**Cartillas Matemáticas**

# Números Naturales y Recursión

Daniel Crespin
Escuela de Matemáticas, Facultad de Ciencias
Universidad Central de Venezuela
http://euler.ciens.ucv.ve/~dcrespin/Pub

*A Edith Iglesias de Ricabarra, 1927-2006*

Contenido

## 1. Introducción

Esta cartilla es una exposición extensa de los sistemas de números naturales, definidos como conjuntos bien ordenados inductivos y minimales. Está dirigida a los estudiantes de la Licenciatura en Matemáticas y explica la fundamentación de los números naturales sin recorte en los detalles.

No es este un texto introductorio, por consiguiente el nivel *no es* el más bajo posible. En esa dirección hay obras como la ampliamente conocida *Aritmética* de Aurelio Baldor [1] que contiene la exposición elemental más popular y didáctica en idioma español sobre el tema de los números naturales; dicho libro logra desarrollar el tema de los naturales sin utilizar –ni siquiera lo menciona– el principio de inducción.

He procurado aprovechar la experiencia previa de un lector que con anterioridad dedicó esfuerzos a las Matemáticas. Supongo que ya enfrentó la construcción de sistemas de números y que tuvo oportunidad de familiarizarse con las ideas, notaciones y técnicas elementales de la teoría de conjuntos. Estas notas le servirán para repasar sus contactos preliminares con los conjuntos mediante un tema matemático de amplio consumo.

Suponemos que los conjuntos y las funciones, objetos muy elementales, son suficientemente conocidos y a partir de ellos paulatinamente incorporamos los diversos tipos de relaciones de orden, de familias de subconjuntos y de funciones que nuestro tópico requiere. Todos estos ingredientes se examinan con lupa –sin llegar al microscopio de la formalización– y se vinculan progresivamente entre si.

A diferencia del punto de vista usual, el tema de los naturales se expone en este texto utilizando intersecciones de colecciones de conjuntos, conjuntos invariantes, teoremas de recursión y funciones aditivas. A todo lo largo de la cartilla se utilizan sin advertencia y con naturalidad las notaciones usuales, las construcciones típicas y el lenguaje corriente de los conjuntos y las funciones. Cualquiera de los textos siguientes cubre con creces las necesidades conjuntistas de esta cartilla: Halmos [6], Kelley [7] y Suppes [15].

Los numerosos enunciados –sumamente sencillos– que encontrará el lector van creando un ambiente, una ubicación, para que eventualmente resalten con brillo propio y se aprecien con adecuados contrastes las particularidades y excelencias de los objetos centrales de este discurso: Los sistemas de números naturales.

Existen presentaciones muy concisas de los naturales, por ejemplo, a veces basta decir:

$\mathbb{N}$ *es un conjunto con un elemento* $0 \in \mathbb{N}$ *y una función inyectiva* $s : \mathbb{N} \to \mathbb{N}$ *cuya imagen es* $s(\mathbb{N}) = \mathbb{N} - \{0\}$ *y la cual verifica el siguiente Principio de Inducción:*

*Si* $A \subseteq \mathbb{N}$ *es tal que*

*i)* $0 \in A$

*ii)* $n \in A \;\Rightarrow\; s(n) \in A$

*entonces* $A = \mathbb{N}$.

Desde luego, este enunciado deja pendientes las definiciones de orden, suma y producto, así como la demostración de propiedades fundamentales como la conmutatividad o el teorema de recursión.

En el otro extremo, para exposiciones extensas y detalladas de los sistemas de números naturales, y también de los enteros, racionales, reales y complejos, pueden consultarse Cohen-Ehrlich [3], Fefferman [4] y el clásico libro de Landau [8] que, históricamente, fue el primer texto moderno sobre la construcción de sistemas de números.

Intercalados en la exposición se encuentran ejemplos extemporáneos, varios basados en los números reales –a pesar de que los reales formalmente deben ubicarse después– porque nos pareció que favorecen la comprensión de algunos conceptos. Para minimizar los riesgos de confusión, los párrafos con comentarios y ejemplos que no son lógicamente necesarios o corresponden a tópicos posteriores van precedidos por un lunar ($\bullet$) y aparecen en letra pequeña.

Es usual referirse a 'el sistema' de números naturales como si solamente hubiese uno, lo cual, a pesar de no ser cierto, constituye costumbre de viejo arraigo. La verdad es que hay toda una categoría con objetos los sistemas de números naturales y morfismos los isomorfismos entre ellos. En el broche final, sección 55, añadiré comentarios al asunto de la unicidad.

## 2. Bosquejo

La cartilla se inicia con un repaso de temas básicos, a saber, orden y cotas, elementos primero y último, buen orden, función sucesor, funciones monótonas e isomorfismos, conjuntos invariantes e inductivos, y minimalidad. Son nociones requeridas para dar la siguiente definición:

*Un sistema $\mathbb{N}$ de números naturales es un conjunto bien ordenado inductivo y minimal.*

Estudiamos entonces –cuidando todos los pormenores– la recursión y las composiciones iteradas, $g^n = g \circ \overset{n}{\smile\!\!\!\cdots} \circ g$, de una función consigo misma, de las cuales obtendremos posteriormente diversas propiedades de la suma y el producto de números naturales. La recursión permite demostrar que dos sistemas cualesquiera de números naturales son isomorfos y que el isomorfismo es único.

La suma de naturales se define mediante iteraciones de la función sucesor. Demostramos la asociatividad, conmutatividad, existencia de elemento neutro, compatibilidad con el orden y leyes de cancelación.

Se introducen las funciones aditivas y las sumas iteradas de funciones –en particular las sumas iteradas $I + \overset{n}{\smile\!\!\!\cdots} + I$ de la función identidad– que se utilizan para definir el producto de números naturales. Se demuestran para el producto sus propiedades asociativa, conmutativa, existencia de elemento neutro, compatibilidad con el orden y leyes de cancelación. Se prueban asimismo las propiedades distributivas del producto respecto a la suma.

En la sección sobre división entera probamos la existencia y unicidad del cociente y el resto.

La penúltima sección, 54, es una revisión a vuelo de pájaro de las secciones previas e incluye también comentarios sobre los sistemas de números posteriores en la jerarquía de riqueza estructural –o tal vez de complicación– a los naturales: Los números enteros $\mathbb{Z}$, los racionales $\mathbb{Q}$, los reales $\mathbb{R}$ y los complejos $\mathbb{C}$.

La sección final, 55, expone comentarios del autor sobre los números, las matemáticas, las ideas e, inevitablemente, sobre la naturaleza de los seres humanos.

## 3. Orden y cotas

Recordemos que si son $X, Y, Z$ conjuntos la *función identidad* de $X$, denotada $I_X : X \to X$, se define por $I_X(x) = x$. Para cada $y \in Y$ hay una *función constante* $c_y : X \to Y$, dada por $c_y(x) = y$ para los $x \in X$. Si $f : X \to Y$, $g : Y \to Z$ son funciones entonces

$$g \circ f : X \to Z$$

es la *función compuesta* definida por la relación $g \circ f(x) = g(f(x))$.

Un *orden* o *relación de orden* en $X$, denotada $\leq$, es una relación reflexiva, transitiva y antisimétrica, es decir, si $x, y, z \in X$ entonces

$$\begin{aligned} & x \leq x \\ & (x \leq y \wedge y \leq z) \;\Rightarrow\; x \leq z \\ & (x \leq y \wedge y \leq x) \;\Rightarrow\; x = y \end{aligned}$$

Un *conjunto ordenado* es un conjunto $X$ con un orden. Es usual abreviar '$X$ es un conjunto ordenado' diciendo simplemente '$X$ es un orden'.

Cuando se cumple $x \leq y$ decimos que $x$ es *menor* que $y$ o que $x$ *precede* a $y$; en tal caso también $y$ es *mayor* que $x$, o $y$ *sigue* a $x$.

Si $x$ es menor que $y$ y si además $x \neq y$ lo denotamos mediante $x < y$ y decimos que $x$ es *estrictamente menor* que $y$, o *precede estrictamente* a $x$, o que $y$ es *estrictamente mayor* que $x$, o *sigue estrictamente* a $x$. Por consiguiente

$$x < y \;\Leftrightarrow\; x \leq y \wedge x \neq y$$

Usaremos asimismo las notaciones $y \geq x$, $y > x$ como equivalentes a $x \leq y$, $x < y$ respectivamente.

Toda expresión donde aparece alguno de los símbolos $\leq$, $<$, $\geq$ ó $>$ es una *desigualdad*. Si los símbolos son $<$ ó $>$ diremos que se trata de una *desigualdad estricta*.

Pares de desigualdades como $x \leq y$ y $z \leq w$ tienen *igual sentido* mientras que $x \leq y$ y $w \geq z$ tienen *sentido contrario*. Asimismo con desigualdades estrictas, $x < y$ y $z < w$ tienen igual sentido siendo $x < y$ y $z > w$ de sentido contrario.

• *Orden vacío.* Nótese que el conjunto vacío es un conjunto ordenado. En efecto, hay una única relación $\emptyset \subseteq \emptyset \times \emptyset$ y esta satisface las condiciones en la definición de orden. Por ejemplo, es reflexiva, pues en caso contrario existiría al menos un $x \in \emptyset$ tal que $x \leq x$ es falso, pero esto no puede ocurrir porque $\emptyset$ no tiene elementos.

Dos elementos son *comparables* si uno de ellos sigue al otro. En otras palabras, $x, y \in X$ son comparables si se cumple $x \leq y$ ó $y \leq x$. El orden del conjunto $X$ es *total*, o $X$ es una *cadena*, si dos elementos cualesquiera son comparables

$$x, y \in X \;\Rightarrow\; (x \leq y \vee y \leq x)$$

La definición de desigualdad estricta implica la siguiente

**1.-** *Ley de Tricotomía:* En un orden total dos elementos $x, y \in X$ satisfacen una y solo una de las tres condiciones siguientes:

$$x < y \qquad x = y \qquad y < x$$

Sea $A$ un subconjunto de $X$. El elemento $c_I \in X$ es *cota inferior* de $A$, y $A$ es *acotado inferiormente* (por $c_I$), si $c_I$ es menor que todos los elementos de $A$

$$a \in A \;\Rightarrow\; c_I \leq a$$

Denotamos por $C_I(A)$ el conjunto de las cotas inferiores de $A$

$$C_I(A) = \{c \in X \,|\, a \in A \;\Rightarrow\; c \leq a\}$$

Parafraseando la definición tenemos

**2.-** Las cotas inferiores forman una clase que es no vacía si y solo si el conjunto es acotado inferiormente:

$$C_I(A) \neq \emptyset \quad \Leftrightarrow \quad (\exists\, c_I \in X \ni (a \in A \;\Rightarrow\; c_I \leq a))$$

• *Cotas inferiores como función de conjuntos.* Sea $\mathcal{P}(X)$ el conjunto de partes de $X$

$$\mathcal{P}(X) = \{A \,|\, A \subseteq X\}$$

Podemos considerar a $C_I$ como una función de $\mathcal{P}(X)$ en si mismo, esto es

$$C_I : \mathcal{P}(X) \to \mathcal{P}(X)$$

Esta función asigna al elemento $A \in \mathcal{P}(X)$ el valor $C_I(A) \in \mathcal{P}(X)$ y tiene las propiedades siguientes

$$\begin{array}{l} C_I(\emptyset) = X \\ C_I(X) = \emptyset \vee C_I(X) = \{p\} \\ A \subseteq B \;\Rightarrow\; C_I(A) \supseteq C_I(B) \end{array}$$

La segunda condición dice que el conjunto total $X$ tiene lo sumo una cota inferior, esto es, si existe cota inferior para todo el conjunto $X$ entonces es única. Compare con **4** y **5** más abajo.

Un elemento $c_S \in X$ es *cota superior* de $A$, y $A$ es *acotado superiormente* (por $c_S$), si $c_S$ es mayor que todos los elementos de $A$

$$a \in A \;\Rightarrow\; a \leq c_S$$

Denotamos por $C_S(A)$ el conjunto de las cotas superiores de $A$

$$C_S(A) = \{c \in X \mid a \in A \;\Rightarrow\; a \leq c\}$$

Inmediatamente se tiene

**3.-** Las cotas superiores son una clase no vacía si y solo si el conjunto es acotado superiormente

$$C_S(A) \neq \emptyset \quad \Leftrightarrow \quad (\exists\, c_S \in X \ni a \in A \;\Rightarrow\; a \leq c_S)$$

• *Cotas superiores como función de conjuntos.* De forma similar a $C_I$, podemos considerar que $C_S$ es una función en el conjunto de partes de $X$

$$C_S : \mathcal{P}(X) \to \mathcal{P}(X)$$

Al elemento $A \in \mathcal{P}(X)$ corresponde $C_S(A) \in \mathcal{P}(X)$ y se cumple

$$\begin{array}{l} C_S(\emptyset) = X \\ C_S(X) = \emptyset \vee C_S(X) = \{u\} \\ A \subseteq B \;\Rightarrow\; C_S(A) \supseteq C_S(B) \end{array}$$

• *Cotas en el conjunto de partes.* En el conjunto $\mathcal{P}(X)$ de partes de $X$ podemos considerar la relación de contención

$$A \subseteq B \Leftrightarrow (x \in A \;\Rightarrow\; x \in B) \tag{1}$$

Esta es una relación reflexiva, transitiva y antisimétrica, luego es una relación de orden; y es independiente de cualquier relación, de orden u otro tipo, que pueda estar definida en $X$.

Si $A$ es un elemento de $\mathcal{P}(X)$, es decir, $A \subseteq X$, entonces $\emptyset \subseteq A \subseteq X$. Luego $\emptyset$ precede y $X$ sigue a cualquier elemento $A \in \mathcal{P}(X)$.

Consideremos subconjuntos $\mathcal{A}$ del conjunto ordenado $\mathcal{P}(X)$, es decir, $\mathcal{A} \subseteq \mathcal{P}(X)$. Esto significa que $\mathcal{A}$ es un conjunto cuyos elementos son subconjuntos de $X$

$$A \in \mathcal{A} \;\Rightarrow\; A \subseteq X$$

Se tiene entonces que la intersección de $\mathcal{A}$

$$\bigcap \mathcal{A} = \{x \mid \forall A \in \mathcal{A}, x \in A\}$$

es cota inferior de $\mathcal{A}$

$$\forall A \in \mathcal{A}, \; \bigcap \mathcal{A} \subseteq A$$

y la unión

$$\bigcup \mathcal{A} = \{x \,|\, \exists\, A \in \mathcal{A} \ni x \in A\}$$

es cota superior

$$\forall A \in \mathcal{A},\; A \subseteq \bigcup \mathcal{A}$$

Además, un conjunto $C \subseteq X$ es cota inferior de $\mathcal{A}$ si y solo si está contenido en la intersección

$$C \subseteq \bigcap \mathcal{A}$$

y es cota superior si y solo si contiene a la unión

$$\bigcup \mathcal{A} \subseteq C$$

Por consiguiente el conjunto de las cotas inferiores de $\mathcal{A}$ está formado por los conjuntos contenido es la intersección

$$C_I(\mathcal{A}) = \{C \,|\, C \subseteq \bigcap \mathcal{A}\}$$

y el de las cotas superiores por los que contienen a la unión

$$C_S(\mathcal{A}) = \{C \,|\, \bigcup \mathcal{A} \subseteq C\}$$

En general un subconjunto puede tener muchas cotas inferiores, pero en el subconjunto mismo no puede haber más de una:

**4.-** En un conjunto ordenado cada subconjunto contiene a lo sumo una de sus cotas inferiores, es decir, si $X$ es ordenado y $A \subseteq X$ entonces

$$c, c' \in A \wedge c, c' \in C_I(A) \;\Rightarrow\; c = c'$$

Por una parte $c'$ está en $A$ y $c$ es cota inferior, luego $c \leq c'$; asimismo, $c$ está en $A$ y $c'$ es cota inferior, por lo que $c' \leq c$. Por antisimetría $c = c'$.

El resultado anterior puede expresarse así:

**5.-** La intersección de un conjunto con (el conjunto de) sus cotas inferiores tiene a lo sumo un elemento

$$A \cap C_I(A) = \{c\} \quad \vee \quad A \cap C_I(A) = \emptyset$$

Los correspondientes enunciados para cotas superiores son los siguientes:

**7.-** La intersección de un conjunto con sus cotas superiores tiene a lo sumo un elemento

$$A \cap C_S(A) = \{c\} \quad \vee \quad A \cap C_S(A) = \emptyset$$

• *Conjunto acotado sin cotas en él.* El conjunto de los racionales tiene partes acotadas que no contienen ninguna de sus cotas. Así, en el conjunto $X = \mathbb{Q}$ de los números racionales sea

$$A = \{r \in \mathbb{Q} \,|\, r^2 < 2\}$$

Entonces $A$ es acotado inferior y superiormente y $A \cap C_S(A) = A \cap C_I(A) = \emptyset$.
Hay también ejemplos en la recta real. En $\mathbb{R}$ los conjuntos abiertos no contienen ninguna de sus cotas (vea el inserto que sigue al enunciado 10) y en particular los abiertos acotados de $\mathbb{R}$ tienen cotas pero no las contienen.

## 4. Elementos primero y último

Sea $X$ un conjunto ordenado y considere un subconjunto $A \subseteq X$. El elemento $p \in A$ es *primero*, si es cota inferior de $A$. En otras palabras, $p$ es un elemento de $A$ que es menor que, o igual a, todos los elementos de $A$

$$p \in A \wedge (a \in A \;\Rightarrow\; p \leq a)$$

Recalcamos que en esta definición el elemento primero de $A$ debe pertenecer a $A$: $p \in A$. En particular,

**8.-** El conjunto vacío no tiene primer elemento.

En cuanto a la unicidad del primer elemento, se razona como en **4**: Si otro elemento $p' \in A$ es primer elemento entonces ambos están en $A$ y ambos son cotas inferiores de $A$, luego $p \leq p'$ y $p' \leq p$ por lo que $p' = p$, luego

**9.-** Un subconjunto de un conjunto ordenado $X$ tiene a lo sumo un primer elemento.

Si un subconjunto $A \subseteq X$ tiene primer elemento lo denotamos por $p(A)$. Las definiciones y **9** implican

**10.-** Un subconjunto tiene primer elemento si y solo si su intersección con el conjunto de sus cotas inferiores es no vacía, y en tal caso la intersección consta exactamente del primer elemento

$$\begin{aligned} \exists\, p(A) \ &\Leftrightarrow\ A \cap C_I(A) \neq \emptyset \\ &\Leftrightarrow\ A \cap C_I(A) = \{p(A)\} \end{aligned}$$

• *Los abiertos de* $\mathbb{R}$ *no tienen primer elemento.* En el conjunto $\mathbb{R}$ de los números reales, y respecto al orden usual, ningún conjunto abierto $A$ (por ejemplo la semirrecta $A = (x, \infty)$) puede tener primer elemento. El motivo es que todo elemento es estrictamente mayor que algún otro elemento del mismo abierto. En otras palabras, si $q \in A$ entonces existe $\epsilon > 0$ tal que $(q - \epsilon, q + \epsilon) \subseteq A$ de manera que $q - \epsilon \in A$ y por ser $q - \epsilon < q$ vemos que $q$ no es primer elemento. Por el contrario, todo conjunto $B \subseteq \mathbb{R}$ cerrado y acotado inferiormente tiene primer elemento, a saber, su ínfimo $p = \inf B \in B$.

Es natural considerar también en subconjuntos $A$ de conjuntos ordenados $X$ la siguiente definición. El elemento $u \in A$ es *último* si es cota superior de $A$

$$u \in A \wedge (a \in A \ \Rightarrow\ a \leq u)$$

Razonamientos similares a los usados respecto al primer elemento implican para el último elemento los siguientes enunciados.

**11.-** El conjunto vacío no tiene último elemento.

**12.-** Cada subconjunto de $X$ tiene a lo sumo un último elemento.

**13.-** Un subconjunto tiene último elemento si y solo si su intersección con el conjunto de sus cotas superiores es no vacía, y en tal caso la intersección consta exactamente del último elemento

$$\begin{aligned} \exists\, u(A) \ &\Leftrightarrow\ A \cap C_S(A) \neq \emptyset \\ &\Leftrightarrow\ A \cap C_S(A) = \{u(A)\} \end{aligned}$$

• *Elementos primero y último respecto a la inclusión.* En el conjunto de partes $\mathcal{P}(X)$ ordenado por inclusión la colección $\mathcal{A} \subseteq \mathcal{P}(X)$ tiene primer elemento si y solo si la intersección es uno de sus miembros: $\bigcap \mathcal{A} \in \mathcal{A}$; y tiene último elemento si y solo si la unión está entre sus miembros: $\bigcup \mathcal{A} \in \mathcal{A}$.

## 5. Axioma de Elección

Sea $X$ un conjunto, $\mathcal{P}(X)$ el conjunto de las partes de $X$ y $\mathcal{P}_0(X)$ el conjunto de las partes no vacías de $X$, esto es

$$\mathcal{P}_0(X) = \{A \mid A \subseteq X \ \wedge \ A \neq \emptyset\}$$

de manera que $\emptyset \notin \mathcal{P}_0(X)$ y $\mathcal{P}(X) = \mathcal{P}_0(X) \cup \{\emptyset\}$.

Denotaremos mediante $\mathcal{A}$ una colección de partes no vacías de $X$, esto es,

$$\mathcal{A} \subseteq \mathcal{P}_0(X)$$

Una *función de elección* para $\mathcal{A}$ es una función con dominio $\mathcal{A}$ que transforma su miembros en elementos de si mismos. En otras palabras

$$e : \mathcal{A} \to X$$

es una función de elección si para todo $A \in \mathcal{A}$ se cumple a condición

$$e(A) \in A$$

Sea $X$ un conjunto cualquiera. ¿Existe o no función de elección para $\mathcal{P}_0(X)$? Incontables desvelos –vinculados a dolorosas locuras y suicidios– hicieron sospechar y eventualmente permitieron obtener prueba de lo siguiente: La existencia de funciones de elección no se puede deducir de los demás axiomas –los que suelen aceptarse con menos preocupación– de la Teoría de Conjuntos. Ocurre que dichas funciones de elección hacen falta para obtener una serie de resultados muy codiciados y utilizados por varias generaciones de matemáticos. En consecuencia hay amplio consenso para convertir la existencia de funciones de elección en un postulado y aceptar el siguiente

Axioma de Elección (Auswahlaxiom): *Para cualquier $X$ existen funciones de elección*

$$e : \mathcal{P}_0(X) \to X$$

Asumiremos este axioma y lo utilizaremos en la sección **??** para inferir que los números naturales tiene la esperada propiedad de ser suficientes para contar los elementos de cualquier conjunto finito.

Con el Axioma de Elección se cuelan una serie de consecuencias sorprendentes entre las cuales destaca el Principio de Buena Ordenación, explicado abajo en la sección 6.

• *Enunciados equivalentes al Axioma de Elección.* Hay información legible y sustancial sobre los enunciados equivalentes al Axioma de Elección en [16].

Las funciones de elección para $\mathcal{P}_0(X)$ lo son también para $\mathcal{A}$, es decir, el Axioma de Elección, enunciado para la colección $\mathcal{P}_0(X)$ de *todas* las partes no vacías de $X$, implica

**14.-** Para cualquier $\mathcal{A} \subseteq \mathcal{P}_0(X)$ existen funciones de elección.

## 6. Buen orden

Sea $X$ un conjunto; mantenemos la notación $\mathcal{P}_0(X)$ para la colección de los subconjuntos no vacíos de $X$. Supongamos que $X$ está provisto de un orden $\leq$. Por definición $X$ *está bien ordenado* si todo subconjunto no vacío tiene primer elemento, esto es, si

$$A \in \mathcal{P}_0(X) \;\Rightarrow\; \exists\, p(A) \in A$$

Cuando esto ocurre decimos que la relación $\leq$, y también que el conjunto $X$, es un *buen orden*.

Según la definición si $X$ está bien ordenado entonces $A \to p(A)$ es una función cuyo dominio es toda la colección $\mathcal{P}_0(X)$

$$p : \mathcal{P}_0(X) \to X$$

Si $X$ es no vacío entonces $X \in \mathcal{P}_0(X)$ y por lo tanto

**15.-** Todo conjunto bien ordenado no vacío tiene primer elemento, es decir, si $X \neq \emptyset$ está bien ordenado entonces existe $p(X) \in X$ que verifica

$$x \in X \;\Rightarrow\; p(X) \leq x$$

• *El vacío es un buen orden.* El conjunto vacío es un conjunto bien ordenado. Porque si no lo fuese existiría un subconjunto no vacío $A \subseteq \emptyset$ sin primer elemento; pero tal $A$ no puede existir. Es el único conjunto bien ordenado sin primer elemento.

El primer elemento de un conjunto bien ordenado y no vacío $X$ es un elemento distinguido que tiene un desempeño especial en las definiciones y razonamientos; será denotado $0_X$, así,

$$0_X = p(X)$$

Enunciamos el

PRINCIPIO DE BUENA ORDENACIÓN: *Todo conjunto tiene un buen orden.*

Este principio es equivalente al Axioma de Elección, pero no lo utilizaremos y omitimos su deducción. Para nuestros propósitos será suficiente con el Axioma de Infinito enunciado en la sección 13.

• *Los enteros no son un buen orden.* En el conjunto $\mathbb{Z}$ de los enteros el orden usual no es un buen orden; por ejemplo, el conjunto $A = \{\ldots, -n, \cdots -2, -1\}$ de los enteros negativos no tiene primer elemento.

• *Los reales no son un buen orden.* El conjunto $\mathbb{R}$ de los números reales con el orden usual no está bien ordenado porque tiene subconjuntos como $A = (0, 1)$ (intervalo abierto) que no tienen primer elemento.

• *Problema del buen orden.* En 1904 Zermelo demostró que el Axioma de Elección equivale al Principio de Buena Ordenación. Este resultado desató en su momento intensa controversia. Mientras por una parte el Axioma de Elección luce inocuo y digerible sin dispepsias, el Principio de Buena Ordenación constituye un cólico mayor. El motivo es que –aplicado en particular al conjunto de los números reales– afirma que en $\mathbb{R}$ existe un buen orden. Pero nadie fue capaz (ni lo ha sido hasta el presente) de definir explícitamente un buen orden en $\mathbb{R}$. Se concluye que existe una relación, el buen orden de $\mathbb{R}$, sin que esté al alcance de persona alguna especificarla mediante una fórmula.

• *Ordinales y metáforas.* Entre los conjuntos bien ordenados destacan los ordinales. Proporcionan –además de otras cosas– un curioso modelo de los números naturales. Según una metáfora un conjunto es como una caja que encierra a sus elementos. El conjunto vacío es entonces una caja vacía y este sería el ordinal nulo ($0 = \emptyset$). Hay también un conjunto, que no es vacío, y cuyo único elemento es el conjunto vacío; es el ordinal unitario ($1 = \{0\} = \{\emptyset\}$) y corresponde con una caja que no es vacía porque contiene un elemento, aunque el elemento en cuestión es simplemente una caja vacía. El siguiente ordinal es metafóricamente una caja que contiene dos elementos: Uno de los elementos es una caja vacía y el otro es una caja que no es vacía porque contiene una caja vacía ($2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$). En el caso general

$$n = \{0, 1, \ldots, n - 1\}$$

y se trata entonces de cajas que, si no son vacías, es porque contienen otras cajas. Pero las cajas más internas siempre estarán vacías. La metáfora final parece decir que los ordinales son interminables matrioshkas cuyas poco agraciadas muñecas tienen seis caras planas de cartón.

Fácilmente se prueba que la buena ordenación pasa a los subconjuntos.

**16.-** Si $X$ está bien ordenado entonces todo subconjunto $A \subseteq X$ está bien ordenado.

Esto se debe a que los subconjuntos no vacíos de $A$ son también subconjuntos de $X$, lo cual asegura la existencia del primer elemento.

Si $X$ es un conjunto bien ordenado ocurre en particular que todo subconjunto con dos elementos, $A = \{x, y\} \subseteq X$, tiene primer elemento. Si el primer elemento es $x$ entonces $x \leq y$; si el primer elemento es $y$ entonces $y \leq x$. En todo caso $x$ e $y$ son comparables, luego

**17.-** Todo buen orden es un orden total.

• *Las partes no son un buen orden.* Si $X$ tiene más de un punto, digamos $\{x, y\} \subseteq X$ con $x \neq y$, el conjunto $\mathcal{P}(X)$ de sus partes no está –respecto a la inclusión– totalmente ordenado porque los elementos $\{x\} \in \mathcal{P}(X)$ e $\{y\} \in \mathcal{P}(X)$ no son comparables (no se cumple $\{x\} \subseteq \{y\}$ ni tampoco $\{y\} \subseteq \{x\}$), luego $\mathcal{P}(X)$ no puede ser un conjunto bien ordenado. Desde luego, el Principio de Buena Ordenación proclama que siempre existe en $\mathcal{P}(X)$ *algún* buen orden, aunque este no sea el orden natural de la contención.

Siempre es posible añadir un elemento más al final de un conjunto ordenado $X$: Considere un elemento $\omega$ que no pertenezca a $X$, $\omega \notin X$. Puede tomarse $\omega = X$. Defina $X^+ = X \cup \{\omega\}$ y extienda el orden de $X$ a $X^+$ mediante la condición

$$x \leq \omega \qquad \forall x \in X$$

**18.-** Si $X$ está bien ordenado entonces también $X^+$ está bien ordenado y tiene último elemento $\omega$.

• *Conjunto bien ordenado* $\mathbb{N}^+$. Por ejemplo, si $X = \mathbb{N} = \{0, 1, \ldots, n, \ldots\}$ entonces $\omega = \mathbb{N}$ y $X^+ = \mathbb{N} \cup \{\mathbb{N}\}$ tiene último elemento.

• *Eliminar último elemento de* $\mathbb{N}^+$. En dirección opuesta, si un conjunto bien ordenado $X$ tiene último elemento $u(X)$ es posible descartarlo y el resultado, $X^- = X - \{u(X)\}$, sigue siendo bien ordenado, pero puede ocurrir que a pesar del descarte $X^-$ siga teniendo último elemento. Por ejemplo, si $X$ es finito y tiene dos o más elementos entonces eliminando el último resulta un conjunto que aún posee un último elemento. Otro ejemplo es $\mathbb{N}^+ = \mathbb{N} \cup \{\mathbb{N}\}$ y $\mathbb{N}^{++} = \mathbb{N}^+ \cup \{\mathbb{N}^+\}$; eliminar el último elemento de $\mathbb{N}^{++}$ produce $\mathbb{N}^+$ que tiene todavía último elemento.

## 7. Inyecciones, suryecciones y biyecciones

Recordemos que una función $f : X \to Y$ es *inyectiva* o es una *inyección* si transforma elementos distintos en elementos distintos, esto es, si para $x, x' \in X$ se tiene

$$x \neq x' \;\Rightarrow\; f(x) \neq f(x')$$

Esto equivale a la siguiente condición: Si dos elementos tienen imágenes iguales entonces son iguales

$$f(x) = f(x') \;\Rightarrow\; x = x'$$

El conjunto de las funciones inyectivas de $X$ en $Y$ se denotará mediante $\mathrm{Iny}(X, Y)$ de manera que

$$\mathrm{Iny}(X, Y) = \{f : X \to Y \mid f(x) = f(x') \;\Rightarrow\; x = x'\}$$

Una función es *suryectiva* o *suryección* si todo elemento del rango (conjunto de llegada $Y$) es valor de la función

$$y \in Y \;\Rightarrow\; \exists\, x \in X \ni f(x) = y$$

Las funciones suryectivas de $X$ en $Y$ forman un conjunto denotado $\mathrm{Sur}(X, Y)$ de manera que

$$\mathrm{Sur}(X, Y) = \{f : X \to Y \mid y \in Y \;\Rightarrow\; \exists\, x \in X \ni f(x) = y\}$$

Una función $f : X \to Y$ es *biyectiva* o es una *biyección* si es tanto inyectiva como suryectiva.

Recordemos además que estas propiedades de $f$ se expresan mediante inversión funcional: La función $f : X \to Y$ es inyectiva o suryectiva según tenga inversa $g : Y \to X$ a izquierda o a derecha respectivamente

$$g \circ f = I_X \qquad f \circ g = I_Y$$

y $f$ es biyectiva si y solo si tiene inversa bilátera, esto es, si existe $g : Y \to X$ que cumple simultáneamente las dos condiciones anteriores.

El conjunto vacío no tiene elementos. Indicaremos que $X$ es el conjunto vacío mediante la expresión $|X| = 0$; asimismo la expresión $|X| \neq 0$ indica que $X$ no es vacío.

Un conjunto $X$ *tiene exactamente un elemento*, o es *unipuntual* si existe $x \in X$ tal que $X = \{x\}$; diremos además que $X = \{x\}$ es el *unipuntual de* $x$. La igualdad $X = \{x\}$ en esta definición significa que $X \neq \emptyset$ y que $z \in X \;\Rightarrow\; z = x$. Para indicar que $X$ es unipuntual usaremos la expresión $|X| = 1$. El conjunto $X$ *tiene a lo sumo un elemento*, o es *a lo sumo unipuntual* si $X = \emptyset$ o $X = \{x\}$, lo que se indicará mediante $|X| \leq 1$.

El conjunto $X$ *tiene exactamente dos elementos*, o es *bipuntual* si existen $x, y \in X$ tal que $X = \{x, y\}$. La última igualdad significa que existen $x, y \in X$ con $x \neq y$ para los cuales se tiene que $z \in X \;\Rightarrow\; z = x \vee z = y$.

Sean $\mathrm{Iny}(X,Y)$, $\mathrm{Sur}(X,Y)$, $\mathrm{Biy}(X,Y)$ los conjuntos de inyecciones, suryecciones y biyecciones respectivamente, con dominio $X$ y rango $Y$. Las definiciones implican el resultado siguiente:

**19.-** Una función es inyectiva, suryectiva o biyectiva según las imágenes inversas de los elementos del rango sean a lo sumo unipuntual, no vacías o unipuntuales respectivamente, es decir

$$\begin{aligned} f \in \mathrm{Iny}(X,Y) &\Leftrightarrow (y \in Y \;\Rightarrow\; |f^{-1}(y)| \leq 1) \\ f \in \mathrm{Sur}(X,Y) &\Leftrightarrow (y \in Y \;\Rightarrow\; |f^{-1}(y)| \neq 0) \\ f \in \mathrm{Biy}(X,Y) &\Leftrightarrow (y \in Y \;\Rightarrow\; |f^{-1}(y)| = 1) \end{aligned}$$

## 8. Sucesores

Sea $X$ un conjunto ordenado cualquiera y considere un elemento $x \in X$. El conjunto de los *seguidores* de $x$, denotado $S(x)$, está formado por los elementos que lo siguen estrictamente

$$S(x) = \{y \mid x < y\}$$

Este conjunto puede ser vacío, y si no lo es puede ocurrir que no tenga primer elemento.

Cuando el conjunto de seguidores no es vacío y tiene primer elemento definimos el *seguidor inmediato* o *sucesor* del elemento $x$, denotado por $s(x)$ o por $x^+$, como el primero de sus seguidores

$$s(x) = x^+ = p(S(x))$$

Sea $K = K(X)$ el conjunto de los elementos para los cuales está definido el sucesor

$$K = \{x \mid \exists\, p(S(x)) \in S(x)\} \subseteq X$$

La *función sucesor* es la función $s : K \to X$ que a cada elemento hace corresponder su sucesor.

• *En* $\mathbb{R}$ *no hay sucesores.* Respecto al orden usual en la recta real, los seguidores de un número forman una semirrecta abierta que no posee primer elemento y por lo tanto ningún número real tiene sucesor. Es decir, si $x \in \mathbb{R}$ entonces $S(x) = (x, \infty)$ y como en el abierto $(x, \infty)$ no hay primer elemento se sigue que el sucesor $s(x)$ no está definido. Este razonamiento vale para todo $x \in \mathbb{R}$, luego $K(\mathbb{R}) = \emptyset$.

De las definiciones se deduce que

**20.-** Todo elemento con sucesor lo precede estrictamente

$$x \in K \;\Rightarrow\; x < s(x)$$

En particular

**21.-** Si un elemento tiene sucesor entonces son distintos

$$x \in K \;\Rightarrow\; x \neq s(x)$$

Si un conjunto tiene primer elemento $p(X)$ entonces **20** implica que $p(X)$ no sigue estrictamente a ningún elemento de $X$:

**22.-** El primer elemento no es sucesor

$$p(X) \notin s(K(X))$$

En particular

**23.-** En un conjunto con primer elemento la función sucesor $s : K(X) \to X$ no es suryectiva.

Puesto que el sucesor de un elemento es el primero entre sus (estrictos) seguidores, entre ellos no queda ninguno:

**24.-** Entre un elemento y su sucesor no hay otros elementos

$$x \leq y \leq s(x) \;\Rightarrow\; (y = x \vee y = s(x))$$

En efecto, si asumimos como hipótesis que $x \leq y \leq s(x)$ entonces en caso de no cumplirse $x = y$ se verifica $x < y$ y obtenemos

$$\begin{aligned} x < y \quad &\Rightarrow \quad y \in S(x) \\ &\Rightarrow \quad s(x) \leq y \\ &\Rightarrow \quad s(x) = y \end{aligned}$$

Las implicaciones se deducen así: La primera por definición del conjunto de seguidores $S(x)$; la segunda por definición del primer elemento $s(x) = p(S(x)) \in S(x)$; la última por la hipótesis de ser $y \leq s(x)$ y por la antisimetría de la relación de orden.

**25.-** La función sucesor conserva estrictamente el orden, es decir, si $x, y \in K$ entonces

$$x < y \;\Rightarrow\; s(x) < s(y)$$

Esto es cierto porque $x < y$ implica $y \in S(x)$, de donde se infiere que $s(x) \leq y < s(y)$. Posteriormente veremos funciones más generales, las estrictamente monótonas, que también poseen esta propiedad.

## 9. Buen orden y sucesores

Supondremos en esta sección que $X$ está bien ordenado. Bajo esta hipótesis la existencia de primer elemento en cualquier parte no vacía está garantizada y para que $s(x)$ esté definido basta que algún elemento le siga: $S(x) \neq \emptyset$. Por lo tanto, salvo un caso excepcional, en los conjuntos bien ordenados todo elemento tiene sucesor.

**26.-** Si $X$ está bien ordenado entonces la función sucesor está definida para todo elemento $x$ que *no sea* el último elemento de $X$

$$K(X) = X - u(X)$$

En efecto, si $x$ no es último elemento entonces $S(x) \neq \emptyset$ y la buena ordenación dice que hay en $S(x)$ primer elemento. Por el contrario si $u = u(X)$ se tiene $S(u) = \emptyset$ y $s(u)$ no está definido. Esto implica el enunciado siguiente:

**27.-** Si $X$ está bien ordenado entonces la función sucesor está definida en todo $X$ si y solo si $X$ no posee último elemento.

$$K(X) = X \Leftrightarrow \nexists\ u(X) \in X$$

Una formulación equivalente es

**28.-** Si $X$ está bien ordenado entonces la función sucesor está definida en todo $X$ si y solo si $X$ no posee último elemento

$$s : X \to X \Leftrightarrow \nexists\ u(X) \in X$$

Como caso particular de **22** tenemos

**29.-** Si $X$ está bien ordenado entonces el primer elemento no es sucesor

$$\forall x,\ \ s(x) \neq 0_X$$

Lo cual nos dice que

**30.-** La imagen de la función sucesor está contenida en el conjunto sin su primer elemento

$$s(K(X)) \subseteq X - \{0_X\}$$

y en consecuencia (o bien directamente por **22**) tenemos

**31.-** En un conjunto bien ordenado la función sucesor $s : K(X) \to X$ no es suryectiva.

Puesto que un buen orden es un orden total la ley de tricotomía y **25** implican

**32.-** En un conjunto bien ordenado la función sucesor es inyectiva

$$s(x) = s(y) \quad \Rightarrow \quad x = y$$

COPIADO DE 'CONJUNTOS' INCLUIR SUBSUCESIONES

## 10. Conjuntos finitos

Un conjunto es *finito*, o *finito en el sentido de Dedekind*, si toda inyección del conjunto en si mismo es suryección, es decir, $X$ es finito si

$$\mathrm{Iny}(X, X) \subseteq \mathrm{Sur}(X, X)$$

En caso contrario el conjunto es *infinito*, es decir, $X$ es infinito si existe alguna inyección del conjunto en si mismo que no es suryectiva.

$$\mathrm{Iny}(X, X) \subsetneqq \mathrm{Sur}(X, X)$$

Para indicar que el conjunto $X$ es finito usaremos la notación $|X| < \infty$.

**33.-** Todo conjunto equipotente con un conjunto finito es finito

$$|X| < \infty \wedge \mathrm{Biy}(X, Y) \neq \emptyset \Rightarrow |Y| < \infty$$

**34.-** Un conjunto es finito si y solo si toda inyección en si mismo es biyección

$$|X| < \infty \Leftrightarrow \mathrm{Iny}(X, X) \subseteq \mathrm{Biy}(X, X)$$

**35.-** Un conjunto es finito si y solo si toda suryección en si mismo es inyección

$$|X| < \infty \Leftrightarrow \mathrm{Sur}(X, X) \subseteq \mathrm{Iny}(X, X)$$

**36.-** Un conjunto es finito si y solo si toda suryección en si mismo es biyección

$$|X| < \infty \Leftrightarrow \mathrm{Sur}(X, X) \subseteq \mathrm{Biy}(X, X)$$

**37.-** Un conjunto es finito si y solo si los conjuntos de inyecciones, suryecciones y biyecciones en si mismo son iguales entre si

$$|X| < \infty \Leftrightarrow \mathrm{Iny}(X, X) = \mathrm{Sur}(X, X) = \mathrm{Biy}(X, X)$$

He aquí algunos ejemplos de conjuntos finitos:

**38.-** El conjunto vacío es finito

$$|\emptyset| < \infty$$

**39.-** Todo conjunto unipuntual es finito

$$|\{x\}| < \infty$$

**40.-** Todo conjunto bipuntual es finito

$$|\{x, y\}| < \infty$$

**41.-** Todo subconjunto de un conjunto finito es finito

$$|X| < \infty \ \wedge \ A \subseteq X \quad \Rightarrow \quad |A| < \infty$$

**42.-** La imagen de un conjunto finito por una función es finito

$$f : X \to Y \ \wedge \ |X| < \infty \quad \Rightarrow \quad |f(X)| < \infty$$

**43.-** Un conjunto finito unido a un punto es finito

$$|X| < \infty \quad \Rightarrow \quad |X \cup \{x_0\}| < \infty$$

Si $x_0 \in X$ entonces $X \cup \{x_0\} = X$ y no hay nada que probar.

Si $x_0 \notin X$ sea $f : X \cup \{x_0\} \to X \cup \{x_0\}$ una inyección. Hay que probar que $f$ es suryección.

Una primera posibilidad es que $x_0$ sea punto fijo de $f$, $f(x_0) = x_0$; entonces la restricción de $f$ a $X$ es una inyección que transforma $X$ en $X$, $f|X : X \to X$; por la hipótesis de finitud $f|X$ es suryección, la junta $f = f|X \cup 1_{\{x_0\}}$ también es suryección y queda probado que $X \cup \{x_0\}$ es finito.

La segunda posibilidad es que sea $f(x_0) \neq x_0$ de modo que $f(x_0) \in X$.

Defina $\tau : X \cup \{x_0\} \to X \cup \{x_0\}$ como la biyección que traspone $x_0$ y $f(x_0)$, esto es, $\tau(x_0) = f(x_0)$, $\tau(f(x_0)) = x_0$ y $\tau(x) = x$ si $x \in X - \{x_0, f(x_0)\}$.

Entonces $\tau \circ f : X \cup \{x_0\} \to X \cup \{x_0\}$ es una inyección con punto fijo $x_0$ y por el caso anterior resulta que $\tau \circ f$ es biyección, luego $f = \tau \circ \tau \circ f$ es composición de biyecciones y por lo tanto biyección. Queda probado que $X \cup \{x_0\}$ es finito. Más generalmente,

La hipótesis de finitud de $X$ es esencial para la validez del siguiente resultado

**44.-** Si un conjunto es finito entonces subconjuntos equipotentes tienen complementos equipotentes

$$(|X| < \infty \ \wedge \ A \subseteq X \ \wedge \ B \subseteq X \ \wedge \ |A| = |B|) \quad \Rightarrow \quad |X - A| = |X - B|$$

Por hipótesis existe una biyección $\phi : A \to B$. Según **??** hay dos posibilidades: $X - A \leq X - B$ o $X - B \leq X - A$. En el primer caso existe una inyección $\psi : X - A \to X - B$; la junta $\phi \cup \psi : X = A \cup (X - A) \to X = B \cup (X - B)$ es entonces inyección y la finitud de $X$ implica que $\phi \cup \psi$ es biyeccion, por lo que $\psi$ tiene que ser biyección y $|X - A| = |X - B|$. En el segundo caso existe una inyección $\psi : X - B \to X - A$ y se aplica a $\phi \cup \psi$ el mismo razonamiento para concluir nuevamente que $|X - A| = |X - B|$.

**45.-** La union de dos conjuntos finitos es un conjunto finito.

$$|X| < \infty \ \text{ y } \ |Y| < \infty \quad \Rightarrow \quad |X \cup Y| < \infty$$

Suponga primeramente que los conjuntos son disjuntos, $X \cap Y = \emptyset$.

Sea $f : X \cup Y \to X \cup Y$ una inyección. Si $X$ e $Y$ fuesen invariantes por $f$, $f(X) \subseteq X$ y $f(Y) \subseteq Y$, entonces $f|X : X \to X$ y $f|Y : Y \to Y$ son inyecciones y por la hipótesis de finitud son suryecciones por lo que su junta $f = (f|X) \cup (f|Y)$ es suryectiva.

Si $X$ no es invariante por $f$ entonces tampoco lo es $Y$, y viceversa, de manera que si uno de ellos es invariante ambos lo son. Considere los siguientes subconjuntos $A, B$ de $X \cup Y$

$$A = X \cap f(Y) \subseteq f(Y) \subseteq X \cup Y \tag{2}$$

$$B = Y \cap f(X) \subseteq f(X) \subseteq X \cup Y \tag{3}$$

Las restricciones $f|A : A \to$, $f|B$ son biyecciones. Defina $\tau : X \cup Y \to X \cup Y$ como la biyección que intercambia $f(X) \cap Y$ con $X \cap f(Y)$, esto es, la función $\tau : X \cup Y \to X \cup Y$ definida mediante

$X \cap f^{-1}(Y) \xrightarrow{f} f(X) \cap Y$

$f^{-1}(X) \cap Y \xrightarrow{f} X \cap f(Y)$

$$\tau(z) = \begin{cases} y \text{ if } z = f(y) \in X \cap f(Y) \\ x \text{ if } z = f(x) \in f(X) \cap Y \\ z \text{ if } z \in (X \cup Y) - ((X \cap f(Y)) \cup (f(X) \cap Y)) \end{cases}$$

Lo cual equivale a

$$\tau|(f(X) \cap Y) = f|(f(X) \cap Y)\tau|(X \cap f(Y)) = f^{-1}|(X \cap f(Y))$$

$\tau|(f(X) \cap Y) = f^{-1}|(f(X) \cap Y) : f(X) \cap Y \to X \cap f^{-1}(Y)$, $\tau|(X \cap f(Y)) = f^{-1}|(X \cap f(Y)) : X \cap f(Y) \to f^{-1}(X) \cap Y$, $\tau|(X \cap f(X)) = 1_{X \cap f(X)} : X \cap f(X) \to X \cap f(X)$, $\tau|(Y \cap f(Y)) = 1_{Y \cap f(Y)} : Y \cap f(Y) \to Y \cap f(Y)$.

$$\tau(x)$$

Como consecuencia de **27**, **31** y **32** llegamos a

**46.-** Si $X$ está bien ordenado y no tiene último elemento entonces $X$ es infinito.

• *Poseer último elemento no implica finitud.* La existencia de último elemento no es suficiente para garantizar finitud. Por ejemplo, el conjunto $\mathbb{N}^+$ tiene último elemento y sin embargo es infinito.

## 11. Comparación de conjuntos ordenados

La noción de función monótona se introdujo previamente –sección **??**, página **??**– en el contexto del teorema del punto fijo para una función monótona de partes de un conjunto, el cual llamamos teorema del conjunto fijo. Más generalmente una función entre conjuntos ordenados es *monótona* o *conserva el orden* si cada vez que un elemento del dominio precede a otro entonces su imagen precede la del otro, esto es, si $X, Y$ son conjuntos ordenados y si $h : X \to Y$ es una función entonces $h$ es monótona si

$$x \leq y \;\Rightarrow\; h(x) \leq h(y)$$

La función *conserva estrictamente el orden* o es *estrictamente monótona* si en la expresión anterior se pueden reemplazar las desigualdades por desigualdades estrictas:

$$x < y \;\Rightarrow\; h(x) < h(y)$$

Denotemos por $\mathrm{Mon}(X, Y)$ al conjunto de las funciones monótonas y por $\mathrm{EMon}(X, Y)$ el de las funciones estrictamente monótonas.

**47.-** Toda función estrictamente monótona es monótona

$$\mathrm{EMon}(X,Y) \subseteq \mathrm{Mon}(X,Y)$$

**48.-** Si el dominio es está totalmente ordenado entonces las funciones estrictamente monótonas son inyectivas, esto es, si $X$ es un orden total se cumple

$$\mathrm{EMon}(X,Y) \subseteq \mathrm{Iny}(X,Y)$$

Obviamente

**49.-** La función identidad es estrictamente monótona

$$I_X \in \mathrm{EMon}(X,X)$$

La monotonía de funciones se conserva al componerlas:

**50.-** La composición de funciones monótonas es monótona y la de estrictamente monótonas es estrictamente monótona

$$\begin{gathered} h \in \mathrm{Mon}(X,Y) \wedge h \in \mathrm{Mon}(Y,Z) \;\Rightarrow\; g \circ h \in \mathrm{Mon}(X,Z) \\ h \in \mathrm{EMon}(X,Y) \wedge h \in \mathrm{EMon}(Y,Z) \;\Rightarrow\; g \circ h \in \mathrm{EMon}(X,Z) \end{gathered}$$

En efecto, por ser $h$ y $g$ monótonas se tiene $x \leq x' \;\Rightarrow\; h(x) \leq h(x') \;\Rightarrow\; g(h(x)) \leq g(h(x')) \;\Rightarrow\; g \circ h(x) \leq g \circ h(x')$, luego $\in \mathrm{Mon}(X,Z)$. El caso estricto tiene demostración similar.

Por otra parte, el enunciado **25** puede reformularse así:

**51.-** La función sucesor $s : K(X) \to X$ es estrictamente monótona

$$s \in \mathrm{EMon}(K(X),X)$$

La función $h : X \to Y$ *conserva doblemente el orden* o es *doblemente monótona* si cumple: Un elemento del dominio precede a otro si y solo su imagen precede la del otro

$$x \leq x' \Leftrightarrow h(x) \leq h(x')$$

Un *isomorfismo ordenado*, o simplemente *isomorfismo*, de un conjunto ordenado en otro es una función biyectiva y doblemente monótona. En detalle, sean $X, Y$ conjuntos ordenados. Un isomorfismo de $X$ en $Y$ es una función biyectiva

$$\varphi : X \to Y$$

que satisface

$$x \leq y \Leftrightarrow \varphi(x) \leq \varphi(y)$$

• *Necesidad de la doble monotonía.* En general la equivalencia ($\Leftrightarrow$) en esta definición no puede reemplazarse con una implicación ( $\Rightarrow$ ), es decir, la condición $x \leq y \;\Rightarrow\; h(x) \leq h(y)$ no es suficiente para garantizar que una función biyectiva $h$ sea un isomorfismo, esto es, para que $h(x) \leq h(y) \;\Rightarrow\; x \leq y$. Por ejemplo, sean

$$\begin{array}{l} X = \{a, b, c\} \text{ con orden } \{(a, a), (b, b), (c, c), (a, b), (a, c)\} \subseteq X \times X \\ Y = \{1, 2, 3\} \text{ con orden } \{(1, 1), (2, 2), (3, 3), (1, 2), (1, 3), (2, 3)\} \subseteq Y \times Y \end{array}$$

entonces

$$h(a) = 1,\; h(b) = 2,\; h(c) = 3$$

es una biyección que conserva el orden pero no es isomorfismo porque en $Y$ se tiene $h(b) = 2 \leq 3 = h(c)$ mientras que $b \leq c$ no se cumple en $X$.

Dos conjuntos ordenados son *isomorfos* si existe entre ellos algún isomorfismo, esto es, si $\mathrm{Iso}(X, Y) \neq \emptyset$. Denotamos por $\mathrm{Iso}(X, Y)$ el conjunto de los isomorfismos ordenados del conjunto ordenado $X$ en el conjunto ordenado $Y$

$$\mathrm{Iso}(X, Y) = \{\varphi \,|\, \varphi \in \mathrm{Biy}(X, Y) \;\wedge\; x \leq y \Leftrightarrow \varphi(x) \leq \varphi(y)\}$$

La definición implica:

**52.-** Los isomorfismos conservan estrictamente el orden

$$\varphi \in \mathrm{Iso}(X, Y) \;\Rightarrow\; \varphi \in \mathrm{EMon}(X, Y)$$

El resultado siguiente es inmediato:

**53.-** La función identidad es un isomorfismo y la composición de isomorfismos es isomorfismo

$$\begin{array}{l} I_X \in \mathrm{Iso}(X, X) \\ \varphi \in \mathrm{Iso}(X, Y) \wedge \phi \in \mathrm{Iso}(Y, Z) \;\Rightarrow\; \phi \circ \varphi \in \mathrm{Iso}(X, Z) \end{array}$$

Fácilmente se obtiene también

**54.-** Una biyección entre conjuntos ordenados es isomorfismo si y solo si su inversa es isomorfismo

$$\varphi \in \mathrm{Biy}(X,Y) \;\Rightarrow\; (\varphi \in \mathrm{Iso}(X,Y) \Leftrightarrow \varphi^{-1} \in \mathrm{Iso}(Y,X))$$

Respecto a la transformación de cotas mediante isomorfismos observamos que

$$c' \in Y \Leftrightarrow \exists\, !c \in X \ni c' = \varphi(c)$$

y además

$$a' \in \varphi(A) \Leftrightarrow \exists\, !a \in A \ni a' = \varphi(a)$$

la monotonía de $\varphi$ implica entonces que

$$c' \leq a' \Leftrightarrow c \leq a$$

por consiguiente

$$c' \in C_I(\varphi(A)) \Leftrightarrow c \in C_I(A)$$

y estas relaciones implican

**55.-** La imagen del conjunto de las cotas inferiores es igual al conjunto de las cotas inferiores de la imagen

$$\varphi(C_I(A)) = C_I(\varphi(A))$$

Con modificaciones obvias se obtiene

**56.-** La imagen del conjunto de las cotas superiores es igual al conjunto de las cotas superiores de la imagen

$$\varphi(C_S(A)) = C_S(\varphi(A))$$

Una consecuencia de **55** y **56** es que los isomorfismos conservan la acotación:

**57.-** Un conjunto es acotado inferiormente si y solo si su imagen es acotada inferiormente

$$C_I(A) \neq \emptyset \Leftrightarrow C_I(\varphi(A)) \neq \emptyset$$

Análogamente

**58.-** Un conjunto es acotado superiormente si y solo si su imagen es acotada superiormente
$$C_S(A) \neq \emptyset \Leftrightarrow C_S(\varphi(A)) \neq \emptyset$$

Asimismo, invocando **10** y **13** vemos que los isomorfismos conservan la existencia de primer elemento y que los transforma entre si.

**59.-** Un subconjunto tiene primer elemento si y solo si su imagen tiene primer elemento, esto es, para $A \subseteq X$ y $\varphi \in \mathrm{Iso}(X, Y)$

$$\exists\, p(A) \in A \Leftrightarrow \exists\, p(\varphi(A)) \in \varphi(A)$$

**60.-** La imagen del elemento primero es el elemento primero de la imagen

$$\varphi(p(A)) = p(\varphi(A))$$

Lo mismo ocurre con el último elemento

**61.-** Un subconjunto tiene último elemento si y solo si su imagen tiene último elemento
$$\exists\, u(A) \in A \Leftrightarrow \exists\, u(\varphi(A)) \in \varphi(A)$$

**62.-** La imagen del último elemento es el último elemento de la imagen

$$\varphi(u(A)) = u(\varphi(A))$$

Los conjuntos de seguidores se comportan como cabe esperar

**63.-** La imagen del conjunto de seguidores es el conjunto de seguidores de la imagen
$$\varphi(S(x)) = S(\varphi(x))$$

Esto equivale a $x < y \Leftrightarrow \varphi(x) < \varphi(y)$ lo cual es cierto debido a la doble monotonía y a **52**.

En $X$ está contenido el dominio $K(X)$ de la función sucesor $s_X : K(X) \to X$; asimismo, hay un dominio $K(Y) \subseteq Y$ para la función sucesor en el rango $s_Y : K(Y) \to Y$.

**64.-** Un elemento tiene sucesor inmediato si y solo si su imagen tiene sucesor inmediato

$$\exists\, s_X(x) = p(S(x)) \in S(x) \Leftrightarrow \exists\, s_Y(\varphi(x)) = p(S(\varphi(x))) \in S(\varphi(x))$$

Con los enunciados anteriores podemos concluir que

**65.-** Un isomorfismo transforma el dominio de la función sucesor de $X$ en el dominio de la función sucesor de $Y$ y la imagen del sucesor en el sucesor de la imagen: Si $\varphi \in \mathrm{Iso}(X,Y)$ entonces

$$\varphi(K(X)) = K(Y) \qquad \varphi(s_X(x)) = s_Y(\varphi(x))$$

Esto equivale a

**66.-** La composición de la función sucesor con el isomorfismo es igual a la composición del isomorfismo con la función sucesor

$$\varphi \circ s_X = s_Y \circ \varphi$$

y puede reformularse como la igualdad

$$\varphi(x^+) = \varphi(x)^+$$

Los isomorfismos conservan la buena ordenación:

**67.-** Si dos conjuntos ordenados son isomorfos y uno es un buen orden también lo es el otro, es decir, si $\varphi \in \mathrm{Iso}(X,Y)$ entonces

$$X \text{ es buen orden } \Leftrightarrow Y \text{ es buen orden}$$

## 12. Conjuntos invariantes

Repasaremos en esta sección –para aplicarlas después a la función sucesor– algunas propiedades de los conjuntos invariantes.

Consideremos una función de un conjunto cualquiera $X$ en si mismo

$$f : X \to X$$

Un conjunto es *invariante por* $f$, o $f$*-invariante*, o –confusión descartada– *invariante* si contiene a su propia imagen por la función, es decir, $A \subseteq X$ es invariante si $f(A) \subseteq A$. Los conjuntos invariantes forman una colección, denotada $\mathcal{I}^f(X)$, contenida en $\mathcal{P}(X)$

$$\mathcal{I}^f(X) = \{A \mid f(A) \subseteq A\}$$

Obviamente el conjunto vacío y el conjunto total son invariantes:

$$\emptyset, X \in \mathcal{I}^f(X)$$

Examinemos el comportamiento de los conjuntos invariantes respecto a la unión.

**68.-** La unión de dos conjuntos invariantes es invariante

$$A, B \in \mathcal{I}^f(X) \;\Rightarrow\; A \cup B \in \mathcal{I}^f(X)$$

Esto se debe a que la imagen de la unión de dos conjuntos es la unión de las imágenes, $f(A \cup B) = f(A) \cup f(B)$, y entonces

$$f(A \cup B) = f(A) \cup f(B) \subseteq A \cup B$$

El mismo razonamiento proporciona un resultado ligeramente más general. Considere la unión $A \cup B$ de subconjuntos cualesquiera $A, B$ de $X$ (no necesariamente invariantes).

**69.-** Si la imagen de cada uniendo está contenida en la unión entonces la unión es invariante

$$f(A) \subseteq A \cup B \wedge f(B) \subseteq A \cup B \;\Rightarrow\; f(A \cup B) \subseteq A \cup B$$

La invariancia de la unión vale igualmente si tenemos además un tercer uniendo $C$ con $f(C) \subseteq A \cup B \cup C$. Para uniones arbitrarias considere una familia de subconjuntos de $X$, es decir, $\mathcal{A} \subseteq \mathcal{P}(X)$, entonces

**70.-** Si la imagen de cada uniendo está contenida en la unión entonces la unión es invariante

$$(\forall A' \in \mathcal{A},\ f(A') \subseteq \bigcup \mathcal{A}) \ \Rightarrow\ \bigcup \mathcal{A} \in \mathcal{I}^f(X)$$

La hipótesis dice que $f(A') \subseteq \bigcup_{A\in\mathcal{A}} A$ y el resultado se deduce de la propiedad de ser la imagen de la unión igual a la unión de las imágenes: $f(\bigcup_{A\in\mathcal{A}} A) = \bigcup_{A\in\mathcal{A}} f(A)$.

**71.-** La intersección de conjuntos invariantes es invariante, esto es, si $\mathcal{A}$ es una colección de conjuntos invariantes, $\mathcal{A} \subseteq \mathcal{I}^f(X)$, entonces también su intersección es un conjunto invariante

$$\bigcap \mathcal{A} = \{x \,|\, \forall A \in \mathcal{A},\ x \in A\} \in \mathcal{I}^f(X)$$

En efecto, un elemento de la intersección está en todos los miembros de la colección y, por ser estos invariantes, su imagen por $f$ está nuevamente en todos los miembros, es decir, en la intersección, lo cual prueba que la intersección es invariante.

El razonamiento anterior se puede reformular así: La condición $x \in \bigcap \mathcal{A}$ significa que $\forall A \in \mathcal{A},\ x \in A$; por ser $A$ invariante $f(x) \in A$, luego $f(x) \in \bigcap \mathcal{A}$ y esto dice que $\bigcap \mathcal{A}$ es $f$-invariante.

Cualquier conjunto $B \subseteq X$ está contenido en al menos un conjunto invariante, a saber, en $X$. Por consiguiente la clase de los conjuntos invariantes que contienen a $B$ es no vacía. Para precisar, denotemos por $\mathcal{I}^f(X;B)$ la colección de los subconjuntos invariantes que contienen a $B$

$$\mathcal{I}^f(X;B) = \{A \,|\, B \subseteq A \in \mathcal{I}^f(X)\}$$

entonces la colección es no vacía porque $X$ es uno de sus miembros, $X \in \mathcal{I}^f(X;B)$. La intersección de la colección, denotada $[B]^f$, es el *conjunto invariante generado por* $B$ de manera que

$$[B]^f = \bigcap \mathcal{I}^f(X;B) = \bigcap \{A \,|\, B \subseteq A \in \mathcal{I}^f(X)\}$$

Esta intersección contiene a $B$ y **71** garantiza que es invariante.

$$B \subseteq [B]^f \in \mathcal{I}^f(X;B) \subseteq \mathcal{I}^f(X)$$

Obviamente $[B]^f$ está contenido en todos los intersectandos, luego

**72.-** El conjunto invariante generado por $B$ es el menor conjunto invariante que contiene a $B$

$$A \in \mathcal{I}^f(X; B) \;\Rightarrow\; [B]^f \subseteq A$$

Para elementos $x \in X$ denotaremos por $[x]^f$ al conjunto invariante generado por $B = \{x\}$, o sea, $[x]^f = [\{x\}]^f$. Por lo tanto

$$[x]^f = \bigcap\{A \mid x \in A \in \mathcal{I}^f(X)\}$$

## 13. Conjuntos inductivos

En esta sección $X$ denota un conjunto bien ordenado y no vacío con función sucesor

$$s : K(X) = X - u(X) \to X$$

Una *parte $s$-inductiva* o *subconjunto $s$-inductivo* es un conjunto que contiene al primer elemento, está contenido en el dominio de la función sucesor y es $s$-invariante. En general la función sucesor $s$ está sobreentendida y la omitimos diciendo simplemente 'parte inductiva' o 'subconjunto inductivo'.

Denotamos por $\mathcal{I}^s_0(X)$ la colección de las partes inductivas de $X$

$$\mathcal{I}^s_0(X) = \{D \mid 0_X \in D \in \mathcal{I}^s(K(X))\}$$

Cuando el conjunto bien ordenado $X$ resulta ser parte inductiva de si mismo, $X \in \mathcal{I}^s_0(X)$, decimos que $X$ es un *conjunto inductivo*. En tal caso la condición $X \in \mathcal{I}^s(K(X))$ exige que el dominio de la función sucesor sea todo $X$, es decir, $K(X) = X$.

Como consecuencia de **27** podemos expresar la inductividad de un conjunto bien ordenado sin mencionar explícitamente la función sucesor:

**73.-** Un conjunto bien ordenado es inductivo si y solo si *no* tiene último elemento

$$X \in \mathcal{I}^s(K(X)) \Leftrightarrow \nexists\, u(X)$$

Cuando $X = \{0_X\}$ consta de un único elemento este no tiene sucesor y $K$ es vacío; no hay entonces partes inductivas. Véase también **76**.

Es importante resaltar que la noción de parte inductiva está referida al primer elemento del conjunto bien ordenado $X$. Todos los subconjuntos no vacíos de $Y \subseteq X$ están bien ordenados, pero en general el primer elemento no es el mismo, $0_Y \neq 0_X$, y entonces $Y \notin \mathcal{I}^s(K(X))$. Compare con **90** más abajo.

• *Los conjuntos inductivos son relativos.* Con el orden inducido toda parte $A \subseteq X$ es un conjunto bien ordenado. Puede ser incluso un conjunto $s_A$-invariante con primer elemento igual al de $X$, y por lo tanto inductivo: $0_X \in A \in \mathcal{I}_0^{s_A}(A)$. Y sin embargo puede no ser una parte inductiva de $X$: $A \notin \mathcal{I}_0^s(X)$. Por ejemplo, en $X = \mathbb{N}$ los números pares, $A = \{0, 2, 4, \dots\}$, no son una parte inductiva de $\mathbb{N}$. El motivo: respecto a $\mathbb{N}$ hay en $A$ 'brechas', a saber, faltan todos los impares. $A$ es $s_A$-invariante pero no es $s_X$-invariante.

El orden de un conjunto bien ordenado $X$ se puede restringir a sus subconjuntos y en particular a sus partes inductivas. Estas resultan ser, según **16**, conjuntos bien ordenados. Y son también conjuntos inductivos.

**74.-** Toda parte inductiva es un conjunto inductivo

$$D \in \mathcal{I}_0^s(X) \;\Rightarrow\; D \in \mathcal{I}_0^s(D)$$

En efecto, por ser $D \in \mathcal{I}_0^s(X)$ la función sucesor está definida en todo $D$ y su imagen está contenida en $D$, esto es, $s : D \to D$. Luego $D \in \mathcal{I}_0^s(D)$.

Por lo tanto **46** y **73** implican

**75.-** Toda parte inductiva de un conjunto bien ordenado es un subconjunto infinito sin último elemento.

**76.-** Si $X$ es finito entonces no tiene partes inductivas.

En sentido figurado las partes inductivas –y en particular los conjuntos inductivos– son conjuntos ordenados muy grandes (infinitos) sin 'tapón' al final.

La existencia de conjuntos inductivos no puede demostrarse (partiendo de los otros principios de la teoría de conjuntos). Su existencia debe ser postulada como un axioma que a continuación enunciamos y asumimos.

Axioma de Infinito: *Existe al menos un conjunto inductivo.*

Aceptando este axioma se infiere como corolario inmediato de **75** que existe al menos un conjunto infinito.

• *Enunciado natural del axioma de infinito.* El nombre 'Axioma de Infinito' sugiere que su enunciado podría ser: *Existe un conjunto infinito.* Es posible hacer tal modificación. La existencia de un conjunto inductivo se obtiene entonces invocando el Principio de Buena

Ordenación –consecuencia otrora controvertida del Axioma de Elección– para inferir que el decretado conjunto infinito admite un buen orden y probando después que este contiene una parte inductiva, a saber, el subconjunto $s$-invariante $[0_X]^s$ generado por el primer elemento. Véase **79**. Luego, en presencia del Axioma de Elección y sus consecuencias, basta postular la existencia de un conjunto infinito para obtener la existencia de un conjunto inductivo.

En adelante supondremos que el conjunto bien ordenado $X$ es inductivo, es decir, asumimos que

$$X \in \mathcal{I}_0^s(X)$$

y en particular que $K(X) = X$.

De las definiciones se desprende el siguiente enunciado.

**77.-** La intersección de partes inductivas es una parte inductiva

$$\mathcal{C} \subseteq \mathcal{I}_0^s(X) \ \Rightarrow \ \bigcap \mathcal{C} \in \mathcal{I}_0^s(X)$$

Esto implica que hay partes inductivas contenidas en todas las demás.

**78.-** Si $X$ es inductivo entonces contiene una parte inductiva, denotada $\mathbb{N}_X$, que está contenida en todas las demás, es decir, existe $\mathbb{N}_X \in \mathcal{I}_0^s(X)$ tal que

$$Y \in \mathcal{I}_0^s(X) \ \Rightarrow \ \mathbb{N}_X \subseteq Y$$

En efecto, basta tomar $\mathbb{N}_X$ igual a la intersección de todos los subconjuntos inductivos

$$\mathbb{N}_X = \bigcap \mathcal{I}_0^s(X)$$

Llamaremos a $\mathbb{N}_X$ *parte inductiva minimal* de $X$. El conjunto inductivo $X$ es un *conjunto inductivo minimal* si es igual a su parte inductiva minimal

$$X = \mathbb{N}_X$$

Puesto que todas las partes inductivas contienen al primer elemento $0_X$ se sigue que

**79.-** La parte inductiva minimal es igual al conjunto invariante generado por el primer elemento

$$\mathbb{N}_X = [0_X]^s$$

Porque siendo $\mathbb{N}_X$ un conjunto $s$-invariante y $0_X \in \mathbb{N}_X$ se cumple $[0_X]^s \subseteq \mathbb{N}_X$. Por otra parte si $Y \in \mathcal{I}^s(X;\{0\})$ entonces $Y$ es $s$-invariante y $0 \in Y \subseteq X = K(X)$ (hemos supuesto que $X$ es inductivo). Por minimalidad $\mathbb{N}_X \subseteq Y$, luego $\mathbb{N}_X \subseteq \bigcap \mathcal{I}^s(X;\{0\}) = [0_X]^s$. Queda probado que $\mathbb{N}_X = [0_X]^s$.

## 14. Números naturales

Un *sistema de números naturales* es un conjunto inductivo minimal. Hay tantos sistemas de números naturales como conjuntos inductivos minimales. Un *número natural* o simplemente un *natural* es un elemento de un sistema de números naturales.

• *Naturales como orden.* Según la definición adoptada los sistemas de números naturales son estructuras ordenadas. Se trata de conjuntos dotados de relaciones de orden especiales: Bien ordenado, sin último elemento y minimal en la clase de los conjuntos $s$-invariantes que contienen al primer elemento $0_X$. En esta formulación no intervienen explícitamente las operaciones de suma y producto, por lo tanto un sistema de números naturales no es –a nivel de esta definición– una estructura algebraica. Las operaciones de suma y producto se obtienen a partir de la función sucesor y esta se define exclusivamente en términos de la estructura de orden.

• *La axiomatización de los naturales fue tardía.* Es de presumir que la Geometría como conjunto de reglas empíricas es muy antigua; su axiomatización se inicia con los *Elementos* de Euclides que data del siglo III a.C., es decir, ocurre hace dos mil trescientos años. El uso de los naturales –el acto de contar– se remonta a tiempos por lo menos tan antiguos como la Geometría. Pero las primeras axiomatizaciones de los naturales surgieron recién el siglo XIX; se deben a Charles S. Peirce, en 1881, y a Giuseppe Peano, en 1885. La formulación axiomática de Lawvere [10] en 1964, requirió otras ocho décadas. Al respecto véase Bedoya [2]; Luque Arias [11]; y Oostra [12], [13].

Podemos reformular **78** así:

**80.-** Un conjunto inductivo $X$ es un sistema de números naturales si y solo si $X = \mathbb{N}_X$.

**81.-** Todo conjunto inductivo $X$ contiene un único sistema de números naturales, a saber, el conjunto inductivo generado por $0_X$

$$\mathbb{N}_X = I[0_X]$$

Se probó en **75** que todo conjunto inductivo es infinito, en particular

**82.-** Los sistemas de números naturales son conjuntos infinitos.

Invocamos ahora el Axioma de Infinito y 81 para concluir que

**83.-** Existen sistemas de números naturales.

Denotamos mediante $\mathbb{N}$ un sistema particular de números naturales que entre los muchos existentes queda privilegiado precisamente porque nos referimos a él con la notación $\mathbb{N}$. Su primer elemento se denota 0 (en vez de $0_{\mathbb{N}}$) y se denomina *cero*; el sucesor de 0 se denota 1 (en lugar de $1_{\mathbb{N}}$), y es el *uno* o *unidad*. Un número natural es *positivo* si es distinto de 0. El conjunto de los naturales positivos se denota por $\mathbb{N}^+$. Por tricotomía y por definición de primer elemento se tiene

**84.-** Un natural es positivo si y solo si es estrictamente mayor que cero

$$n \neq 0 \Leftrightarrow 0 < n$$

Por otra parte **20** se formula así:

**85.-** El sucesor de un natural lo sigue estrictamente

$$n < s(n)$$

Considere números naturales $m \leq k$. El *intervalo* (de naturales) de extremo inferior $m$ y extremo superior $k$ es el conjunto, denotado $[m, k]_{\mathbb{N}}$, de los naturales que siguen al extremo inferior y preceden al superior

$$[m, k]_{\mathbb{N}} = \{n \,|\, m \leq n \leq k\}$$

Obviamente los extremos pertenecen al intervalo: $m \in [m, k]_{\mathbb{N}}$ y $k \in [m, k]_{\mathbb{N}}$.

Cuando el extremo inferior es cero se tiene el *intervalo inicial* de extremo $k$

$$[0, k]_{\mathbb{N}} = \{n \,|\, 0 \leq n \leq k\}$$

Utilizando nuevamente la ley de tricotomía inferimos

**86.-** Los naturales son unión disjunta del intervalo inicial de extremo $n$ y los seguidores de $n$

$$\mathbb{N} = [0,n]_{\mathbb{N}} \cup S(n) \qquad [0,n]_{\mathbb{N}} \cap S(n) = \emptyset$$

**87.-** Un natural es cota superior de un conjunto si y solo si el conjunto está contenido en el intervalo inicial de extremo el natural

$$n \in C_S(A) \Leftrightarrow A \subseteq [0,n]_{\mathbb{N}}$$

En el caso de los números naturales **24** adopta la siguiente forma

**88.-** El intervalo de extremos un natural y su sucesor no contiene otros elementos, es decir, si $n \in \mathbb{N}$ entonces

$$[n, s(n)]_{\mathbb{N}} = \{n, s(n)\}$$

El venerable principio que enunciamos a continuación es la esencia de los sistemas de números naturales. Consideremos un sistema $\mathbb{N}$ y un subconjunto $A \subseteq \mathbb{N}$.

**89.-** *Principio de Inducción:* Si un subconjunto contiene al primer elemento, y si cada vez que contiene a un natural contiene también a su sucesor, entonces es igual a todo el sistema, esto es,

$$\left.\begin{array}{r} 0 \in A \\ \wedge \\ n \in A \;\Rightarrow\; n^+ \in A \end{array}\right\} \;\Rightarrow\; A = \mathbb{N}$$

En efecto, $A$ es un subconjunto de $\mathbb{N}$ y la condición es precisamente la de ser inductivo. Por la minimalidad de $\mathbb{N}$ se sigue que $A = \mathbb{N}$.

En el contexto del principio de inducción la condición $n \in A$ es la *hipótesis de inducción* o *hipótesis inductiva.*

El principio de inducción tiene numerosísimas aplicaciones a lo largo y ancho de toda la Matemática. Para los usos más elementales véase por ejemplo Golovina y Yaglom [5] y Sominski [14].

Como aplicación del principio de inducción demostraremos que $S(n)$ es un sistema de naturales respecto al primer elemento $n^+ \in S(n)$.

**90.-** El conjunto de los seguidores de un natural es un sistema de números naturales con primer elemento el sucesor del natural.

Debemos probar que $S(n)$ es una parte inductiva con primer elemento $n^+$ y es minimal, o sea, es un conjunto bien ordenado con primer elemento $n^+$, es $s$-invariante y $\mathbb{N}_{S(n)} = S(n)$.

Según **16** el subconjunto $S(n) \subseteq \mathbb{N}$ es un buen orden; su primer elemento es, por definición de sucesor, $s(n) = n^+$, y es $s$-invariante porque $m \in S(n) \Rightarrow n < m < s(m)$.

Falta probar la condición de minimalidad, es decir, si $A[n^+] \subseteq S(n)$ es una parte inductiva (con primer elemento $n^+$) entonces $A[n^+] = S(n)$. Por **86**, la union, que denotamos $A$, del intervalo inicial con extremo $n$ y $A[n^+]$ es disjunta

$$A = [0, n]_{\mathbb{N}} \cup A[n^+] \qquad [0, n]_{\mathbb{N}} \cap A[n^+] = \emptyset$$

Obviamente $A \subseteq \mathbb{N}$ y su primer elemento es 0; veamos que es $s$-invariante. Por tricotomía hay para cada elemento $m \in A$ tres posibilidades:

1) $m < n$. Entonces $s(m) \leq n$ de donde $s(m) \in [0, n]_{\mathbb{N}} \subseteq S(n) \subseteq A$.
2) $m = n$. En este caso $s(m) = s(n) = n^+ \in S(n) \subseteq A$.
3) $n \in A[n^+]$. Se cumple $s(m) \in s(A[n^+]) \subseteq A[n^+] \subseteq A$.

Por **69** concluimos que $A$ es $s$-invariante y por lo tanto inductivo. El principio de inducción implica entonces que $A = \mathbb{N}$, luego

$$\begin{aligned} S(n) &= S(n) \cap \mathbb{N} \\ &= S(n) \cap A \\ &= S(n) \cap ([0, n]_{\mathbb{N}} \cup A[n^+]) \\ &= (S(n) \cap [0, n]_{\mathbb{N}}) \cup (S(n) \cap A[n^+]) \\ &= \emptyset \cup (S(n) \cap A[n^+]) \\ &= S(n) \cap A[n^+] \end{aligned}$$

Estas igualdades se justifican razonando como sigue: La primera porque $S(n) \subseteq \mathbb{N}$; la segunda porque, según hemos demostrado, $A = \mathbb{N}$; la tercera por la definición de $A$; la cuarta por la propiedad distributiva de la intersección respecto a la unión; la quinta por **86**; y la última es obvia.

Como $S(n) = S(n) \cap A[n^+] \subseteq A[n^+]$ y $A[n^+] \subseteq S(n)$ tenemos $S(n) = A[n^+]$ y por consiguiente $S(n)$ es minimal: $\mathbb{N}_{S(n)} = S(n)$. Luego $S(n)$ es un sistema de números naturales con primer elemento $n^+$.

En particular:

**91.-** El conjunto $\mathbb{N}^+ = S(0)$ de naturales positivos es un sistema de números naturales con primer elemento 1.

En el caso del sistema $S(n)$ de números naturales el principio de inducción se expresa así:

**92.-** Si $A' \subseteq S(n)$ satisface $n^+ \in A'$ y si $k \in A'$ implica $k^+ \in A'$ entonces $A' = S(n)$

El siguiente resultado es otra consecuencia del principio de inducción y reemplaza –en el caso de los naturales– la contención de **30** por una igualdad.

**93.-** La imagen de la función sucesor es el conjunto de los naturales positivos

$$s(\mathbb{N}) = \mathbb{N} - \{0\}$$

Sea $A = \{0\} \cup s(\mathbb{N})$. Es evidente que $0 \in A$, y $A$ es invariante porque $A \subseteq \mathbb{N} \;\Rightarrow\; s(A) \subseteq s(\mathbb{N}) \subseteq A$. Por el principio de inducción, $A = \mathbb{N}$. Luego todo natural positivo es un sucesor: $s(\mathbb{N}) = \mathbb{N} - \{0\}$.

Más aún, hay la siguiente unicidad:

**94.-** Todo natural positivo es sucesor de un único natural

$$n > 0 \;\Rightarrow\; \exists\,!\, m \in \mathbb{N} \ni s(m) = n$$

La existencia de $m$ es precisamente **93** y su unicidad se desprende de **32**, esto es, de la inyectividad de $s$.

## 15. Antecesores

El *antecesor inmediato* o simplemente *antecesor* de un natural $n$ es el único natural $m$ del cual es sucesor. Por **94** el antecesor de cualquier natural, salvo 0, existe y es único. El antecesor de $n$ se designará mediante $n^-$. La *función antecesor*, denotada $a : \mathbb{N} - \{0\} \to \mathbb{N}$, asigna al natural positivo $n$ su antecesor, esto es

$$a(n) = n^-$$

Por ejemplo, $a(1) = 0$, $a(2) = 1$, $a(3) = 2$, etc.

Las definiciones tienen las siguientes consecuencias.

**95.-** El antecesor de un natural positivo lo precede estrictamente

$$a(n) < n$$

**96.-** El sucesor del antecesor de un natural positivo es el natural positivo

$$(n^-)^+ = s(a(n)) = n$$

**97.-** El antecesor del sucesor de un natural es el natural

$$(n^+)^- = a(s(n)) = n$$

Estos dos enunciados equivalen a los siguientes

**98.-** La composición de la función sucesor con la función antecesor es la identidad de $\mathbb{N} - \{0\}$

$$s \circ a = I_{\mathbb{N}-\{0\}}$$

**99.-** La composición de la función antecesor con la función sucesor es la identidad de $\mathbb{N}$

$$a \circ s = I_{\mathbb{N}}$$

Usando antecesores en lugar se sucesores podemos reformular **24**

**100.-** Entre un natural y su antecesor no hay otros naturales

$$a(n) \leq m \leq n \ \Rightarrow \ m = a(n) \vee m = n$$

lo cual implica

**101.-** El intervalo de extremo inferior el antecesor de un natural y extremo superior el natural tiene como únicos elementos al natural y a su antecesor

$$[a(n), n]_{\mathbb{N}} = \{a(n), n\}$$

**102.-** Todo intervalo inicial de extremo un natural positivo es unión disjunta del intervalo inicial de extremo su antecesor con el unipuntual del natural, es decir, si $0 < n$ entonces

$$[0, n]_{\mathbb{N}} = [0, a(n)]_{\mathbb{N}} \cup \{n\} \qquad [0, a(n)]_{\mathbb{N}} \cap \{n\} = \emptyset$$

Podemos aplicar el concepto de antecesor inmediato para probar

**103.-** La primera cota superior de un conjunto de naturales pertenece al conjunto, es decir, si $\emptyset \neq A \subseteq \mathbb{N}$ y $C_S(A) \neq \emptyset$ entonces

$$p = p(C_S(A)) \in A$$

Según **87** y **102**, $A \subseteq [0, p]_{\mathbb{N}} = [0, a(p)]_{\mathbb{N}} \cup \{p\}$. Si fuese $p \notin A$ entonces $A \subseteq [0, a(p)]_{\mathbb{N}}$ y $a(p) < p$ sería cota superior, $a(p) \in C_S(A)$, contrario a la condición de ser $p$ el primer elemento de $C_S(A)$.

**104.-** Todo conjunto no vacío y acotado superiormente de números naturales tiene último elemento, es decir, si $\emptyset \neq A \subseteq \mathbb{N}$ entonces

$$C_S(A) \neq \emptyset \;\Rightarrow\; \exists\, u(A) \in A$$

En efecto, sea $u = p(C_S(A)) \in C_S(A)$ la primera de las cotas superiores. Por el resultado anterior $u \in A$, luego $A \cap C_S(A) \neq \emptyset$ y aplicamos **13**.

## 16. Dígitos

Los primeros elementos de $\mathbb{N}$ se denotan con los nombres (que dependen del idioma utilizado) y símbolos especiales siguientes:

| **Elemento** | **Nombre** | **Símbolo** |
|---|---|---|
| Primer elemento de $\mathbb{N}$: | Cero | 0 |
| Sucesor de 0, $s(0) = 0^+$ | Uno | 1 |
| Sucesor de 1, $s(1) = 1^+$ | Dos | 2 |
| Sucesor de 2, $s(2) = 2^+$ | Tres | 3 |
| Sucesor de 3, $s(3) = 3^+$ | Cuatro | 4 |
| Sucesor de 4, $s(4) = 4^+$ | Cinco | 5 |
| Sucesor de 5, $s(5) = 5^+$ | Seis | 6 |
| Sucesor de 6, $s(6) = 6^+$ | Siete | 7 |
| Sucesor de 7, $s(7) = 7^+$ | Ocho | 8 |
| Sucesor de 8, $s(8) = 8^+$ | Nueve | 9 |

Esta nomenclatura originó en India, durante la Edad Media fue llevada a España por los árabes y de allí pasó a Suramérica. Puede ampliarse a todo $\mathbb{N}$ y entonces constituye el *sistema decimal de numeración posicional*. Los símbolos son los *dígitos del sistema Arábigo-Hindú*.

Para otro sistema $\mathbb{N}_X \neq \mathbb{N}$ de números naturales tenemos un primer elemento $0_X$ y sus sucesores $1_X = s_X(0_X)$, $2_X = s_X(1_X)$, etc. que, desde luego, no son necesariamente los mismos de $\mathbb{N}$.

• *Origen anatómico del sistema Arábigo-Hindú.* Indiscutiblemente el sistema Arábigo-Hindú se inspiró en los dedos de las manos. Otras nomenclaturas, como la numeración romana, son menos eficientes y de alcance limitado.

• *Virtudes de la notación Arábigo-Hindú.* El número natural concebido como elemento de un conjunto bien ordenado, inductivo y minimal es angustiosamente xerófilo. El ciudadano común no estudia conjuntos ordenados, ordinales, etc. Ninguno de nosotros aprendió los números naturales como ordinales (o cardinales) finitos ni como conjuntos inductivos minimales, sino que desde corta edad pasamos por un largo proceso educativo donde progresivamente los fuimos conociendo por sus apelativos, sus guarismos y usándolos para contar. Un amplio sector de la raza humana los ha asimilado y los utiliza cotidianamente. Esto es en gran parte posible gracias al sistema de numeración. En efecto, los números en la vida diaria no son entidades abstractas sino que se identifican por sus símbolos y nombres con lo cual adquieren cédula de identidad y personalidad propia. El uso diario los transforma en una especie de sociedad jerarquizada cuyos miembros se reconocen y ubican por nombre y apellido. Al respecto vea las secciones que siguen: 17, 18 y 19.
Con la nomenclatura posicional Arábigo-Hindú las operaciones aritméticas de suma y producto se traducen en reglas relativamente simples: Las que todos aprendimos en la escuela primaria. Como contraste, las operaciones aritméticas bajo el sistema romano de numeración son mucho más trabajosas.

## 17. Números como símbolos

Los símbolos del sistema de numeración arábigo-hindú proporcionan un conjunto bien ordenado muy particular, a saber

$$\mathbb{N}_S = \{0, 1, 2, 3, \dots, 1000, 1001, 1002, \dots\}$$

Este conjunto de símbolos se obtiene yuxtaponiendo dígitos, es pragmáticamente infinito, y satisface todos los requerimientos de la definición de sistema de números naturales. Con este enfoque los números no son distintos de los símbolos utilizados para representarlos. Dicho de otro modo, un número no sería un concepto o idea abstracta sino un tipo particular de marca hecha en una superficie y percibida por una persona debidamente educada. La persona humana, su contexto cultural y en particular la educación adquieren crucial importancia.

## 18. Sistema nominal escrito

La definición de sistema de números naturales adoptada en esta cartilla también permite considerar los números como si fueran esencialmente la colección de sus nombres escritos; estos sistemas –al menos uno en cada idioma– lo llamaremos *sistema nominal escrito*. Así, el sistema nominal escrito español, $\mathbb{N}_E$, es el conjunto bien ordenado, inductivo y minimal cuyos elementos son los nombres de los números *escritos en idioma español*

$$\mathbb{N}_E = \{\text{Cero, Uno, Dos, Tres}, \ldots, \text{Mil, Mil Uno, Mil Dos}, \ \ldots\}$$

Las reglas para nombrar los números son tales que el conjunto de los nombres satisface las condiciones para ser un sistema de números naturales.

## 19. Sistema nominal hablado

Los nombres escritos pueden ser reemplazados por sonidos, es decir, por los nombres hablados. El sistema de números naturales así obtenido consiste en los sonidos que resultan al pronunciar en voz alta los nombres de los números. Lo denominamos *sistema nominal hablado*; al igual que los sistemas escritos, cambian con el idioma. Estos números consisten en sonidos articulados que surgen en la conversación, las discusiones, conferencias, etc. Los números pronunciados o sonoros tienen la particularidad de ser efímeros: Duran lo que el sonido de la palabra, lo cual resalta la importancia que para su uso tiene la memoria.

• *Aprendizaje elemental.* Los sistemas nominales escritos y hablados de números naturales se perciben como menos abstractos y proporcionan la experiencia básica para aprender a contar. Son enseñados a los niños en las escuelas elementales.

• *Traducción consistente.* En cada idioma los nombres de los números son distintos y por lo tanto los correspondientes sistemas nominales escritos resultan ser diferentes. Por ejemplo, en idioma inglés el sistema nominal escrito es

$$\begin{aligned}\mathbb{N}_I = \{&\text{Zero, One, Two, Three}, \ldots\\ &\ldots, \text{One Thousand, One Thousand and One, One Thousand and Two}, \ldots\}\end{aligned}$$

Pero, según se verá en el enunciado 140, el sistema inglés $\mathbb{N}_I$ es isomorfo con el sistema español $\mathbb{N}_E$ mediante isomorfismo único, de manera que los dos sistemas pueden ser comparados sin ambigüedad. Igual situación ocurre al comparar con un sistema hablado de números naturales. La traducción entre soportes físicos e idiomas cualesquiera está garantizada por 140.

• *Axiomas físicos.* Los sistemas escritos y hablados de números naturales plantean un problema especial. Para satisfacer la definición de sistema de números naturales los nombres de los números –tanto los escritos como los hablados– deben formar conjuntos infinitos. Ya en la sección 17 se mencionó que el conjunto de los símbolos de los números es potencialmente ilimitado. Pero las palabras escritas son marcas sobre una superficie y las pronunciadas son sonidos. Se trata de realidades físicas. ¿Qué es un sistema infinito de palabras escritas o habladas? Ni siquiera es claro que el Universo sea infinito ni se vislumbra criterio para decidir esta cuestión. La salida más cómoda es postular la infinitud de los sistemas físicos requeridos, por ejemplo, con el siguiente:

Axioma Físico de Infinito: *Para cada lenguaje natural existen sistemas nominales escrito y hablado de números naturales.*

Puesto que los símbolos escritos y los sonidos son objetos físicos, el axioma se refiere al mundo físico. Este postulado establece como acto de fe –o de conveniencia– la existencia física de las infinitas expresiones escritas y las infinitas expresiones habladas que se requieren para un sistema de naturales.

Dado que no es posible escribir o pronunciar los nombres de todos los números, la infinitud debe entenderse en un sentido pragmático e histórico. Esto significa lo siguiente: Los sistemas nominales son físicamente infinitos porque cada vez que un agente externo nos presenta una lista física de números, o la pronuncia, siempre ha sido y sigue siendo posible añadir un número más. De manera que para demostrar la *no existencia* de infinitos números la parte interesada debe asumir la carga de la prueba y presentar de manera efectiva y convincente una lista finita a la cual es imposible añadir un número más.

El uso de los números a todo lo largo de la aventura humana llamada Historia indica que el Axioma Físico de Infinito es, para cualquier propósito práctico, perfectamente aceptable. Por otra parte tiene una garantía difícil de superar: El horror al aburrimiento. Un Universo sin infinitos es tan aburrido que resulta intolerable. Las teorías consistentes que postulan la finitud de los sistemas de números naturales –si es que existen– están relegadas al depósito de las curiosidades.

Es creencia generalizada que los axiomas están reservados a las Matemáticas y son inútiles para forzar las realidades físicas. Desde Galileo la moda en Física supuestamente ha sido observar, medir y hacer desfilar los resultados para que juzgue el inefable público. Pero este admirable esquema es otro ideal platónico en desacuerdo con el crudo ejercicio de la Ciencia. Una hojeada a las publicaciones en algunas áreas de la Física Teórica demuestra que la simple existencia de complicadas estructuras matemáticas basta para proponerlas como explicación de alejadas utopías físicas. El Axioma Físico de Infinito va en sentido inverso: Es un modesto postulado acerca del Universo físico que pudiera inducir algunas reflexiones en Matemáticas, Filosofía y Física.

• *Reconocimiento de patrones.* Los símbolos representativos de los números se identifican sin dificultad aunque aparezcan en circunstancias diversas y bajo numerosas variantes: Son a veces congruentes entre si –como en distintos ejemplares impresos de una misma obra– pero también pueden diferir en forma y tamaño, como ocurre cuando hay distintas fuentes tipográficas. Las cifras escritas a mano, a pesar de estar sujetas a mayores variaciones, se leen con igual soltura. Basta que se conserven ciertos rasgos para que la identificación sea inmediata.
Análogamente, los sonidos articulados que representan a un número pronunciado (vocablo) difieren –según la ocasión y la persona que los profiere– en su intensidad, tono, timbre, etc. Pero basta que mantengan algunas características para que resulten comprensibles.
Que unos cuantos rasgos o características basten para identificar números es un ejemplo del paradigmático *reconocimiento de patrones*, mecanismo neuronal relacionado con la memoria, capaz de establecer asociación entre diferentes percepciones, y que hace posible en particular la lectura y la comunicación verbal. En un contexto muy general se trata de una habilidad –congénita, aprendida, o combinada– presente en todas las especies provistas de sistema nervioso. El reconocimiento de patrones ocurre cuando una vaca encuentra su ternero, una hormiga su camino y un predador a su presa. Hay gran cúmulo de datos sobre el tema pero su completo esclarecimiento sigue siendo un desafío científico.

## 20. Recursión

Es posible creer en el Teorema de Recursión sin necesidad de demostrarlo, pero ya que sus inventores consideraron que era necesaria una prueba, bien podemos ejecutarla con lujo de detalles.

En esta sección estudiaremos la noción de recursión y demostraremos su existencia y unicidad. La naturaleza del procedimiento de recursión obliga a segmentarlo en cautelosos pasos: 0-recursión, $n$-recursión y recursión. Como telón de fondo mantenemos un sistema de números naturales privilegiado, como antes se indicó, por ser el aquí designado mediante $\mathbb{N}$.

La recursión proporciona una manera de construir sucesiones; véase la definición de sucesión en la sección 36. La recursión consiste en asignar a cada natural un elemento de un conjunto de acuerdo al siguiente procedimiento: El valor que corresponde al primer natural, 0, se especifica arbitrariamente. Al sucesor de un natural se asigna el valor que toma una función –previamente convenida– sobre valor que correspondió al natural.

Consideremos un conjunto no vacío $Y$ que llamaremos *rango de recursión* y cuyos elementos son los *(posibles) valores de la recursión*; $y_0 \in Y$ es el *punto inicial* o *valor inicial* de la recursión; y $F : Y \to Y$ es una función denominada *fórmula* de la recursión. Las recursiones a definir dependen de los tres objetos $Y, y_0, F$, que constituyen sus *datos*, y son la 0-recursión, la $n$-recursión y la $\infty$-recursión siendo esta última la recursión propiamente dicha.

Como en la sección 14 denotamos por $[0, n]_{\mathbb{N}}$ al intervalo inicial de extremo $n$. Sean $Y$ un rango de recursión, $y_0$ un punto inicial y $F : Y \to Y$ una fórmula. Una 0-*recursión* (de datos $Y, y_0, F$) es una función $f_0 : [0, 0]_{\mathbb{N}} = \{0\} \to Y$ tal que $f_0(0) = y_0$, esto es, $f_0$ es la función, definida en el primer elemento $0 \in \mathbb{N}$, cuyo valor es $y_0$. El enunciado siguiente es obvio.

**105.-** Existe una 0-recursión y es única.

Denotemos por $\mathcal{R}_0$ el conjunto de las 0-recursiones. Hemos obtenido, a partir de definiciones, que $\mathcal{R}_0$ es no vacío y es unipuntual, $\mathcal{R}_0 = \{f_0\}$.

Si consideramos otro sistema $\mathbb{N}'$ de números naturales –distinto del privilegiado– con función sucesor $s' : \mathbb{N}' \to \mathbb{N}'$, tendremos elementos

$$0',\ 1' = s'(0'),\ \ldots,\ n'^{+} = s'(n'), \ldots$$

y a este sistema corresponde una $0'$-recursión $f'_{0'} : \{0'\} \to Y$ que es la única función perteneciente al conjunto $\mathcal{R}'_{0'} = \{f'_{0'}\}$.

Considere un natural $n > 0$. Una $n$-*recursión* (de datos $Y, y_0, F$) es una función

$$f_n : [0, n]_{\mathbb{N}} = \{0, \ldots, n\} \to Y$$

que satisface la *condición inicial*

$$f_n(0) = y_0$$

y que para todo $m < n$ y verifica la siguiente *condición recursiva*

$$f_n(m^+) = F(f_n(m))$$

Los *valores* de la $n$-recursión son $y_0 = f_n(0), y_1 = f_n(1), \ldots, y_n = f_n(n)$. Usaremos la notación $h \in \mathcal{R}_n$ para indicar que la función $h$ es una $n$-recursión de datos $Y, y_0, F$; como se verá, para datos dados hay una única $n$-recursión, $h = f_n$.

• *Ejemplo de notación críptica.* El conjunto $\mathcal{R}_n$ admite la siguiente formulación jeroglífica:

$$\mathcal{R}_n = \{h \mid h : [0,n]_{\mathbb{N}} \to Y \ni h(0) = y_0 \wedge \forall m \in [0, n-1]_{\mathbb{N}}\ h(m^+) = F(h(m))\} \subseteq Y^{[0,n]_{\mathbb{N}}}$$

**106.-** La restricción de una $n$-recursión es una $n'$-recursión

$$f_n \in \mathcal{R}_n \wedge n' \leq n \quad \Rightarrow \quad f_n \mid [0,n']_{\mathbb{N}} \in \mathcal{R}_{n'}$$

En efecto, considere $0 \leq n' \leq n$ y la restricción

$$f_{n'} = f_n \mid [0,n']_{\mathbb{N}} : [0,n']_{\mathbb{N}} \to Y$$

Entonces $f_{n'}$ tiene el valor inicial correcto, $f_{n'}(0) = f_n(0) = y_0$, y para $0 \leq m < n'$ se tendrá asimismo $m < n$, por consiguiente

$$\begin{aligned} f_{n'}(m^+) &= f_n(m^+) \\ &= F(f_n(m)) \\ &= F(f_{n'}(m)) \end{aligned}$$

siendo estas tres igualdades consecuencia respectivamente de ser $f_{n'}$ restricción de $f_n$; de $f_n \in \mathcal{R}_n$; y, nuevamente, de ser $f_{n'}$ restricción de $f_n$. Se ha probado que $f_{n'}$ es una $n'$-recursión: $f_{n'} \in \mathcal{R}_{n'}$.

Después de $n = 0$ la siguiente recursión ocurre con $n = 0^+ = 1$. Una 1-recursión es una función $f_1 : [0,1]_{\mathbb{N}} = \{0,1\} \to Y$ tal que $f_1(0) = 0$ y $f_1(1) = f_1(0^+) = F(f_1(0)) = F(y_0)$. Luego existe al menos una 1-recursión. En cuanto a la unicidad, sean $f_1, f_1' \in \mathcal{R}_1$, entonces $f_1'(0) = y_0 = f_1(0)$ y $f_1'(1) = f_1'(0^+) = F(f_1'(0)) = F(y_0) = F(f_1(0)) = f_1(1)$, luego $f_1' = f_1$ y la 1-recursión es única o, equivalentemente, $\mathcal{R}_1$ tiene un único elemento:

**107.-** Existe una 1-recursión y es única

$$\mathcal{R}_1 = \{f_1\}$$

**108.-** Si existe una $n$-recursión entonces existe una $n^+$-recursión.

En efecto, suponga $f_n \in \mathcal{R}_n$ y defina $f_{n^+} : [0,n^+]_{\mathbb{N}} = \{0,\ldots,n,n^+\} \to Y$ de modo que su restricción a $\{0,\ldots,n\}$ sea igual a $f_n$, esto es, $f_{n^+} \mid [0,n]_{\mathbb{N}} = f_n$; defina además $f_{n^+}(n^+) = F(f_n(n))$. Entonces $f_{n^+}$ asume el valor inicial correcto, $f_{n^+}(0) = f_n(0) = y_0$.

Para $m < n$ tenemos

$$\begin{array}{rcl} f_{n^+}(m^+) & = & f_n(m^+) \\ & = & F(f_n(m)) \\ & = & F(f_{n^+}(m)) \end{array}$$

siendo las igualdades anteriores deducidas así: La primera porque $f_{n^+}$ y $f_n$ coinciden sobre $[0,n]_{\mathbb{N}}$; la segunda por la propiedad recursiva de $f_n$; la última, una vez más porque $f_{n^+}$ y $f_n$ coinciden sobre $[0,n]_{\mathbb{N}}$.

Para $m = n$ la definición de $f_{n^+}$ nos dice que $f_{n^+}(n^+) = F(f_n(n)) = F(f_{n^+}(n))$. Luego $f_{n^+}$ es una $n^+$-recursión: $f_{n^+} \in \mathcal{R}_{n^+}$.

**109.-** Si la $n$-recursión es única entonces también es única la $n^+$-recursión.

Sean $f'_{n^+}$ una $n^+$-recursión cualquiera. Por **106** la restricción $f'_n = f'_{n^+} \mid [0,n]_{\mathbb{N}}$ es una $n$-recursión y por la hipótesis $f'_n = f_n$ lo cual significa que $f'_{n^+}(m) = f_n(m)$ para todo $m < n$. Con el último valor tenemos

$$\begin{array}{rcl} f'_{n^+}(n^+) & = & F(f'_{n^+}(n)) \\ & = & F(f'_n(n)) \\ & = & F(f_n(n)) \\ & = & f_{n^+}(n^+) \end{array}$$

luego $f'_{n^+} = f_{n^+}$ y $\mathcal{R}_{n^+}$ tiene un único elemento.

**110.-** Para todo $n \geq 0$ existe una $n$-recursión y es única

$$\mathcal{R}_n = \{f_n\}$$

En efecto, sea $A$ el conjunto de los $n \in \mathbb{N}$ tales que $\mathcal{R}_n$ tiene un único elemento. Por **105** sabemos que $0 \in A$, y por **108** y **109** concluimos que $n \in A \quad \Rightarrow \quad n^+ \in A$, luego $A = \mathbb{N}$ y **110** queda probado.

En cuanto a relación entre la $n$-recursión respecto a $\mathbb{N}$ y la existencia de otro(s) sistema(s) $\mathbb{N}'$ de números naturales –equivalente(s) con $\mathbb{N}$, como se verá en el enunciado 140– los mismos razonamientos utilizados para $\mathbb{N}$ aseguran que hay para cada $n' \in \mathbb{N}'$ una única $n'$-recursión $f'_{n'} : [0,n']_{\mathbb{N}'} \to Y$ con su respectivo conjunto unipuntual $\mathcal{R}'_{n'} = \{f'_{n'}\}$.

Una $\infty$-*recursión*, o simplemente *recursión* (de datos $Y, y_0, F$) es una función

$$f : \mathbb{N} \to Y$$

que satisface la condición inicial

$$f(0) = y_0$$

y que cumple para todo $n \geq 0$ la condición recursiva

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

Así, la recursión difiere de la $n$-recursión en que su dominio, en lugar de ser el intervalo $[0, n]_{\mathbb{N}} \subsetneq \mathbb{N}$, es el conjunto infinito $\mathbb{N}$ de todos los números naturales. La notación $f \in \mathcal{R}$ indica que $f$ es una recursión de datos $Y, y_0, F$.

**111.-** Las restricciones de una recursión son $n$-recursiones

$$f \in \mathcal{R} \wedge n \in \mathbb{N} \quad \Rightarrow \quad f \,|\, [0, n]_{\mathbb{N}} \in \mathcal{R}_n$$

En efecto, sea $f_n = f \,|\, [0, n]_{\mathbb{N}}$, entonces $f_n(0) = f(0) = y_0$ y

$$\begin{aligned} f_n(m^+) &= f(m^+) \\ &= F(f(m)) \\ &= F(f_n(m)) \end{aligned}$$

para todo $m < n$, por consiguiente $f_n \in \mathcal{R}_n$.

**112.-** Existe una recursión

$$\mathcal{R} \neq \emptyset$$

Según **110** para todo $n$ existe una única $n$-recursión $f_n \in \mathcal{R}_n$. Defina entonces $f : \mathbb{N} \to Y$ mediante

$$f(n) = f_n(n)$$

Se sigue que $f(0) = f_0(0) = y_0$ y

$$\begin{aligned} f(n^+) &= f_{n^+}(n^+) \\ &= F(f_{n^+}(n)) \\ &= F(f_n(n)) \\ &= F(f(n)) \end{aligned}$$

Las cuatro igualdades se justifican así: La primera por la definición de $f$; la segunda por la fórmula recursiva de $f_{n^+}$; la tercera porque, según vimos en **109**, la restricción de $f_{n^+}$ a $[0, n]_{\mathbb{N}}$ es la única $n$-recursión; la cuarta nuevamente por la definición de $f$. Queda probado que la función $f$ es efectivamente una recursión, por lo tanto $\mathcal{R} \neq \emptyset$. Falta solo la unicidad en el siguiente

**113.-** *Teorema de Recursión:* Existe una única recursión

$$\mathcal{R} = \{f\}$$

Sean $f, f' : \mathbb{N} \to Y$ recursiones, entonces **111** implica que para todo $n > 0$ se tiene que las restricciones $f_n = f \mid [0, n]_{\mathbb{N}}$ y $f'_n = f' \mid [0, n]_{\mathbb{N}}$ son $n$-recursiones, y por la unicidad de estas $f'_n = f_n$, en particular $f'_n(n) = f_n(n)$. Luego $f'(n) = f'_n(n) = f_n(n) = f(n)$ y $f' = f$. Queda así probada la unicidad.

El valor $f(n) \in Y$ es el *$n$-ésimo valor* de la recursión. También podemos referirnos a $f(n)$ como el elemento obtenido mediante *aplicación sucesiva de la fórmula $F$ al valor inicial $y_0$ tantas veces como lo indica $n \in \mathbb{N}$.*

Si $\mathbb{N}'$ es otro sistema de números naturales hay una única recursión $f' : \mathbb{N}' \to Y$ y el correspondiente conjunto unipuntual es $\mathcal{R}' = \{f'\}$. En este caso diremos que la recursión es *con índices en* $\mathbb{N}'$.

• *Generalizaciones de la recursión.* Una primera generalización del teorema de recursión se obtiene reemplazando la fórmula $F : Y \to Y$ por una colección de formulas $F_n : Y \to Y$, $n \geq 0$, y la condición recursiva por $f(n^+) = F_n(f(n))$. Más aún, es posible variar los rangos tomando $F_n : Y_n \to Y_{n+1}$; en este caso la recursión resulta ser una función $f : \mathbb{N} \to Y = \bigcup_{n \geq 0} Y_n$.
Una segunda dirección de generalización consiste en sustituir $\mathbb{N}$ por un conjunto bien ordenado cualquiera $X$. Hay que añadir condiciones especiales cuando $X$ tiene elementos límite; estos son los que, aparte del inicial $0_X$, no están en la imagen de la función sucesor.

• *Recursión y axiomática de Lawvere.* En la definición categórica de Lawvere [10] no aparece inicialmente ningún conjunto $\mathbb{N}$ cuyos elementos sean los naturales, es decir, no aparecen elementos $0, 1, \ldots, n, \ldots$. Su axiomática es esencialmente una 'versión morfismo' de la tesis del teorema de recursión.

## 21. Recursión funcional

Sea $Z$ un conjunto y $g : Z \to Z$ una función. Tomemos como rango de recursión al conjunto de las funciones de $Z$ en $Z$, esto es

$$Y = Z^Z$$

como valor inicial la función identidad

$$y_0 = I_Z \in Y = Z^Z$$

y como fórmula de recursión la composición a derecha con $g$, es decir, $F = g^*$ donde

$$g^*(h) = h \circ g : Z^Z \to Z^Z$$

Nótese que la función $g : Z \to Z$ transforma *elementos* de $Z$ mientras que la función $g^* : Z^Z \to Z^Z$ transforma *funciones* pertenecientes a $Z^Z$.

Para los datos $Z^Z$, $I_Z$, $g^*$ el teorema de recursión **113** garantiza la existencia de $f : \mathbb{N} \to Z^Z$ tal que

$$\begin{array}{rcl} f(0) & = & I_Z \\ f(n^+) & = & g^*(f(n)) = f(n) \circ g \end{array}$$

La *composición iterada* $n$ *veces* o $n$*-ésima iteración de* $g$ es la función $f(n) \in Z^Z$; la denotaremos por $g^n$, o bien mediante $g \circ \overset{n}{\smile\!\!\!\!\!\cdots} \circ g$

$$g^n = g \circ \overset{n}{\smile\!\!\!\!\!\cdots} \circ g = f(n)$$

En el contexto de composiciones iteradas el natural $n$ es el *exponente de iteración*.

Las primeras composiciones iteradas son

$$\begin{array}{l} g^0 = I_Z \\ g^1 = g \\ g^2 = g^1 \circ g = g \circ g \\ \quad \vdots \end{array}$$

En general la definición de composición iterada implica inmediatamente

**114.-** La composición de la $n$-ésima iteración de una función consigo misma es igual a su $n^+$-ésima iteración:

$$g^n \circ g = (g \circ \overset{n}{\smile\!\!\!\!\!\cdots} \circ g) \circ g = g^{n^+}$$

Por otra parte un razonamiento inductivo demuestra

**115.-** La composición de una función con su $n$-ésima iteración es igual su $n^+$-ésima iteración:

$$g \circ g^n = (g \circ \overset{n}{\cdots} \circ g) \circ g = g^{n^+}$$

Basta probar que el conjunto $A$ de los exponentes que cumplen la condición

$$A = \{n \mid g \circ g^n = g^{n^+}\} \subseteq \mathbb{N}$$

es inductivo. Obviamente $0 \in A$. Asumimos como hipótesis de inducción que $n \in A$, o sea $g \circ g^n = g^{n^+}$, y obtenemos

$$\begin{array}{rcl} g \circ g^{n^+} & = & g \circ (g^n \circ g) \\ & = & (g \circ g^n) \circ g \\ & = & g^{n^+} \circ g \\ & = & g^{n^{++}} \end{array}$$

lo cual significa que $n^+ \in A$. Concluimos que $A = \mathbb{N}$ y por lo tanto que el enunciado **115** es valido para todo $n$. Las cuatro igualdades anteriores se justifican así: La primera por definición de $g^{n^+}$; la segunda por la asociatividad de la composición de funciones; la tercera por hipótesis de inducción; y la cuarta por definición de $g^{n^{++}}$.

Juntando los dos enunciados anteriores tenemos

**116.-** La composición de la $n$-ésima iteración de una función consigo misma es igual a su composición con la $n$-ésima iteración, e igual también a su $n^+$-ésima iteración

$$g^n \circ g = g \circ g^n = g^{n^+}$$

Más generalmente,

**117.-** La composición de la iteración $n$-ésima con la $m$-ésima es la iteración $s^m(n)$-ésima

$$g^n \circ g^m = g^{s^m(n)}$$

Para la prueba considere el conjunto

$$A = \{m \mid g^n \circ g^m = g^{s^m(n)}\}$$

Entonces $g^n \circ g^0 = g^n \circ I_X = g^n = g^{s^0(n)}$, luego $0 \in A$. Si suponemos $m \in A$ se tiene

$$\begin{aligned} g^n \circ g^{m^+} &= g^n \circ (g^m \circ g) \\ &= (g^n \circ g^m) \circ g \\ &= g^{s^m(n)} \circ g \\ &= g^{s(s^m(n))} \\ &= g^{s^{m^+}(n)} \end{aligned}$$

siendo estas igualdades justificadas así: La primera por **116**; la segunda por asociatividad de la composición de funciones; la tercera por la hipótesis de inducción; la cuarta por definición de composición iterada; y la última por **118**. Queda probado que $A = \mathbb{N}$.

Para intercambiar $n$ y $m$ en este resultado (ver **120** más abajo) necesitamos como resultado preliminar la proposición **119**. Comenzamos aplicando **116** a la función sucesor, esto es, tomamos $Z = \mathbb{N}$, $Y = \mathbb{N}^{\mathbb{N}}$ y $g = s : \mathbb{N} \to \mathbb{N}$:

**118.-** La composición de la $n$-ésima iteración de la función sucesor consigo misma es igual a su composición con la $n$-ésima iteración, e igual también a su $n^+$-ésima iteración

$$s^n \circ s = s \circ s^n = s^{n^+}$$

Por definición el *$n$-ésimo sucesor* de un natural es el natural obtenido aplicándole la iteración $n$-ésima de la función sucesor, o sea, el $n$-ésimo sucesor de $k$ es $s^n(k)$.

Una consecuencia de **118** es:

**119.-** El natural $n$ es el $n$-ésimo sucesor de 0

$$n = s^n(0)$$

El caso $n = 0$ se sigue de $0 = I_{\mathbb{N}}(0) = s^0(0)$. Definamos $A = \{n \mid n = s^n(0)\}$, entonces si $n \in A$ se tiene que

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

por lo que $n^+ \in A$ y concluimos que $A = \mathbb{N}$. Las igualdades se obtienen como sigue: La primera y la segunda por **118**; la tercera por la hipótesis de inducción; y la última por definición de $n^+$.

Ahora podemos intercambiar $n$ y $m$ en el lado derecho de la igualdad obtenida en **117**:

**120.-** La composición de la iteración $n$-ésima con la $m$-ésima es la iteración $s^n(m)$-ésima

$$g^n \circ g^m = g^{s^n(m)}$$

Sea $A = \{m \mid g^n \circ g^m = g^{s^n(m)}\}$. Demostramos en **119** que el $n$-ésimo iterado de 0 es $n$, esto es, $s^n(0) = n$, por lo tanto

$$g^n \circ g^0 = g^n \circ I_X = g^n = g^{s^n(0)}$$

e inferimos que $0 \in A$. Si asumimos como hipótesis de inducción que $m \in A$ tenemos

$$\begin{aligned} g^n \circ g^{m^+} &= g^n \circ (g^m \circ g) \\ &= (g^n \circ g^m) \circ g \\ &= g^{s^n(m)} \circ g \\ &= g^{s(s^n(m))} \\ &= g^{s^{n^+}(m)} \end{aligned}$$

La primera igualdad es por **114**; la segunda por la asociatividad de la composición de funciones; la tercera por la hipótesis de inducción; la cuarta nuevamente por **114**; y la última por **118**. Esto prueba que $A$ es inductivo y en consecuencia **120** queda demostrado.

Juntando **117** y **120** resulta

**121.-** La composición de la iteración $n$-ésima de una función con la $m$-ésima es igual a la iteración $s^m(n)$-ésima, igual asimismo a la iteración $s^n(m)$-ésima, e igual también a la composición de la iteración $m$-ésima con la $n$-ésima

$$g^n \circ g^m = g^{s^m(n)} = g^{s^n(m)} = g^m \circ g^n$$

En el caso especial de la función sucesor, $g = s$, se tiene

**122.-** La composición de la iteración $n$-ésima de la función sucesor $s : \mathbb{N} \to \mathbb{N}$ con su iteración $m$-ésima es su iteración $s^m(n)$-ésima y es también igual a su iteración $s^n(m)$-ésima

$$s^n \circ s^m = s^{s^m(n)} = s^{s^n(m)} = s^m \circ s^n$$

Los sistemas de números naturales no son únicos pero todo lo expuesto sobre recursión funcional respecto al sistema privilegiado $\mathbb{N}$ se aplica por igual a cualquier otro sistema $\mathbb{N}'$: Para $\mathbb{N}'$, es decir, con los datos $Z^Z, I_Z, g^*$, están definidas las iteraciones $g^{n'} : Z \to Z$ con exponentes de iteración $n' \in \mathbb{N}'$.

Consideremos a continuación el comportamiento bajo iteración de la inyectividad y propiedades similares.

**123.-** Si la función a iterar es inyectiva, suryectiva o biyectiva entonces todas las iteraciones son respectivamente inyectivas, suryectivas o biyectivas

$$\begin{array}{rcl} g \in \mathrm{Iny}(Y,Y) & \Rightarrow & g^m \in \mathrm{Iny}(Y,Y) \\ g \in \mathrm{Sur}(Y,Y) & \Rightarrow & g^m \in \mathrm{Sur}(Y,Y) \\ g \in \mathrm{Biy}(Y,Y) & \Rightarrow & g^m \in \mathrm{Biy}(Y,Y) \end{array}$$

La prueba se efectúa por inducción en $m$ observando, para los respectivos pasos inductivos, que los conjuntos de funciones $\mathrm{Iny}(Y,Y)$, $\mathrm{Sur}(Y,Y)$ y $\mathrm{Biy}(Y,Y)$ son cerrados bajo composición. Con argumentos similares se prueba

**124.-** Si la función a iterar es monótona entonces todas las iteraciones son monótonas

$$g \in \mathrm{Mon}(Y,Y) \;\Rightarrow\; g^m \in \mathrm{Mon}(Y,Y)$$

Sea $X$ un conjunto ordenado. Una función $f : X \to X$ es *eyectiva (estrictamente)*, o es una *eyección*, si $x < f(x)$. La definición se aplica a funciones con dominio y rango iguales entre si. El conjunto de las eyecciones de $X$ se denota $\mathrm{Eye}(X)$

• *Justificación del término.* Se puede usar 'sobrediagonal' o 'incrementante' en lugar de eyección, pero por razones eufónicas es preferible arriesgarse con este neologismo.

**125.-** La composición de eyecciones es una eyección

$$f, g \in \mathrm{Eye}(X) \ \Rightarrow \ g \circ f \in \mathrm{Eye}(X)$$

Razonando como en **123** se tiene

**126.-** Si el exponente de iteración es positivo y la función a iterar es eyectiva entonces la iteración es eyectiva

$$0 < m \quad \wedge \quad g \in \mathrm{Eye}(Y, Y) \qquad \Rightarrow \qquad g^m \in \mathrm{Eye}(Y, Y)$$

El enunciado que sigue es consecuencia obvia de **85**:

**127.-** La función sucesor es eyectiva.

Como caso particular de **32** la función sucesor $s : \mathbb{N} \to \mathbb{N}$ es inyectiva; por **51** es estrictamente monótona; y por el resultado anterior es eyectiva. Obtenemos:

**128.-** Las iteraciones de la función sucesor son inyectivas y monótonas; si el exponente de iteración es positivo entonces las iteraciones son estrictamente monótonas y eyectivas, es decir

$$m > 0 \ \Rightarrow \ s^m \in \mathrm{Iny}(\mathbb{N}, \mathbb{N}) \cap \mathrm{EMon}(\mathbb{N}, \mathbb{N}) \cap \mathrm{Eye}(\mathbb{N}, \mathbb{N})$$

La eyectividad de las iteraciones de la función sucesor posee la siguiente reformulación:

**129.-** Los sucesores iterados de un natural lo siguen. Si el exponente de iteración es positivo entonces lo siguen estrictamente

$$n \leq s^m(n) \qquad 0 < m \ \Rightarrow \ n < s^m(n)$$

## 22. Recursiones elementales

Esta sección presenta dos recursiones que sobresalen por su sencillez. Mantenemos la notación $I_X : X \to X$ para la función identidad del conjunto $X$, $I_X(x) = x$.

Supongamos que el rango de valores de recursión es $\mathbb{N}$, que el valor inicial es 0 y que la fórmula es la función sucesor: $Y = \mathbb{N}$, $y_0 = 0$, $F(n) = n^+ = s(n)$. Se cumple $I_{\mathbb{N}}(0) = 0$ y $I_{\mathbb{N}}(n^+) = n^+ = s(I_{\mathbb{N}}(n))$. Luego la función identidad cumple los requisitos para ser la recursión y, debido a la unicidad, tiene que ser igual a la recursión, esto es

**130.-** La recursión de fórmula la función sucesor y punto inicial 0 es la función identidad, esto es, si $Y = \mathbb{N}$ y $y_0 = 0$ entonces

$$F = s \quad \Rightarrow \quad f = I_{\mathbb{N}}$$

Este resultado dice que la función sucesor es un caso particular de recursión y por lo tanto permite considerar las recursiones como generalizaciones de la función sucesor.

Consideremos ahora una recursión cuya fórmula fija el punto inicial, es decir, $Y$ es cualquier conjunto y el punto inicial $y_0 \in Y$ es un punto fijo de la fórmula

$$F(y_0) = y_0$$

Denotemos por $f$ la correspondiente recursión, de manera que $f(0) = y_0$ y $f(n^+) = F(f(n))$. Sea $A$ el conjunto de los naturales en los cuales $f$ toma el valor $y_0$

$$A = \{n \mid f(n) = y_0\}$$

entonces $0 \in A$ y si $n \in A$ se tiene $f(n^+) = F(f(n)) = F(y_0) = y_0$, luego $A = \mathbb{N}$ y para todo $n \in \mathbb{N}$ se cumple $f(n) = y_0$. Hemos probado

**131.-** Una recursión cuya fórmula fija el punto inicial es la función constantemente igual al punto inicial

$$n \in \mathbb{N} \ \Rightarrow \ f(n) = y_0$$

## 23. Comparación de sistemas de números naturales

Esta sección, dedicada a isomorfismos entre sistemas de números naturales, ha sido deliberadamente colocada antes de definir y estudiar la suma y el producto. Se enfatiza así que los sistemas de números naturales son estructuras ordenadas cuya caracterización no depende de operaciones aritméticas.

Sean $\mathbb{N}$, $\mathbb{N}'$ dos sistemas de números naturales, es decir, ambos son conjuntos no vacíos, bien ordenados, sin último elemento y minimales como conjuntos inductivos. Los respectivos ceros y funciones sucesor son $0 \in \mathbb{N}$, $0' \in \mathbb{N}'$, $s : \mathbb{N} \to \mathbb{N}$ y $s' : \mathbb{N}' \to \mathbb{N}'$. Veremos a continuación la existencia y unicidad de isomorfismos entre $\mathbb{N}$ y $\mathbb{N}'$.

Apliquemos el teorema de recursión, **113**, al caso $Y = \mathbb{N}'$ con valor inicial $0'$ y fórmula la función sucesor $F = s' : \mathbb{N}' \to \mathbb{N}'$.

**132.-** Existe una única recursión $\varphi : \mathbb{N} \to \mathbb{N}'$ tal que $\varphi(0) = 0'$ y $\varphi(n^+) = \varphi(n)^+$.

Basta observar que la recursividad, $y_{n^+} = F(y_n)$, equivale en este caso a la expresión $\varphi(n^+) = \varphi(n)^+$ y admite la siguiente reformulación:

**133.-** La imagen del sucesor es el sucesor de la imagen

$$\varphi(s(n)) = s'(\varphi(n))$$

Más generalmente tenemos

**134.-** La imagen del $m$-ésimo sucesor es el $m$-ésimo sucesor de la imagen

$$\varphi(s^m(n)) = s'^m(\varphi(n))$$

Procedemos por inducción. El resultado es obvio para $m = 0$ y para $m = 1$ es precisamente **133**. Sea $A = \{m \mid \varphi(s^m(n)) = s'^m(\varphi(n))\}$ y supongamos que $m \in A$. Entonces

$$\begin{aligned} \varphi(s^{m^+}(n)) &= \varphi(s(s^m(n))) \\ &= s'(\varphi(s^m(n))) \\ &= s'(s'^m(\varphi(n))) \\ &= s'^{m^+}(\varphi(n)) \end{aligned}$$

lo cual significa que $m^+ \in A$. Esto prueba que $A = \mathbb{N}$ y por lo tanto **134** es cierto para todo $m$. Las igualdades de la demostración se infieren de la manera siguiente. La primera por la definición de iteración funcional; la segunda por **133**; la tercera por la hipótesis de inducción; y la última por **122**.

**135.-** La recursión $\varphi : \mathbb{N} \to \mathbb{N}'$ es suryectiva

$$\varphi(\mathbb{N}) = \mathbb{N}'$$

Sabemos que $0' = \varphi(0) \in \varphi(\mathbb{N})$. Si $n' = \varphi(n) \in \varphi(\mathbb{N})$ entonces $n'^{+} = s'(n') = s'(\varphi(n)) = \varphi(s(n)) \in \varphi(\mathbb{N})$. Luego $\varphi(\mathbb{N})$ es inductivo y por el principio de inducción aplicado al sistema de naturales $\mathbb{N}'$ concluimos que $\varphi(\mathbb{N}) = \mathbb{N}'$.

Para la prueba del siguiente resultado haremos uso de **19**.

**136.-** La recursión $\varphi : \mathbb{N} \to \mathbb{N}'$ es inyectiva

$$n' \in \mathbb{N}' \;\Rightarrow\; |\varphi^{-1}(n')| = 1$$

Sea $A' = \{n' \,|\, |\varphi^{-1}(n')| = 1\}$. En primer lugar, $\varphi(n) = 0'$ implica $n = 0$. Porque si fuese $n > 0$ entonces $n = s(a(n))$ y de allí

$$0' = \varphi(n) = \varphi(s(a(n))) = s(\varphi(a(n)))$$

lo cual es imposible porque $0'$ no es un sucesor; luego $0' \in A'$. Supongamos $m' \in A'$ y sean $k, j \in \mathbb{N}$ tales que $m'^{+} = \varphi(k) = \varphi(j)$. Puesto que $m'^{+} > 0'$ necesariamente $k > 0$ y $j > 0$. Luego $k = s(a(k))$ y $j = s(a(j))$, de donde

$$m'^{+} = s(m') = \varphi(s(a(k))) = \varphi(s(a(j)))$$

Pero **133** implica entonces que

$$s(m') = s(\varphi(a(k))) = s(\varphi(a(j)))$$

y la inyectividad de $s$ permite deducir que $m' = \varphi(a(k)) = \varphi(a(j))$. Por la hipótesis de inducción $a(k) = a(j)$, luego $k = s(a(k)) = s(a(j)) = j$ y por lo tanto $|\varphi^{-1}(m'^{+})| = 1$ de donde $m'^{+} \in A'$. La inyectividad de $\varphi$ queda probada.

Concluimos que $\varphi$ es biyectiva y por lo tanto

**137.-** La recursión $\varphi : \mathbb{N} \to \mathbb{N}'$ conserva estrictamente el orden

$$n < m \;\Rightarrow\; \varphi(n) < \varphi(m)$$

Falta la doble monotonía para completar la prueba del siguiente resultado fundamental.

**138.-** La recursión $\varphi : \mathbb{N} \to \mathbb{N}'$ es un isomorfismo de conjuntos ordenados.

Supongamos que $n, m \in \mathbb{N}$ son tales que $\varphi(n) \leq \varphi(m)$. Afirmamos que necesariamente $n \leq m$. Porque la otra posibilidad es, de acuerdo a la tricotomía, que $m < n$; pero en tal caso **137** implicaría que $\varphi(m) < \varphi(n)$, contra la hipótesis. Queda probada la doble monotonía y por consiguiente $\varphi$ es un isomorfismo. Veamos la unicidad:

**139.-** Hay a lo sumo un isomorfismo del conjunto ordenado $\mathbb{N}$ en el conjunto ordenado $\mathbb{N}'$.

Sean $\varphi, \phi : \mathbb{N} \to \mathbb{N}'$ isomorfismos y defina $A = \{n \mid \varphi(n) = \phi(n)\}$. Vimos en **60** que los isomorfismos respetan el primer elemento, esto es, $\varphi(0) = 0' = \phi(0)$, lo cual significa que $0 \in A$. Supongamos $n \in A$, entonces

$$\begin{aligned} \varphi(n^+) &= \varphi(n)^+ \\ &= \phi(n)^+ \\ &= \phi(n^+) \end{aligned}$$

siendo cierta la primera igualdad por **65**; la segunda por la hipótesis de inducción; y la última nuevamente por **65**. Por lo tanto $A$ es inductivo, $A = \mathbb{N}$, y $\varphi = \phi$. Queda demostrada la unicidad. Esto completa la prueba del siguiente resultado fundamental:

**140.-** Dados dos sistemas $\mathbb{N}, \mathbb{N}'$ de números naturales hay un único isomorfismo $\varphi : \mathbb{N} \to \mathbb{N}'$.

Este único isomorfismo es el *isomorfismo canónico* entre $\mathbb{N}$ y $\mathbb{N}'$. Puesto que así fue construido en **132**, $\varphi$ es la única recursión con rango $Y = \mathbb{N}'$, valor inicial $y_0 = 0' \in \mathbb{N}'$ y fórmula $F = s'$. Por consiguiente:

**141.-** El isomorfismo canónico entre dos sistemas de números naturales es la única función que conserva elementos iniciales y para la cual la imagen del sucesor es el sucesor de la imagen. Es decir, $\varphi : \mathbb{N} \to \mathbb{N}'$ es el isomorfismo canónico si y solo si

$$\varphi(0) = 0' \qquad \wedge \qquad \varphi(s(n)) = s'(\varphi(n))$$

Sean $Y, y_0, F$ datos de una recursión. Dados dos sistemas de números naturales existen correspondientes recursiones

$$f : \mathbb{N} \to Y \qquad f' : \mathbb{N}' \to Y$$

con índices de recursión $n \in \mathbb{N}$, $n' \in \mathbb{N}'$, ambas con los mismos datos:

$$f(0) = y_0 \quad f(n^+) = F(f(n)) \qquad f'(0') = y_0 \quad f(n'^+) = F(f'(n'))$$

Estas recursiones se relacionan mediante el isomorfismo canónico $\varphi : \mathbb{N} \to \mathbb{N}'$:

**142.-** El $n$-ésimo valor de la recursión indiciada por $\mathbb{N}$ es igual al $\varphi(n)$-ésimo valor de la recursión indiciada por $\mathbb{N}'$

$$y_n = y_{\varphi(n)}$$

Para la prueba sea $A = \{n \,|\, y_n = y_{\varphi(n)}\}$. Es obvio que $0 \in A$ y si $n \in A$ se tiene

$$\begin{aligned} y_{n^+} &= F(y_n) \\ &= F(y_{\varphi(n)}) \\ &= y_{\varphi(n)^+} \\ &= y_{\varphi(n^+)} \end{aligned}$$

Las igualdades se justifican así: La primera por la recursividad de $F$ respecto al primer sistema de naturales; la segunda por la hipótesis de inducción; la tercera por la recursividad de $F$ respecto al segundo sistema de naturales; y la última por **141**. Luego $A$ es inductivo lo cual prueba la proposición.

Podemos aplicar el enunciado a composiciones iteradas. Cada uno de los sistemas de números naturales proporciona exponentes de iteración

$$g^n : Y \to Y,\ n \in \mathbb{N} \qquad g^{\varphi(n)} : Y \to Y,\ \varphi(n) \in \mathbb{N}'$$

**143.-** La $n$-ésima iteración es igual a la $\varphi(n)$-ésima iteración

$$g^n = g^{\varphi(n)}$$

En particular para la función sucesor $g = s : \mathbb{N} \to \mathbb{N}$ se verifica

**144.-** La iteración $n$-ésima de la función sucesor $s$ es igual a su iteración $\varphi(n)$-ésima. Ambas son iguales también a la iteración $\varphi(n)$-ésima de la función sucesor $s'$ y a su iteración $n$-ésima

$$s^n = s^{\varphi(n)'} = s'^{\varphi(n)'} = s'^n$$

De otra parte tenemos

**145.-** La composición del isomorfismo canónico con la iteración $n$-ésima de la función sucesor $s : \mathbb{N} \to \mathbb{N}$ es igual a la composición de la iteración $n$-ésima de la función sucesor $s' : \mathbb{N}' \to \mathbb{N}'$ con el isomorfismo canónico

$$\varphi \circ s^n = s'^n \circ \varphi$$

Sea $A = \{n \mid \varphi \circ s^n = s'^n \circ \varphi\}$. Es inmediato que $0 \in A$. Suponga que $n \in A$, entonces

$$\begin{aligned} \varphi \circ s^{n^+} &= \varphi \circ (s \circ s^n) \\ &= (\varphi \circ s) \circ s^n \\ &= (s' \circ \varphi) \circ s^n \\ &= s' \circ (\varphi \circ s^n) \\ &= s' \circ (s'^n \circ \varphi) \\ &= (s' \circ s'^n) \circ \varphi \\ &= s'^{n^+} \circ \varphi \end{aligned}$$

Por lo tanto $n^+ \in A$ lo cual implica que $A = \mathbb{N}$.

Combinando **144** y **145** es posible intercambiar $n$ y $n' = \varphi(n)$ para obtener diversas fórmulas como por ejemplo

$$\varphi \circ s^{n^+} = s'^{\varphi(n)^+} \circ \varphi$$

## 24. Orden y sucesores

La relación de orden en un sistema $\mathbb{N}$ de números naturales se puede expresar utilizando los sucesores iterados.

Sabemos por **90** que $\mathbb{N}' = S(n) \subseteq \mathbb{N}$ es un sistema de números naturales con primer elemento $0' = n^+$. Según **119** y **144** para cualquier sistema $\mathbb{N}'$ de números naturales las iteraciones de la función sucesor evaluadas en $0'$ proporcionan un isomorfismo. Tomando $\mathbb{N}' = S(n)$ resulta entonces que es biyectiva la función

$$\varphi : \mathbb{N} \to \mathbb{N}' = S(n)$$

definida por

$$\varphi(0) = 0' \qquad \varphi(k) = s^k(n^+)$$

y todo seguidor estricto de $n$, esto es, todo $m \in S(n)$, se expresa como $m = s^k(n^+)$ para un único natural $k$. Dado que $s^{k^+}(n) > 0$, se tiene

**146.-** Un natural sigue estrictamente a otro si y solo si es su sucesor iterado un número positivo de veces; el exponente de iteración es único

$$n < m \Leftrightarrow \exists !\, k > 0 \ni m = s^k(n)$$

Hay un enunciado similar cuando el orden no es estricto

**147.-** Un natural sigue a otro si y solo si es su sucesor iterado; el exponente de iteración es único

$$n \leq m \Leftrightarrow \exists !\, k \in \mathbb{N} \ni m = s^k(n)$$

## 25. Suma

La suma de dos naturales se define como el resultado de aplicar al primero la función sucesor iterada el número de veces que indica el segundo; en particular, sumar la unidad equivale a aplicar la función sucesor (iterada una vez). La suma tiene elemento neutro y es asociativa y conmutativa. A continuación los pormenores.

Definimos la *suma* de los números naturales $n, m \in \mathbb{N}$, denotada $n+m$, como

$$n + m = s^m(n) \in \mathbb{N}$$

Los naturales dados son los *sumandos*; $n$ es el *primer sumando* y $m$ es el *segundo sumando*. También diremos que la suma $n+m$ consiste en *incrementar* $n$ *en* $m$.

El primer sumando, $n$, tiene en la definición un rol distinto al segundo sumando, $m$. Ni siquiera es obvio que la suma así definida sea independiente del orden de los sumandos, por lo que se requerirá prueba. Comenzamos con la siguiente consecuencia de las definiciones:

**148.-** La suma de un natural y de la unidad es igual al sucesor

$$n + 1 = n^+$$

En efecto

$$\begin{aligned} n + 1 &= s^1(n) \\ &= s(n) \\ &= n^+ \end{aligned}$$

**149.-** *Existencia de elemento neutro para la suma.* El cero es elemento neutro para la suma, es decir, la suma de un natural y cero es igual al natural e igual a la suma de cero y el natural

$$n + 0 = n = 0 + n$$

La prueba consiste en las siguientes igualdades

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

justificadas así: La primera por definición de suma; la segunda porque $s^0 = I_{\mathbb{N}}$; la tercera por **119**; y la última, como la primera, por definición de suma.

**150.-** *Asociatividad de la suma* La suma es asociativa, o sea, si de tres naturales se suman los dos primeros y al resultado se suma el tercero, se obtiene lo mismo que sumando al primero el resultado de sumar el segundo y el tercero

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

Esto es consecuencia de

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

La primera y segunda igualdades se deducen de la definición de suma; la tercera de la definición de composición de funciones; la cuarta de **122**; la quinta y la sexta de la definición de suma.

**151.-** *Conmutatividad de la suma.* El orden de los sumandos no altera la suma

$$n + m = m + n$$

La demostración se obtiene de las igualdades

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

La primera y última son consecuencias de la definición de suma y la segunda de **122**.

Veamos que el isomorfismo canónico conserva las sumas. Sean $\mathbb{N}$ y $\mathbb{N}'$ sistemas de números naturales, $\varphi : \mathbb{N} \to \mathbb{N}'$ el isomorfismo canónico dado en **139**:

**152.-** El isomorfismo canónico es aditivo

$$\varphi(n+m) = \varphi(n) + \varphi(m)$$

En efecto

$$\begin{array}{rcl} \varphi(n+m) & = & \varphi(s^m(n)) \\ & = & s'^m(\varphi(n)) \\ & = & s'^{\varphi(m)}(\varphi(n)) \\ & = & \varphi(n) + \varphi(m) \end{array}$$

siendo cierta la primera igualdad por definición de suma en $\mathbb{N}$; la segunda por **134**; la tercera por **144**; y la última por definición de suma en $\mathbb{N}'$.

## 26. Suma y relación de orden

La operación de suma y la relación de orden originan propiedades –muy sencillas– que son esenciales en los sistemas de números naturales.

**153.-** Todo sumando precede a la suma

$$n \in \mathbb{N} \;\Rightarrow\; n \leq n+k$$

Obvio cuando $k = 0$. Si $0 < k$ según **129** $s^k$ es eyectiva, luego $n < s^k(n) = n + k$. Hemos probado **153** y también lo siguiente:

**154.-** Un sumando precede estrictamente a la suma si y solo si el otro sumando es positivo

$$n < n + k \Leftrightarrow 0 < k$$

En particular

**155.-** La suma de un natural y la unidad sigue estrictamente al natural

$$n < n + 1$$

lo cual es también una repetición de **85**.

Deducimos asimismo la

**156.-** *Positividad de la suma.* La suma de naturales positivos es positiva

$$0 < n \wedge 0 < m \qquad \Rightarrow \qquad 0 < n + m$$

Por otra parte, sumar un natural a ambos miembros de una desigualdad no cambia el sentido de la desigualdad:

**157.-** Si un natural precede a otro y a ambos se suma el mismo natural la desigualdad se mantiene

$$n \leq m \;\Rightarrow\; n + k \leq m + k$$

En efecto, vimos en **128** que $s^k$ es monótona, por lo tanto $n + k = s^k(n) \leq s^k(m) = m + k$; y cuando el exponente de iteración $k$ es positivo la función sucesor es estrictamente monótona, luego

**158.-** Si un natural es estrictamente menor que otro y a ambos se suma un mismo natural la desigualdad estricta se mantiene

$$n < m \;\Rightarrow\; n + k < m + k$$

**159.-** Un natural sigue a otro si y solo si es su suma con un tercer natural

$$n \leq m \Leftrightarrow \exists\, k \in \mathbb{N} \ni m = n + k$$

**160.-** Un natural sigue estrictamente a otro si y solo si es su suma con un natural positivo

$$n < m \Leftrightarrow \exists\, k > 0 \ni m = n + k$$

## 27. Leyes de cancelación para la suma

La siguiente propiedad, en conjunción con **200**, es la precursora de todos los métodos de resolución de ecuaciones.

**161.-** *Ley de cancelación de sumandos en igualdades:* Si dos sumas iguales entre si tienen segundos sumandos iguales entonces son iguales los primeros sumandos

$$n + m = k + m \;\Rightarrow\; n = k$$

La hipótesis equivale a $s^m(n) = s^m(k)$ y por ser $s^m$ inyectiva se obtiene $n = k$.

Sumandos iguales, en desigualdades, se pueden cancelar:

**162.-** *Ley de cancelación de sumandos en desigualdades:* Si una suma de dos naturales precede a otra y si los primeros sumandos son iguales entonces el segundo sumando de la primera precede al segundo sumando de la segunda:

$$n + m \leq n + k \;\Rightarrow\; m \leq k$$

La hipótesis es $n + m \leq n + k$. Si se cumpliera $k < m$ entonces **157** implica $n + k < n + m$, que contradice la hipótesis. Luego, por tricotomía, $n + m \leq n + k \;\Rightarrow\; m \leq k$.

Además para las desigualdades estrictas tenemos:

**163.-** *Ley de cancelación de sumandos en desigualdades estrictas:* Si una suma de dos naturales precede estrictamente a otra y si los primeros sumandos son iguales entonces el segundo sumando de la primera precede estrictamente al segundo sumando de la segunda:

$$n + m < n + k \;\Rightarrow\; m < k$$

El razonamiento es como en la proposición anterior, pero invocando **158** en lugar de **157**.

## 28. Suma de funciones

Sea $W$ un conjunto, $\mathbb{N}^W$ el conjunto de las funciones definidas en $W$ a valores naturales

$$\mathbb{N}^W = \{f \mid f : W \to \mathbb{N}\}$$

y sea $c_0 \in \mathbb{N}^W$ la función nula, esto es, la función constante igual a 0. Dadas dos funciones $f, g \in \mathbb{N}^W$ su *suma funcional* o simplemente *suma*, denotada $f + g$, es la función obtenida sumándolas punto a punto sobre los elementos del dominio

$$(f + g)(w) = f(w) + g(w)$$

Considere una función a valores en $W$

$$e : W' \to W$$

de manera que las funciones compuestas $f \circ e$ y $g \circ e$ están bien definidas. Evaluando en los puntos de $W'$ se obtiene

**164.-** La suma de funciones compuesta con otra la es igual a la suma de las composiciones

$$(f+g)\circ e = f\circ e + g\circ e$$

De manera parecida, basta evaluar en puntos de $W$ para probar:

**165.-** La suma de funciones es asociativa, conmutativa y tiene como elemento neutro la función idénticamente nula $c_0$

$$\begin{array}{rcl} (f+g)+h &=& f+(g+h) \\ f+g &=& g+f \\ f+c_0 &=& f \end{array}$$

**166.-** La suma de funciones monótonas, estrictamente monótonas o eyectivas es respectivamente monótona, estrictamente monótona o eyectiva

$$\begin{array}{lcl} f,g\in \mathrm{Mon}(\mathbb{N}) & \Rightarrow & f+g\in \mathrm{Mon}(\mathbb{N}) \\ f,g\in \mathrm{EMon}(\mathbb{N}) & \Rightarrow & f+g\in \mathrm{EMon}(\mathbb{N}) \\ f,g\in \mathrm{Eye}(\mathbb{N}) & \Rightarrow & f+g\in \mathrm{Eye}(\mathbb{N}) \end{array}$$

Por otra parte, la suma de funciones es compatible con isomorfismos canónicos; sea $\varphi:\mathbb{N}\to\mathbb{N}'$ un tal isomorfismo:

**167.-** La composición del isomorfismo canónico con una suma de funciones es igual a la suma de las composiciones

$$\varphi\circ(f+g) = \varphi\circ f + \varphi\circ g$$

Porque si $w\in W$ entonces

$$\begin{array}{rcl} \varphi\circ(f+g)(w) &=& \varphi((f+g)(w)) \\ &=& \varphi(f(w)+g(w)) \\ &=& \varphi(f(w))+\varphi(g(w)) \\ &=& \varphi\circ f(w)+\varphi\circ g(w) \end{array}$$

La tercera igualdad resulta de **152** y las otras son consecuencias inmediatas de las respectivas definiciones.

## 29. Funciones aditivas

Definida la suma de naturales podemos introducir el concepto de función aditiva con las cuales se simplificará posteriormente la demostración de propiedades básicas del producto.

Una función $f : \mathbb{N} \to \mathbb{N}$ es *aditiva* si para $n, m \in \mathbb{N}$ cualesquiera cumple

$$f(n+m) = f(n) + f(m)$$

Denotamos por $\mathrm{Adi}(\mathbb{N})$ el conjunto formado por estas funciones

$$\mathrm{Adi}(\mathbb{N}) = \{f \mid f : \mathbb{N} \to \mathbb{N} \wedge f(n+m) = f(n) + f(m)\}$$

• *Forma de las funciones aditivas.* Todas las funciones aditivas en $\mathbb{N}$ son producto por un número natural, esto es, se expresan como $f(n) = c\,n$, siendo $c = f(1)$. Véase **187**.

Es inmediato que

**168.-** La función nula $f = c_0$ y la función identidad $f = I_{\mathbb{N}}$ son aditivas

$$c_0, I_{\mathbb{N}} \in \mathrm{Adi}(\mathbb{N})$$

**169.-** La suma de funciones aditivas es aditiva

$$f, g \in \mathrm{Adi}(\mathbb{N}) \;\Rightarrow\; f + g \in \mathrm{Adi}(\mathbb{N})$$

**170.-** Toda función aditiva toma valor 0 en $n = 0$

$$f \in \mathrm{Adi}(\mathbb{N}) \quad \Rightarrow \quad f(0) = 0$$

Las igualdades $f(n) + f(0) = f(n+0) = f(n) = f(n) + 0$ y **161** implican que necesariamente $f(0) = 0$.

El siguiente resultado es obvio:

**171.-** Las funciones aditivas transforman el sucesor de un natural en la imagen del natural sumada con la imagen de la unidad

$$f(n+1) = f(n) + f(1)$$

Como consecuencia tenemos:

**172.-** Si dos funciones aditivas son iguales en $n = 1$ entonces son iguales, es decir, si $f, g \in \text{Adi}(\mathbb{N})$

$$f(1) = g(1) \quad \Rightarrow \quad f = g$$

Sea $A = \{n \mid f(n) = g(n)\}$. Por **170**, $0 \in A$; y por hipótesis $1 \in A$. Supongamos $n \in A$, entonces $f(n^+) = f(n) + f(1) = g(n) + g(1) = g(n^+)$ y vemos que $n^+ \in A$. Luego $A = \mathbb{N}$ y **172** queda demostrado.

**173.-** La composición de funciones aditivas es aditiva

$$f, g \in \text{Adi}(\mathbb{N}) \;\Rightarrow\; g \circ f \in \text{Adi}(\mathbb{N})$$

lo cual se deduce de las siguientes igualdades

$$\begin{array}{rcl} g \circ f(n+m) & = & g(f(n+m)) \\ & = & g(f(n) + f(m)) \\ & = & g(f(n)) + g(f(m)) \\ & = & g \circ f(n) + g \circ f(m) \end{array}$$

siendo cierta la primera por definición de composición de funciones; la segunda por la aditividad de $f$; la tercera por la aditividad de $g$; y la cuarta por definición de composición.

## 30. Suma funcional iterada

Sea $h \in \mathbb{N}^W$. La *traslación por* $h$ es la corespondencia $T_h : \mathbb{N}^W \to \mathbb{N}^W$ dada por

$$T_h(f) = f + h$$

En este contexto $f + h$ es la *trasladada de* $f$ *por* $h$ y $h$ es el *módulo de traslación*. En el siguiente enunciado todas las composiciones son con el isomorfismo canónico:

**174.-** La compuesta de la trasladada es igual a la trasladada de la compuesta, con módulo compuesto

$$\varphi \circ T_h(f) = T_{\varphi \circ h} \circ \varphi(f)$$

Basta observar que

$$\begin{aligned}\varphi \circ T_h(f) &= \varphi \circ (f+h)\\ &= \varphi \circ f + \varphi \circ h\\ &= T_{\varphi \circ h}(\varphi \circ f)\\ &= (T_{\varphi \circ h} \circ \varphi)(f)\end{aligned}$$

La segunda igualdad deriva de **167** y las restantes son consecuencias de definiciones.

Como caso particular de composición iterada tomemos rango de valores igual al conjunto $Z$ de funciones de $W$ en $\mathbb{N}$, $Z = \mathbb{N}^W$, punto inicial la función constante igual a cero, $y_0 = c_0 \in Z$ y fórmula $g : Z \to Z$ igual a la traslación de módulo $h$, es decir

$$g = T_h : Z \to Z$$

Para $m \in \mathbb{N}$ queda entonces definida la *traslación por $h$ iterada $m$ veces* como la composición iterada dada por la siguiente fórmula:

$$g^m = T_h^m = T_h \circ \overset{m}{\overbrace{\cdots}} \circ T_h$$

Su valor en $f \in Z = \mathbb{N}^W$ se denotará mediante

$$T_h^m(f) = f + (h + \overset{m}{\overbrace{\cdots}} + h)$$

y es la *trasladada de $f$ de módulo $h$ iterada $m$ veces*. Para los primeros valores de los exponentes de iteración las trasladadas iteradas toman en $f \in \mathbb{N}^W$ los valores siguientes

$$\begin{aligned}&T_h^0(f) = f + h + \overset{0}{\overbrace{\cdots}} + h = I_Z(f) = f\\ &T_h^1(f) = f + h + \overset{1}{\overbrace{\cdots}} + h = T_h(f) = f + h\\ &T_h^2(f) = f + h + \overset{2}{\overbrace{\cdots}} + h = T_h(T_h^1(f)) = T_h(f+h) = (f+h)+h\\ &\qquad\qquad\vdots\end{aligned}$$

y en general

$$T_h^{m^+}(f) = f + (h + \overset{m^+}{\overbrace{\cdots}} + h) = (f + (h + \overset{m}{\overbrace{\cdots}} + h)) + h$$

Podemos generalizar **174** al caso iterado:

**175.-** La compuesta de la trasladada iterada $m$ veces es igual a la trasladada iterada $m$ veces de la compuesta, con módulo compuesto

$$\varphi \circ T_h^m(f) = T_{\varphi \circ h}^m(\varphi \circ f)$$

Sea $A = \{m \,|\, \varphi \circ T_h^m(f) = T_{\varphi \circ h}^m(\varphi \circ f)\}$. Es inmediato que $0 \in A$. Suponga que $m \in A$. Las siguientes igualdades proporcionan el paso inductivo:

$$\begin{aligned}
\varphi \circ T_h^{m^+}(f) &= \varphi \circ (T_h^m \circ T_h(f)) \\
&= (\varphi \circ T_h^m) \circ T_h(f) \\
&= T_{\varphi \circ h}^m \circ (\varphi \circ T_h(f)) \\
&= T_{\varphi \circ h}^m \circ (T_{\varphi \circ h}(\varphi \circ f)) \\
&= (T_{\varphi \circ h}^m \circ T_{\varphi \circ h})(\varphi \circ f) \\
&= T_{\varphi \circ h}^{m^+}(\varphi \circ f)
\end{aligned}$$

La primera y la última se deducen de la definición de composición iterada; la segunda y la penúltima de la asociatividad de composición de funciones; la tercera es la hipótesis inductiva; la cuarta es **174**.

La *suma iterada $m$ veces* de la función $h$, denotada mediante $h + \overset{m}{\cdots} + h$ y también –notación más breve– mediante $[m \cdot h]$, es el valor obtenido en $Z = \mathbb{N}^W$ al aplicar la traslación iterada $T_h^m$ al valor inicial $f = c_0$, es decir,

$$h + \overset{m}{\cdots} + h = [m \cdot h] = T_h^m(c_0)$$

Dado que $c_0$ es elemento neutro la notación para las sumas iteradas es consistente con la introducida antes para las traslaciones iteradas.

Las primeras sumas iteradas son

$$\begin{aligned}
&h + \overset{0}{\cdots} + h = [0 \cdot h] = 0h = T_h^0(c_0) = I_Z(c_0) = c_0 \\
&h + \overset{1}{\cdots} + h = [1 \cdot h] = 1h = T_h^1(c_0) = T_h(c_0) = c_0 + h = h \\
&h + \overset{2}{\cdots} + h = [2 \cdot h] = 2h = T_h^2(c_0) = T_h(T_h(c_0)) = T_h(h) = h + h \\
&\qquad\qquad\qquad\qquad \vdots
\end{aligned}$$

En el contexto de las sumas iteradas $[m \cdot h]$ el natural $m$ se denomina *coeficiente de iteración*, es decir, el coeficiente de iteración de $[m \cdot h]$ es igual al exponente de iteración de $T_h^m$.

Las definiciones implican inmediatamente:

**176.-** La suma iterada $m^+$ veces de la función $h$ es igual a la suma iterada $m$ veces sumada con $h$,

$$h + \overset{m^+}{\overbrace{\cdots}} + h = (h + \overset{m}{\overbrace{\cdots}} + h) + h$$

Este enunciado se expresa expresa asimismo mediante la relación

$$T_h^{m^+}(c_0) = T_h^m(c_0) + h$$

y también como

$$[m^+ \cdot h] = [m \cdot h] + h$$

Sea $g : W' \to W$ de manera que está definida la compuesta $h \circ g : W' \to N'$, entonces

**177.-** La suma iterada compuesta con $g$ es igual a la suma iterada de la compuesta $h \circ g$

$$[m \cdot h] \circ g = [m \cdot h \circ g]$$

La igualdad es cierta para $m = 0$. Suponga que vale para $m$. Para $m^+$ se cumple

$$\begin{aligned} [m^+ \cdot h] \circ g &= ([m \cdot h] + h) \circ g \\ &= [m \cdot h] \circ g + h \circ g \\ &= [m \cdot h \circ g] + h \circ g \\ &= [m^+ \cdot h \circ g] \end{aligned}$$

Estas igualdades tienen las justificaciones siguientes. La primera por **176**; la segunda por **164**; la tercera por la hipótesis inductiva; y la última nuevamente por **176**.

**178.-** Las sumas iteradas de funciones monótonas o aditivas son respectivamente monótonas o aditivas

$$\begin{aligned} h \in \mathrm{Mon}(\mathbb{N}) &\quad\Rightarrow\quad [m \cdot h] \in \mathrm{Mon}(\mathbb{N}) \\ h \in \mathrm{Adi}(\mathbb{N}) &\quad\Rightarrow\quad [m \cdot h] \in \mathrm{Adi}(\mathbb{N}) \end{aligned}$$

Supongamos que $h$ es monótona y sea $A = \{m \,|\, [m{\cdot}h] \in \mathrm{Mon}(\mathbb{N})\}$. Puesto que $[0 \cdot h] = c_0 \in \mathrm{Mon}(\mathbb{N})$ se tiene $0 \in A$. Si $m \in A$ entonces $[m^+ \cdot h] = [m \cdot h] + h$ y por la primera implicación de **166** se concluye que $m^+ \in A$; luego $A = \mathbb{N}$. Con funciones aditivas se toma $A = \{m \,|\, [m \cdot h] \in \mathrm{Adi}(\mathbb{N})$ y se utiliza **169**.

Por otra parte:

**179.-** Las sumas iteradas a coeficiente de iteración positivo de funciones estrictamente monótonas o eyectivas son respectivamente estrictamente monótonas o eyectivas, es decir, si $m > 0$ entonces

$$\begin{array}{lcl} h \in \mathrm{EMon}(\mathbb{N}) & \Rightarrow & [m \cdot h] \in \mathrm{EMon}(\mathbb{N}) \\ h \in \mathrm{Eye}(\mathbb{N}) & \Rightarrow & [m \cdot h] \in \mathrm{Eye}(\mathbb{N}) \end{array}$$

Supongamos que $h$ es estrictamente monótona y sea $A = \{m \,|\, [m \cdot h] \in \mathrm{EMon}(\mathbb{N})\}$; es inmediato que $1 \in A$. Si $m \in A$ entonces la segunda implicación de **166** permite deducir que $m^+ \in A$ y concluimos que $A = \mathbb{N}^+$. Si $h$ es eyectiva se razona de manera similar pero invocando la tercera implicación de **166**.

Sea una vez más $\varphi : \mathbb{N} \to \mathbb{N}'$ un isomorfismo canónico entre sistemas de números naturales, $f : \mathbb{N} \to \mathbb{N}$ una función aditiva. Se cumple entonces:

**180.-** La composición del isomorfismo canónico con una función aditiva es aditiva

$$f \in \mathrm{Adi}(\mathbb{N}) \;\Rightarrow\; \varphi \circ f \in \mathrm{Adi}(\mathbb{N}')$$

Esto resulta de

$$\begin{array}{rcl} (\varphi \circ f)(n+m) & = & \varphi(f(n+m)) \\ & = & \varphi(f(n) + f(m)) \\ & = & \varphi(f(n)) + \varphi(f(m)) \\ & = & (\varphi \circ f)(n) + (\varphi \circ f)(m) \end{array}$$

La primera igualdad resulta de la definición de composición de funciones; la segunda de la aditividad de $f$; la tercera de la aditividad del isomorfismo canónico, **152**; la última de la definición de composición de funciones.

Sea $h : W \to \mathbb{N}$. La composición del isomorfismo canónico con la suma iterada $[m \cdot h]$ es la función

$$\varphi \circ [m \cdot h] : \mathbb{N} \to \mathbb{N}'$$

Para $m' \in \mathbb{N}'$ las sumas iteradas $[m' \cdot I'] : \mathbb{N}' \to \mathbb{N}'$ están bien definidas y componiéndolas con el isomorfismo canónico obtenemos la función

$$[m' \cdot I'] \circ \varphi : \mathbb{N} \to \mathbb{N}'$$

que es igual a la anterior:

**181.-** La composición del isomorfismo canónico con la suma iterada $m$ veces de $h$ es igual a la suma iterada $\varphi(m)$ veces de $\varphi \circ h$

$$\varphi \circ [m \cdot h] = [\varphi(m) \cdot \varphi \circ h]$$

Esto puede reformularse como

$$\varphi \circ T_h^m(c_0) = T_{\varphi \circ h}^{\varphi(m)}(c_0')$$

siendo $c_0' = \varphi \circ c_0 : W \to \mathbb{N}'$ la función idénticamente nula; en virtud de **143** esta última igualdad equivale a

$$\varphi \circ T_h^m(c_0) = T_{\varphi \circ h}^m(c_0')$$

que se obtiene invocando **175** con $f = c_0$.

## 31. Sumas iteradas de la identidad

La función $h$ considerada en la sección anterior puede tomarse igual a la identidad, $h = I = I_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$. Considere las sumas iteradas $I + \overset{m}{\overbrace{\cdots}} + I = [m \cdot I]$. Como casos particulares de fórmulas para las sumas iteradas de funciones tenemos que, con los primeros valores de $m$, las sumas iteradas de la identidad son

$$\begin{aligned}
I + \overset{0}{\overbrace{\cdots}} + I &= [0 \cdot I] = 0I = T_I^0(c_0) = I_Z(c_0) = c_0 \\
I + \overset{1}{\overbrace{\cdots}} + I &= [1 \cdot I] = 1I = T_I^1(c_0) = T_I(c_0) = c_0 + I = I \\
I + \overset{2}{\overbrace{\cdots}} + I &= [2 \cdot I] = 2I = T_I^2(c_0) = T_I(T_I(c_0)) = T_I(I) = I + I \\
&\vdots
\end{aligned}$$

y en el caso general **176** implica:

**182.-** La suma iterada $m^+$ veces de la función identidad es igual a su suma iterada $m$ veces sumada a su vez con la misma función identidad.

$$I + \overset{m^+}{\overbrace{\cdots}} + I = (I + \overset{m}{\overbrace{\cdots}} + I) + I$$

resultado equivale a la fórmula

$$[m^+ \cdot I] = [m \cdot I] + I$$

**183.-** Las sumas iteradas de la función identidad son monótonas y aditivas

$$[n \cdot I] \in \mathrm{Mon}(\mathbb{N}) \cap \mathrm{Adi}(\mathbb{N})$$

En efecto, vimos en **49** que la función identidad es estrictamente monótona, y por consiguiente es monótona; y en **178** demostramos que las sumas iteradas de funciones monótonas son monótonas, por lo tanto $[n \cdot I] \in \mathrm{Mon}(\mathbb{N})$. La identidad es aditiva por **168** y **178** garantiza entonces que $[n \cdot I] \in \mathrm{Adi}(\mathbb{N})$.

Cuando $0 < m$ vale lo siguiente:

**184.-** Las sumas iteradas a coeficiente de iteración positivo de la función identidad son estrictamente monótonas y eyectivas, es decir, si $m > 0$ entonces

$$[m \cdot I] \in \mathrm{EMon}(\mathbb{N}) \cap \mathrm{Eye}(\mathbb{N})$$

Este enunciad se obtiene de **179** tomando $h = I$.

En el caso inyectivo tenemos:

**185.-** Las sumas iteradas a coeficiente de iteración positivo de la función identidad son inyectivas

$$h \in \mathrm{Iny}(\mathbb{N}) \;\Rightarrow\; [m \cdot h] \in \mathrm{Iny}(\mathbb{N})$$

Suponemos que $x \neq y$ y queremos concluir que $[m \cdot h](x) \neq [m \cdot h](y)$. Por tricotomía hay dos posibilidades: $x < y$ o $y < x$; como $I$ es estrictamente monótona se tiene, de acuerdo con **179**, que $[m \cdot h]$ es estrictamente monótona y por consiguiente en el primer caso $[m \cdot h](x) < [m \cdot h](y)$ mientras que en el segundo $[m \cdot h](y) < [m \cdot h](x)$. En consecuencia $[m \cdot h](x) \neq [m \cdot h](y)$ como deseábamos demostrar.

El valor en 1 de una suma iterada de la función identidad es el coeficiente de iteración:

**186.-** La suma iterada $m$ veces de la función identidad evaluada en 1 es igual a $m$

$$[m \cdot I](1) = m$$

Sea $A = \{m \mid [m \cdot I](1) = m\}$; obviamente $0 \in A$ y si suponemos que $m \in A$ se tiene

$$\begin{array}{rcl} [m^+ \cdot I](1) & = & ([m \cdot I] + I)(1) \\ & = & [m \cdot I](1) + 1 \\ & = & m + 1 = m^+ \end{array}$$

Esta igualdades son respectivamente consecuencia de **182**, de la definición de suma de funciones y de **148**. Queda probado que $A$ es inductivo y por lo tanto $A = \mathbb{N}$. Las funciones aditivas son exactamente las sumas iteradas de la identidad:

**187.-** Toda función aditiva es igual a una suma iterada de la identidad con coeficiente de iteración igual a su valor en la unidad, es decir,

$$f \in \mathrm{Adi}(\mathbb{N}) \quad \Rightarrow \quad f = [m \cdot I]$$

siendo $m = f(1)$.

Sea $f$ aditiva, tomemos $n = f(1)$ y considere $A = \{m \mid f(m) = [n \cdot I](m)\}$. Puesto que $f$ y $[n \cdot I]$ son aditivas se cumple $f(0) = 0 = [n \cdot I](0)$ por lo que $0 \in A$. Suponga que $m \in A$, entonces

$$\begin{array}{rcl} f(m^+) & = & f(m) + f(1) \\ & = & [n \cdot I](m) + f(1) \\ & = & [n \cdot I](m) + n \\ & = & [n \cdot I](m) + [n \cdot I](1) \\ & = & [n \cdot I](m^+) \end{array}$$

igualdades estas que se deducen de **171**, de la hipótesis de inducción, de la definición de $n$, de **186**, y de la aditividad de $[n \cdot I]$. Queda probado que $A = \mathbb{N}$ y el resultado es cierto.

## 32. Producto

Multiplicar dos números naturales es iterar la suma del primero consigo mismo tantas veces como lo indique el segundo. En otras palabras, la multiplicación es una suma iterada siendo los sumandos todos iguales al primer natural, y estando repetida la iteración las veces que indique el segundo. Puede haber ninguna (cero) iteración, una iteración, dos iteraciones, etc. La definición de producto se apoya en las sumas iteradas de la función identidad.

Definimos el *producto de $n$ por $m$*, denominado asimismo *multiplicación de $n$ por $m$* y denotado $nm$ o también $n \cdot m$, como el resultado de aplicar a $n$ la suma iterada $m$ veces de la función identidad

$$nm = [m \cdot I](n)$$

De acuerdo con esta definición de producto se cumple lo siguiente

$$\begin{aligned} nm &= [m \cdot I](n) \\ &= (I + \overset{m}{\smile\!\!\cdots} + I)(n) \\ &= T_I^m(c_0)(n) \end{aligned}$$

El natural $n$ es el *primer factor* o *multiplicando* y $m$ es el *segundo factor* o *multiplicador*.

El producto de números naturales tiene como elemento neutro la unidad $1 = 0^+ = s(0)$:

**188.-** *Existencia de elemento neutro para el producto:* La unidad es elemento neutro para el producto

$$1\,n = n = n\,1$$

Puesto que $[1 \cdot I] = I$ tenemos

$$n\,1 = [1 \cdot I](n) = I(n) = n$$

Se demostró en **186** que la suma iterada $n$ veces de la función identidad tiene en 1 el valor $n$, luego la definición de producto implica

$$1\,n = [n \cdot I](1) = n$$

Puesto que $[0 \cdot h] = c_0$ se tiene $n \cdot 0 = [0 \cdot I](n) = c_0(n) = 0$. Por otra parte $[m \cdot I]$ es aditiva y según **170** su valor en 0 es 0:

$$[m \cdot I](0) = 0$$

por lo tanto

**189.-** Si un factor es cero entonces el producto es cero

$$n \cdot 0 = 0 = 0 \cdot m$$

Hay dos leyes distributivas, según aparezca la operación de suma en el multiplicando o en el multiplicador:

**190.-** *Distributividad con suma a izquierda:* Si el multiplicando incrementa en $m$ entonces el producto incrementa en el resultado de multiplicar $m$ y el multiplicador

$$(n+m)k = nk + mk$$

En efecto, la función $[k \cdot I]$ es suma iterada de la función identidad y por **183** es aditiva; por lo tanto

$$\begin{aligned} (n+m)k &= [k \cdot I](n+m) \\ &= [k \cdot I](n) + [k \cdot I](m) \\ &= nk + mk \end{aligned}$$

**191.-** *Distributividad con suma a derecha:* Si el multiplicador incrementa en $k$ entonces el producto incrementa en el resultado de multiplicar el multiplicando por $k$.

$$n(m+k) = nm + nk$$

Las funciones $[(m+k) \cdot I]$ y $[m \cdot I] + [k \cdot I]$ son sumas iteradas de la identidad y por consiguiente son aditivas, **183**; sus valores en 1 son

$$[(m+k) \cdot I](1) = m + k \qquad ([m \cdot I] + [k \cdot I])(1) = m + k$$

De acuerdo con **172** estos valores determinan las funciones; luego las funciones son iguales y concluimos que

$$\begin{aligned} n(m+k) &= [(m+k) \cdot I](n) \\ &= ([m \cdot I] + [k \cdot I])(n) \\ &= [m \cdot I](n) + [k \cdot I](n) \\ &= nm + nk \end{aligned}$$

A continuación tenemos la

**192.-** *Asociatividad del producto:* El producto es asociativo

$$(nm)k = n(mk)$$

Por **173** la composición $[k \cdot I] \circ [m \cdot I]$ es aditiva, y también $[(mk) \cdot I]$ es una función aditiva; los valores de estas funciones en 1 son iguales

$$\begin{aligned} [k \cdot I] \circ [m \cdot I](1) &= [k \cdot I]([m \cdot I](1)) = [k \cdot I](m) = mk \\ [(mk) \cdot I](1) &= mk \end{aligned}$$

y como, según **172**, los valores en 1 las determinan, tienen que ser la misma función

$$[k \cdot I] \circ [m \cdot I] = [(mk) \cdot I]$$

Por lo tanto

$$\begin{aligned} (nm)k &= [k \cdot I](nm) \\ &= [k \cdot I]([m \cdot I](n)) \\ &= ([k \cdot I] \circ [m \cdot I])(n) \\ &= [(mk) \cdot I](n) \\ &= n(mk) \end{aligned}$$

La tercera igualdad se deduce de la definición de composición de funciones y las demás de la definición de producto.

Los naturales $n$ y $m$ pueden intercambiarse sin modificar el valor del producto. La demostración utiliza directamente el principio de inducción:

**193.-** *Conmutatividad del producto:* El orden de los factores no altera el producto

$$nm = mn$$

Sea $A = \{m \mid \ nm = mn\}$. Sabemos por **189** que $0 \in A$. Asuma la hipótesis inductiva $m \in A$, esto es, suponga que $nm = mn$. Para $m^+$ se tiene

$$\begin{aligned} nm^+ &= n(m+1) \\ &= nm + n \\ &= mn + n \\ &= (m+1)n \\ &= m^+n \end{aligned}$$

La primera igualdad es cierta por definición del sucesor de $m$, $m+1$; la segunda por distributividad a derecha, **191**; la tercera por la hipótesis inductiva; la cuarta por distributividad a izquierda, **190**; y la última nuevamente por definición del sucesor $m^+$. Luego $A$ es inductivo y $A = \mathbb{N}$.

**194.-** *Positividad del producto:* El producto de naturales positivos es positivo

$$n, m > 0 \;\Rightarrow\; nm > 0$$

Basta demostrar la siguiente cadena de relaciones:

$$\begin{array}{rcl} 0 & < & 1 \\ & \leq & (a(n)m + a(m)) + 1 \\ & = & a(n)m + m \\ & = & (a(n)+1)m \\ & = & nm \end{array}$$

Estas expresiones se justifican así: La primera porque 1 es el sucesor de 0, $s(0) = 1$, y porque todo natural precede estrictamente a su sucesor, **85**; la segunda porque la suma de un natural y 1 sigue a 1, **153**; la tercera por asociatividad de la suma y porque el sucesor del antecesor de un natural $m > 0$ es $m$, **96**; la cuarta por la propiedad distributiva, **190**; y la última porque el sucesor del antecesor de $n > 0$ es $n$, **96**.

Puesto que todo natural no nulo es positivo la propiedad anterior equivale a la siguiente:

**195.-** *Integridad del producto:* Si ambos factores son no nulos entonces el producto es no nulo

$$n \neq 0 \wedge m \neq 0 \;\Rightarrow\; nm \neq 0$$

Por ejemplo, si $\varphi : \mathbb{N} \to \mathbb{N}'$ es el isomorfismo canónico y si $I : \mathbb{N} \to \mathbb{N}$, $I' : \mathbb{N}' \to \mathbb{N}'$ son las identidades entonces es evidente que

**196.-** $I' = \varphi \circ I \circ \varphi^{-1}$

Estamos en condiciones de demostrar:

**197.-** El isomorfismo canónico es multiplicativo

$$\varphi(nm) = \varphi(n)\varphi(m)$$

En efecto

$$\begin{array}{rcl} \varphi(nm) & = & \varphi([m \cdot I](n)) \\ & = & (\varphi \circ [m \cdot I])(n) \\ & = & ([\varphi(m) \cdot \varphi \circ I])(n) \\ & = & ([\varphi(m) \cdot \varphi \circ I \circ \varphi^{-1}])(\varphi(n)) \\ & = & [\varphi(m) \cdot I'](\varphi(n)) \\ & = & \varphi(m)\varphi(n) \end{array}$$

La primera igualdad es cierta por definición de producto; la segunda por definición de composición de funciones; tercera por **181** con $h = I$; la cuarta por **177** con $g = \varphi^{-1}$; la quinta por **196**; y la última por definición de composición.

## 33. Producto y orden

Veremos en esta sección las relaciones básicas entre producto y orden.

**198.-** Si un natural precede a otro y se multiplican ambos por un mismo natural entonces el producto por el primero precede al producto por el segundo

$$n \leq m \;\Rightarrow\; nk \leq mk$$

El resultado es obvio si $k = 0$. En el caso $k > 0$ **183** establece que la suma iterada $[k \cdot I]$ es monótona, luego $nk = [k \cdot I](n) < [k \cdot I](m) = mk$. Este razonamiento también demuestra el caso estricto:

**199.-** Si un natural precede estrictamente a otro y se multiplican ambos por un mismo natural no nulo entonces el producto por el primero precede estrictamente al producto por el segundo

$$n < m \quad \wedge \quad k \neq 0 \quad \Rightarrow \quad nk < mk$$

## 34. Leyes de cancelación para el producto

La siguiente propiedad, junto a **161**, origina los métodos de resolución de ecuaciones.

**200.-** *Ley de cancelación de factores no nulos en igualdades:* Si un natural multiplicado por un factor no nulo es igual al producto de otro natural por el mismo factor entonces el primer natural es igual al segundo, es decir, si $k \neq 0$ entonces

$$nk = mk \;\Rightarrow\; n = m$$

En **183** se probó que, para $k > 0$, la suma iterada de la identidad $[k \cdot I]$ es inyectiva, luego

$$nm = nk \;\Rightarrow\; [k \cdot I](n) = [k \cdot I](m) \;\Rightarrow\; n = m$$

Para las desigualdades tenemos

**201.-** *Ley de cancelación de factores positivos en desigualdades:* Si un natural multiplicado por un factor positivo precede al producto de otro natural por el mismo factor entonces el primer natural precede al segundo, es decir, si $0 < k$ entonces

$$nk \leq mk \ \Rightarrow \ n \leq m$$

Por reducción al absurdo, si fuese $m < n$ entonces por ser $0 < k$ **199** implicaría $mk < nk$, lo cual contradice la condición $nk \leq mk$.

En el caso estricto se cumple

**202.-** *Ley de cancelación de factores positivos en desigualdades estrictas:* Si un natural multiplicado por un factor positivo es estrictamente menor que otro natural multiplicado por mismo factor entonces el primer natural es estrictamente menor que el segundo, es decir, si $0 < n$ entonces

$$nk < mk \ \Rightarrow \ n < m$$

Razonamos por reducción al absurdo como en el enunciado anterior. Si fuese cierto que $m \leq n$ entonces **198** implicaría que $mk \leq nk$, contra la condición $nk < mk$.

## 35. División entera

La existencia de cociente entero con resto es una de las características esenciales de los naturales.

En general este tópico se pospone hasta la introducción de los enteros debido a que entre naturales no siempre es posible efectuar restas $q - q'$ (el resultado puede ser negativo). Pero esta carencia se suple fácilmente como veremos más abajo.

La *división entera* proporciona un número que indica cuantas veces cabe un natural en otro y, si la cabida no es exacta, proporciona también un resto. Más precisamente, dado un natural $a \in \mathbb{N}$, llamado (en el contexto de la división entera) el *dividendo*, y otro natural no nulo $b$, el *divisor*, existen dos naturales: uno de ellos el *cociente* $q$, y el otro, el *resto* $r$, tales que el dividendo es igual a la suma del resto con el producto del divisor por el cociente y el resto es menor que el divisor. En otras palabras

**203.-** *Existencia de Cociente y Resto:* Dados $a, b \in \mathbb{N}$, $b > 0$, existen $q, r \in \mathbb{N}$ únicos tales que

$$a = bq + r \qquad 0 \leq r < b$$

Para probar la existencia de $q$ y $r$ sea $M$ el conjunto de los naturales que multiplicados por $b$ no exceden $a$

$$M = \{m \,|\, bm \leq a\}$$

Este conjunto es no vacío porque contiene a cero:

$$0 = b\,0 \leq a \;\Rightarrow\; 0 \in M$$

Por otra parte, $1 \leq b$ y por lo tanto para cualquier $m \in M$ se tiene

$$m = 1 \cdot m \leq b \cdot m \leq a$$

lo cual indica que $a$ es cota superior de $M$, $a \in C_S(M)$. El último elemento de $M$, que sabemos existe por **104**, es el cociente de la division con resto; en efecto, sea $q = u(M) \in M$ de modo que vale el siguiente par de relaciones

$$q \in M \qquad q^+ \notin M$$

equivalentemente

$$bq \leq a \qquad a < bq^+$$

De acuerdo con **147** existe $r \in \mathbb{N}$ tal que $a = bq + r$. Sustituyendo en la última desigualdad $a$ por $bq + r$ y aplicando **191** se tiene

$$a = bq + r < bq^+ = bq + b$$

lo cual implica, según **163**, que $r < b$. La existencia del cociente y el resto está demostrada.

Probemos ahora la unicidad. Supongamos otra expresión $a = bq' + r'$ con $0 \leq r' < b$. Por reducción al absurdo, si fuese $q < q'$ entonces $q' = q + t$ con $0 < t$. Por consiguiente

$$a = bq + r = bq' + r' = b(q + t) + r' = bq + (bt + r')$$

lo cual permite deducir por medio de **161** que $r = bt + r'$. Pero por ser $1 \leq t$ se cumple

$$b = b1 \leq bt \leq bt + r' = r$$

luego $b \leq r$ lo cual contradice la condición $r < b$. Por consiguiente $q = q'$ y $bq + r = bq + r'$, que a su vez implica, nuevamente por **161**, $r = r'$. La otra posibilidad, $q' < q$, es un simple intercambio. Queda probada la unicidad del cociente y del resto. La demostración de **203** está completa.

Dadas dos funciones con un dominio común cualquiera $W$ y a valores naturales

$$f, g : W \to \mathbb{N}$$

definimos su *producto* $fg : W \to \mathbb{N}$ efectuándolo punto a punto, esto es, mediante la expresión

$$fg(w) = f(w)g(w)$$

Utilizando además la suma de funciones definida en la sección 30 llegamos a una versión funcional del cociente con resto. En efecto, sean

$$A : \mathbb{N} \times (\mathbb{N} - \{0\}) \to \mathbb{N} \qquad B : \mathbb{N} \times (\mathbb{N} - \{0\}) \to \mathbb{N}$$

las proyecciones sobre el primer y segundo factor respectivamente, esto es

$$A(a, b) = a \qquad B(a, b) = b$$

Defina las funciones $Q : \mathbb{N} \times (\mathbb{N} - \{0\}) \to \mathbb{N})$ como el cociente de dividir $a$ entre $b$ y $R : \mathbb{N} \times (\mathbb{N} - \{0\}) \to \mathbb{N})$ como el resto, entonces podemos reformular **203** como

**204.-** Existen funciones definidas sobre $\mathbb{N} \times (\mathbb{N} - \{0\})$ y a valores en $\mathbb{N}$

$$Q : \mathbb{N} \times (\mathbb{N} - \{0\}) \to \mathbb{N} \qquad R : \mathbb{N} \times (\mathbb{N} - \{0\}) \to \mathbb{N}$$

tales que

$$A = BQ + R$$

## 36. Sucesiones

Sean $\mathbb{N}$ un sistema de números naturales y $A$ un conjunto. Una *sucesión* en $A$ es una función

$$a : \mathbb{N} \to A$$

cuyo dominio son los naturales y que toma valores en $A$; el valor $a(n)$ que toma en el elemento $n \in \mathbb{N}$ es el *término $n$-ésimo* y se designa también como

$a_n$ de manera que $a(n) = a_n$. Las notaciones usuales para designar la sucesión $a$ son

$$\{a_n\} \qquad \{a_n\}_{n\geq 0} \qquad \{a_n\}_{n\in\mathbb{N}}$$

El *primer término* de la sucesión es $a_0$. Una sucesión es *estrictamente creciente* si para todo $n$ se cumple $a_n < a_{n+1}$. Las sucesiones estrictamente crecientes tienen las siguientes propiedades.

## 37. Infinitud de los naturales

Repetimos aquí lo demostrado en **??**:

**205.-** El conjunto de los números naturales es infinito

$$|\mathbb{N}| = \infty$$

## 38. Finitud de los intervalos

**206.-** Todo intervalo inicial de naturales es finito

$$|[0,n]_{\mathbb{N}}| < \infty$$

Para la prueba sea $A$ el conjunto de los naturales que son extremo superior de intervalos iniciales finitos

$$A = \{n \in \mathbb{N} \mid |[0,n]_{\mathbb{N}}| < \infty\}$$

El intervalo $[0,0]_{\mathbb{N}}$ es unipuntual y por lo tanto finito; luego $0 \in A$. De acuerdo con **??**, se tiene que $n \in A \Rightarrow n^+ \in A$. Luego $A = \mathbb{N}$.

## 39. Naturales y conjuntos infinitos

Un conjunto es *numerable* si es equipotente con el conjunto de los números naturales, en otras palabras, $X$ es numerable si $\mathrm{Biy}(\mathbb{N}, X) \neq \emptyset$. En la sección **??** introdujimos la notación $X \sim Y$ para indicar que $X$ e $Y$ son conjuntos equipotentes. Así, $X \sim \mathbb{N}$ y $\mathbb{N} \sim X$ dicen que $X$ es numerable.

La composición de biyecciones es biyección, por lo tanto

**207.-** Conjuntos equipotentes a numerables son numerables

$$\mathbb{N} \sim X \wedge X \sim Y \;\Rightarrow\; \mathbb{N} \sim Y$$

Si un conjunto es infinito también lo son todos sus equipotentes, luego

**208.-** Todo conjunto numerable es infinito

$$X \sim \mathbb{N} \;\Rightarrow\; |X| = \infty$$

Puesto que la identidad $1_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ es una biyección se tiene

**209.-** El conjunto de los números naturales es numerable.

$$\mathbb{N} \sim \mathbb{N}$$

**210.-** Todo conjunto infinito contiene subconjuntos numerables

Más específicamente

**211.-** Para todo conjunto infinito existen funciones inyectivas de los naturales en el conjunto, esto es,

$$|X| = \infty \;\Rightarrow\; \mathrm{Iny}(\mathbb{N}, X) \neq \emptyset$$

**212.-** Un conjunto no vacío para el cual no hay suryecciones desde un intervalo inicial es infinito; esto es, si $X \neq \emptyset$ y si para todo $n \in \mathbb{N}$ se cumple

$$\mathrm{Sur}([0, n]_{\mathbb{N}}, X) = \emptyset$$

entonces $X$ es infinito.

**213.-** Si $X$ es infinito entonces para todo $n \in \mathbb{N}$ se tiene

$$\mathrm{Sur}([0,n]_{\mathbb{N}}, X) = \emptyset$$

**214.-** Si un conjunto es infinito toda función de un intervalo inicial en el conjunto deja puntos fuera de su imagen, esto es, si $h : [0,n]_{\mathbb{N}} \to X$ es una función entonces

$$|X| = \infty \;\Rightarrow\; h([0,n]_{\mathbb{N}}) \neq \emptyset$$

Uno de los axiomas de la teoria de conjuntos postula que las partes $\mathcal{P}$ del conjunto $X$ forman un conjunto. Por lo tanto

## 40. Naturales y conjuntos finitos

**215.-** Todo intervalo inicial de naturales es finito

$$|[0,n]_{\mathbb{N}}| < \infty$$

Para la prueba sea $A$ el conjunto de los naturales que son extremo superior de intervalos iniciales finitos

$$A = \{n \in \mathbb{N} \,|\, |[0,n]_{\mathbb{N}}| < \infty\}$$

El intervalo $[0,0]_{\mathbb{N}}$ es unipuntual y por lo tanto finito; luego $0 \in A$. De acuerdo con **??**, se tiene que $n \in A \;\Rightarrow\; n^+ \in A$. Luego $A = \mathbb{N}$.

Demostraremos ahora que todo conjunto finito no vacío es equipotente a algún intervalo inicial de naturales. Supondremos en el resto de esta sección que el conjunto $X$ no es vacío.

Sea $U = \{x\}$ un conjunto unipuntual

**216.-** Un conjunto es no vacío si y solo para hay funciones inyectivas de $U$ en el conjunto

$$X \neq \emptyset \Leftrightarrow \mathrm{Iny}(U, X) \neq \emptyset$$

**217.-** Para todo conjunto no vacío existen funciones inyectivas de algún intervalo inicial en el conjunto, esto es,

$$X \neq \emptyset \;\Rightarrow\; \mathrm{Iny}(\mathbb{N}, X) \neq \emptyset$$

Sabemos por **??** que las imágenes de conjuntos finitos mediante funciones son conjuntos finitos. Recíprocamente, si un conjunto es infinito no puede haber suryecciones de un intervalo de naturales en el conjunto, luego

Sea $X$ un conjunto que no admite cobertura finita, entonces $X$ es infinito.

Todo conjunto $X \neq \emptyset$ es rango al menos una inyección finita.

Sea $X$ un conjunto que no admite cobertura finita, entonces $X$ es infinito.

Considere las inyecciones finitas en $\mathcal{I}(X)$ y la función $f = f_e : \mathcal{I}(X)$

Considere una sucesión finita $\varphi : [0, n]_{\mathbb{N}} \to X$, $x_{n+1} \in X - \varphi([0, n]_{\mathbb{N}})$ un elemento fuera de la imagen de la sucesion y sea

$$c : \{n+1\} \to X$$

la función definida en el unipuntual $\{n+1\} \subseteq [0, n+1]_{\mathbb{N}}$ cuyo valor es $x_{n+1}$. Esta junta extiende la $n$-sucesión a una $n+1$-sucesión entonces

**218.-** Si la $n$-función es inyectiva y el elemento no esta en su imagen entonces la extensión es inyectiva, es decir

$$\in \mathrm{Iny}([0, n]_{\mathbb{N}}, X) \;\wedge\; \quad \Rightarrow\; \varphi \vee c \in \mathrm{Iny}([0, n+1]_{\mathbb{N}}, X)$$

En particular no existen biyecciones de un intervalo finito sobre un conjunto infinito. Por el contrario, cualquier conjunto finito es equipotente con algún intervalo inicial. que todo conjunto finito es equipotente con alguno de ellos. Para la prueba consideremos el conjunto $Y_n$ de las inyecciones del intervalo inicial $[0, n]_{\mathbb{N}}$ en un conjunto infinito $X$

$$Y_n = \mathrm{Iny}([0, n]_{\mathbb{N}}, X)$$

y la unión $Y$ de todos estos conjuntos

$$Y = \bigcup_{n \in \mathbb{N}} \mathrm{Iny}([0, n]_{\mathbb{N}}, X)$$

**219.-** Si un conjunto $F$ es finito y no vacío entonces es equipotente con algún intervalo inicial de naturales

$$|X| < \infty \;\Rightarrow\; \exists\, n \in \mathbb{N} \ni \operatorname{Biy}([0,n]_{\mathbb{N}}, X) \neq \emptyset$$

La prueba, que invoca el Axioma de Elección, consta de los siguientes 5 pasos.

1$^{o}$)El intervalo inicial de naturales $[0,0]_{\mathbb{N}}$ es unipuntual; invocamos **??** para concluir que hay inyecciones de $U = [0,0]_{\mathbb{N}}$ en $X$

$$\operatorname{Iny}([0,0]_{\mathbb{N}}, X) \neq \emptyset$$

y por lo tanto el conjunto

$$Y = \bigcup_{n \in \mathbb{N}} \operatorname{Iny}([0,n]_{\mathbb{N}}, X)$$

tampoco es vacío. Este conjunto consta de *todas* las funciones inyectivas a valores en $X$ con dominio algún intervalo inicial de naturales.

2$^{o}$)Por reducción al absurdo. Supongamos que para ningún $n$ hay biyecciones, esto es, cualquiera que sea $n$ se tiene $\operatorname{Biy}([0,n]_{\mathbb{N}}, X) = \emptyset$; entonces las inyecciones de intervalos en $X$ no pueden ser suryectivas

$$\varphi \in Y \quad \Rightarrow \quad \varphi([0,n]_{\mathbb{N}}) \subsetneqq X$$

lo cual equivale a que cada imagen tenga complemento no vacío

$$\emptyset \neq X - \varphi([0,n]_{\mathbb{N}}) \in \mathcal{P}_0(X)$$

Según el Axioma de Elección hay

$$e : \mathcal{P}_0 \to X$$

que es función de elección para $\mathcal{P}_0(X)$. Esta funcion verifica

$$e(X - \varphi([0,n]_{\mathbb{N}})) \in X - \varphi([0,n]_{\mathbb{N}})$$

Definamos la función

$$f_n : \operatorname{Iny}([0,n]_{\mathbb{N}}, X) \to \operatorname{Iny}([0,n+1]_{\mathbb{N}}, X)$$

especificando su valor $f_n(\varphi) \in \text{Iny}([0, n+1]_{\mathbb{N}}, X)$ sobre $\varphi \in \text{Iny}([0, n]_{\mathbb{N}}$ de la manera siguiente:

$$f(\varphi(k)) = \begin{cases} \varphi(k) & \text{si} \quad 0 \leq k \leq n \\ e(X - \varphi_n([0, n]_{\mathbb{N}})) & \text{si} \quad k = n+1 \end{cases}$$

Queda entonces definida

$$f : Y \to Y$$

por la condición

$$f|Y_n = f_n$$

Tomemos como punto inicial una función cualquiera (necesariamente constante) $y_0 = c_{x_0} \in Y_0 = \text{Iny}(\{0\}, X)$; si aplicamos el teorema de recursión **??** concluimos que existe una sucesión $y_n$ con

$$y_{n+1} = f(y_n)$$

**220.-** El $n$-ésimo término de la recursión, $y_n$, es una inyección con dominio $[0, n]_{\mathbb{N}}$ a valores en $X$.

TEORIA AXIOMATICA DE CONJUNTOS Versión Preliminar Lewin, Renato A. - Teoría Axiomática de Conjuntos.pdf

Recíprocamente, supongamos que para toda $f \in \text{Iny}([0, n]_{\mathbb{N}}$ se tiene que $f$ no es suryectiva, esto es, $f([0, n]_{\mathbb{N}}) \subsetneqq X$, de manera qu $X - f([0, n]_{\mathbb{N}}) \neq \emptyset$.

• *Contar conjuntos finitos.* El resultado **??** significa que los intervalos iniciales de números naturales proporcionan modelos para todos los conjuntos finitos: Al comparar conjuntos finitos con intervalos iniciales de naturales encontramos que ningún conjunto finito queda excluido. Un conjunto finito con cantidad tal de elementos que no sea equipotente con ningún intervalo de naturales no existe. En este sentido –salvo equipotencia o, equivalentemente, salvo biyección– los intervalos de naturales proporcionan una colección completa de modelos para los conjuntos finitos.

Lo anterior también se puede interpretar de la manera siguiente: Los números naturales siempre son adecuados para contar los elementos de los conjuntos finitos.

FALTAN: Finitud de los intervalos y el siguiente enunciado:

Sea $\mathbb{N}$ un sistema de números naturales. Todo subconjunto infinito $A \subseteq \mathbb{N}$ esta bien ordenado, es inductivo y minimal, luego es un sistema de números naturales. Hay un único isomorfismo $\varphi : \mathbb{N} \to A$. Este isomorfismo verifica

$$n < m \Leftrightarrow \varphi(n) < \varphi(m)$$

y

$$A = \{\varphi(n) \,|\, n \in \mathbb{N}\}$$

Denotemos por $n_j$ el elemento $\varphi(j)$, entonces

$$A = \{n_j \,|\, j \in \mathbb{N}\}$$

Los *subsistemas (de números naturales)* de $\mathbb{N}$ son sus subconjuntos infinitos. Es decir, $A$ es un subsistema de $\mathbb{N}$ si es uno de sus subconjuntos infinitos: $A \subseteq \mathbb{N}$, $|A| = \infty$. El concepto de subsistema facilita el manejo de las subsucesiones.

## 41. Subsucesiones

## 42. Divisibilidad

Para facilitar la exposición la asociatividad, conmutatividad, distributividad y demás propiedades elementales básicas se utilizaran, de esta sección en adelante, sin resaltarlas explícitamente. En todos los casos donde aparentemente exista una omisión el lector podrá fácilmente suplir cualquier detalle o argumento elemental requerido.

Sean $a \neq 0$ y $b$ naturales. $a$ es *divisor* de $b$, denotado $a|b$, si existe $c \in \mathbb{N}$ tal que $b = ac$. Para indicar que $a$ *no* es divisor de $b$ usaremos $a \nmid b$. Recalcamos que el divisor es siempre distinto de cero: $a \neq 0$.

La siguientes frases tienen todas el mismo significado: $a$ es *divisor* de $b$; $a$ *divide* $b$; $b$ es *múltiplo* de $a$; $b$ es *divisible* por $a$.

La divisiblidad es reflexiva y transitiva, tiene a la unidad como divisor universal y al cero cero múltiplo universal, es decir, se cumplen las siguientes reglas:

**221.-** Reflexividad: Todo elemento es divisor de si mismo

$$a|a$$

Para probarlo basta observar que $a = a \cdot 1$.

**222.-** Transitividad: Si un elemento divide a otro, y este a un tercero, entonces el primero divide al tercero

$$a|b \quad \wedge \quad b|c \quad \Rightarrow \quad a|c$$

En efecto, $b = ad$ y $c = be$, y sustituyendo $b$ en la segunda igualdad se obtiene $c = a(de)$.

**223.-** La unidad es divisor universal, esto es, todo elemento es múltiplo de 1

$$1|a$$

Porque la relación $a = 1 \cdot a$ implica $1|a$.

**224.-** El cero es múltiplo universal, es decir, todo elemento divide a 0

$$a|0$$

Según 189, $0 = a \cdot 0$ y por lo tanto $a|0$.

**225.-** Los múltiplos conservan la divisibilidad: Si un elemento divide a otro, cualquier multiplo no nulo del primero divide al correspondiente múltiplo del segundo

$$a|b \quad \wedge \quad c \neq 0 \quad \Rightarrow \quad ac|bc$$

Por hipótesis $b = ad$ luego $bc = (ad)c = (ac)d$ y $ac|bc$.

**226.-** Los divisores de un natural no nulo son menores que el dividendo

$$a \neq 0 \ \wedge \ b \neq 0 \ \wedge \ a|b \ \Rightarrow \ a \leq b$$

Sea $b = ac$, entonces $1 \leq a$ implica $a = a \cdot 1 \leq a \cdot c = b$.

Sean $b, c \in \mathbb{N}$. Un natural $d$ es *combinación lineal (con coeficientes naturales)* de los naturales $b$ y $c$ si es de la forma

$$d = rb + sc$$

con $r, s \in \mathbb{N}$. Tenemos entonces

**227.-** Si un natural divide otros dos, entonces divide cualquiera de sus combinaciones lineales

$$a|b \quad \wedge \quad a|c \quad \Rightarrow \quad a|rb + sc$$

Si $b = ae$ y $c = af$ entonces $rb = aer$ y $sc = afs$. Por consiguiente $rb + sc = aer + afs = a(er + fs)$, de donde $a|(rb + sc)$.

El conjunto de los divisores de $b \neq 0$, denotado $D(b)$, está formado por los naturales no nulos de los cuales es múltiplo

$$D(b) = \{a \mid a|b\}$$

El conjunto de los divisores de un natural esta formado por números que no lo exceden

$$D(a) \subseteq [1, a]_{\mathbb{N}}$$

## 43. Irreducibles

Un natural $a$ es *irreducible* si sus únicos divisores son la unidad y él mismo

$$D(a) = \{1, a\}$$

El siguiente es un teorema clásico fundamental

**228.-** Un natural es irreducible si y solo si es primo.

Supongamos que $p$ es irreducible y que $p|ab$. Si $p$ no divide $a$ entonces

$$b = pq + r$$

con $0 \leq r < p$. $p|ab = (pq + r)b = pqb + rb$ por ser $p$ irreducible el máximo común divisor de $a$ y $p$ es 1 y aplicando **??** obtenemos

## 44. Primos

Infinitud de primos. Tabla de primos. Algoritmos para calcular tablas de primos. Densidad de primos. Decidir si un natural es primo. Primos.

## 45. Cuadrados

Cuadrados perfectos; sucesión de cuadrados.

## 46. Cubos

Cubos perfectos; sucesión de cubos.

## 47. Potencias

Sucesión de potencias $k$ de los naturales. Las potencias de un numero natural se definen mediante recursión y son operaciones exactas.

## 48. Teorema Fundamental de la Aritmética

## 49. Raíces

Raíces naturales de un natural por defecto y por exceso. Caso exacto.

## 50. Exponentes

Sucesión de potencias de una base fija. Exponentes

## 51. Logaritmos

Logaritmos en una base, por defecto y por exceso.

## 52. Sucesión doble de las potencias

Sucesiones de potencias y exponentes contenidas en una sucesión doble.

## 53. Sistemas posicionales

## 54. Recapitulación

Según definición, un sistema de números naturales es un conjunto bien ordenado, inductivo y minimal. Esto significa son conjuntos infinitos con un buen orden donde las iteraciones de la función sucesor evaluadas en el cero proporcionan todos los elementos del conjunto.

El teorema de recursión garantiza que es posible obtener recursiones definidas por datos cualesquiera –conjunto de valores, punto inicial y fórmula– que resultan ser únicas para los datos en cuestión.

Dados dos sistemas de números naturales hay entre ellos un único isomorfismo como conjuntos bien ordenados, esto es, una función biyectiva que conserva el orden. Este isomorfismo canónico se construye como una recursión con valor inicial el primer elemento y fórmula la función sucesor.

• *Caracterización categórica.* La definición dada es una *caracterización categórica* del sistema de números naturales porque además de proporcionar propiedades definitorias implica que dos de estos sistemas son isomorfos. No toda definición es una caracterización categórica. La definición de grupo (conjunto $G$ con operación asociativa, poseedora de elemento neutro y de inversos) no proporciona una caracterización categórica. Esto se debe a que hay muchos objetos estructuralmente distintos entre si (no isomorfos) que satisfacen la definición. En situaciones así es natural plantearse problemas de clasificación. Estos consisten –para los grupos– en obtener descripciones sistemáticas de las clases de isomorfismo de grupos. Por el contrario con los naturales no hay problemas de clasificación: Dos sistemas de naturales son siempre isomorfos mediante isomorfismo único y por lo tanto hay una sola clase de isomorfismo.

Las operaciones aritméticas básicas entre naturales son la suma o adición y el producto o multiplicación.

La suma de dos naturales consiste en sumar 1 al primero de ellos tantas veces como lo indica el segundo. Esta operación se expresa en términos de la función sucesor iterada. La suma de un natural con cero es el natural y la suma de un natural con la unidad es el sucesor del natural.

La suma o adición tiene elemento neutro y es conmutativa, asociativa y compatible con la relación de orden. Satisface leyes de cancelación tanto para igualdades como para desigualdades. La operación de suma es compatible con la relación de orden. El isomorfismo canónico entre sistemas de números naturales es compatible con la suma. La suma de naturales satisface la condición de positividad.

El producto de dos naturales es el natural obtenido a partir del primero de ellos sumándolo consigo mismo tantas veces como indica el segundo. En particular el producto de un natural por cero es cero y el producto de un natural por la unidad es el natural.

El producto o multiplicación tiene elemento neutro, es conmutativo, y asociativo. La operación de producto es compatible con la relación de orden y se cumplen, tanto para igualdades como para desigualdades, leyes de cancelación de factores no nulos. El isomorfismo canónico entre sistemas de números naturales conserva productos. El producto de naturales cumple la condición de positividad.

La suma y el producto se relacionan emtre si mediante las propiedades distributivas.

La division entera es una operación entre dos naturales –el dividendo y el divisor– que tiene como resultado un par de naturales –el cociente y el resto– que se caracterizan porque el dividendo es igual al producto del divisor por el cociente, sumado con el resto. El resto es siempre estrictamente menor que el divisor.

Los sistemas de números naturales sirven de base a otros sistemas: Los enteros, las clases residuales de enteros, los números racionales, los reales y los complejos. Se sigue que son también el fundamento de estructuras ulteriores como espacios vectoriales, álgebras, y las teorías que se apoyan en estos, a saber, el Álgebra, el Análisis y la Topología. Los números naturales proporcionan la materia esencial para construir todo el edificio matemático.

• *Construcción de sistemas de números.* Los sistemas de números de uso común en Matemáticas se construyen a partir de los sistemas de naturales. A continuación damos una descripción –a grandes rasgos y omitiendo detalles– de estos procesos constructivos, todos los cuales se pueden someter a un desmenuzamiento tan detallado como el efectuado con los naturales en esta cartilla.

De $\mathbb{N}$ a $\mathbb{Z}$

A partir de un sistema $\mathbb{N}$ de números naturales se construye un correspondiente sistema de enteros, denotado $\mathbb{Z}$ (del alemán *Zahlen* =números).

Sea $\mathbb{N}$ un sistema de naturales, considere el producto conjuntista $\mathbb{N} \times \mathbb{N}$ y sobre este la relación de equivalencia

$$(n, m) \sim (q, p) \Leftrightarrow n + p = q + m$$

Denotaremos por $n - m$ la clase de equivalencia de $(n, m) \in \mathbb{N} \times \mathbb{N}$

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

El *sistema de enteros* de $\mathbb{N}$ es el conjunto cociente

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

Los elementos de $\mathbb{Z}$ son las clases $n - m$.

El conjunto $\mathbb{Z}$ está naturalmente dotado (a partir de las propiedades de $\mathbb{N}$) de relación de orden, de suma y de producto respecto a los cuales es un *dominio bien ordenado*, siendo esta condición una caracterización categórica de los sistemas de números enteros: Dos dominios bien ordenados son isomorfos (como anillos unitarios) y además el isomorfismo conserva el orden y es único. Los *naturales de* $\mathbb{Z}$ son los elementos del conjunto $\mathbb{N}_{\mathbb{Z}} = \{n - 0 \mid n \in \mathbb{N}\}$, que resulta ser un sistema de naturales y por lo tanto isomorfo con $\mathbb{N}$ mediante isomorfismo único. Un entero $e$ es igual a un natural positivo, $e \in \mathbb{N}_{\mathbb{Z}} - \{0\}$, o al opuesto respecto a la suma de un natural positivo, $-e \in \mathbb{N}_{\mathbb{Z}} - \{0\}$, o a cero, $e = 0$. El valor absoluto del entero $n - m \in \mathbb{Z}$, denotado $|n - m|$, se define así:

$$|n - m| = \begin{cases} n - m & \text{si } m \leq n \\ m - n & \text{si } n \leq m \end{cases}$$

Mencionamos aquí que dados un sistema $\mathbb{Z}$ de números enteros y un $n \in \mathbb{Z}$ el conjunto $\mathbb{Z}_n$ de las *clases residuales módulo* $n$ es el conjunto cociente de $\mathbb{Z}$ por la relación de equivalencia

$$a \sim b \Leftrightarrow n|(b - a)$$

Resulta que $\mathbb{Z}_n$ es un anillo conmutativo unitario y finito con $n$ elementos. Además $\mathbb{Z}_n$ es un cuerpo si y solo si $n$ es número primo.

A partir de un sistema de números enteros se puede construir un correspondiente sistema de números racionales.

De $\mathbb{Z}$ a $\mathbb{Q}$

Sea $\mathbb{Z}$ un sistema de números enteros. Sobre el producto $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ considere la relación

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

Denotaremos por $a/b$ la clase de equivalencia de $(a, b)$. El sistema de números racionales de $\mathbb{Z}$, denotado $\mathbb{Q}$ o $\mathbb{Q}[\mathbb{Z}]$ (del italiano *Quotiente*=cociente, y/o del español(?) *Quebrado* =fracción numérica) es el conjunto cociente

$$\mathbb{Q} = \mathbb{Q}[\mathbb{Z}] = \mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$$

El conjunto $\mathbb{Q}$ está naturalmente dotado de una relación de orden y de operaciones de suma y producto respecto a las cuales resulta ser el cuerpo de cocientes de un dominio bien ordenado, lo cual es una caracterización categórica: Dos cuerpos de cocientes de dominios bien ordenados son isomorfos. Además el isomorfismo conserva el orden y es único. Por ser un cuerpo todo elemento no nulo $q = a/b \in \mathbb{Q} - \{0\}$ tiene inverso multiplicativo $q^{-1} = b/a \in \mathbb{Q} - \{0\}$. Los *enteros de* $\mathbb{Q}$ son los elementos del conjunto $\mathbb{Z}_{\mathbb{Q}} = \{a/1 \mid a \in \mathbb{Z}\}$ el cual es un dominio bien ordenado y por consiguiente isomorfo con $\mathbb{Z}$. Un racional $r$ es igual a un entero, $r = a \in \mathbb{Z}_{\mathbb{Q}}$, o al cociente de dos enteros, $r = a/b$ con $0 \neq b \in \mathbb{Z}_{\mathbb{Q}}$.

El valor absoluto de un racional $m/k$, designado mediante $|m/k|$, se define como $|m/k| = |m|/|k|$.

Un sistema de números racionales origina un correspondiente sistema de números reales.

De $\mathbb{Q}$ a $\mathbb{R}$

Sea $\mathbb{Q}$ un sistema de números racionales, y sean $\mathbb{Z} = \mathbb{Z}_{\mathbb{Q}}$ los enteros de $\mathbb{Q}$, $\mathbb{N} = \mathbb{N}_{\mathbb{Z}}$ los naturales de $\mathbb{Z}$. Estos naturales se usarán como índices. Una sucesión de racionales $a : \mathbb{N} \to \mathbb{Q}$,

$$a = \{a(n)\}_{n\in\mathbb{N}} = \{a_n\}_{n\in\mathbb{N}}$$

es *sucesión de Cauchy* si términos de índices suficientemente grandes son arbitrariamente próximos entre si, esto es, si (denotando por $\epsilon$ un racional)

$$\forall \epsilon > 0 \ \exists \ n_0 = n_0(\epsilon) \in \mathbb{N} \ni n, m \geq n_0 \ \Rightarrow \ |a_n - a_m| < \epsilon$$

Denote por $\mathcal{C}$ o por $\mathcal{C}[\mathbb{Q}]$ el conjunto de las sucesiones de Cauchy de racionales. Este conjunto de sucesiones tiene operaciones de suma y producto (término a término) respecto a las cuales es un anillo (y también recibe de $\mathbb{Q}$ una relación de preorden, *i.e.* reflexiva y transitiva, pero no antisimétrica, lo cual complica un poco los detalles de la construcción).

Una sucesión $\{a_n\}_{n\in\mathbb{N}}$ es *equivalente a cero* si los términos de índice suficientemente grande son arbitrariamente próximos a cero, esto es, si

$$\forall \epsilon > 0 \ \exists \ n_0 = n_0(\epsilon) \in \mathbb{N} \ni n \geq n_0 \ \Rightarrow \ |a_n| < \epsilon$$

Sea $\mathcal{I}$ el conjunto de las sucesiones equivalentes a cero; este resulta ser un ideal maximal en $\mathcal{C}$. El sistema de los números reales de $\mathbb{Q}$ es el cociente del anillo $\mathcal{C}$ por el ideal $\mathcal{I}$. Esto significa que se define en $\mathcal{C}$ la siguiente relación de equivalencia

$$a = \{a_n\}_{n\in\mathbb{N}} \sim b = \{b_n\}_{n\in\mathbb{N}}$$

si la diferencia es equivalente a cero, $b - a \in \mathcal{I}$. Denotemos por $[a] = [\{a_n\}_{n\in\mathbb{N}}]$ la clase de equivalencia de $a$. Entonces el cuerpo $\mathbb{R} = \mathbb{R}[\mathbb{Q}]$ es el conjunto cociente

$$\mathbb{R} = \{[a] \mid a \in \mathcal{C}\}$$

El conjunto $\mathbb{R}$ está dotado naturalmente de una relación de orden y de operaciones de suma y producto provenientes del orden y las operaciones de $\mathbb{Q}$. Se definen en $\mathbb{R}$ sucesiones de Cauchy del mismo modo que en $\mathbb{Q}$ y se prueba que $\mathbb{R}$ es completo, es decir, que toda sucesión de Cauchy tiene limite. Resulta entonces que $\mathbb{R}$ es un cuerpo ordenado arquimediano y completo, propiedades que constituyen una caracterización categórica de $\mathbb{R}$: Dos cuerpos ordenados arquimedianos y completos son isomorfos (como cuerpos). Además el isomorfismo tiene que conservar el orden y es único. Los racionales de $\mathbb{R}$ son el conjunto $\mathbb{Q}_{\mathbb{R}}$ obtenido de las clases de equivalencia de sucesiones racionales constantes, es decir, para cada racional $q = a/b$ sea $\{q\}$ la sucesión constantemente igual a $q$, es decir

$$\{q\}(n) = q$$

entonces $\mathbb{Q}_{\mathbb{R}} = \{[\{q\}] \,|\, q \in \mathbb{Q}\}$.

Todo número real $r = [\{a_n\}_{n\in\mathbb{N}}] \in \mathbb{R}$ resulta ser limite de una sucesión de Cauchy de racionales, a saber, de la sucesión $\{\{a_n\}\}_{n\in\mathbb{N}}$ (téngase presente que $a_n \in \mathbb{Q}$ implica $\{a_n\} \in \mathbb{Q}_{\mathbb{R}}$).

Entre las numerosísimas propiedades que desde el punto de vista del Análisis Matemático posee $\mathbb{R}$ cabe destacar que las funciones continuas sobre intervalos cerrados y acotados alcanzan su máximo y su mínimo (teorema de los valores extremos) y que todo polinomio de grado impar tiene una raíz (consecuencia del teorema del valor intermedio de Weierstrass).

Un sistema $\mathbb{R}$ de números reales permite construir un correspondiente sistema $\mathbb{C} = \mathbb{C}[\mathbb{R}]$ de números complejos.

De $\mathbb{R}$ a $\mathbb{C}$
Sea $\mathbb{R}$ un sistema de números reales. Considere el producto $\mathbb{C} = \mathbb{R}\times\mathbb{R} = \{(x, y) \,|\, x, y \in \mathbb{R}\}$. Usaremos la notación $x_{\mathbb{C}} = (x, 0)$, en particular $1_{\mathbb{C}} = (1, 0)$. El elemento $\imath = (0, 1)$ es la *unidad imaginaria*. Con operaciones de adición y multiplicación definidas mediante

$$(x, y) + (z, w) = (x + z, y + w)$$
$$(x, y)(z, w) = (xz - yw, xw + yz)$$

$\mathbb{C}$ es un cuerpo con elemento nulo $0_{\mathbb{C}} = (0, 0)$ y unidad multiplicativa $1_{\mathbb{C}} = (1, 0)$.

Los reales de $\mathbb{C}$ son el conjunto $\mathbb{R}_{\mathbb{C}} = \{(x, 0) \,|\, x \in \mathbb{R}\} = \{(x, 0)1_{\mathbb{C}} \,|\, x \in \mathbb{R}\} = \mathbb{R} \times \{0\}$ que es de manera natural un cuerpo ordenado arquimediano y completo, luego unívocamente isomorfo con $\mathbb{R}$.

Cualquier múltiplo real de la unidad imaginaria, $\imath y_{\mathbb{C}} = (0, y)$, es un número *imaginario puro*. Se cumple que $\imath^2 = -1_{\mathbb{C}}$ y todo número complejo $z = (x, y)$ se expresa como suma de un número real de $\mathbb{C}$ y un imaginario puro

$$z = (x, y) = x_{\mathbb{C}} + \imath y_{\mathbb{C}}$$

Un cuerpo $\mathbb{K}$ que contenga un subcuerpo $\mathbb{R}$ ordenado, arquimediano y completo, y que además contenga un elemento cuyo cuadrado es igual a $-1 \in \mathbb{R}$, contiene un único subcuerpo isomorfo con el cuerpo $\mathbb{C}$ recién construido, a saber, contiene el subcuerpo $\mathbb{C}_{\mathbb{K}} = \{x + \imath y \,|\, x, y \in \mathbb{R}\}$. Sin embargo el isomorfismo no es único. Entre sistemas de números complejos hay siempre dos isomorfismos que difieren entre si en una conjugación, $x + \imath y \to x - \imath y$.

Los números complejos admiten la siguiente caracterización categórica: Son cuerpos que contienen un subcuerpo de números reales, es decir, ordenado arquimediano y completo, y poseen un elemento $\imath$ cuyo cuadrado es $-1 \in \mathbb{R}$, y además todo elemento del cuerpo se obtiene sumando un real con un múltiplo de $\imath$. Como ya se indicó, dos cuerpos que satisfagan estas condiciones son isomorfos mediante dos posibles isomorfismos.

El teorema de Gauss (hubo precursores) afirma que $\mathbb{C}$ es algebráicamente cerrado, esto es, que todo polinomio con coeficientes en $\mathbb{C}$ tiene raíces en $\mathbb{C}$. Existen muchas demostraciones pero una de las pruebas de mayor circulación se apoya en los antes mencionados teorema de los valores extremos y de existencia de ceros de polinomios reales de grado impar. Véase el libro de Lang [9].

## 55. Broche

Las ideas que siguen proporcionan material para reflexionar sobre las Matemáticas y su inseparable compañero, el ser humano.

Durante veinte años he sostenido un acentuado interés por las redes neurales –o neuronales en parla hispánica– el cual surgió al vislumbrar que los objetos matemáticos tal vez fuesen agrupamientos de neuronas. Después de cuatro lustros, varios teoremas acerca de perceptrones y un par de programas informáticos sigo sin superar el nivel del atisbo especulativo. Pero no toda idea interesante requiere o tiene demostración empírica. Sin necesidad de otros lubricantes resbalo hacia las concepciones siguientes.

Con insistencia he mencionado a lo largo de la cartilla que existen muchos sistemas de números naturales. Debemos pensar no en *un* sistema sino al menos en *una categoría* –en el sentido matemático– de sistemas de números naturales (¿también muchas categorías?). Los objetos de la categoría son los sistemas de números naturales y los morfismos son los isomorfismos canónicos.

El argumento para preferir la multitudinaria categoría al solitario sistema es el siguiente: Cada persona que aprendió los números naturales los lleva entretejidos en sus neuronas. Los sistemas de números son individuales y humanos. Cada una de esas estructuras neuronales personalizadas constituye un sistema particular de números naturales. Son tan personales como los computadores. Dado que hay tantos seres humanos sobre el planeta resulta mucho más natural postular –en vez de un sistema único– toda una categoría de números naturales.

El conocimiento científico, en particular las Matemáticas, existe como resultado de un proceso social. Los individuos se comunican, comparan las estructuras neuronales que llamamos ideas y constatan que –admirablemente– existe concordancia suficiente para considerarlas equivalentes. La comparación se efectúa de las maneras más disímiles y con impredecibles consecuencias: De la conversación a la corrección de ejercicios; desde la nota marginal en latín hasta el evento mediático. Esta consistencia interpersonal ocurre con muchas otras hipotéticas estructuras neuronales que provienen, allende el discurso científico, de la política, la religión, el arte, etc. Sin embargo, la consistencia puede quedar desvirtuada por factores como el error, la ignorancia, la deshonestidad y el despropósito.

Cada sistema de números naturales, concebido como entidad neuronal existente en un individuo, posee también particularidades que lo distinguen de los poseídos por otras personas. Esto se refleja en las distintas maneras de enfrentar y resolver problemas. La notable concordancia coexiste con múltiples grados de desacuerdo y discrepancia que se revelan al comparar honradamente los detalles.

Por una parte –y sin limitarnos a las consideraciones matemáticas– el alto grado de correlación interpersonal entre las estructuras neuronales posibilita el lenguaje y es la base de la comunicación. De otra parte los desacuerdos originan pluralidad y conflictos que dinamizan la trama social. Son mecanismos que convalidan y simultáneamente contraponen conceptos, creencias e ideas de cualquier naturaleza.

La Historia y la actualidad contemporánea proporcionan ejemplos extremos donde, a consecuencia de concordancias y desacuerdos, aparecen tanto la indiferencia como el fanatismo, la sumisión total y el odio, e incuso conflictos sociales violentos y hasta las conflagraciones bélicas. Es de suponer que los aspectos más destructivos del ser humano correspondan con estructuras neuronales; entre estos se pueden mencionar la codicia, la ambición de poder, el excesivo egoísmo, la envidia y las tendencias criminales. En presencia de necesidades primarias insatisfechas –hambre, desamparo, ignorancia, enfermedad– todos estos mecanismos se convierten en armas para luchar por las formas básicas de la justicia.

Afortunadamente existen contrapesos que son otras estructuras y maneras de funcionar como el altruismo, la lucha por los grandes ideales, la búsqueda desinteresada del conocimiento y la dedicación a mejorar la condición humana en todos sus niveles. El amor –me refiero a sus manifestaciones más elevadas– ocupa el trono en la tierra del bien. Son alternativas que han demostrado ser capaces de reducir desniveles en las sociedades sin pasar por los horrores bélicos.

El sistema personal de números naturales, más allá de los axiomas y las deducciones formales, se apoya en la estructura psicológica y en el entorno social. Su asimilación requiere un basamento previo cimentado por las experiencias más tempranas de la vida. Es un proceso condicionado por el lenguaje y la capacidad de imaginar, y está matizado por vivencias cotidianas de las cuales somos poco conscientes. Asimilar un concepto consiste en integrarlo –en mayor o menor grado– al resto del individuo.

Para el matemático activo su sistema de números naturales está en permanente ampliación y desarrollo. Recibe información y conocimientos adicionales que modifican la comprensión de $\mathbb{N}$. Y mediante elaboración creativa descubre propiedades o enfoques novedosos previamente desconocidos.

La sociedad sustenta las Matemáticas y como retribución recibe conceptos, herramientas e ideología que haciendo maromas en el andamiaje social participan en la educación, la tecnología, la ciencia e incluso –digo con justificado orgullo paternal– el arte. El objeto biológico elemental que aparentemente intermedia todas estas interacciones es la neurona. Los entramados de neuronas revelan una extraordinaria riqueza funcional y una sorprendente capacidad de adaptación.

En resumen, reconocemos en los sistemas de números naturales, como en las ideas matemáticas en general y en todo producto mental compartido de la vida social del ser humano, cuatro aspectos fundamentales:

*Individualidad.* Cada persona posee su propio sistema.

*Unicidad.* Al comparar dos individuos sus sistemas estos concuerdan notablemente.

*Diversidad.* No hay dos mentes con exactamente el mismo sistema de números.

*Dinamismo.* El sistema se modifica y amplía permanentemente.

Se ha logrado asociar áreas particulares del cerebro con determinadas funciones mentales, incluso con la habilidad matemática. Pero hasta ahora no ha sido posible aislar y circunscribir en la anatomía y la neurofisiología de una persona ningún *concepto específico*, en particular el concepto de sistema de números naturales. Es tentador especular que estos sistemas pudieran ser estructuras neuronales de ciclos y de arborescencias reconocibles por su particular topología y por la manera de incrustarse en el encéfalo. Madejas dotadas de topologías e interconexiones características y susceptibles a neurotransmisores, hormonas y otros elíxires neurales corresponderían con diversos artefactos mentales.

La naturaleza última de los números naturales se presta a controversia. Un enfoque –sugerido arriba– es que todas las ideas, incluidas todas las ideas matemáticas, emanan de la materia organizada y son esencialmente actividad cerebral. Los números naturales corresponderían con la existencia de cierto tipo de conexiones neuronales y con cierto patrón de actividad en estas. Aprender y asimilar un concepto consiste entonces en escuchar, conversar, discutir, leer, escribir, intercambiar, ejercitar, reflexionar y, en general, involucrarse –evitando, por favor, inútiles excesos– con los procesos vinculados al tema. Así se generan y robustecen conexiones neuronales apropiadas.

Otro punto de vista –diametralmente opuesto– es el platonismo clásico. Según este existiría una especie de universo paralelo colmado de felicidad y perfección donde moran las almas y los arquetipos de las ideas, dedicadas aquellas al goce supremo de contemplarlas idílicamente a estas. Allá se encontrarían en su forma más pura y acabada cada uno de los conceptos accesibles a la mente humana, incluyendo todo lo estudiado en esta cartilla. No existirían en realidad el aprendizaje o la creación sino un trabajoso protocolo de recuerdo mediante el cual el alma, prisionera de la cárcel que es el cuerpo, trémula implora por las ideas que en amorosa comunión y sin esfuerzo se entregaban en el paraíso momentáneamente perdido por transitar en este torpe mundo material. Desde aquel Edén baja hasta nosotros deslizándose por el tobogán de la compasión todo lo que ingenuamente creemos aprender o descubrir por esfuerzo propio.

Cualquiera sea el modelo favorito del lector, espero que la cartilla haya mostrado que se pueden presentar en forma novedosa incluso los temas más consolidados.

Oteyeva, Caracas, el 8 de Julio de 2007

# Índice Alfabético

## Referencias

[1]Baldor, Aurelio. *Aritmética*, Publicaciones Cultural, Mexico, 1962 (Hay numerosas reimpresiones).

[2]Bedoya Mejía, Lina M. *Peano, Lawvere, Peirce: Tres Axiomatizaciones de los Números Naturales*, Universidad del Tolima, Ibagué. 2003.

[3]Cohen, Leon W. and Ehrlich, Gertrude. *The structure of the Real Number System*, Van Nostrand, New York, 1963.

[4]Fefferman, Solomon. The Number Systems. Addison Wesley, Reading, Mass. 1964.

[5]Golovina, L. y Yaglom, I. *Inducción en la Geometría*, MIR, Moscú, 1976.

[6]Halmos, Paul R. *Teoría Intuitiva de los Conjuntos*, CECSA, México, 1965.

[7]Kelley, John L. *Topología General*, EUDEBA, Buenos Aires, 1965.

[8]Landau, Edmund. *Foundations of Analysis*, Chelsea, New York, 1951.

[9]Lang, Serge. *Analisis I*, Addison Wesley, Reading, Mass. 1968.

[10]Lawvere, F. William. *An Elementary Theory of the Category of Sets*, Proc. N. A. S. Vol. 52, 1964.

[11]Luque Arias, Carlos J. *El Concepto de Número Natural Según Giusseppe Peano*, Memorias XIII Encuentro de Geometría y I de Aritmética. Bogotá. 2002

[12]Oostra, Arnold. *El Concepto de Número Natural Según Charles S. Peirce*, Memorias XIII Encuentro de Geometría y I de Aritmética. Bogotá. 2002

[13]Oostra, Arnold. *Acerca Del Artículo On The Logic Of Number, de Charles S. Peirce*, Boletín de Matemáticas. Nueva Serie, Volumen X No. 1 (2003), pp. 13-20.

[14]Sominski, I. S. *Método de Inducción Matemática*, MIR, Moscú, 1975.

[15]Suppes, Patrick M. *Teoría Axiomática de Conjuntos*, Norma, Cali, 1968.

[16]Wikipedia, Axiomas de Zermelo-Fraenkel (consultado enero 29, 2008)