Notas a [Hal66] (Parte 3: Números naturales)*

Álgebra Superior I / Actuaría 2016-I

1. Números como conjuntos

1.1. Conjuntos inductivos

Definición 1.1. Sea a un conjunto cualquiera. Definimos *sucesor de a* como el conjunto

$$a^+ = a \cup \{a\}.$$

Lo primero que debemos notar de la definición de sucesor es que $a \in a^+$. Esto quizá no es deseable si queremos pensar un conjunto como un número, sin embargo es un detalle técnico que con el tiempo será irrelevante, no es una propiedad que nos importe, se trata de alguna forma de un compromiso que haremos para aceptar que el concepto de número naturales cabe en la teoría de conjuntos.

Con esta notación estamos en posición de trasladar los símbolos que comúnmente usamos como número naturales a la teoría de conjuntos de la siguiente manera:

$$\begin{aligned} 0 &= \varnothing \\ 1 &= 0^+ \\ 2 &= 1^+ \\ &\vdots \end{aligned}$$

Dejaremos entonces en entendido el significado de símbolos como 1456 o 334. Estos símbolos cobrarán perfecto sentido cuando la teoría esté desarrollada lo suficiente, sin embargo no deberíamos tener problema en aceptar este hecho.

Así definidos, los números constituyen una colección de la que no tenemos certeza que sea una conjunto.Por supuesto, esto requiere un importante axioma que nos permitirá establecer con precisión que son los números naturales. Presentamos primero una definición que debe dejar claro que todos los conjuntos que hemos presentado son parte de sus elementos.

*Secciones 11, 12, 13 y 14 de [Hal66]

Definición 1.2. Un conjunto A se dice *inductivo* si, $0 \in A$ y, siempre que $a \in A$ entonces $a^+ \in A$.

Verificaremos ahora una propiedad importante de los conjuntos inductivos, que bajo la intersección son cerrados.

Proposición 1.1. *Sea $\mathcal{F}$ una familia de conjuntos inductivos. Entonces, $\bigcap \mathcal{F}$ es un conjunto inductivo*

Demostración. Primero debemos notar que si $A \in \mathcal{F}$, entonces $0 \in A$ al ser A inductivo. En ese caso $0 \in \bigcap \mathcal{F}$.

Supongamos ahora un elemento $a \in A$ de forma que $A \in \mathcal{F}$. En ese caso $a^+ \in A$ al ser A inductivo. Como hemos tomado el conjunto A de manera arbitraria, podemos concluir que, si $a \in A$ para todo $A \in \mathcal{F}$, entonces $a^+ \in A$ para todo $A \in \mathcal{F}$. En otras palabras $a^+ \in \bigcap F$ siempre que $a \in \bigcap \mathcal{F}$. Debemos concluir entonces que el conjunto $\bigcap \mathcal{F}$ es inductivo como buscábamos. $\square$

Podemos pensar que la mejor forma de definir a los números naturales, es tomando el conjunto inductivo *más pequeño*. Sin embargo, cabe preguntarnos ahora, si esa particular familia será vacía. Para garantizar que esta no lo es requerimos un axioma adicional.

Axioma (de infinitud)**.** Existe un conjunto inductivo.

Estamos ahora en posición de dar una definición del conjunto de los números naturales. Tomemos como I el conjunto inductivo que garantiza el Axioma de infinitud. Definimos

$$\mathbb{N} = \bigcap \{x \in \mathcal{P}(I) \mid x \text{ es inductivo}\} .$$

Este conjunto debe ser inductivo por la proposición 1.1 y, aunque parecería que dicho conjunto está limitado al espectro de A, es posible mostrar que el conjunto es en verdad el más pequeño posible.

Teorema 1.2. *Para todo conjunto inductivo A, tenemos $\mathbb{N} \subset A$. Además, si X es un conjunto inductivo contenido en todo conjunto inductivo, entonces $X = \mathbb{N}$.*

Demostración. Notemos primero que $A \cap I$ debe ser inductivo y además subconjunto de I. Como $\mathbb{N}$ está definido por la intersección de todos los subconjuntos inductivos de I, debemos tener en particular que $\mathbb{N} \subset A \cap I$. Como $A \cap I \subset A$, lo anterior implica $\mathbb{N} \subset A$.

Ahora, supongamos que X es un conjunto inductivo de forma que éste es un subconjunto de todo subconjunto inductivo. En particular debemos tener que $X \subset \mathbb{N}$. Por el párrafo anterior, al ser X inductivo, debemos tener que $\mathbb{N} \subset X$, en ese caso $X = \mathbb{N}$, como afirma el teorema. $\square$

El teorema anterior termina de amarrar la propiedad que buscábamos para $\mathbb{N}$: que sea el conjunto inductivo más pequeño.

Definición 1.3. Por *número natural*, entenderemos cualquier elemento de $\mathbb{N}$. Llamaremos por eso a $\mathbb{N}$ *el conjunto de los números naturales.*

1.2. Propiedades de los números

Ahora que tenemos una construcción básica sobre el marco de la teoría de conjuntos, propondremos lo que comúnmente se conoce como aritmética a través de enunciados propuestos como una definición axiomática por el matemático italiano Giuseppe Peano en 1889. Bajo nuestra formulación, dicho enunciados no resultan axiomáticos en su naturaleza, sino resultados en el marco de la teoría de conjuntos.

Lema 1.3. *Para cada* $m \in \mathbb{N}$*, si* $n \in m$ *entonces* $m \not\subset n$*.*

Demostración. Usaremos el hecho que $\mathbb{N}$ es el menor conjunto inductivo. Para eso tomaremos $S \subset \mathbb{N}$ como el conjunto

$$S = \{m \in \mathbb{N} \mid \text{para todo } n \in \mathbb{N}, \text{ si } n \in m, \text{ entonces } m \not\subset n\}$$

y probaremos que S es inductivo. Como para todo n, $n \notin 0$, entonces $0 \in S$. Supongamos ahora que $m \in S$, y notemos que si $m^+ \subset n$ entonces $m \subset n$ y en consecuencia $n \notin m$, por hipótesis sobre m. Podemos entonces concluir dos cosas: la primera, por contraposición de lo anterior, si $n \in m$, entonces $n \not\subset m^+$ y la segunda que $m^+ \not\subset m$. En otras palabras si $n \in m^+$ entonces $m^+ \not\subset n$ por lo que $m^+ \in S$. Por lo que S es inductivo. Como S es inductivo, entonces $\mathbb{N} \subset S$ y en consecuencia $\mathbb{N} = S$. Eso quiere decir que cualquier número natural satisface la propiedad que buscábamos. □

Lema 1.4. *Para cada* $m \in \mathbb{N}$*, si* $n \in m$*, entonces* $n \subset m$

Demostración. Procedemos de igual forma que en el caso anterior. Definimos $S \subset \mathbb{N}$ como el conjunto

$$S = \{m \in \mathbb{N} \mid \text{para todo } n \in m \text{ entonces } n \subset m\}.$$

En ese caso $0 \in S$ por vacuidad. Supongamos que $m \in S$, entonces si $n \in m^+$ una de dos o $n \in m$ o $n = m$; si $n \in m$, entonces $n \subset m \subset m^+$, si por el contrario $n = m \subset m^+$, de cualquier forma $n \subset m^+$. Eso implica que $m^+ \in S$ por lo que S es inductivo y en ese caso $\mathbb{N} = S$. Esto implica que cada número natural tiene la propiedad que buscamos. □

Teorema 1.5 (Axiomas de Peano)**.** *Lo siguiente es válido para cualesquiera elementos* n *y* m *de* $\mathbb{N}$*:*

1. $0 \in \mathbb{N}$.
2. *Si* $n \in \mathbb{N}$ *entonces* $n^+ \in \mathbb{N}$.
3. *Si* $S \subset \mathbb{N}$ *tal que* $0 \in \mathbb{N}$ *y* $n \in S$ *implica* $n^+ \in \mathbb{N}$*, entonces* $S = \mathbb{N}$.
4. *Siempre* $n^+ \neq 0$.
5. *Si* $n^+ = m^+$ *entonces* $n = m$.

Demostración. Los enunciado en 1 y 2 son resultado de ser $\mathbb{N}$ inductivo. El enunciado en 3 es resultado de ser el menor conjunto inductivo. El enunciado en 4 es consecuencia de la definición de sucesor, pues $n \in n^+$ por lo que $n^+ \neq \varnothing = 0$. En único enunciado que requiere prueba es 5.

Supongamos entonces que $n^+ = m^+$, como $n \in n^+$ entonces $n \in m^+$ por lo que debe ser o $n = m$ o $n \in m$. De manera similar podemos concluir que $m = n$ o $m \in n$. Supongamos que $n \neq m$, en ese caso debemos tener que $n \in m$ y $m \in n$. Por el lema 1.4, $n \in m \subset n$ por lo que $n \in n$ que implica que $n \subset n$ pero el lema 1.3 afirma que esto no puede suceder. Debemos entonces concluir que $n = m$. □

Ejercicios

Ejercicio 1.1. Sean m y $n$elementos de $\mathbb{N}$. Si $m = n$ prueba que $m^+ = n^+$.

Ejercicio 1.2. Prueba que $n \notin n$ para cada elemento de $n \in \mathbb{N}$.

Ejercicio 1.3. Si $n \in \mathbb{N}$ y $n \neq 0$, entonces $0 \in n$.

2. Aritmética

2.1. Teorema de recursión

Teorema 2.1. *Sea A un conjunto cualquiera, $f\colon A \to A$ una función y $a \in A$. Entonces existe una función $u\colon \mathbb{N} \to A$ de forma que $u(0) = a$ y para cada $n \in \mathbb{N}$*

$$u(n^+) = f(u(n))$$

Demostración. Vamos a probar primero que existe un subconjunto $u \subset \mathbb{N} \times A$ del cual verificaremos resulta una función total. Primero, sea

$$\mathcal{C} = \left\{X \in \mathcal{P}(\mathbb{N} \times A) \mid (0, a) \in X \text{ y } (n, x) \in X \text{ implica } (n^+, f(x)) \in X\right\}.$$

Como $\mathbb{N} \times A$ es un subconjunto de si mismo y contiene todas las parejas posibles, entonces $\mathbb{N} \times A \in \mathcal{C}$. El conjunto $\mathcal{C}$ es entonces no vacío.

Definimos

$$u = \bigcap \mathcal{C},$$

afirmamos que satisface la propiedad que define a $\mathcal{C}$. En efecto, si $(n, x) \in u$ entonces para cada $A \in \mathcal{C}$, $(n, x) \in A$, en ese caso $(n^+, f(x)) \in A$ de lo que podemos deducir que $(n^+, f(x)) \in u$. Esto quiere decir que $u \in \mathcal{C}$. Además, si $v \in \mathcal{C}$, debemos tener que $u \subset v$ por definición de intersección; en otras palabras u es el conjunto más pequeño que pertenece a $\mathcal{C}$.

Definimos ahora el conjunto $S \subset \mathbb{N}$ como

$$S = \{n \in \mathbb{N} \mid \text{existe } x \in A \text{ tal que, } (n, x) \in u \text{ y } (n, y) \in u \text{ implica } x = y\}.$$

Probaremos a continuación que el conjunto S es inductivo.

Afirmamos primero que $0 \in S$. Sabemos que $(0, a) \in u$, queremos mostrar que no puede existir $b \neq a$ tal que $(0, b) \in u$. Supongamos que existe tal elemento, entonces si $v = u \backslash \{(0, b)\} \subset u$. Afirmamos $v \in \mathcal{C}$; en efecto, si $(n, x) \in v$ entonces $(n, x) \in u$ por lo que $(n^+, f(x)) \in u$, como $n^+ \neq 0$, entonces $(n^+, f(x)) \neq (0, b)$ por lo que $(n^+, f(x)) \in v$. Sin embargo, eso implicaría que v es más pequeño que u lo que es una contradicción, en ese caso no puede existir $(0, b) \in u$ con $b \neq a$.

Afirmamos ahora que $n \in S$ y deseamos concluir que $n^+ \in S$. Como $n \in S$, debe existir un único $x \in A$ tal que $(n, x) \in u$, como u es un elemento de $\mathcal{C}$, debemos tener $(n^+, f(x))$. Supongamos que existe y tal que $(n^+, y) \in u$ pero $f(x) \neq y$. Procedemos definiendo $v = u \backslash \{(n^+, y)\} \subset u$. Afirmamos que $v \in \mathcal{C}$; en efecto, si $(m, z) \in v$ entonces $(m, z) \in u$, tenemos entonces dos posibilidades, $m = n$ o $m \neq n$. Para la primera, al tener $(n, z) \in u$ y $(n, x) \in u$ y por hipótesis, debemos tener que $z = x$, por lo que podemos afirmar sin más que $(m^+, f(z)) = (n^+, f(x)) \neq (n^+, y)$. Para la segunda, debemos tener que $m^+ \neq n^+$ y en efecto $(m^+, f(z)) \neq (n^+, y)$. De cualquier forma, logramos concluir que $(m^+, f(z)) \in v$ al ser $(m^+, f(z)) \neq (n^+, y)$. Lo anterior afirma lo que queríamos probar acerca de v: $v \in \mathcal{C}$. Esto es por supuesto una contradicción pues u no sería el conjunto más pequeño contenido en $\mathcal{C}$, lo que nos lleva a descartar que existe $y \neq f(x)$. En ese caso $n^+ \in S$ al ser el elemento $f(x)$ el único posible que acompaña a n^+ en u.

Como S es inductivo $S = \mathbb{N}$, por lo que u debe ser una función total de $\mathbb{N}$ en A. Basta probar que u cumple las propiedades que pide el teorema. De entrada, por la definición de $\mathcal{C}$, entonces $(0, a) \in u$, en otras palabras $u(0) = a$. Ahora, $u(n)$ debe cumplir que $(n, u(n)) \in u$ y como $u \in \mathcal{C}$, entonces $(n^+, f(u(n))) \in u$ o lo que es lo mismo $u(n^+) = f(u(n))$. Por lo que u es la función que buscábamos. $\square$

2.2. Operaciones

Teorema 2.2. *Existe una función* $s \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *tal que* $s(m, 0) = m$ *y* $s(m, n^+) = (s(m, n))^+$.

Demostración. Sea $m \in \mathbb{N}$. Usaremos el teorema de recursión para la función $f(x) = x^+$ y $a = m$. En ese caso existe una función $u_m \colon \mathbb{N} \to \mathbb{N}$ tal que $u_m(0) = m$ y $u_m(n^+) = (u_m(n))^+$. como

$$s(m, n) = u_m(n).$$

Afirmamos que esta función tiene las propiedades que buscamos. En efecto,

$$s(m, 0) = u_m(n) = m$$

y

$$s(m, n^+) = u_m(n^+) = (u_m(n))^+$$

$\square$

Definición 2.1. Sean m y n elementos de $\mathbb{N}$ cualquiera. Definimos *la suma de m con n* como el número

$$m + n = s(m, n).$$

Con esta notación, el teorema 2.2 afirma simplemente que $m + 0 = m$ y $m + n^+ = (m + n)^+$. Debemos notar que, a pesar de parecer ya la suma que conocemos, no sabemos si ésta es conmutativa o si es asociativa. Probaremos estos hechos a continuación usando el principio de inducción de manera repetida.

Teorema 2.3. *Para cualesquiera m, n y k números naturales, tenemos*

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

Demostración. Tomemos el conjunto

$$S = \{n \in \mathbb{N} \mid \text{Para cualesquiera } k, m \in \mathbb{N}, (k + m) + n = k + (m + n)\}.$$

Afirmamos que este conjunto es inductivo. En efecto, debemos verificar $0 \in S$ al tener

$$\begin{aligned}(k + m) + 0 &= k + m \\ &= k + (m + 0).\end{aligned}$$

También, si $n \in S$, debemos tener $(k + m) + n = k + (m + n)$, en ese caso

$$\begin{aligned}(k + m) + n^+ &= ((k + m) + n)^+ \\ &= (k + (m + n))^+ \\ &= k + (m + n)^+ \\ &= k + (m + n^+).\end{aligned}$$

Por lo que $n^+ \in S$. Entonces S es inductivo como afirmamos y $S = \mathbb{N}$. El resultado sigue de este hecho. □

Lema 2.4. *Para todo número natural n,*

$$0 + n = n.$$

Demostración. Sea $S \subset \mathbb{N}$ tal que

$$S = \{n \in \mathbb{N} \mid 0 + n = n\}.$$

Afirmamos que S es inductivo. En efecto, como $0 + 0 = 0$, entonces $0 \in S$, además si $n \in S$, i.e. $0 + n = n$, entonces

$$\begin{aligned}0 + n^+ &= (0 + n)^+ \\ &= n^+,\end{aligned}$$

por lo que $n^+ \in S$. Al ser S inductivo $S = \mathbb{N}$ de lo que sigue el resultado. □

Lema 2.5. *Para cualesquiera números m y n,*

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

Demostración. Sea $S \subset \mathbb{N}$ tal que

$$S = \left\{ n \in \mathbb{N} \mid \text{Para todo } m \in \mathbb{N},\ m^+ + n = (m+n)^+ \right\}.$$

Afirmamos que S es inductivo. En efecto, como

$$\begin{aligned} m^+ + 0 &= m^+ \\ &= (m+0)^+ \end{aligned}$$

entonces $0 \in S$. Si suponemos $n \in S$, debemos tener que $m^+ + n = (m+n)^+$, por lo que

$$\begin{aligned} m^+ + n^+ &= \left(m^+ + n\right)^+ \\ &= \left((m+n)^+\right)^+ \\ &= \left(m + n^+\right)^+, \end{aligned}$$

por lo que n^+ pertenece a S. En ese caso S es inductivo como afirmamos y $S = \mathbb{N}$. De aquí sigue el resultado. $\square$

Teorema 2.6. *Para cualesquiera m y n números naturales,*

$$m + n = n + m$$

Demostración. Sea $S \subset \mathbb{N}$ tal que

$$S = \{ m \in \mathbb{N} \mid \text{Para todo } n \in \mathbb{N}\ m + n = n + m \}.$$

Afirmamos que S es inductivo. En efecto, $0 \in S$ al tener

$$\begin{aligned} 0 + n &= n \\ &= n + 0. \end{aligned}$$

Ahora, si $m \in \mathbb{N}$, debemos tener $m + n = n + m$, en ese caso

$$\begin{aligned} m^+ + n &= (m+n)^+ \\ &= (n+m)^+ \\ &= n + m^+, \end{aligned}$$

por lo que $m^+ \in S$. Al ser S inductivo debemos tener $S = \mathbb{N}$ por lo que el resultado sigue. $\square$

Podemos definir de manera muy sencilla como resolver una ecuación que sólo involucre sumas. Habrá que tener cuidado, esto hecho no afirma que existen inversos para la función suma sino que podemos entregar una condición para que los números sean iguales.

Teorema 2.7. *Para cualesquiera números n, m y r, si $n+r=m+r$ entonces $n=m$.*

Demostración. Sea m y n elementos de $\mathbb{N}$ y sea $S \subset \mathbb{N}$ tal que

$$S = \{r \in \mathbb{N} \mid n+r = m+r \text{ implica } n = m\}.$$

Entonces, $0 \in S$ de manera inmediata. Supongamos que $r \in S$, entonces $n+r = m+r$ implica $n = m$, y afirmemos también que $n + r^+ = m + r^+$, en ese caso debemos tener que $(n+r)^+ = (m+r)^+$ por lo que $n+r = m+r$ lo que por hipótesis implica que $n = m$. Esto quiere decir que $r^+ \in S$ y S es entonces inductivo. El resultado sigue pues m y n son arbitrarios. □

Teorema 2.8. *Existe una función $p\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ de forma que $p(m,0) = 0$ y $p(m,n^+) = p(m,n) + m$.*

Demostración. Ejercicios 2.3. □

Definición 2.2. Sean m y n números naturales. Definimos *el producto de m con n* por el número

$$m \cdot n = p(m,n).$$

Lo que afirma el teorema 2.6 sobre el producto entre dos números resulta simplemente en $m\cdot 0 = 0$ y $m \cdot n^+ = m\cdot n + m$.

2.3. Orden en los naturales

Definición 2.3. Dos números naturales m y n se dicen comparables si

$$m \in n \text{ o } n \in m \text{ o } m = n.$$

Teorema 2.9. *Cualesquiera números naturales m y n son comparables.*

Corolario 2.10. *Solamente sucede una de tres posibilidades,*

$$m \in n \text{ o } n \in m \text{ o } m = n.$$

Corolario 2.11. *Si $m \neq n$, entonces $m \in n$ si y sólo si $m \subset n$.*

Ejercicios

Ejercicio 2.1. Recuerda que para $m \in \mathbb{N}$ se definió la función s_m de manera inductiva como: $s_m(0) = m$ y $s_m(n^+) = (s_m(n))^+$. Sea

$$s = \{((m,n),l) \in (\mathbb{N}\times\mathbb{N})\times\mathbb{N} \mid l = s_m(n)\},$$

demuestra que s es una función de $\mathbb{N}\times\mathbb{N}$ en $\mathbb{N}$.

Ejercicio 2.2. Prueba que $n \neq n^+$ para todo $n \in \mathbb{N}$.

Ejercicio 2.3. Usando el teorema de recursión, encuentra para cada $m \in \mathbb{N}$ una función p_m de forma que: $p_m(0) = 0$ y $p_m(n^+) = p_m(n) + m = s_m(p_m(n))$. Sea

$$p = \{((m,n),l) \in (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \mid l = p_m(n)\},$$

demuestra que p es una función de $\mathbb{N} \times \mathbb{N}$ en $\mathbb{N}$.

Ejercicio 2.4. Sea R la relación en $\mathbb{N}$ definida por

$$R = \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid \text{existe } r \in \mathbb{N} \backslash \{0\} \text{ tal que } n = m + r\}.$$

1. Demuestra que R es una relación irreflexiva y transtiva.
2. Demuestra que para todo m, $(0,m) \in R$.
3. Demuestra que para cada $n \in \mathbb{N}$, $(n,n^+) \in R$.
4. Si $m \in \mathbb{N}$ y

$$T = \{n \in \mathbb{N} \mid n \neq m \text{ o } (n,m) \in R \vee (m,n) \in R\},$$

demuestra que $T = \mathbb{N}$ (Sugerencia: Usa inducción).

Ejercicio 2.5. Sea R la relación en $\mathbb{N}$ definida por

$$R = \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid \text{existe } r \in \mathbb{N} \text{ tal que } n = m + r\}.$$

Demuestra lo siguiente

1. R es una relación reflexiva, transtiva y antisimétrica.
2. Demuestra que para todo m, $(0,m) \in R$.
3. Para todo $n \in \mathbb{N}$, si $(m,n) \in R$ y (n,m^+) entonces $n = m$ o $n = m^+$.
4. Si $m \in \mathbb{N}$ y

$$T = \{n \in \mathbb{N} \mid (n,m) \in R \text{ o } (m,n) \in R\},$$

demuestra que $T = \mathbb{N}$ (Sugerencia: Usa inducción).

Ejercicio 2.6. Demuestra que $m + 1 = m^+$, para todo $m \in \mathbb{N}$.

Ejercicio 2.7. Demuestra que

1. $0 \cdot n = 0$ para todo $n \in \mathbb{N}$.
2. $m^+ \cdot n = m \cdot n + n$ para todo m y n en $\mathbb{N}$.
3. $m \cdot n = n \cdot m$ para todo m y n en $\mathbb{N}$.

Ejercicio 2.8. Demuestra que para cualesquiera m, n y k,

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

Ejercicio 2.9. Demuestra que $m \cdot 1 = m$.

Ejercicio 2.10. Demuestra que para cualesquiera m, n y k,

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

Ejercicio 2.11. Sea $r \neq 0$. Demuestra que para todo m y n en $\mathbb{N}$ si $r \cdot m = r \cdot n$ entonces $m = n$

Ejercicio 2.12. Demuestra que existe una función $e \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que para cualesquiera k y m, $e(k, 0) = 1$ y $e(k, m^+) = e(k, m) \cdot k$. Denotamos a esta función como

$$k^m = e(k, m)$$

.

Ejercicio 2.13. Demuestra que para cualesquiera k, m y n,

$$k^{m+n} = k^m \cdot k^n.$$

Ejercicio 2.14. Demuestra que para cualesquiera k, m y n,

$$(k^m)^n = k^{(m \cdot n)}$$

Ejercicio 2.15. Demuestra para todo n,

$$k^1 = k.$$

3. Orden

3.1. El orden como una relación

Esta sección está destinada únicamente a presentar un lenguaje en el cual se presenten matemáticamente los conceptos de orden que surgirán en la estructura de los números naturales. En particular se debe poner atención en las definiciones de orden total y buen orden.

Definición 3.1 (Orden parcial estricto)**.** Sea R una relación en A. Llamaremos a R un *orden parcial estricto en* A, si es una relación transitiva y irreflexiva.

Para un orden parcial estricto R en A, convendremos en escribir $a < b$ en lugar de $(a, b) \in R$, así como $a \not< b$ cuando $(a, b) \notin R$. Asociaremos otro símbolo a una relación de orden parcial, diremos que $a \leq b$ si $a < b$ o $a = b$.

Proposición 3.1. *Si $<$ es un orden parcial estricto, entonces la relación $\leq$ es transitiva, reflexiva y simétrica.*

Diremos también que una pareja de un conjunto A y un orden parcial estricto $<$ es un conjunto parcialmente ordenado. De manera correcta, se deberá indicar esto como $(A, <)$ sin embargo, será común simplemente decir que A es un conjunto parcialmente ordenado implicando que viene acompañado de una relación de orden.

Definición 3.2. Sea A un conjunto parcialmente ordenado y sea $S \subset A$. Decimos que:

- $a \in S$ es un *máximo en* S, si para todo elemento $b \in S$, tenemos $b \leq a$.
- $a \in S$ es un *mínimo en* S, si para todo elemento $b \in S$, tenemos $a \leq b$.

Proposición 3.2. *En un conjunto parcialmente ordenado, si un máximo o un mínimo existen, entonces son únicos.*

Demostración. Supongamos que a y b son mínimos en A. Por definición a es menor o igual que cualquier otro elemento en A, en particular lo es de b, en ese caso$a \leq b$. De la misma forma debemos tener que $b \leq a$. Por antisimetría de $\leq$, tenemos que $a = b$. Por lo que si A tiene un mínimo, éste es único. De manera análoga, podemos probar que si A tiene un máximo, éste es también único. $\square$

Definición 3.3. Sea $(A, <)$ un conjunto parcialmente ordenado. El orden $<$ se dice que es un *buen orden* si cada subconjunto no vacío de A tiene mínimo, en este caso decimos que $(A, <)$ es *un conjunto bien ordenado.*

Definición 3.4. Sea $(A, <)$ un conjunto parcialmente ordenado. Entonces, cualesquiera dos elementos a y b se dicen *comparables* si es cierto que $a < b$ o $b < a$ o $a = b$.

Definición 3.5. Un orden parcial en un conjunto A, se dice *total* o *lineal*, si para cualquier par de elementos de A son comparables. Un conjunto parcialmente ordenado cuyo orden es total se dice *conjunto totalmente ordenado.*

Proposición 3.3. *Todo buen orden es un orden total.*

Demostración. Sea $(A, <)$ un conjunto bien ordenado. Deseamos concluir que dos elementos cualquiera a y b en A sean comparables. Para esto consideremos el subconjunto de A $\{a, b\}$; al estar el conjunto bien ordenado, dicho conjunto debe tener un mínimo, sea c el mínimo. Esto quiere decir por definición que $c \in \{a, b\}$, en otras palabras, o $c = a$ o $c = b$, si $c = a$, entonces $c \leq b$, mientras que si $c = b$ entonces $b \leq a$. Por lo que a y b resultan comprables como se deseaba. $\square$

Para terminar esta sección resta conectar el lenguaje que se ha introducido hasta ahora de teoría del orden a los números naturales.

Teorema 3.4. *La pareja* $(\mathbb{N}, \in)$ *es un conjunto parcialmente ordenado.*

Corolario 3.5. *La pareja* $(\mathbb{N}, \in)$ *es un conjunto totalmente ordenado.*

Bajo la luz de los resultados anteriores es que se adopta la siguiente convención, inspirada precisamente en la notación de la teoría del orden.

Definición 3.6. Diremos que m *es menor que* n, en símbolos $m < n$, si $m \in n$. Diremos que m *es menor o igual que* n, en símbolos $m \leq n$ si $m < n$ o $m = n$.

Existe otro resultado interesante acerca de los números naturales que está vinculado con la teoría del orden. Sin embargo, responderemos a este hecho con una demostración ligada a principios inductivos en la siguiente sección. Debemos notar que llamaremos al principio en cuestión *de buen orden*, lo cual constituye una clara referencia a esta sección. Cuando dicho principio sea probado como consecuencia de la inducción, el lector no debe tener problema en admitir que los números naturales constituyen entonces un conjunto bien ordenado, desde el punto de vista de teoría del orden.

Ejercicios

Ejercicio 3.1. Sea R una relación transitiva, reflexiva y antisimétrica en A. Si definimos R^* como $(a,b) \in S$ si y sólo si $(a,b) \in R$ y $a \neq b$, demuestra que S es un orden parcial estricto.

Ejercicio 3.2. Recuerda que dado un orden parcial estricto $<$ la relación asociada $\leq$ es transitiva, reflexiva y antisimétrica. Usando la construcción del problema anterior, demuestra que $<=\leq^*$.

Ejercicio 3.3. Sea E un conjunto cualquier y sean A y B subconjuntos de E. Decimos que $A < B$ si $A \subset B$ y $A \neq B$. Muestra que $<$ define una relación de orden parcial estricto.

Ejercicio 3.4. Sean A y B conjuntos no vacíos. Definimos un orden sobre el conjunto

$$B^A = \{f \colon A \to B\}.$$

como: $f \leq g$ si y sólo si $\mathrm{dom}(f) \subset \mathrm{dom}(g)$ y para todo $x \in \mathrm{dom}(f)$ se tiene $f(x) = g(x)$. Muestra que la relación es transitiva, reflexiva y antisimétrica. ¿Por qué esto es suficiente para probar que es un orden?

4. Inducción y orden

4.1. Tipos de inducción

Existen algunas versiones distintas del concepto al que llamamos inducción, sin embargo se trata del mismo concepto con otra presentación. Formularemos en esta sección a que nos referimos con inducción en el marco de la teoría de números naturales hasta ahora presentada. Comencemos presentando un hecho que nos hemos encontrado en diversas ocasiones.

Principio de inducción. Sea $A \subset \mathbb{N}$ de forma que:

- $0 \in A$ y
- si $m \in A$, entonces $m + 1 \in A$.

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

El principio de inducción presentado coincide con uno de los postulados de Peano para los números naturales (teorema 1.5). En ese sentido, el principio de inducción es una propiedad que tienen los naturales como los hemos formulado. Sin embargo, parecería que puede existir una proposición más fuerte acerca del principio de inducción. Proveeremos primero una definición.

Definición 4.1. Sea m cualquier número natural. Definimos *el conjunto de predecesores de m*[1] como el conjunto,

$$P(m) = \{n \in \mathbb{N} \mid n \leq m\}.$$

Principio de indcucción completa. Sea $A \subset \mathbb{N}$ de forma que:

- $0 \in A$ y
- $m + 1 \in A$ siempre que $P(m) \subset A$.

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

Lema 4.1. *Para cualquier número natural m,*

$$P(m + 1) = P(m) \cup \{m + 1\}$$

Demostración. Probaremos el resultado por inducción. Sea

$$S = \{m \in \mathbb{N} \mid P(m + 1) = P(m) \cup \{m + 1\}\}.$$

En ese caso, $0 \in S$; en efecto, las única posibilidades para tener $n \leq 1$ son o $n \in 1$ o $n = 1$, pero si $n \in 1$, entonces $n = 0$, en resumen si $n \leq 1$ entonces $n = 0$ o $n = 1$. Esto implica que $P(1) = \{0, 1\}$

Supongamos ahora que $m \in S$; en ese caso si $n \leq m + 2$ entonces $n \in m + 2$ o $n = m + 2$. En caso que $n \in m + 2$, debemos tener que $n \in m + 1$ o $n = m + 1$ por lo que $n \leq m + 1$. En resumen, si $n \leq m + 2$ entonces $n \leq m + 1$ o $n = m + 2$ por lo que debemos tener $P(m + 2) = P(m + 1) \cup \{m + 2\}$. Esto implica que $m + 1 \in S$ mostrando que es este conjunto es inductivo. En conclusión $S = \mathbb{N}$ y de esto sigue el resultado. □

Teorema 4.2. *El principio de inducción completa es válido en $\mathbb{N}$.*

Demostración. Consideremos A como un conjunto descrito por la hipótesis de inducción completa, i.e., $0 \in A$ y $m+1 \in A$ siempre que $P(m) \subset A$. Supongamos entonces el conjunto como

$$S = \{m \in \mathbb{N} \mid P(m) \subset A\}.$$

Afirmamos que S es inductivo. En efecto, como $P(0) = \{0\}$, entonces $0 \in S$. Supongamos que $m \in S$, entonces $P(m) \subset A$; por hipótesis debemos tener que

[1]Este proceso es en realidad absolutamente innecesario, m como conjunto contiene a todos sus predecesores. Pero se presenta de esta manera para abandonar poco a poco está idea algo extraña que los números contienen otros números.

$m+1 \in A$ pero como $P(m+1) = P(m) \cup \{m+1\}$, entonces $P(m+1) \subset A$, en otras palabras $m+1 \in S$. Debemos concluir que $S = \mathbb{N}$.

Debemos notar ahora un detalle final: si $m \in S$ entonces $P(m) \subset A$ en particular como $m \in P(m)$, $m \in A$. En otras palabras $S \subset A$, y como $S = \mathbb{N}$ entonces $\mathbb{N} \subset A$ y en consecuencia $A = \mathbb{N}$. Esta igualdad es la que se afirma en el principio de inducción completa. $\square$

Como podemos notar, la demostración anterior pone de manifiesto que el principio de inducción completa es un caso particular del caso del principio de inducción. Esto es un hecho notable. Porque parecería que la condición sobre el principio de inducción completa es más fuerte, sin embargo es el lema 4.1 el que nos revela que el conjunto de predecesores se comporta de manera similar la operación de sucesor.

Presentaremos ahora un principio de inducción que de nueva cuenta tiene apariencia de ser un caso general, pero esto resulta sólo una ilusión pues de nueva cuenta resulta ser consecuencia del principio de inducción.

Principio de indcucción generalizado. Sea $A \subset \mathbb{N}$ y sea $n \in \mathbb{N}$ tales que:

- $n \in A$ y
- si $m \in A$, entonces $m+1 \in A$.

Entonces, $\{m \in \mathbb{N} \mid n \leq m\} \subset A$.

Teorema 4.3. *El principio de inducción generalizada es válido en* $\mathbb{N}$.

Demostración. Sean A un conjunto y $n \in \mathbb{N}$ descritos en la hipótesis del principio de inducción generalizado, i.e., $n \in A$ y si $m \in A$ entonces $m+1 \in A$. Definimos el conjunto

$$S = \{r \in \mathbb{N} \mid n + r \in A\}.$$

Afirmamos que éste conjunto es simplemente $\mathbb{N}$.

Primero, como $n+0 = n \in A$, entonces $0 \in S$. Supongamos ahora que $r \in S$; en ese caso $n+r \in A$ y por la forma en que hemos tomado A, $n+(r+1) \in A$, por lo que $r+1 \in S$. En ese caso $S = \mathbb{N}$ como afirmamos.

Tomemos finalmente $T = \{m \in \mathbb{N} \mid n \leq m\}$. Por el párrafo anterior debemos tener que para todo natural r, tenemos $n+r \in A$, y por el ejercicio 4.6, esto significa que $n \leq n+r$, debemos tener $T \subset A$. El resultado sigue de este hecho. $\square$

4.2. Buen orden en los naturales

Volquemos nuestra atención ahora sobre el principio de buen orden. A diferencia de los otros principios que hemos mostrado, este es peculiar: no involucra conjuntos que guarden relación con los conjuntos inductivos. Su enunciado es en realidad idéntico a la definición de conjunto bien ordenado. A pesar de esto, mostraremos que es resultado del principio de inducción por igual, mostrando que el principio de inducción contiene mucha más información de la esperada.

Principio de buena ordenación. Cualquier subconjunto $A \neq \varnothing$ de números naturales tiene un mínimo, i.e., un número $k \in A$ tal que para todo número $m \in A$, se satisface $k \leq m$.

Lema 4.4. *Sean m y n un par de números naturales y sea A cualquier subconjunto de números naturales. Entonces, si para todo $n \leq m$ se tiene que $n \notin A$, debemos tener*

$$A \subset \{k \in \mathbb{N} \mid m+1 \leq k\}.$$

Teorema 4.5. *El principio de buena ordenación es válido en $\mathbb{N}$.*

Demostración. Deseamos probar un subconjunto no vacío A de $\mathbb{N}$ tiene un elemento mínimo procedemos por contraposición. Para esto supondremos que A no tiene un elemento mínimo. Definamos el conjunto

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

Comencemos probando que $0 \in S$. Procedemos por contradicción: Si $0 \notin B$, entonces $0 \in A$, pero sabemos que para todo $n \in \mathbb{N}$, tenemos que $0 \leq n$. En particular, esto debe suceder para todo $n \in A$. En ese caso, 0 sería un mínimo de A, lo que es contradictorio. Concluimos entonces que $0 \in S$.

Supongamos ahora que $P(m) \subset S$, probaremos que $m+1 \in S$ y lo probaremos de igual forma por contradicción. Supongamos que $m+1 \notin S$, en ese caso $m+1 \in A$. Sin embargo, por hipótesis de inducción, para cada $n \leq m$ tenemos que $n \notin A$; por el lema anterior, se tiene que $m+1 \leq k$ para cada $k \in A$, por lo que $m+1$ resultaría un mínimo de A. Este resultado es contradictorio por lo que $m+1 \in S$. Por el principio de inducción completa $S = \mathbb{N}$.

Basta realizar una observación: $S = \mathbb{N} \backslash A$. Si $S = \mathbb{N}$ entonces $A = \varnothing$. Hemos probado con lo anterior, si A no tiene mínimo, entonces $A = \varnothing$. De esto sigue el principio de buena ordenación. □

Ejercicios

Ejercicio 4.1. Sean m y n un par de números naturales y sea A cualquier subconjunto de números naturales. Si para todo $n \leq m$ se tiene que $n \notin A$, demuestra que

$$A \subset \{k \in \mathbb{N} \mid m+1 \leq k\}.$$

Ejercicio 4.2. Para cualesquier números naturales, demuestra que $m < n$ si y sólo si $m+1 < n+1$.

Ejercicio 4.3. Demuestra que si $n < m$ entonces $n+k < m+k$. Sugerencia: Usa inducción sobre k.

Ejercicio 4.4. Si $m < n$ y $k < l$, entonces $m+k < n+l$.

Ejercicio 4.5. Demuestra que si $m < n+1$ entonces $m \leq n$.

Ejercicio 4.6. En este ejercicio demostraremos que $m \leq n$ si y sólo si existe un único número natural k tal que $n = m+k$.

1. Usando inducción sobre n, demuestra que $m \leq n$ implica que existe un número natural k tal que $n = m + k$.

2. Usando inducción sobre k, demuestra que $m + k = n$ implica que $m \leq n$. Sugerencia: Recuerda que $0 < k + 1$.

3. Finalmente, asume que, si $n = m + k'$, entonces $k = k'$

El número k descrito en este ejercicio, usalmente se denota por $n - m$.

Ejercicio 4.7. Demuestra que $m < n$ si y sólo si existe un número natural $r \neq 0$ tal que $n = m + r$. Sugerencia: Usa el ejercicio anterior.

Ejercicio 4.8. Demuestra que, para $r \neq 0$, si $m < n$ entonces $m \cdot r < n \cdot r$

5. Algunas definiciones adicionales

5.1. Sumas

Puede resultar extraño que hemos ya definido la suma y que de nueva cuenta aparece como un tema. Lo que intentamos aquí es sin embargo formalizar el concepto de suma arbitraria, como una definición recursiva y en consecuencia producto del teorema de recursión.

En primera instancia, ¿a qué nos referimos con suma? A una expresión del tipo

$$a_1 + \cdots + a_n.$$

Podemos ver que los puntos indican *algo* pero de manera quisquillosa no podríamos[2] decir que significan. Debemos justificar expresiones de este tipo. Desarmando en su totalidad la expresión anterior vemos que el primero problema resulta en interpretar

$$a_1, \ldots, a_n, \ldots.$$

Esto es realidad sencillo de arreglar, consideraremos $a : \mathbb{N} \to \mathbb{N}$ como una función para la cual escribiremos

$$a_i = a(i);$$

una vez que tenemos aclarado esto, podemos usar el teorema de recursión para concluir que existe esta función.

Teorema 5.1. *Para cada función* $a \colon \mathbb{N} \to \mathbb{N}$ *existe una función* $F \colon \mathbb{N} \to \mathbb{N}$ *de forma que* $F(0) = a_0$ *y* $F(n+1) = F(n) + a_{n+1}$.

Demostración. Usando el teorema de recursión sobre el punto $(0, a_0)$ y la función $f \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dada por $f(m,n) = (m+1, n + a_{m+1})$ obtenemos una función $w \colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ de forma que $w(0) = (0, a_0)$ y $w(n+1) = f(w(n))$. De

[2] El autor del texto no puede, al menos no manera que alguna ambigüedad no se haga presente.

esta función extraeremos la función que buscamos. Denotemos $w(m)_1$ y $w(m)_2$ como los valores $\pi_1(w(n))$ y $\pi_2(w(n))$ respectivamente.

Afirmamos que $w(m)_1 = m+1$ para todo m natural. Para probar esta afirmación usaremos inducción. Notamos primero que $w(0)_1 = 0$; además, si $w(m)_1 = m$ entonces

$$\begin{aligned} w(m+1) &= f(w(m)) \\ &= f\left(w(m)_1, w(m)_2\right) \\ &= f(m, w(m)_2) \\ &= (m+1, w(m)_2 + a_{m+1}). \end{aligned}$$

En ese caso $w(m+1)_1 = m+1$ como afirmamos.

Resta verificar que $F = \pi_2 \circ w$ es la función que afirma el teorema. En efecto, $F(0) = a_0$ y además

$$\begin{aligned} w(m+1) &= f\left(w(m)_1, w(m)_2\right) \\ &= f(m, F(m)) \\ &= (m+1, F(m) + a_{m+1}), \end{aligned}$$

por lo que $F(m+1) = F(m) + a_{m+1}$ como queríamos. Esto concluye la prueba.

□

La función del teorema anterior tiene una notación especial:

$$\sum_{i=0}^{n} a_i = F(n),$$

es costumbre también escribir

$$a_0 + \cdots + a_n = F(n).$$

Cualquiera de las dos formas hará referencia a la función que afirma el teorema anterior y así hemos aclarado que significa una peculiar noción *ad infinitum* usando el teorema de recursión.

Podemos incluso definir una noción general del concepto de suma, por ejemplo, si $k \leq n$ podemos dar significado a

$$\sum_{i=k}^{n} a_i,$$

a través de utilizar el siguiente razonamiento. Dada una función $a\colon \mathbb{N} \to \mathbb{N}$ Podemos definir una función $(a)^k\colon \mathbb{N} \to \mathbb{N}$ como

$$(a)^k(i) = \begin{cases} 0 & \text{si } i < k \\ a_i & \text{si } i \geq k; \end{cases}$$

en ese caso definimos,

$$\sum_{i=k}^{n} a_i = \sum_{i=0}^{n} (a_i)^k.$$

Podemos incluso seguir este procedimiento ahora para símbolos más generales, por ejemplo,

$$\sum_{\substack{i=0\\ i\neq k+1}}^{n} a_i = \sum_{i=0}^{k} a_i + \sum_{i=k+2}^{n} a_i.$$

Lo mismo que hemos hecho para las sumas, podemos hacerlo para definir las sumas. Construiremos estos conceptos como ejercicios.

5.2. Factorial

Podemos definir además un concepto importante en matemáticas a través de un resultado del teorema de recursion. De manera intuitiva podemos decir que el factorial de una numero n de manera intuitiva como:

$$n! = n \cdot (n-1) \cdot \cdots \cdot 1.$$

Podríamos de hecho definirlo sin mucho problema ahora que tenemos muchos de los símbolos que hemos introducido. Siguiendo los resultados de los problemas 5.2 y 5.3, podemos simplemente definir

$$n! = \prod_{i=1}^{n} i.$$

Las propiedades del factorial están precisamente controladas por la definición del producto, y precisamente la notación que intuitivamente presentamos, coincide con el significado más general del producto arbitrario.

5.3. Divisibilidad

Hemos definido en los ejercicios de la sección anterior, el significado muy limitado de la resta de dos naturales. Asumimos que $n - m$ tiene significado solamente cuando $m \leq n$, lo interesante del resultado es la naturaleza del orden en los naturales. Intentaremos proveer un significado para la división, para eso presentamos una definición más débil que la existencia de un inverso.

Definición 5.1. Sean m y n números naturales. Decimos que n divide a m o que n es múltiplo de n si, existe k tal que $n \cdot k = m$. En símbolos $n|m$.

Debemos notar que la esta definición es lo suficiente débil como para admitir que $0|0$. Esta extrañeza no es coincidencia, sin embargo dará problemas al introducir la siguiente notación, ésta se basa en el hecho que el número que garantiza la divisibilidad: Usaremos el símbolo

$$\frac{m}{n}$$

si existe un número k tal que $m \cdot k = n$, representando al único número que cumple con esta propiedad. Esto quiere decir que

$$n \cdot \frac{m}{n} = m.$$

No hay que perder de vista que el símbolo es un simple formalismo y sólo para prevenir confusión en el futuro, prohibiremos el símbolo $\frac{0}{0}$ (a pesar que el formalismo que hemos introducido, es capaz de darle significado).

Ejercicios

Ejercicio 5.1. En este ejercicio daremos otra construcción del conjunto de predecesores de m.

1. Muestra que existe una función $P\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$ de forma que $P(0) = \{0\}$ y $P(m+1) = P(m) \cup \{m+1\}$. Sugerencia: Usa la función $f\colon \mathbb{N} \times \mathcal{P}(\mathbb{N}) \to \mathbb{N} \times \mathcal{P}(\mathbb{N})$ dada por

$$f(m, S) = (m+1, S \cup \{m+1\}).$$

2. Demuestra que para cada $m \in \mathbb{N}$, se tiene

$$P(m) = \{n \in \mathbb{N} \mid n \leq m\}$$

.

Ejercicio 5.2. Para definir el producto arbitrario, demuestra que para cada función $a\colon \mathbb{N} \to \mathbb{N}$, existe una función $F\colon \mathbb{N} \to \mathbb{N}$ de forma que $F(0) = a_0$ y $F(n+1) = F(n) \cdot a_{n+1}$. A esta función la denotamos

$$\prod_{i=0}^{n} a_i.$$

Ejercicio 5.3. Encuentra una defnición adecuada para

$$\prod_{i=k}^{n} a_i$$

y también para

$$\prod_{\substack{i=0 \\ i \neq k+1}}^{n} a_i$$

Ejercicio 5.4. Demuestra que

$$\sum_{i=0}^{n} a_i = a_0 + \sum_{i=1}^{n} a_i.$$

Ejercicio 5.5. Demuestra que

$$\sum_{i=0}^{n} m = (n+1) \cdot m.$$

Ejercicio 5.6. Demuestra que

$$\prod_{i=0}^{n} m = m^{n+1}.$$

Ejercicio 5.7. Demuestra que

$$(n+m)! = \left(\prod_{k=m+1}^{n+m} k\right) \cdot m! = \left(\prod_{k=n+1}^{n+m} k\right) \cdot n!$$

Ejercicio 5.8. Demuestra que si $n|m$ existe un único número k tal que $n \cdot k = m$.

Ejercicio 5.9. Demuestra que

$$\frac{n+m}{k} = \frac{n}{k} + \frac{m}{k}.$$

Ejercicio 5.10. Demuestra que

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

6. Introducción a cardinalidad

6.1. Conjuntos finitos

Una vez que hemos presentado la suficiente teoría de números naturales, podemos comenzar a explorar algunas ideas respecto a lo finito. Una idea interesante para abrir es la llamada paradoja de Galileo que se encuentra publicada en el texto *Discurso y demostración matemática, en torno a dos nuevas ciencias*[3] Galileo presenta el siguiente razonamiento: Existen números que son cuadrado de un entero y otros que no lo son, esto quiere decir que la colección de todos los números es *más grande* que el conjunto de los números que son cuadrados como de los que no lo son. A pesar de esto, cualquier cuadrado se le puede asociar un entero y a cualquier entero se le puede asociar un cuadrado, por lo que no puede haber más de un tipo que de otro.

La paradoja residió en el hecho que una parte no puede ser igual al todo. Sin embargo, Galileo mismo respondió a la paradoja que el mismo planteó: Esta noción es válida sólo para colecciones finitas.

Esta idea, juega un rol en la teoría de conjuntos. Para explorarla, volveremos un poco en nuestros pasos utilizando algunas de las nociones que nos parecían

[3]Discorsi e dimostrazioni matematiche, intorno à due nuove scienze

extravagantes en los números naturales. Este planteamiento fructificará rápidamente mostrando que Galileo habría encontrado de alguna forma una noción que caracteriza a las colecciones infinitas.

Definición 6.1. Sea A y B conjuntos. Decimos que A y B *son equivalentes* si existe una función biyectiva $f\colon A \to B$; en ese caso escribiremos $A \cong B$.

Lema 6.1. *Sea $n \in \mathbb{N}$. Para cualquier subconjunto propio $S \subset n$, existe un número natural $m < n$ de forma que S y m son equivalentes.*

Demostración. Usaremos inducción sobre n. Para $n = 0$, por vacuidad el resultado debe ser cierto pues no existe subconjunto propio de 0 que sea equivalente a 0 (no existe un subconjunto propio de 0). Supongamos ahora que cada subconjunto propio de n es equivalente a algún número m tal que $m < n$. Queremos probar el mismo resultado para el sucesor de n, para esto supongamos

$$S \subset n^+ = n \cup \{n\}.$$

Podemos tener dos posibilidades: $n \notin S$ o $n \in S$.

Por un lado $n \notin S$, entonces $S \subset n$ si es un subconjunto propio, entonces, por hipótesis de inducción, existe m tal que $S \cong m$ y además $m < n < n^+$ de lo que el resultado sigue. Si por el contrario, $S = n$, entonces a través de la identidad tenemos que $S \cong n$ y como $n < n^+$, el resultado sigue de igual forma.

Supongamos ahora que $n \in S$. Como S es un subconjunto propio de n^+, entonces existe $k \in n^+$ tal que $k \notin S$, como $n \in S$, entonces $k \neq n$ y por tanto debemos tener que $k \in n$. Definimos entonces una función $f\colon S \to n$ como

$$f(i) = \begin{cases} i & \text{si } i \neq n \\ k & \text{si } i = n \end{cases}.$$

Basta observar que si $i \neq j$ entonces $f(i) \neq f(j)$, por lo que debemos concluir la función es inyectiva. Por un lado sabemos que $f[S] \subset n$. Si $f[S] = n$ entonces f es biyectiva y tendríamos $S \cong n$ siendo $n < n^+$ de lo que sigue el resultado. Por otro lado, si $f[S]$ fuera un subconjunto propio de n, entonces podemos utilizar la hipótesis de inducción para encontrar m tal que $f[S] \cong m$ con $m < n < n^+$. Esto anterior afirma que existe una función biyectiva $g\colon f[S] \to m$, afirmamos que $g \circ f$ es una biyección entre S y m. En efecto, $g \circ f$ es inyectiva pues tanto f como g lo son; también, al ser g sobreyectiva, si $j \in m$ entonces existe $s \in f[S]$ de forma que $g(s) = j$. Como $s \in f[S]$ entonces existe $i \in S$ de forma que $s = f(i)$ conectando estas igualdades concluir que $j = g(s) = g(f(i))$ por lo que $g \circ f$ es sobreyectiva. Podemos entonces concluir que $S \cong m$ y esto termina la prueba. $\square$

Lema 6.2. *Sea n un número natural. Si $S \subset n$ es un subconjunto propio, entonces S y n no son equivalentes.*

Demostración. Usaremos inducción sobre n. Para $n = 0$ el resultado debe ser cierto al no existir subconjunto propio de 0. Supongamos que cualquier subconjunto propio de n no es equivalente a n. Queremos probar lo mismo para n^+ para lo cual procedemos por contradicción. Supongamos entonces que $S \subset n^+$ y que S es equivalente a n^+, i.e., existe una función biyectiva $f \colon n^+ \to S$. Tenemos de nueva que analizar dos posibilidades: $n \notin S$ o $n \in S$.

Si $n \notin S$, entonces S es un subconjunto propio de n. Podemos restringir la función f al conjunto $n \subset n^+$ obteniendo $f|_n \colon n \to S$ la cual tendrá que ser biyectiva, por lo que $S \cong n$ que deriva en una contradicción con la hipótesis de inducción.

Si por otro lado $n \in S$, entonces $S \backslash \{n\} \subset n$ es un subconjunto propio. Pero

$$S \backslash \{n\} \cong n^+ \backslash \{n\} = n,$$

por lo que n sería equivalente a uno de sus subconjuntos propios lo que contradice la hipótesis de inducción.

Debemos concluir con esto que S no puede ser equivalente a n^+ si S es un subconjunto propio de n^+. De esto sigue el resultado. □

En contraste a lo anterior, el conjunto $\mathbb{N}$ admite una función biyectiva de éste a un subconjunto propio. Basta considerar la función $\mathbb{N} \to \mathbb{N} \backslash \{0\}$ que asigna $n \mapsto n^+$, notando que por los postulados de Peano es inyectiva y sobreyectiva. Resumimos este hecho en la siguiente proposición.

Proposición 6.3. *Existe una función biyectiva de* $\mathbb{N}$ *en* $\mathbb{N} \backslash \{0\}$.

Teorema 6.4. *Un conjunto es equivalente a lo más a un número natural.*

Demostración. Supongamos que $S \cong n$ y también que $S \cong m$. En ese caso $m \cong n$. Si $m \neq n$, entonces o m es un subconjunto propio de n o n es un subconjunto propio de m, cualquiera de estas posibilidades contradice el lema anterior por lo que $m = n$. □

Definición 6.2. Diremos que un conjunto es finito si es equivalente a un número natural. En otro caso, es infinito.

Teorema 6.5. *Un conjunto* S *es infinito si es equivalente a un subconjunto propio de si mismo.*

Demostración. Supongamos que S fuera equivalente a n para algún $n \in \mathbb{N}$, en ese caso existe una función biyectiva $f \colon S \to n$. En ese caso si $T \subset S$ es un subconjunto propio, entonces $f[T] \subset n$ es un subconjunto propio, por lo que $f[T]$ no puede ser equivalente a n y en consecuencia a S. Hemos probado que si S es finito, entonces no es equivalente a un subconjunto propio de si mismo. Por contraposición, de esto sigue el resultado. □

Corolario 6.6. *El conjunto* $\mathbb{N}$ *es infinito.*

Podemos comenzar a definir determinados resultados deseables acerca de conjuntos finitos, usando los naturales para determinar su tamaño. Proponemos la siguiente definición.

Definición 6.3. Sea S un conjunto. Si S es finito, denotamos por $|S|$ al único número natural al que S es equivalente. Por otro lado, si existe una función biyectiva de S en $\mathbb{N}$, escribiremos $|S| = \omega$.

Debemos notar que en ese sentido un conjunto con $|S| = 0$ es el conjunto vacío y además $|n| = n$ lo que en realidad es deseable pues son los naturales los que están «contando» los elementos de un conjunto. También $|\mathbb{N}| = \omega$, este hecho inspirará después el concepto de conjunto contable. De alguna manera la notación $|\cdot|$ sugiere que estamos midiendo el tamaño de algunos conjuntos respecto a los naturales. A manera de ejemplo podemos afirmar de manera muy sencilla que

$$|\{1, 3, 6, 7, 8\}| = 5.$$

6.2. Contando conjuntos finitos

El objetivo de esta sección es presentar algunos resultados que facilitarán la comparación de subconjuntos finitos. Los resultados, desde el punto de vista intuitivo serán tan naturales que una vez que tengamos garantía que el resultado es válido, podremos depender de la intuición.

Teorema 6.7. *Para cualquier conjunto finito T, si $S \subset T$, entonces S es finito y $|S| \leq |T|$.*

Demostración. Si $S = T$, entonces $|S| = |T|$ y el resultado sigue. Supongamos que $S \subset T$ es un subconjunto propio de T y supongamos que $f\colon T \to |T|$ es una función biyectiva. En ese caso $f[S] \subset |T|$ es un subconjunto propio por lo que el lema 6.1 implica que existe m tal $f[S] \cong m$ con $m < |T|$. Lo anterior implica que $S \cong m$ por lo que $|S| = m$ y en ese caso $|S| < |T|$. □

Corolario 6.8. *Para cualquier conjunto S, el conjunto $S \cap T$ es finito.*

Demostración. Esto se debe simplemente a $S \cap T \subset T$, pero por hipótesis T es finito. El resultado del teorema. □

Lema 6.9. *Sean S y T finitos. Entonces $S \cup T$ es finito. Además se tiene $|S \cup T| \leq |S| + |T|$ donde la igualdad se da si $S \cap T = \varnothing$.*

Demostración. Sean $m = |S|$ y $n = |T|$ y sean $f\colon S \to m$ y $g\colon T \to n$ ambas funciones biyectivas. Definimos la función $h\colon S \cup T \to m + n$ como

$$h(x) = \begin{cases} f(x) & \text{si } x \in S \\ m + g(x) & \text{si } x \in T \backslash S \end{cases}.$$

Así definida, la función debe ser inyectiva. En ese caso $h[S \cup T] \subset m + n$ y en consecuencia $S \cup T$ debe ser finito y $|S \cup T| \leq m + n$.

Para probar la segunda parte del teorema, supongamos que $S \cap T = \varnothing$; afirmamos que la función h es sobreyectiva, en efecto si $i \in m + n$ sólo puede pasar una de dos cosas: $i < m$ o $m \leq i$. Si por un lado $i < m$, como la función

f es sobreyectiva existe un elemento s del conjunto S tal que $f(s) = i$ por lo que $h(s) = i$. Si por otro lado $m \leq i$, entonces existe k tal que $i = m + k$ pero $i < m+n$ por lo que $k < n$, en ese caso, como g es biyectiva, existe un elemento t de T de forma que $g(t) = k$ por lo que $h(t) = m + g(t) = i$. En cualquier caso para cualquier $i \in n + m$ existe un elemento de $x \in S \cup T$ tal que $h(x) = i$ por lo que h es sobreyectiva. Al ser h una biyección, podemos entonces concluir que $|S \cup T| = m + n$. □

Teorema 6.10. *Para algún $n \neq 0$ sea $\{S_i\}_{i\in n}$ una familia de conjuntos finitos. Entonces,*

$$\bigcup_{i\in n} S_i$$

es también finito. Además,

$$\left|\bigcup_{i\in n} S_i\right| \leq \sum_{i=0}^{n-1} |S_i|,$$

de donde la igualdad se da si la familia $\{S_i\}_{i\in n}$ es disjunta.

Demostración. Probaremos el resultado por inducción. Para $n = 1$, sólo debemos notar

$$\bigcup_{i\in 1} S_i = S_0,$$

como por hipótesis S_0 es finito, debemos tener que

$$\left|\bigcup_{i\in 1} S_i\right| = |S_0| = \sum_{i=0}^{0} |S_i|.$$

Supongamos ahora el resultado para n, i.e.,

$$\bigcup_{i\in n} S_i$$

es finito con

$$\left|\bigcup_{i\in n} S_i\right| \leq \sum_{i=0}^{n-1} |S_i|.$$

Para probar para resultado para su sucesor, sólo debemos notar una cosa

$$\bigcup_{i\in n+1} S_i = \bigcup_{i\in n} S_i \cup S_{n+1},$$

pues en ese caso, el conjunto en cuestión es la unión de conjuntos finitos y en consecuencia debe ser finito. Además, por la hipótesis de inducción y el lema anterior,

$$\begin{aligned}\left|\bigcup_{i\in n+1} S_i\right| &= \left|\bigcup_{i\in n} S_i \cup S_{n+1}\right|\\ &\leq \left|\bigcup_{i\in n} S_i\right| + |S_{n+1}|\\ &\leq \sum_{i=0}^{n-1} |S_i| + |S_{n+1}|\\ &= \sum_{i=0}^{n} |S_i|.\end{aligned}$$

Por el lema, la igualdad se da cuando los conjuntos S_i son disjuntos. Esto afirma el teorema □

Lema 6.11. *Para cualquier conjunto finito S y cualquier conjunto b, el conjunto $S \times \{b\}$ es finito con $|S \times \{b\}| = |S|$.*

Demostración. Basta establecer una función biyectiva entre $S \times \{b\}$ y S; para esto nos será suficiente la proyección $\pi_1 \colon S \times \{b\} \to S$. Sabemos por un lado que las proyecciones son inyectivas, en este caso en particular mostraremos que es también sobreyectiva. Para esto tomamos $s \in S$, por lo que la pareja $(s, b) \in S \times \{b\}$ y además $\pi_1(s, b) = s$. Al existir una función biyectiva entre S y $S \times \{n\}$, afirmamos simplemente que

$$|S| \cong S \cong S \times \{b\},$$

por lo que $|S \times \{b\}| = |S|$, como afirma el teorema. □

Teorema 6.12. *Para conjuntos finitos A y B, el conjunto $A \times B$ también es finito. Además $|A \times B| = |A| \cdot |B|$.*

Demostración. Supongamos que $m \cong A$ y $n \cong B$, de forma que

$$\bigcup_{b\in B} A \times \{b\} \cong \bigcup_{i\in n} A \times \{i\},$$

basta notar que, si $i \neq j$,

$$A \times \{i\} \cap A \times \{j\} = \varnothing.$$

En ese caso, por el teorema 6.10, tenemos que

$$\begin{aligned}\left|\bigcup_{i\in n} A \times \{i\}\right| &= \sum_{i=0}^{n-1} |A \times \{i\}|\\ &= \sum_{i=0}^{n-1} m\\ &= mn.\end{aligned}$$

Basta observar que

$$A \times B = \bigcup_{b \in B} A \times \{b\},$$

por lo que

$$A \times B \cong mn,$$

y por la forma en que se tomaron m y n, esto termina la prueba. $\square$

Lema 6.13. *Sea $m \in \mathbb{N}$. Entonces,*

$$B^{m+1} \cong B^m \times B$$

Teorema 6.14. *Sean A y B conjuntos finitos. Entonces el conjunto B^A es finito. Además*

$$\left|B^A\right| = |B|^{|A|}.$$

Demostración. Sea $B \cong n$. Mostraremos primero por inducción que $|B^m| = n^m$. Para $m = 0$, debemos notar B^0 es un conjunto que tiene sólo un elemento, la única función es un conjunto que tiene sólo un elemento, la función $f\colon \varnothing \to B$. En ese caso $|B^0| = 1 = n^0$.

Supongamos ahora que se satisface $|B^m| = n^m$; entonces por el lema **??**,

$$B^{m+1} \cong B^m \times B.$$

En ese caso

$$\left|B^{m+1}\right| = |B^m| \cdot |B| = n^m \cdot n = n^{m+1};$$

de lo que sigue la afirmación.

Supongamos ahora que $s\colon A \to m$ es una función biyectiva. Probaremos ahora que $B^A \cong B^m$; en efecto, definimos la función $G\colon B^A \to B^m$ definida por $G(f) = f \circ s$, de la cual afiramos es biyectiva. Si $G(f) = G(f')$ entonces $f \circ s = f' \circ s$, como s tiene inversa podemos concluir que $f = f'$ por lo que G resulta inyectiva. Por otro lado si $g\colon m \to B$, definimos la función $f = g \circ s^{-1}$ para la cual

$$G(f) = (g \circ s^{-1}) \circ s = g,$$

por lo que G es sobreyectiva. En conclusión G resulta una función biyectiva.

Por último, notamos que

$$\left|B^A\right| = |B^m| = n^m.$$

De lo anterior, el resultado propuesto en el teorema sigue. $\square$

Lema 6.15. *Sea E un conjunto cualquiera. Entonces $\mathcal{P}(E) \cong 2^E$.*

Teorema 6.16. *Sea E un conjunto finito. Entonces $\mathcal{P}(E)$ es finito y*

$$|\mathcal{P}(E)| = 2^{|E|}.$$

Ejercicios

Ejercicio 6.1. Sean A y B conjuntos y sea $f\colon A \to B$ una función biyectiva. Demuestra que, si $a \in A$, entonces $g\colon A\backslash\{a\} \to B\backslash\{f(a)\}$ definida por $g(x) = f(x)$ para todo $x \in A\backslash\{a\}$, es también una función biyectiva.

Ejercicio 6.2. Sea $A \cong B$ y sea también $a \in A \cap B$. Demuestra $A\backslash\{a\} \cong B\backslash\{a\}$

Ejercicio 6.3. Sea $f\colon A \to B$ una función inyectiva. Si $S \subset A$ es un subconjunto propio, entonces $f[S] \subset B$ es un subconjunto propio.

Ejercicio 6.4. Sea $f\colon A \to B$ una función inyectiva. Si $S \subset A$, demuestra que $S \cong f[S]$.

Ejercicio 6.5. Demuestra que si $m + i < m + j$ entonces $i < j$.

Ejercicio 6.6. Demuestra que si A y B son conjuntos finitos, entonces

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Ejercicio 6.7. Sean A y B conjunto cualquiera. Si $S \cong B$, prueba que

$$\bigcup_{b\in B} A \times \{b\} \cong \bigcup_{s\in S} A \times \{s\},$$

Referencias

[Gó07] Gómez Laveaga, Carmen: *Introducción a la Teoría Intuitiva de Conjuntos.* Las prensas de Ciencias, 2007.

[Hal66] Halmos, Paul Richard: *Teoría Intuitiva de Conjuntos.* Compañia Editorial Continental, 1966.

Comentario. 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 mediocremente proponer algo nuevo. El único objectivo al que sirven es preparar el curso de Álgebra Superior I impartido en la carrera de Actuaría de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.