LA AXIOMATIZACION Y LOS NUMEROS NATURALES I

POR

EWALD BURGER

1.-INTRODUCCION.

Desde hace un siglo, existe la tendencia a reducir los diversos conceptos de la matemática a conceptos puramente lógicos. Basta recordar los nombres clásicos de DEDEKIND, CANTOR, FREGE, RUSSELL, ZERMELO, y los de los numerosos y famosos lógicos matemáticos de hoy en día, y considerar los muchos sistemas lógicos que se han construído, para ver el gran interés que hay por este problema de reducción.

Pertenecen a esta clase de sistemas también las diversas teorías axiomáticas de conjuntos, pues el concepto mismo de conjunto es de naturaleza puramente lógica. En efecto, un conjunto no es otra cosa que la extensión de una propiedad P, siendo el concepto de propiedad (o sea de atributo), y su correspondiente concepto linguístico de predicado, de naturaleza lógica y siendo posible a la visión extensional de los matemáticos identificar la extensión de una propiedad con la propiedad misma, se comprende que la reducción de los conceptos matemáticos a los de la teoría de conjuntos puede ser considerada como una reducción a la lógica. No teniendo tiempo para considerar en detalle los dichos sistemas formales de grandes lógicas y de la teoría de conjuntos, tenemos que dejar a un lado su descripción formal y el estudio detallado de sus cualidades formales. -

Describiremos, en cambio, en términos intuitivos, y en **principio** cómo se realiza esta reducción de las matemáticas a la teoría de conjuntos y, por tanto, a la lógica.

Para este fin es útil **distinguir** las disciplinas abstractas de la matemática de las disciplinas concretas. Las disciplinas abstractas definen sus conceptos fundamentales de manera implícita, es decir, por medio de un sistema de axiomas, sin decir cuáles son los objetos de que va a tratarse. Es bien conocido que la teoría de grupos habla de elementos - cualesquiera y cuya naturaleza no interesa. En cambio algunas disciplínas de la matemática, sobre todo las clásicas: Análisis (complejo o real) y la teoría de los números, intentan dar una definición o al menos una descripción explícita de sus conceptos fundamentales: a saber, los números (complejos, reales, racionales, naturales). Es verdad que en esas disciplinas también el procedimiento axiomático con sus definiciones implícitas se ha extendido mucho por ser muy cómodo y sencillo. Pero este procedimiento no es siempre completamente adecuado, al menos en la teoría de números, donde el sistema de PEANO, por ejemplo no puede aclarar en qué sentido existe la serie de los números naturales, y, por esto, no puede asegurar, en las - aplicaciones elementales (por ejemplo, al contar) que existe el cardinal del conjunto de los números naturales, o en qué sentido existe. Volveremos a este problema más tarde.

Es bastante claro que al desarrollar tales teorías abstractas sólo se suponen conocidos e intuitivamente comprendidos los conceptos lógicos, sobre todo los de la teoría de conjuntos. Vamos a considerar dos - ejemplos:

EJEMPLO 1.- Un grupo es un conjunto G en el cual está definida una operación binaria que a cada pareja ordenada (x,y) de elementos de G hace corresponder un elemento $xy \in G$; esta operación satisface además las condiciones siguientes:

(G1) $(xy)z = x(yz)$, para todo $x,y,z \in G$

(G2) existe $e \in G$ tal que $xe = ex = x$ para todo x G

(G3) para todo $y \in G$ existe y' G tal que $yy' = y'y = e$, donde e es el elemento definido en (G2).

EJEMPLO 2.- Un conjunto ordenado (o mejor dicho, completamente ordenado) es un conjunto G en el cual está definida una relación binaria R (es decir, para cada pareja ordenada (x,y) de elementos de G: la relación R tiene lugar, (xRy), ó la relación R no tiene lugar, (no(xRy)), tal que:

(O1) para todo $x,y \in G$, $xRy \Rightarrow$ no (yRx) (asimetría)

(O2) para todo $x,y,z \in G$, $(xRy, \Delta, y\ Rz) \Rightarrow (xRz)$ (transitividad)

(O3) para todo $x,y \in G, (x \neq y) \Rightarrow (xRy, \veebar\ yRx)$ (conectividad)

NOTA: Naturalmente, en lugar de asimetría podría exigirse irreflexividad: (O1') no (xRx), para todo $x \in G$. En efecto, suponiendo esta irreflexividad, la simetría se demuestra de la manera siguiente: xRx, yRx, implica, por (O2); xRx; recíprocamente, suponiendo la simetría, xRx es imposible.

Habiendo subrayado en estas dos definiciones los conceptos y nociones necesarios para comprenderlas, vamos a analizarlos: por una parte, encontramos los conceptos lógicos $\sim$(no), $\wedge$ (y), $\vee$ (ó), $\Rightarrow$ (implica = si... entonces ...), llamados functores de la lógica de predicados; además encontramos las expresiones: "existe ... tal que " , " para todo ...", llamadas cuantores o cuantificadores de la lógica de predicados, y el signo = (igual a; designa identidad); por otra parte, encontramos los conceptos fundamentales de la teoría de conjuntos: conjunto, elemento de, así como también los conceptos de relación, pareja ordenada, operación. - Finalmente aparecen las locuciones: "está definido", "tiene lugar", las cuales, como vamos a ver, no son necesarias para comprender las definiciones anteriores, y apenas sirven como ornamento linguístico para subrayar y destacer algunos detalles de los otros conceptos.

Los conceptos de relación binaria, ternaria, etc., son puramente lógicos, y de la misma naturaleza del de propiedad o atributo unitario extendido a varias variables, a saber: atributo binario, ternario, - etc., esto quiere decir: un predicado es el nombre de un atributo; predicado es un producto linguístico para designar un atributo (propiedad, relación).

El atributo (propiedad o relación) señalado por el predicado es la significación de este predicado. Como en el caso de **propiedad,** se puede considerar la extensión de una relación binaria, ternaria, etc., a saber: el conjunto de todas las parejas ordenadas (x,y) de elementos, x,y, que se encuentran en esta relación binaria, respectivamente, el conjunto de todas las triplas (ternas) ordenadas (x,y,z) de **elementos** x,y,z, que se encuentran en esta relación ternaria, etc; y aceptando una vez más el punto de vista extensional, adecuado para las matemáticas, se pueden identificar las relaciones con sus extensiones, despues de lo cual las relaciones se consideran simplemente como conjuntos, a saber, conjuntos cualesquiera de parejas ordenadas, de ternas ordenadas, etc. Luego es claro también que la locución "la relación R tiene lugar entre x e y " no quiere decir más que: $(x,y)\in R$ (es decir: la pareja ordenada (x,y) es elemento de (la extensión de) la relación R). Por otra parte, a la noción de relación se pueden reducir las nociones de función y de operación. He aquí las definiciones correspondientes:

DEFINICION 1.1.- Sea R una relación binaria. Al conjunto

$$\mathcal{Q}(R) = \{x / \text{ existe } y,\ (x,y)\in R\}$$

se le llama el domino o predominio de la relación R. Al conjunto

$$\wp(R) = \{y / \text{ existe } x,\ (x,y)\in R\}$$

se le llama el codominio o **postdominio** de la relación R.

DEFINICION 1.2.- Una relación binaria R es una función con dominio de argumentos A y dominio de valores B si, y sólo si:

$$\text{(F1)}\quad \mathcal{Q}(R) = A, \wedge, \wp(R) \subseteq B$$

$$\text{(F2)}\quad (x,y)\in R, \wedge, (x,y')\in R \Rightarrow y = y'$$

En este caso se acostumbra escribir: $R: A \rightarrow B$, lo cual se lee: R es una función (o aplicación) de A en B. Algunos llaman al conjunto de argumentos A la fuente de R y al dominio de valores B, la meta de R.

DEFINCION 1.3.- R es una operación definida sobre G si, y sólo si, R es una función con dominio de argumentos GxG (conjunto de todas las parejas ordenadas (x,y) con $x,y\in G$) y dominio de valores G.

Ahora bien, si R es una función, escribimos

$$y = R(x) \iff (x,y) = (x,R(x)) \in R.$$

Así, por ejemplo, si R es una función con conjunto de argumentos $A_1 x A_2$, entonces

$$z = R(x,y) \iff ((x,y),z) \in R, \qquad (x,y) \in A_1 x A_2$$

Con estas definiciones es fácil ver que las locuciones: "está definida", " con las condiciones siguiente", son superfluas.

DEFINICION 1.4.- Un grupo es una pareja (G,F) donde G es un conjunto, F una operación binaria, y

(G1) para todo $x,y,z \in G: (F(F(x,y),z) = F(x,F(y,z)))$

(G2) existe $e \in G$: (para todo $x \in G: (F(x,e) = F(e,x) = x)$

(G3) para todo $x \in G$, esiste $x' \in G: (F(x,x') = F(x',x) = e)$

De manera análoga, un conjunto ordenado es una pareja ordenada (G,R), donde G es un conjunto y R es una relación binaria tal que $\mathcal{Q}(R) \subseteq G$, $\mathcal{R}(R) \subseteq G$ y (O1),(O2),(O3).

Quedan por analizar los conceptos de pareja ordenada, terna ordenada, etc, y, naturalmente, cabe preguntar por la naturaleza de estos conceptos. ¿Pueden reducirse al simple concepto de conjunto? En particular ¿cómo puede expresarse lo de "ordenado" sin utilizar el concepto de número natural? En primer lugar, es evidente que el concepto de pareja no ordenada es un concepto de la teoría pura de conjuntos. Damos en seguida su definición y la de algunos otros conceptos.

DEFINICION 1.5.- a) Se llama conjunto vacío al conjunto

$$\phi = \{z \,/\, z \neq z\}$$

b) Se llama conjunto unitario a un conjunto de la forma

$$\{x\} = \{z \,/\, z = x\}$$

c) Una pareja no ordenada será, por definición, un conjunto de la forma

$$\{x,y\} = \{z \,/\, z = x, \vee, z = y\}.$$

NOTA: Si en una pareja no ordenada $\{x,y\}$ tenemos $x = y$, entondes $\{x,y\} = \{x\}$; en efecto: $\{x,y\} = \{z/z = x, \vee, z = y\} = \{z/z = x, \vee, z = x\} = \{z/z = x\} = \{x\}$.

Regresando al concepto de pareja ordenada vamos a presentar la reduccion del concepto de pareja ordenada al de pareja no ordenada, reducción, desarrollada por WIENER y KURATOWSKI. He aquí la definición de pareja ordenada:

DEFINICION 1.6.- $(x,y) = \{\{x\}, \{x,y\}\}$

Esta definición se justifica por el teorema siguiente que demuestra la cualidad característica de pareja ordenada a saber:

<u>TEOREMA</u> 1.1.- $\{\{x\}, \{x,y\}\} = \{\{x'\}, \{x',y'\}\} \Leftrightarrow x = x', \wedge, y = y'$.

DEMOSTRACION: La implicación de derecha a izquierda es trivial, porque con la hipótesis: $x = x', \wedge, y = y'$, los dos conjuntos de la izquierda tienen los mismos elementos y por esto son iguales. En detalle, se han de considerar dos pasos: primero se deduce como arriba que $\{x\} = \{x'\}$, y que $\{x,y\} = \{x',y'\}$; con esto se ve que los dos conjuntos del teorema tienen en efecto los mismos elementos.

Recíprocamente, supongamos que $\{\{x\},\{x,y\}\} = \{\{x'\},\{x',y'\}\}$. Entonces distingamos dos casos: a) $x \neq y$. Como según la hipótesis x,y es un elemento de $\{\{x'\},\{x',y'\}\}$, debe ser igual a $\{x'\}$ ó a $\{x',y'\}$; como $x \neq y$, no puede ser $\{x,y\} = \{x'\}$; por lo tanto, $\{x,y\} = \{x',y'\}$ y, por consiguiente, $x' \neq y'$. Análogamente, $\{x\}$ es un elemento de $\{\{x'\},\{x',y'\}\}$ y, por tanto, deber ser igual a $\{x'\}$, de donde $x = x'$. Entonces resulta de la igualdad $\{x,y\} = \{x',y'\}$ que: $y = x', \vee, y = y'$. Pero $y = x'$ es imposible, porque $x = x'$ y $y \neq x$. Por tanto, resulta $y = y'$.

b) $x = y$. Entonces $\{x,y\} = \{x\}$ y, por consiguiente, $\{\{x\},\{x,y\}\} = \{\{x\}\}$. Tomemos pues por hipótesis: $\{\{x\}\} = \{\{x'\},\{x',y'\}\}$. De aquí resulta $\{x'\} = \{x',y'\} = \{x\}$, o bien, $x' = y' = y = x$.

Después de haber dado esta definición de pareja ordenada, es posible dar una definición adecuada de terna, ordenada, etc., a saber:

DEFINICION 1.7.- $(x,y,z) = (x,(y,z))$

Según esta definición tendremos el teorema siguiente:

TEOREMA 1.2.- $(x,y,z) = (x',y',z')$ $x = x'$, $,y = y'$, $z = z'$.

DEMOSTRACION: $(x,(y,z)) = (x',(y',z')) \Leftrightarrow x=x', \wedge, (y,z) = (y',z') \Leftrightarrow x = x', \wedge, y = y', \wedge, z = z'$, como queríamos demostrar.

Por este procedimiento de KURATOWSKI - WIENER se logra finalmente una reducción de los conceptos fundamentales de nuestros ejemplos a los conceptos de la teoría de conjuntos, y, evidentemente, es posible la misma reducción para otros ejemplos del mismo género y para las teorías - abstractas de la matemática en general.

Dirijámonos, pues, a las teorías concretas de la matemática, es decir el análisis y la teoría de números. Aquí surge el interesante problema de la reducción del concepto de número a los conceptos de la teoría de conjuntos. Es bien conocido cómo se efectúa tal reducción para los números complejos, reales, racionales y enteros, utilizando en esta reducción el concepto de número natural, a saber:

DEFINICION 1.8.- a) Número complejo $\underline{\underline{df}}$ pareja ordenada de números reales.

b) Número real $\underline{\underline{df}}$ cortadura de DEDEKIND en los números racionales.

c) Número racional $\underline{\underline{df}}$ clase de parejas de números enteros.

d) Número entero $\underline{\underline{df}}$ clase de parejas de números naturales.

Naturalmente, lo primero que se debe definir es número entero como clase de parejas de números naturales, siendo los miembros de cada pareja minuendo y sustraendo, y representando las parejas de esta clase diferencias iguales. Luego, los números racionales se definen como clases de parejas de números enteros, siendo los miembros de cada pareja numerador y denominador, y representando las parejas de la misma clase, quebrados iguales. Después, como es sabido podemos definir un número real como una cortadura de DEDEKIND; recordemos que una tal cortadura es una partición del conjunto Q de los números racionales en dos clases C_1 , C_2 siendo C_1 la parte inferior de la cortadura y C_2 la parte superior; más formalmente, la definición de cortadura de DEDEKIND se escribe así:

$$\text{CORTADURA} = \{C_1, C_2\} \text{ donde } C_1 \subseteq Q, C_1 \neq \phi, \ C_2 \subseteq Q, C_2 \neq \phi, C_1 \cap C_2 = \phi,$$
$$C_1 \cup C_2 = Q; \ \rho \in C_1, \wedge, \rho' < \rho \Rightarrow \rho' \in C_1; \ \rho \in C_2, \wedge, \rho' > \rho \Rightarrow \rho' \in C_2.$$

Es claro que para comprender esta definición formal sólo necesitamos conocer las nociones de la teoría de conjuntos y de los números racionales con su orden.

Por último, un número complejo se define como una pareja de números reales.

Después de recordar las reducciones de las diversas clases de números a los números naturales (en definitiva) cabe preguntar por la naturaleza de éstos. Esta interesante pregunta sobre la naturaleza de los números naturales constituye el problema principal de nuestras conferencias, y vamos a ocuparnos de ella a continuación.

Es claro que hacemos más precisa la pregunta al ponerla en la forma siguiente: Es posible dar una definición del concepto de número natural utilizando solamente los conceptos de la teoría pura de conjuntos?

2.-NUMEROS NATURALES Y CONJUNTOS.

DEFINICIONES RECURRENTES.

Fué DEDEKIND quien dió una respuesta afirmativa a la última pregunta formulada en el parágrafo anterior en su famosa memoria "Was sind und was sollen die Zahlen": Construyó una teoría de los números naturales utilizando como base sólo la teoría de conjuntos. Otras teorías semejantes fueron desarrolladas por FREGE, RUSSELL, CANTOR, ZERMELO y V.NEUMANN, algunas basadas en la teoría de los números cardinales, otras en la de los números ordinales.

Como los números ordinales según el procedimiento de V. NEUMANN se pueden trasladar más fácilmente de la teoría intuitiva de conjuntos a la moderna teoría axiomática, consideremos solamente las teorías de números naturales basadas en números ordinales.

Comencemos por una versión de la teoría de CANTOR - ZERMELO, en la cual los números naturales se definen como los números ordinales finitos.

Naturalmente, sobre todo aquí, se trata de dar una caracterización de la finitud de los números ordinales sin utilizar el concepto de número natural, Si, en cambio, supusiéramos conocida la serie de los números naturales: 0, 1, 2, 3,..., entonces los números ordinales finitos se caracterizarían como los tipos de orden de los segmentos de esta serie determinados por sendos elementos, y eso de la manera siguiente: el tipo de orden del segmento determinado por n, es decir: $0, 1, \ldots, n-1$, es precisamente el número ordinal finito que vamos a identificar con el número natural n. Pero se puede demostrar el siguiente teorema que da una caracterización de los tipos de orden de los dichos segmento de la serie de los números naturales sin utilizar en esta caracterización el concepto de número natural:

TEOREMA 2.1.- Un conjunto ordenado $(G,<)$ tiene el mismo tipo de orden de un segmento $0, 1, \ldots, n-1$ de la serie de los números naturales si, y sólo si, $(G,<)$ es doblemente bien ordenado, es decir: cada subconjunto no vacío de G contiene un elemento mínimo y un - elemento máximo con respecto al orden $<$ definido sobre G.

DEMOSTRACION: Evidentemente, cada segmento $0, 1, \ldots, n-1$ de la serie de los números naturales es doblemente bien ordenado; por tanto, todo otro conjunto con el mismo tipo de orden es un conjunto doblemente bien ordenado.

Recíprocamente, supongamos $(G,<)$ un conjunto doblemente bien ordenado, no vacío. Consideremos el subconjunto H G de todos los elementos g G que tienen la propiedad siguiente: el conjunto

$$A_g = \{ g' \in G / g' \leq g \}$$

considerado con el orden $(<)$ inducido por G, es decir, el conjunto ordenado $(A_g, <)$, tiene el mismo tipo de orden de un segmento de la serie de los números naturales. H no es vacío, porque el elemento mínimo $g_0 \in G$ determina un subconjunto $A_{g_0} = \{g_0\}$ de H, tal que $(A_{g_0}, <)$

tiene el mismo tipo de orden del segmento determinado por el número 1 en la serie de los números naturales. A causa del doble buen orden de $(G,<)$, hay un elemento máximo $\hat{g}\in H$. Afirmamos que g es el elemento **máximo** de G; pues en caso contrario, existiría un elemento mínimo g_o entre los elementos de G mayores que $\hat{g}$. Entonces $A_{\hat{g}_o} = A_{\hat{g}} \cup \{\hat{g}_o\}$, y siendo $(A_{\hat{g}},<)$ del tipo de orden de un segmento $0,1\ldots,n-1$ de la serie de los números naturales, $(A_{\hat{g}_o},<)$ será del tipo $0,1\ldots,n-1,n$ y por tanto $\hat{g}_o \in H$, contrario a la elección de $\hat{g}$. Por tanto, $\hat{g}$ debe ser el elemento máximo de G, y por eso $A_{\hat{g}}= G$, es decir, $(G,<)$ es del tipo de orden de un segmento de la serie de los números naturales, como queríamos demostrar.

Si el conjunto G es vacío, evidentemente $(G,<)$ tiene el mismo tipo de orden del segmento vacío determinado por el número 0 en la serie de los números naturales.

Naturalmente la demostración del teorema 2.1 supone conocida la serie de los números naturales y sus propiedades. Pero ahora, si suponemos no conocida esta serie, tendremos la posibilidad de <u>definir</u> el concepto de número natural como el tipo de orden de un conjunto doblemente bien ordenado; y el teorema 2.1 nos dice que esta definición está conforme con el concepto intuitivo de número natural. Así pues:

<u>DEFINICION</u> 2.1.- Llamaremos número natural al tipo de orden de un conjunto doblemente bien ordenado.

Después de haber dado esta definición queda el problema de desarrollar la teoría basándose sólo en ella. Como es sabido esto origina, en primer lugar, la tarea de definir los conceptos de <u>cero</u> y de <u>sucesor</u>, y demostrar después la validez de los axiomas de PEANO. Las dos definiciones son fáciles de obtener de acuerdo con nuestro concepto intuitivo de número natural; a saber:

<u>DEFINICION</u> 2.2.- El número natural <u>cero</u> es, por definición, el tipo de orden del conjunto vacío. (Recuérdese que en el conjunto vacío sólo se puede definir un orden, el llamado <u>orden vacío</u>).

DEFINICION 2.3.- Sea $(G,<)$ un conjunto doblemente bien ordenado y llamaremos λ a su tipo. Entonces llamaremos sucesor de λ al tipo de orden λ' del conjunto $(G_1,<)$ que resulta añadiendo a $(G_1,<)$ un único elemento g' mayor que todos los elementos $g \in G$.

Evidentemente, esta última definición es unívoca: al tipo de orden λ' construído en ella no depende del conjunto ordenado $(G,<)$ ni del carácter especial del elemento g'. Pero aparece un pequeño problema en esta definición: ¿de dónde tomar el elemento g' que se debe añadir a G ? ¿Existe tal elemento g' fuera de cualquier conjunto G prefijado?

ZERMELO dió la demostración siguiente de la existencia de tal elemento g': Sea $G_o \subset G$ el subconjunto de todos los elementos de G tales que sean conjuntos y no sean elementos de sí mismos:

$$G_o = \{ g \in G / g \text{ es un conjunto}, \wedge\ , g \notin g \}.$$

$G_o \notin G_o$, porque en caso contrario $G_o \in G_o$, lo cual implica que $G_o \notin G_o$, es contradictorio. Supongamos ahora que $G_o \in G$; entonces, dado que $G_o \notin G_o$, tendríamos que $G_o \in G_o$, lo cual es también contradictorio. Así pues, $G_o \notin G$ y podemos tomar $g' = G_o$.

Naturalmente esta ingeniosa demostración de ZERMELO nos lleva de vuelta a la famosa paradoja de RUSSELL, la cual muestra la no existencia de un conjunto universal. Sin embargo esta demostración de ZERMELO sigue siendo válida en sistemas axiomáticos de la teoría de conjuntos en los cuales la paradoja de RUSSELL está eliminada.

Es fácil demostrar ahora los axiomas de PEANO:

TEOREMA 2.2.- a) 0 es un número natural.

b) El sucesor de un número natural es un número natural.

c) 0 no es sucesor de ningún número natural.

d) Números naturales con sucesores iguales son iguales.

e) Si una propiedad P es tal que la tiene 0, y que si la tiene el número natural n la tiene el sucesor de n, entonces la propiedad P la tienen todos los números naturales.

NOTA.- El principio e) de la inducción completa puede escribirse más formalmente así: Para todo conjunto de números naturales C tal que:

i) $0 \in C$

ii) para todo natural n: $(n \in C \Rightarrow n' \in C) \Rightarrow \left\{ \begin{array}{l} C \text{ es el conjunto de los} \\ \text{números naturales.} \end{array} \right.$

Demostración: a) el conjunto vacío con su único orden, a saber el orden vacío, es trivialmente doblemente bien ordenado, puesto que no posee ningún subconjunto no vacío.

b) Sea n un número natural cualquiera. Sea $(G, <) \in n$ cualquier conjunto ordenado del tipo de orden n. Sea $g' \notin G$ y $(G', <)$ el conjunto ordenado que resulta al añadir g' a $(G, <)$ como elemento máximo. Afirmamos que $(G', <)$ está también doblemente bien ordenado. En efecto: sea H' cualquier subconjunto no vacío de G'. El elemento mínimo de H' es el elemento mínimo en G de $H' \cap G$ si $H' \cap G \neq \phi$, o bien es g' si $H' \cap G = \phi$. El elemento máximo de H' es el elemento máximo de H' en G si $H' \subseteq G$, o bien es g' si $g' \in H'$; por tanto, $(G', <)$ es doblemente bien ordenado y n' es un número natural.

c) 0 no puede ser el sucesor de ningún tipo de orden, puesto que por definición el sucesor n' de un tipo de orden n es el tipo de orden de conjuntos ordenados no vacíos.

d) Demostremos la siguiente proposición más general; Si dos tipos de orden λ y μ tienen sucesores λ' y μ' iguales, entonces λ y μ son iguales.

En efecto: sean $(G, <) \in \lambda$ y $(H, \prec) \in \mu$ conjuntos ordenados cualesquiera de tipos de orden λ y μ, respectivamente; sean $g' \notin G$ y $h' \notin H$, y $(G', <)$ y $(H', \prec)$ los conjuntos ordenados que resultan al añadir g' a G y h' a H como elementos máximos. Puesto que $\lambda' = \mu'$ los conjuntos ordenados $(G', <)$ y $(H', \prec)$ son semejantes, es decir, existe una correspondencia biunívoca B entre G' y H' que conserva las relaciones de orden; como g' y h' son elementos máximos de G' y H' deben corresponderse mediante B. Así resulta al eliminar g' y h', la existencia de una correspondencia biunívoca entre G y H que conserva las relaciones de orden $<$ y $\prec$, lo cual implica que $(G, <)$ y $(H, \prec)$ son del mismo tipo y, por tanto, $\lambda = \mu$.

e) Sea C un conjunto cualquiera de números naturales con las propiedades:

$0 \in G$

para todo natural n: $(n \in C \Rightarrow n' \in C)$

Tenemos que demostrar que todo número natural pertenece C. Sea n cualquier número natural $\neq 0$ y $(G,<)\in n$ (por tanto, $G\neq\emptyset$). A cada elemento $g\in G$ asignémosle el conjunto

$$A_g = \{ g'\in G / g' \leq g \}$$

Sea $H\subset G$ definido por

$$H = \{ g\in G / (A_g, <) \in C \}$$

H no es vacío, porque si g_o es el elemento mínimo de G, entonces $(\{g_o\}, <)\in C$, puesto que $(\{g_o\}, <)\in O'$; luego $g_o\in H\neq\emptyset$. A causa del doble buen orden de G hay un elemento máximo $\hat{g}\in H$. Afirmamos que $\hat{g}$ es elemento máximo de G. En caso contrario, existiría $\hat{g}_o$ mínimo entre los elementos de G mayores que $\hat{g}$. Entonces si $A_{\hat{g}_o} = A_{\hat{g}}\cup\{\hat{g}_o\}$, el tipo de orden de $(A_{\hat{g}_o}, <)$ sería el sucesor del tipo de orden de $(A_{\hat{g}}, <)$ y como g H, el tipo de $(A_{\hat{g}}, <)$ pertenece a C, y por las hipótesis sobre C, también el tipo de $(A_{\hat{g}_o}, <)$ estaría en C, es decir, $\hat{g}_o\in H$, contrario a la elección de $\hat{g}_o$. Por lo tanto, $\hat{g}$ debe ser el elemento máximo de G. Y por eso $A_{\hat{g}} = G$, o lo que es lo mismo, el tipo de orden de $(G,<)$ pertenece a C; es decir, $n\in C$.

Evidentemente esta demostración es un traslado de la del teorema 2.1, reemplazando en aquella el concepto intuitivo de número natural por el de número natural en el sentido de nuestra definición formal. Observemos, además, que en la demostración del teorema 2.2. no se supone conocido ningún teorema sobre los tipos de orden ni sobre los números ordinales. Puede presumirse que su demostración se abreviaría utilizando teoremas convenientes sobre los números ordinales; sobre todo parece posible basar la demostración del principio de inducción completa en el teorema de <u>inducción transfinita</u>, es decir, en el <u>buen orden de la clase de los números ordinales</u>.

En efecto, recordemos las definiciones y teoremas pertinentes: Sea $(G,<)$ un conjunto ordenado, $g\in G$ arbitrario. La cola decreciente determinada por g es el conjunto ordenado

$$(\{ g'\in G / g' < g \}, <)$$

Un tipo de orden λ es <u>menor que</u> un tipo de orden μ, $\lambda<\mu$, si λ es el tipo de orden de una cola decreciente determinada por algún elemento en un conjunto ordenado del tipo μ. Esta relación $<$ entre números ordinales (es decir, entre tipos de buen orden) es una relación de buen orden.

Utilizando esto, la demostración de e) se puede efectuar de la manera siguiente: Admitamos que existe un número natural fuera de C. Entonces, por el buen orden de la clase de los números ordinales hay un mínimo número natural m fuera de C; es claro que $m \neq 0$ (porque, $0 \in C$), y por eso existe un elemento máximo en un conjunto ordenado de tipo m . La cola correspondiente a este elemento máximo es también doblemente bien ordenada, y por eso su tipo de orden es un número natural $n < m$, y $m = n'$; dado que entonces, por hipótesis, $m \in C$, lo cual es contrario a la elección de m; y por tanto, no existe ningún número natural m fuera de C.

Por lo demás, utilizando la relacipn $<$ entre números ordinales y la siguiente propiedad: Cada número ordinal λ es el tipo de orden del conjunto de números ordinales λ en su orden natural, se tiene el resultado siguiente: <u>Cada número natural n es el tipo de orden del conjunto de los números naturales $<$ n en su orden natural</u>. Con eso hemos logrado la solución con la idea intuitiva de la cual partimos, a saber, concebir el número natural n como el tipo de orden del segmento 0,1,...,n - 1.

De manera análoga, muchos teoremas de la teoría de los números naturales podrían demostrarse utilizando convenientes teoremas generales sobre los números ordinales; pero, por otro lado, es bien conocido cómo se desarrolla la teoría de los números naturales basándose sólo en los axiomas de PEANO y sin ninguna referencia a la teoría general de números ordinales; tal desarrollo se encuentra en la memoria citada de DEDEKIND y sobre todo en el conocido libro de LANDAU: Grundlagen der Analysis. Pero si se acepta la definición de número natural que acabamos de dar, entonces será más conveniente en el desarrollo ulterior de la teoría utilizar la definición explícita de número natural en algunos casos y en otros conveniente la teoría general de los números ordinales. Es claro que tal proceder abreviará de manera decisiva muchas de las demostraciones usuales que estriban sólo en los axiomas de PEANO. Vamos a considerar un ejemplo.

Hemos visto arriba cómo la relación $<$ entre números ordinales induce inmediatamente el ordenamiento natural $<$ de los números naturales. Esta relación de orden es el medio más sencillo para la demostración del importante teorema sobre la posibilidad de <u>definir recurren-</u>

temente; en primer lugar, basta considerer el caso especial, llamado teorema de iteración, a saber:

TEOREMA 2.3.- Sea X un conjunto arbitrario, $x_o \in X$ arbitrario, $F:X \to X$ una función arbitraria, N el conjunto de los números naturales. Entonces existe una única función $G:N \to X$ con las propiedades:

$$\text{(I1)} \quad G(0) = x_o$$
$$\text{(I2)} \quad \text{para todo } n \in N: G(n') = F(G(n))$$

NOTA: Tomando $X = N$, $x_o = m_o \in N$, $F:N \to N$ como $F(n) = n'$, se obtiene una función $G:N \to N$ con: $G(0) = m_o$, $G(n') = (G(n))'$; es decir, esta función puede servir para introducir la adición: $G(n) = m_o + n$.

Si se toma $X = N$, $x_o = 0 \in N$, $F:N \to N$ como $F(n) = n_o + n$, se obtiene una función $G:N \to N$ con: $G(0) = 0$, $G(n') = n_o + G(n)$; es decir, esta función G puede servir para introducir la multiplicación: $G(n) = n.n_o$

DEMOSTRACION DEL TEOREMA: La unicidad de G, fácilmente por induccion completa. Sean G_1, G_2, dos funciones con las propiedades características del teorema 2,3. Considerando el conjunto $M = \{n \in N \,/\, G_1(n) = G_2(n),\}$ se ve inmediatamente que $0 \in M$ y que para todo $n \in N$, $n \in M \Rightarrow n' \in M$; por esto, $M = N$, o sea $G_1 = G_2$.

El problema real es la existencia de una función G con las propiedades deseadas. Utilizando el ordenamiento natural de los números naturales y teniendo en cuanta que 0 es el mínimo elemento de N, para este orden, y n' el mínimo elemento de N mayor que n, la existencia de G se puede demostrar de la manera siguiente: para cada $n \in N$ sea

$$A_n = \{m \in N / \ m \leq n\};$$

consideremos el conjunto $M \subseteq N$ de todos los números naturales n con la propiedad siguiente: existe una función $H_n : A_n \to X$ con las propiedades:

$$(a)\ H_n(0) = x_o$$

$$(b)\ \forall m \in N : (m' \leq n \Rightarrow H_n(m') = F(H_n(m)).)$$

Vamos a mostrar que $M = N$ por induccion completa. Evidentemente $0 \in M$ porque $A_o = \{0\}$ y la función $H_o: A_o \rightarrow N$ definida por $H_o(0) = x_o$ tiene las propiedades deseadas, por cuanto no existen elementos $m \in N$ con $m' \leq 0$. Sea $n \in M$ y $H_n: A_n \rightarrow X$ una función que satisface a (a) y (b); entonces la función $H_n: A_{n'} \longrightarrow X$ definida por

$$H_{n'}(m) = \begin{cases} H_n(m) & \text{para } m \leq n \\ F(H_n(n)) & \text{para } m = n' \end{cases}$$

posee evidentemente las propiedades deseadas. Por eso, $n' \in M$, y $M = N$. Además, para cada n la función H_n correspondiente es <u>única</u>, como se ve mediante una demostración análoga a la de la unicidad de la función G. Entonces resulta para $n \leq M$;

$$H_n(v) = H_m(v), \text{ para todo } v \in A_n$$

ya que la función $H_m | A_n$ posee también las propiedades características de la función H_n.

Finalmente, la función buscada G se define por $G(n) = H_n(n)$. En efecto, G así definida tiene las propiedades deseadas.

Del <u>teorema de iteración</u> se deduce fácilmente la posibilidad de otras formas más generales de definiciones recursivas. Así:

<u>TEOREMA</u> 2.4 Sea X un conjunto arbitrario, N el conjunto de los números naturales, $N \times X$ el conjunto producto, $F: N \times X \rightarrow X$ una función, $x_o \in X$ arbitrario, Entonces existe una única función $G: N \rightarrow X$ con las propiedades:

$$(a)\ G(0) = x_o$$

$$(b)\ \forall_n \in N : G(n') = F(n, G(n))$$

NOTA: Tomando $X = N$, $x_o = 0'$, $F(n,x) = N'.x$, se obtiene una función G que se escribe ordinariamente $G(n) = n!$

Demostración del teorema: Sea: $N \times X \rightarrow N \times X$ la función definida por $\Phi(n,x) = (n', F(n,x))$; en virtud del teorema 2,3, existe una función $G^x : N \rightarrow N \times X$ con las propiedades:

$$G^x(0) = (0, x_o);$$
$$\forall n \in N : G^x(n') = \Phi(G^x(n))$$

Afirmamos que el dominio de valores de G^x es la buscada función G. En efecto: por inducción completa se ve inmediatamente que para cada $n \in N$ el valor $G^x(n)$ es una pareja ordenada cuyo primer miembro es n y cuyo segundo miembro es un elemento de X. Por esto el dominio de valores $\wp(G^x)$ es una función $G{:}N \rightarrow X$, es decir, $G^x(n) = (n, G(n))$, y esta función G tiene las propiedades deseadas, a saber:

$$G(0) = x_o, \text{ puesto que } G^x(0) = (0, x_o) \in \wp(G^x)$$

$$G(n') = F(n, G(n)), \text{ puesto que } G(n') = \Phi(G^x(n))$$
$$= (n, G(n)) = (n', F(n, G(n))) \in \wp(G^x)$$

La unicidad tiene una demostración idéntica a la del teorema 2.3.

TEOREMA 2.5.- Sean N el conjunto de los números naturales, y para cada n, $A_n = \{ v \in N \,/\, v \leq n \} \subset N$. Sean X un conjunto arbitrario y $x_o \in X$. Sea $\hat{X}$ el conjunto de todas las funciones $A_n \rightarrow X$, para todo n. Sea $F{:}\,\hat{X} \rightarrow X$ una función arbitraria. Entonces existe una única función $G{:}N \rightarrow X$ con las propiedades:

$$G(0) = x_o$$
$$G(n') = F(G \mid A_n)$$

donde, como de costumbre, $G \mid A_n$ designa la función obtenida por la restricción de G a A_n.

DEMOSTRACION: La unicidad de G se demuestra análogamente al caso del teorema 2.3. En efecto: sean G_1, G_2, dos funciones con las -

propiedades exigidas; vamos a demostrar por inducción sobre n, que para todo n: $G_1 | A_n = G_2 | A_n$. Para $n = 0$, la afirmación es trivial. Supongamos que para algún n, $G_1 | A_n = G_2 | A_n$; entonces $G_1(n') = F(G_1 | A_n) = F(G_2 | A_n) = G_2(n')$, y teniendo en cuenta que $A_{n'} = A_n \cup \{n'\}$, se sigue que $G_1 | A_{n'} = G_2 | A_{n'}$, completandose la inducción.

La Existencia se demuestra mediante el teorema de iteración: sea $\hat{F}: \hat{X} \longrightarrow \hat{X}$ definida por $\hat{F}(f) = \hat{f}$, donde

$$\hat{f}(v) = \begin{cases} f(v) & \text{si } v \leq n \\ F(f) & \text{si } v = n' \end{cases}$$

para $f: A_n \rightarrow X$; resulta pues que $\hat{f}$ es una aplicación de $A_{n'}$ en X. Por el teorema 2.3, existe una función $\hat{G}: N \rightarrow \hat{X}$ con las propiedades $\hat{G}(0) = f_o$, donde $f_o: A_o = \{0\} \longrightarrow X$, $f_o(X_o) = 0$; y $\hat{G}(n') = \hat{F}(\hat{G}(n))$. Por inducción sobre n se ve inmediatamente que $\hat{G}(n) \in X^{A_n}$ y que además: $m \leq n \Longrightarrow \hat{G}(m) = \hat{G}(n) | A_m$. En efecto: para $n = 0$ se sigue que $m = 0$, y la afirmación es trivial; supongamos que la afirmación es verdadera para algún n: entonces, si $m \leq n'$, tenemos, para $m = n'$ que $\hat{G}(n') | A_{n'}$ trivialmente; para $m \leq n$, se tendrá, por hipótesis de inducción que $\hat{G}(m) = G(n) | A_m$; como $\hat{G}(n') = \hat{F}(\hat{G}(n))$, se tendrá $\hat{G}(n') | A_n = \hat{G}(n) | A_n$, y a fortiori, $\hat{G}(n') | A_m = G(n) | A_m$. Así, pues, $\hat{G}(m) = \hat{G}(n') | A_m$, completándose la inducción.

Ahora poniendo $G(n) = \hat{G}(n)|(n)$, se ve fácilmente que:

$$G(0) = \hat{G}(0) | (0) = f_o(0) = x_o$$

y

$$G(n') = \hat{G}(n')|(n) = \hat{F}(\hat{G}(n))|(n') = F(\hat{G}(n)) = F(G | A_n),$$

la última igualdad resultando de que:

$$m \leq n \Longrightarrow G(m) = \hat{G}(n)|(m)$$

es decir, $\hat{G}(n) = G | A_n$.