resultado

$$1+3+5+\cdots+(2n-1)=n^2. \tag{1.4.1}$$

En otras palabras, debemos demostrar que la expresión de la izquierda definida recursivamente es igual a la expresión definida explícitamente por la fórmula de la derecha, para todos los enteros positivos n. Podemos proceder como sigue.

La fórmula es ciertamente correcta cuando $n = 1$ puesto que $1 = 1^2$. Supongamos que es correcta para un valor específico de n, digamos para $n = k$, de modo que

$$1+3+5+\cdots+(2k-1)=k^2.$$

Podemos usar esto para simplificar la expresión definida recursivamente a la izquierda cuando n es igual a $k+1$,

$$\begin{aligned} 1+3+5+\cdots+(2k+1) &= 1+3+5+\cdots+(2k-1)+(2k+1) \\ &= k^2+(2k+1) \\ &= (k+1)^2. \end{aligned} \tag{1.4.2}$$

Por lo tanto si el resultado es correcto cuando $n = k$, entonces lo es cuando $n = k+1$. Se comienza observando que si es correcto cuando $n = 1$, debe ser por lo tanto correcto cuando $n = 2$. Con el mismo argumento como es correcto cuando $n = 2$ debe serlo cuando $n = 3$. Continuando de esta forma veremos que es correcto para todos los enteros positivos n.

La esencia de este argumento es comúnmente llamada *principio de inducción*. Es una técnica poderosa, fácil de aplicar y la aplicaremos frecuentemente. Pero primero debemos examinar sus bases lógicas y para hacerlo necesitamos una formulación más general.

Supongamos que queremos demostrar que un resultado es verdadero para todo $n \in \mathbb{N}$. Con S denotemos al subconjunto de $\mathbb{N}$ para el cual el resultado es correcto: por supuesto, nuestra intención es probar que S es todo $\mathbb{N}$. El primer paso es probar que 1 pertenece a S, y luego demostraremos que si k pertenece a S, también $k+1$. Entonces lo pensamos paso a paso, un procedimiento infinito, y concluimos que $S = \mathbb{N}$. Afortunadamente el pensarlo paso a paso no es esencial debido a que el principio de inducción es consecuencia de los axiomas que elegimos tan cuidadosamente para $\mathbb{Z}$ y $\mathbb{N}$. Más específicamente es consecuencia del axioma del buen orden.

Veamos esto aplicado al ejemplo anterior: supongamos que la fórmula (1.4.1) no fuera cierta, es decir que el conjunto de números naturales que no

cumplen con la fórmula no es vacío. Por el principio de buena ordenación ese conjunto tiene un mínimo, digamos m. Como hemos visto más arriba $m > 1$ y por lo tanto $m - 1 \in \mathbb{N}$. Como m era el mínimo número natural que no cumplía la formula, es claro que $m - 1$ sí la cumple. Haciendo un desarrollo similar a (1.4.2) obtenemos que m cumple con la fórmula, con lo cual se llega a un absurdo que vino de suponer que la fórmula era falsa. Este razonamiento puede ser generalizado en el siguiente teorema.

Teorema 1.4.1 (Principio de inducción)**.** *Supongamos que* S *es un subconjunto de* $\mathbb{N}$ *que satisface las condiciones*

a) $1 \in S$,

b) para cada $k \in \mathbb{N}$, *si* $k \in S$ *entonces* $k + 1 \in S$.

Entonces se sigue que $S = \mathbb{N}$.

Demostración. Si la conclusión es falsa, $S \neq \mathbb{N}$ y el conjunto complementario S^c definido por

$$S^c = \{r \in \mathbb{N} | r \notin S\}$$

es no vacío. Por el axioma del buen orden, S^c tiene un menor elemento m. Como por *a)* el 1 pertenece a S, $m \neq 1$. Se sigue que $m - 1$ pertenece a $\mathbb{N}$ y como m es el mínimo de S^c, $m - 1$ debe pertenecer a S. Poniendo $k = m - 1$ en la condición *b)*, concluimos que m esta en S, lo cual contradice el hecho de que m pertenece a S^c. De este modo, la suposición $S \neq \mathbb{N}$ nos lleva a un absurdo, y por lo tanto tenemos $S = \mathbb{N}$. □

En la práctica, generalmente presentamos una "demostración por inducción" en términos más descriptivos. El hecho de que el resultado es verdadero cuando $n = 1$ se llama *base de la inducción* o *caso base*, *b)* del teorema 1.4.1 es llamado el *paso inductivo* y la suposición de que es verdadero cuando $n = k$ es llamada *hipótesis inductiva*. Cuando se utilizan estos términos, no es necesario introducir explícitamente el conjunto S.

El principio de inducción es útil para probar la veracidad de propiedades relativas a los números naturales. Por ejemplo, consideremos las siguientes propiedades $P(n)$, $Q(n)$ y $R(n)$:

a) $P(n)$ es la propiedad: $2n - 1 < n^2 + 1$,

b) $Q(n)$ es la afirmación: si n es par entonces n es divisible por 4,

c) $R(n)$ es la afirmación: $2n < n - 1$.

Intuitivamente notamos que $P(n)$ es verdadera para cualquier n natural, $Q(n)$ lo es para algunos valores de n y es falsa para otros y $R(n)$ es falsa para todo valor de n. Sin embargo, para verificar realmente que la propiedad $P(n)$

es verdadera para todo n natural no podemos hacerlo probando para cada n en particular. Resulta entonces muy útil la siguiente versión equivalente del principio de inducción.

Teorema 1.4.2. *Sea* $P(n)$ *una propiedad para* $n \in \mathbb{N}$ *tal que:*

a) $P(1)$ *es verdadera.*

b) Para todo $k \in \mathbb{N}$, $P(k)$ *verdadera implica* $P(k+1)$ *verdadera.*

Entonces $P(n)$ *es verdadera para todo* $n \in \mathbb{N}$.

Demostración. Basta tomar

$$S = \{n \in \mathbb{N} | P(n) \text{ es verdadera}\}.$$

Entonces S es un subconjunto de $\mathbb{N}$ y las condiciones *a)* y *b)* nos dicen que $1 \in S$ y si $k \in S$ entonces $k+1 \in S$. Por el teorema 1.4.1 se sigue que $S = \mathbb{N}$, es decir que $P(n)$ es verdadera para todo n. natural. □

En la notación del teorema anterior, *a)* es llamado el *caso base*, *b)* es llamado el *paso inductivo* y $P(k)$ es llamada la *hipótesis inductiva*. El paso inductivo consiste en probar que $P(k) \Rightarrow P(k+1)$ o, equivalentemente, podemos suponer $P(k)$ verdadera y a partir de ella probar $P(k+1)$.

Ejemplo 1.4.3. Sea $a \in \mathbb{Z}$ tal que $0 < a$. Probemos que $0 < a^n$ para todo $n \in \mathbb{N}$.

Demostración.

(*Caso base*) El resultado es verdadero cuando $n = 1$ pues $0 < a = a^1$.

(*Paso inductivo*) Supongamos que el resultado verdadero cuando $n = k$, o sea, que la hipótesis inductiva es $0 < a^k$. Entonces, como $0 < a$, multiplicando por a ambos lados de la desigualdad obtenemos, por la compatibilidad de $<$ con el producto, que $a \cdot 0 < a^k \cdot a$, es decir $0 < a^{k+1}$. Luego el resultado es verdadero cuando $n = k+1$ y por el principio de inducción, es verdadero para todos los enteros positivos n. □

Ejemplo. El entero x_n esta definido recursivamente por

$$x_1 = 2, \qquad x_n = x_{n-1} + 2n, \qquad n \geqslant 2.$$

Demostremos que

$$x_n = n(n+1) \qquad \text{para todo } n \in \mathbb{N}.$$

Demostración.

(*Caso base*) El resultado es verdadero cuando $n = 1$ pues $2 = 1 \cdot 2$.

(*Paso inductivo*) Supongamos que el resultado verdadero cuando $n = k$, o sea, que la hipótesis inductiva es $x_k = k(k+1)$. Entonces

$$\begin{aligned} x_{k+1} &= x_k + 2(k+1) && \text{(por la definición recursiva)} \\ &= k(k+1) + 2(k+1) && \text{(por hipótesis inductiva)} \\ &= (k+1)(k+2). && \text{(propiedad distributiva)} \end{aligned}$$

Luego el resultado es verdadero cuando $n = k+1$ y por el principio de inducción, es verdadero para todos los enteros positivos n. □

Existen varias formas modificadas del principio de inducción. A veces es conveniente tomar como base inductiva el valor $n = 0$, por otro lado puede ser apropiado tomar un valor como 2 o 3 porque los primeros casos pueden ser excepcionales. Cada problema debe ser tratado según sus características. Otra modificación útil es tomar como hipótesis inductiva la suposición de que el resultado es verdadero para todos los valores $n \leqslant k$, más que para $n = k$ solamente. Esta formulación es llamada *el principio de inducción completa*. Todas esas modificaciones pueden justificarse con cambios triviales en la demostración del teorema 1.4.1

El siguiente teorema incorpora todas las modificaciones del principio de inducción mencionadas más arriba.

Teorema 1.4.4 (Principio de inducción completa)**.** *Supongamos que n_0 es cualquier entero (no necesariamente positivo), y sea $\mathbb{Z}_{\geqslant n_0}$ el conjunto de enteros n tal que $n \geqslant n_0$. Sea S un subconjunto de $\mathbb{Z}_{\geqslant n_0}$ que satisface las condiciones:*

a) $n_0 \in S$,

b) si $h \in S$ *para todo* h *en el rango* $n_0 \leqslant h \leqslant k$ *entonces* $k+1 \in S$.

Entonces se sigue que $S = \mathbb{Z}_{\geqslant n_0}$.

Demostración (*). Si la conclusión es falsa, $S \neq \mathbb{Z}_{\geqslant n_0}$ y el conjunto complementario (en X) S^c definido por

$$S^c = \{r \in \mathbb{Z}_{\geqslant n_0} | r \notin S\}$$

es no vacío. Como $\mathbb{Z}_{\geqslant n_0}$ es un conjunto acotado inferiormente por n_0, por el axioma del buen orden, S^c tiene un menor elemento m. Como n_0 pertenece a S, $m \neq n_0$. Se sigue que $m-1$ pertenece a X y como m es el mínimo de S^c, $m-1$ debe pertenecer a S. Poniendo $k = m-1$ en la condición *b)*, concluimos que m esta en S, lo cual contradice el hecho de que m pertenece a S^c. De este modo, la suposición $S \neq \mathbb{Z}_{\geqslant n_0}$ nos lleva a un absurdo, y por lo tanto tenemos $S = \mathbb{Z}_{\geqslant n_0}$. □

Como se podrá observar, la demostración es muy similar a la del teorema 1.4.1. El teorema anterior lo podemos utilizar para la demostración de propiedades dependientes de números enteros.

Teorema 1.4.5. *Sea* n_0 *número entero y sea* $P(n)$ *una propiedad para* $n \geqslant n_0$ *tal que:*

a) $P(n_0)$ *es verdadera.*

b) Si $P(h)$ *verdadera para toda* h *tal que* $n_0 \leqslant h \leqslant k$ *implica* $P(k+1)$ *verdadera.*

Entonces $P(n)$ *es verdadera para todo* $n \geqslant n_0$.

Demostración. Ejercicio. □

Ejemplo. Sean

$$u_1 = 3, \qquad u_2 = 5, \qquad u_n = 3u_{n-1} - 2u_{n-2}, \qquad n \geqslant 3.$$

Probemos que $u_n = 2^n + 1$, para todo $n \in \mathbb{N}$.

Solución. Aquí el caso base es 2, pero para demostrar el resultado debemos verificar el resultado para $n = 1, 2$ y por lo tanto nos tomaremos la licencia de decir que el caso base es $n = 1$ y $n = 2$.

(*Caso base*) El resultado es verdadero cuando $n = 1$ pues $3 = 2^1 + 1$ y para $n = 2$ pues $5 = 2^2 + 1$.

(*Paso inductivo*) Supongamos que $k \geqslant 2$ y el resultado es cierto para los h tales que $1 \leqslant h \leqslant k$. Es decir que $u_h = 2^h + 1$ para $1 \leqslant h \leqslant k$ y $k \geqslant 2$ (hipótesis inductiva), entonces

$$\begin{aligned} u_{k+1} &= 3u_k - 2u_{k-1} && \text{(por definición recursiva)} \\ &= 3(2^k + 1) - 2(2^{k-1} + 1) && \text{(por hipótesis inductiva)} \\ &= 3 \cdot 2^k + 3 - 2 \cdot 2^{k-1} - 2 \\ &= 3 \cdot 2^k + 1 - 2^k \\ &= 2 \cdot 2^k + 1 \\ &= 2^{k+1} + 1. \end{aligned}$$

□

Ejemplo. Sea $a \in \mathbb{Z}$ y $n \in \mathbb{N}$. Definimos a^n de la siguiente manera:

$$a^1 = a, \qquad a^{n+1} = a^n \cdot a \qquad \text{para } n > 1. \tag{1.4.3}$$

Si $n, m \in \mathbb{N}$ verifiquemos las siguientes propiedades

a) $a^n \cdot a^m = a^{n+m}$.

b) $(a^n)^m = a^{nm}$

Solución. Veamos la afirmación *a)*. Se fijará n y se hará inducción sobre m.

(*Caso base*) Debemos ver que $a^n \cdot a^1 = a^{n+1}$, lo cual es verdadero por la definición recursiva (1.4.3).

(*Paso inductivo*) Supongamos que el resultado es verdadero para $m = k$, es decir que $a^n \cdot a^k = a^{n+k}$ (hipótesis inductiva). Veamos que $a^n \cdot a^{k+1} = a^{n+k+1}$. Ahora bien,

$$\begin{aligned} a^n \cdot a^{k+1} &= a^n \cdot a^k \cdot a && \text{(definición (1.4.3))} \\ &= a^{n+k} \cdot a && \text{(hipótesis inductiva)} \\ &= a^{n+k+1} && \text{(definición (1.4.3)).} \end{aligned}$$

Probemos ahora *b)*. Al igual que antes, Se fijará n y se hará inducción sobre m.

(*Caso base*) Debemos ver que $(a^n)^1 = a^n$, lo cual es verdadero por la definición recursiva (1.4.3).

(*Paso inductivo*) Supongamos que el resultado es verdadero para $m = k$, es decir que $(a^n)^k = a^{nk}$ (hipótesis inductiva). Veamos que $(a^n)^{k+1} = a^{n(k+1)}$.

$$\begin{aligned} (a^n)^{k+1} &= (a^n)^k \cdot a^n && \text{(definición (1.4.3))} \\ &= a^{nk} \cdot a^n && \text{(hipótesis inductiva)} \\ &= a^{nk+n} && \text{(por } a\text{)} \\ &= a^{n(k+1)}. \end{aligned}$$

□

§ *Ejercicios*

1) Usar el principio de inducción para demostrar que

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

para todos los enteros positivos n.

2) Hacer una tabla de valores de

$$S_n = 1^3 + 2^3 + \cdots + n^3$$

para $1 \leqslant n \leqslant 6$. Basándose en su tabla sugiera una fórmula para S_n. [Ayuda: los valores de S_n son cuadrados perfectos.] Usar el principio de inducción para establecer que la fórmula es correcta para todo $n \geqslant 1$. (Si el método falla ¡su fórmula es equivocada!)

3) Probar que

$$1^4 + 2^4 + \cdots + n^4 = \frac{1}{30} n(n+1)(2n+1)(3n^2+3n-1).$$

4) Usar el principio de inducción para probar que $2^n > n+1$ para todo entero $n \geqslant 2$.

5) Encontrar el menor entero positivo n_0 para el cual sea verdadero que $n! \geqslant 2^n$. Tomando el caso $n = n_0$ como la base inductiva, demostrar que el resultado vale para $n \geqslant n_0$.

6) En los siguientes casos encontrar los valores apropiados de n_0 para la base inductiva y demostrar que la afirmación es verdadera para todos los $n \geqslant n_0$.

   a) $n^2 + 6n + 9 \geqslant 0$,

   b) $n^3 \geqslant 6n^2$.