24
2ej

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMATICAS

DE LA TEORIA DE ESTRATOS A LAS ESTRUCTURAS MATEMATICAS A TRAVES DE LA TEORIA DE CONJUNTOS.

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A :

CESAREO PALOMINO LOPEZ

CIUDAD UNIVERSITARIA 1993

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INDICE

INTRODUCCION ---------- 1

CAPITULO 1. La Teoría de Estratos ---------- 4

1.1 Introducción ---------- 4
1.2 Axiomas de la Teoría de Estratos ---------- 5
1.3 La Teoría de Conjuntos de Zermelo-Fraenkel ---------- 7

CAPITULO 2. Los Números Naturales ---------- 13

2.1 Clases, Sistemas de Peano y Conjuntos Inductivos ---------- 13
2.2 Unicidad de los Sistemas de Peano ---------- 17
2.3 Relaciones de Orden ---------- 21
2.4 Orden en los Números Naturales ---------- 24
2.5 Axiomas de Peano y la Aritmética de los Números Naturales ---- 30

CAPITULO 3. Los Números Enteros ---------- 36

3.1 Algunas Propiedades Adicionales de $\mathbb{N}$ ---------- 36
3.2 Los Números Enteros y su Orden ---------- 36
3.3 La Aritmética de los Números Enteros ---------- 40
3.4 Unicidad de los Números Enteros ---------- 42
3.5 Los Enteros como Clases de Equivalencia ---------- 45

CAPITULO 4. Los Números Racionales ---------- 47

4.1 Los Números Racionales como Clases de Equivalencia ---------- 47
4.2 El Orden en $\mathbb{Q}$ ---------- 48
4.3 La Aritmética de $\mathbb{Q}$ ---------- 50
4.4 Conjuntos Numerables ---------- 52
4.5 La Unicidad de los Números Racionales ---------- 57

CAPITULO 5. Los Números Reales ---------- 61

5.1 Definición y Propiedades de los Números Reales ---------- 61
5.2 El Orden de los Números Reales ---------- 62
5.3 Unicidad de los Números Reales ---------- 65
5.4 La Aritmética en los Números Reales ---------- 66

CAPITULO 6. Otras Estructuras Matemáticas ---------- 76

6.1 Grupos, Campos y Espacios Vectoriales ---------- 76
6.2 Espacios Topológicos ---------- 78
6.3 Categorías ---------- 79

BIBLIOGRAFIA ---------- 84

INTRODUCCION

Este trabajo se ha concebido como una unificación de una variedad de temas que se cubren en diferentes materias de la carrera de Matemático en la Facultad de Ciencias de la UNAM, es decir, muchos de los temas que se presentan aquí son objeto de estudio durante la carrera, pero nunca en un solo curso. Por ejemplo, los capítulos 3 y 4 que tratan, respectivamente, sobre los números enteros y sobre los racionales se estudian en los cursos de Algebra Superior ; algunos profesores que imparten Cálculo Diferencial e Integral o Análisis Matemático incluyen una parte del material del capítulo 5 sobre los números reales; por otro lado, la definición y las propiedades de los Números Naturales como consecuencia directa de la Teoría de Conjuntos (capítulo 2) se estudian, con algunas variantes, en las materias también llamadas Teoría de los Conjuntos.

Además de lo anterior, una inquietud particular de quien esto escribe ha sido la de observar a los objetos matemáticos desde la óptica de la Teoría de Conjuntos. El interés nace cuando se aprende que en el estudio de la Matemática se es lo más económico posible, en el sentido de que se pretende elaborar teorías a partir de un mínimo de material (axiomas, postulados, etc.) y, desde luego, con el mínimo esfuerzo. El primer material de construcción fueron los conjuntos, con ellos se comprobó que puede construirse una parte considerablemente grande del "edificio" de la Matemática; de hecho, este material continúa presentándose en casi todas (seguramente en todas) las áreas; así que la pregunta surge de manera natural: de los objetos y estructuras de la Matemática ¿qué tanto puede obtenerse a partir de los conjuntos?. A lo largo de este trabajo queda en evidencia que podemos construir casi todos los objetos y estructuras elementales y se muestra también un ejemplo de un concepto de amplia utilización en álgebra que no se sigue de la Teoría de Conjuntos: la Teoría de las Categorías. Aunque existe un concepto de Categoría que sí cabe dentro de la Teoría de Conjuntos, resulta ser que los ejemplos interesantes de Categorías (la de Conjuntos, Grupos, Campos, etc.) siguen manteniéndose fuera aún de esa otra definición.

Por otro lado, el capítulo 1, que versa sobre la Teoría de Estratos es la respuesta a otra inquietud: ¿se pueden construir los conjuntos empleando objetos más elementales?. La respuesta es sí, pero este estudio parece ser más interesante para la filosofía que para la Matemática y la razón parece intuirse: en casi toda la Matemática, la que desarrollan los Matemáticos y aquella de la que se sirven los ingenieros, científicos, etc., no se habla de objetos más sencillos que los conjuntos. También en este capítulo se hace una derivación de los axiomas de Zermelo-Fraenkel de la Teoría de Conjuntos a partir de los de la Teoría de Estratos, se deducen la mayoría de ellos, inluyendo el axioma de regularidad o de buena fundación y se menciona que aún cuando éste sea una consecuencia de la Teoría de Estratos solo ahí se le trabaja puesto que en su momento se observará que su empleo no es

necesario para los desarrollos subsecuentes. Además, nunca se habla del Axioma de Elección, primero porque no se puede extraer como un resultado de la Teoría de Estratos; de hecho si se le trata de deducir se observará una circularidad; es decir, en el intento de deducirlo se lo está utilizando de una manera sutil; más específicamente, cuando se busca el estrato en el cual pretende ubicarse la función de elección se usa elección en el proceso de encontrarlo. En segundo lugar, el Axioma de Elección no se requiere para los fines que se persiguen en este trabajo, sin embargo, su uso en la mayoría de las estructuras que se presentan permite alcanzar resultados interesantes, es por ello que gran parte de los matemáticos lo emplean, además de su (casi) autoevidencia.

En lo que respecta a la forma en que se ha escrito el texto de este trabajo cabe aclarar que, en su mayor parte, es autocontenido, se incluyen todos los conceptos que se requieren para la comprensión del material desarrollado, de manera que no es necesario consultar otras fuentes excepto quizás en alguna parte que en su momento se señala. Además, un nuevo concepto no se introduce hasta que se lo necesita, de manera que si bien pudiera parecer que una determinada idea pudo haberse desarrollado antes no se hace así, sino que se la trabaja hasta el momento necesario; por ejemplo, desde el capítulo 2 se cuenta con el material suficiente para hablar de los conjuntos finitos, infinitos y numerables, pero se comienzan a usar hasta que se trabajan los Números Racionales, es por ello que esos tipos de conjuntos se definen hasta el capítulo 4.

Como parte concluyente en los capítulos 2, 3 y 4, se incluyen resultados que caracterizan a la estructura correspondiente, se muestra que son únicas salvo isomorfismo, con un isomorfismo que involucra el tipo de orden de las mismas. El formato general de los capítulos 2 al 5 consiste en definir de la manera más sencilla e intuitiva posible las estructuras en cuestión para posteriormente establecer su unicidad; la excepción a esta regla es el capítulo sobre los Números Naturales, donde se presentan dos definiciones de número natural que después se comprueba que definen al mismo objeto; se presentan esas dos alternativas porque si bien la primera de ellas es más simple, la segunda es más natural.

El Capítulo 1 es una formalización de la llamada Jerarquía Acumulativa y está basado en un artículo de Goerge Boolos: *The Iterative Conception of Set*; se puede encontrar en la antología de Benacerraf y Putnam que es una colección de artículos que tratan sobre el mismo tema. La bibliografía consultada para los capítulos 2 y 3 se ha tomado de una gran variedad de libros de Teoría de Conjuntos entre los que se citan el de H.B.Enderton, *Elements of Set Theory*; el de T.Jech & K.Hrbaceck, *Introduction to Set Theory* y el de A.G.Hamilton, *Numbers, Sets and Axioms*; etc.; también fueron una fuente importante las notas de clase del curso Teoría de los Conjuntos I por el Profesor Rafael Rojas Barbachano impartido durante el segundo semestre de 1992. Por lo que respecta a los resultados de unicidad para los números racionales y gran parte del capítulo 5 se trabajó en base a una notas sobre el tema proporcionadas por el profesor José Alfredo Amor Montaño. Para el material sobre Lógica Matemática es suficiente si se consulta el libro *A Matehematical Introduction to Logic* por H.B.Enderton.

Al final del texto se encuentra una lista más extensa de artículos y libros de texto precedidos de breves comentarios sobre ellos y en los cualesse puede obtener más información sobre los temas que aquí se tratan.

1. LA TEORIA DE ESTRATOS

1.1 INTRODUCCION

La Teoría de Estratos se presenta como una forma de arribar a una concepción iterativa de conjunto; tal concepción consiste en responder a la pregunta de ¿cómo se construye un conjunto? en lugar de ¿qué es un conjunto?. Un hecho natural es que para construir un objeto se dispone ya del material de construcción, en particular, para construir un conjunto se acepta que se cuenta de antemano con lo que serán sus elementos; también es razonable que se puedan construir conjuntos cuyos elementos sean, ellos mismos, conjuntos; de hecho, este es un procedimiento usual en Matemáticas: se definen nuevos objetos a partir de los definidos anteriormente. Así, se comienza la construcción con elementos que no son conjuntos, a los cuales llamaremos *individuos* y que pueden ser objetos de cualquier especie.

Intuitivamente, la Teoría de Estratos consiste en la construcción de conjuntos mediante un proceso establecido; se comienza con los llamados individuos y con ellos se construye el *estrato cero* que consiste en todas la posibles colecciones que pueden formarse con individuos; enseguida, se forma el *estrato uno* consistente de todas las colecciones de individuos y objetos del estrato cero; el *estrato dos* se formará con todas las colecciones posibles de individuos y objetos de los estratos cero y uno; el *estrato tres*, con colecciones de individuos y objetos de los estratos cero, uno y dos; continuando de esta manera, se tienen los estratos cuatro, cinco, seis,.... Después se asume que se puede construir el *estrato* ω formado por colecciones de individuos y objetos de los estratos cero, uno, dos,...; el estrato ω mas uno, ω mas dos,..., ω mas ω (ó dos ω); el estrato dos ω mas uno, dos ω mas dos,..., tres ω,..., cuatro ω,....

Aquí es importante hacer notar que los nombres asignados a los estratos son solo eso y no se hace referencia a los números naturales cero, uno, dos, etc., ya conocidos; además esto es solo una descripción intuitiva. Por otro lado, en la exposición anterior se observa que una vez que se ha construido un conjunto en algún estrato, este se vuelve a construir en todos los estratos posteriores; se puede eliminar esta característica rearreglando los estratos de manera que un conjunto esté formado en un solo estrato: en el primero en que fue formado de acuerdo al procedimiento anterior.

Dos consideraciones adicionales sobre la formación de estratos:
1) No hay un último estrato.

Esto significa que la construcción de estratos puede prolongarse *infinitamente*, o bien, que siempre puede darse un paso más en la construcción.

2) Sea A un conjunto formado en un estrato y denotemos por Ra cualquier estrato asociado (no importa como) a cada elemento $a \in A$ entonces, hay un estrato posterior a todos los Ra para $a \in A$.

Dada cualquier asociación de un estrato Ra para cada elemento $a \in A$, lo anterior permite extender esa asociación al conjunto A asignándole un estrato que es posterior a todos los Ra.

Por último, es claro que no hay un criterio para elegir objetos que tomen el papel de individuos en la Teoría de Estratos, -e incluso puede no haberlos- ya que ,como se dijo antes, éstos pueden ser objetos de cualquier especie (libros, números, funciones, árboles, etc.). Sin embargo, en vista de esto y tomando en cuenta que los libros, las piedras y las vacas no nos interesan (desde el punto de vista matemático) y los objetos matemáticos (números, funciones, estructuras algebraicas, etc.) los podremos construir, entonces, se puede hacer una elección mas o menos natural: que no haya individuos. Con esto, el estrato cero tiene una sola colección, la colección nula; el estrato uno tiene dos colecciones: la colección nula y la que tiene a la colección nula; el estrato dos tiene cuatro colecciones: la colección nula, ...Las colecciones construidas de esta manera se denominan *conjuntos puros* y simplemente nos referiremos a ellos como *conjuntos* pues solo de ellos nos ocuparemos.

En la siguiente sección se establece formalmente (en forma axiomática) la Teoría de Estratos. Como el objetivo de este capítulo es el de establecer los axiomas de Zermelo-Fraenkel para los conjuntos y y estos se escriben en un lenguaje de primer orden 3 con símbolo predicado no-lógico $\in$, escribiremos los axiomas de la Teoría de Estratos en un lenguaje de primer orden 2-variado $\mathfrak{C}$ que es 3 mas los predicados A, de dos argumentos, que se entenderá como "_ *anterior que* _" y F, también de dos argumentos, entendido como "- *es formado en* _". Así que en esta teoría, *una colección* x *sera un conjunto si y solo si existe un estrato* s *en donde fue construido*:

$$\exists s(xFs).$$

1.2 AXIOMAS DE LA TEORIA DE ESTRATOS (T.E.)

Sea el lenguaje de primer orden 2-variado $\mathfrak{C}$ descrito en el párrafo anterior con variables r,s,t,r',s',t' que varían sobre estratos y variables w,x,y,z,w',x',y',z' que varían sobre conjuntos.

De acuerdo con la descripción de la sección anterior, y para su buen funcionamiento, se requiere que ningún estrato sea anterior a si mismo; este es el primer axioma:

TE1: $\forall s(\neg sAs)$

Si se piensa un poco, la relación A debe ser transitiva:

TE2: $\forall r \forall s \forall t(rAs \wedge sAt \Rightarrow rAt)$

El siguiente axioma, junto con los anteriores, dice que la relación A define un orden lineal:

TE3: $\forall s \forall t (sAt \vee s=t \vee tAs)$

Hay un estrato que es anterior a todos los demás:

TE4: $\exists r \forall t (r \neq t \Rightarrow rAt)$

Siempre se puede construir el estrato inmediato posterior a uno dado:

TE5: $\forall s \exists t (sAt \wedge \forall r (rAt \Rightarrow (rAs \vee r=s)))$

Un axioma que puede no ser intuitivamente claro pero que es absolutamente necesario, pues permitirá, entre otras cosas, la construcción de conjuntos infinitos; postula la existencia del estrato ω que fué descrito en la sección anterior; lo que afirma es que existe un estrato s que no es el primero y que no tiene un estrato inmediato anterior, por lo que debe ser un estrato posterior a un número infinito de estratos:

TE6: $\exists s ((\exists t\, tAs) \wedge \forall t (tAs \Rightarrow \exists r (tAr \wedge rAs)))$

Será de interés que cada conjunto esté formado en un único estrato:

TE7: $\forall x \exists s (xFs \wedge \forall t (xFt \Rightarrow t=s))$

Cada conjunto está formado por objetos (conjuntos) que fueron construidos antes que él:

TE8: $\forall x \forall y \forall r \forall s (x \in y \wedge xFr \wedge yFs \Rightarrow rAs)$

Dados un conjunto formado en un estrato y cualquier estrato anterior, se puede encontrar aquí o en algún estrato posterior, un elemento del conjunto:

TE9: $\forall x \forall s \forall t (xFs \wedge tAs \Rightarrow \exists y \exists r (y \in x \wedge yFr \wedge (t=r \vee tAr)))$

Ahora, falta por plantear que es posible formar un estrato con todas las colecciones de objetos de los estratos anteriores cuidando de no volver a formar las que ya se habían construido, esto implica el uso de fórmulas del lenguaje $\mathfrak{E}$ que describen las propiedades deseadas; tenemos, por tanto, un esquema de axioma:

Sea φ una fórmula de $\mathfrak{E}$ en donde la ocurrencia de la variable y no es libre; entonces, el siguiente es un axioma:

TE10: $\forall s \exists y \forall x (x \in y \Leftrightarrow (\varphi(x) \wedge \exists t (tAs \wedge xFt)))$

Finalmente, de acuerdo a la descripción intuitiva de la formación de estratos, se nota que estos están construidos inductivamente; es decir, habrá un *principio de inducción* para estratos y conjuntos análogo al de los números naturales.

Para ello necesitamos la siguiente definición: decimos que un estrato *se cubre* por un predicado si tal predicado se aplica a cada conjunto del estrato.

Con esto, nuestro principio de inducción deberá decir algo como esto:

Si un estrato se cubre por un predicado siempre que se cubra cada estrato anterior a él entonces todo estrato se cubre por el predicado.

Para escribirlo en el lenguaje $\mathfrak{C}$ usamos fórmulas φ y φ' de él tales que φ es igual a φ' excepto porque en φ' no ocurre en forma libre la variable t:

TE11: $\forall s(\forall t(\ tAs \Rightarrow \forall x(\ xFt \Rightarrow \varphi'\ )) \Rightarrow \forall x(\ xFs \Rightarrow \varphi\ )\ ) \Rightarrow \forall s\forall x(\ xFs \Rightarrow \varphi)$

Para terminar esta sección hacemos ver que la restricción de emplear un lenguaje de primer orden 2-variado es solo por simplicidad de la escritura y porque estamos empleando dos tipos de variables, uno para estratos y otro para conjuntos; pero podemos emplear un lenguaje univariado introduciendo dos predicados adicionales de un argumento, el predicado S(_) que significa "ser estrato" y el predicado C(_) entendido como "ser conjunto". Con esto podemos manejar las variables r,s,t,u,v,w,x,y,z del nuevo lenguaje y reescribir los axiomas TE1-TE11, por ejemplo:

TE1': $\forall x(\ S(x) \Rightarrow \neg\ xAx\ )$
TE4': $\exists x\forall y(\ S(x) \wedge S(y) \wedge x \neq y \Rightarrow\ xAt\ )$
TE7': $\forall x(\ C(x) \Rightarrow \exists y(\ S(y) \wedge xFy \wedge \forall z(\ S(z) \wedge xFz \Rightarrow z=y\ )))$

1.3 LA TEORIA DE CONJUNTOS DE ZERMELO-FRAENKEL

Si bien este trabajo pudo haber comenzado presentando directamente los axiomas de Zermelo-Fraenkel (ZF)para los conjuntos, la exposición de las secciones anteriores permitirá derivarlos de la Teoría de Estratos.

La mayoría de las deducciones de los "axiomas" de ZF tienen la siguiente forma general: a partir de uno o más conjuntos se prueba la existencia de otro conjunto localizando el estrato donde éste deba encontrarse y haciendo ver que todos los que serán sus elementos se encuentran en estratos anteriores, una vez hecho esto, el esquema de axiomas TE10 permite construir, en aquel estrato, el conjunto con las propiedades deseadas.

Axioma del Conjunto Vacío.

ZF1: $\exists x\forall y(\ y \notin x\ )$

"Existe en conjunto que no tiene elementos."
Para derivarlo de la Teoría de Estratos, se debe hacer ver que hay un estrato en donde se construye una colección con las propiedades requeridas.
Por TE4 hay un estrato inicial *s* y por TE10 con $\varphi \equiv$ "x=x":
(1) $\forall s\exists y\forall x\ (x \in y \Leftrightarrow x=x \wedge \exists t\ (tAs \wedge xFt)\ )$
entonces, para el estrato inicial s $\neg\exists t\ (tAs \wedge xFt)$, así, por
(1) $\exists y\forall x\ (x \notin y)$.

Axioma del Par.

ZF2: $\forall x\forall y\exists w\forall z\ (z \in w \Leftrightarrow z=x \vee z=y)$
"Para cualesquiera dos conjuntos hay un conjunto cuyos elementos son exactamente ellos dos."
Nuevamente, se necesita hacer ver que hay un estrato en donde hay un conjunto con las propiedades requeridas por ZF2.
Sean x,y dos conjuntos, por TE7 ellos están formados en dos estratos y por TE3 uno de ellos, t, es posterior o igual al otro, sea s el estrato inmediato siguiente a t (TE5) y tómese con TE10

$\varphi \equiv$ "$z=x \vee z=y$"

(2)....$\forall s \exists y \forall z (z \in y \Leftrightarrow (z=x \vee z=y) \wedge \exists t (zFt \wedge tAs))$

Aplicamos (2) al estrato s y se tiene la existencia de un conjunto *y* tal que sus elementos están formados antes que *s* y tiene a *x* y a *y* , este es el conjunto que se busca.

Axioma de la Unión.

ZF3: $\forall x \exists y \forall z (z \in y \Leftrightarrow \exists w (w \in x \wedge z \in w))$

"Para cualquier conjunto x hay un conjunto (la *unión* de x) que tiene a todos los elementos de todos los elementos de x."

Sea s el estrato en que está formado x (TE7); por TE8, todos los elementos de x están formados antes de s y también por TE8 todos los elementos de cada elemento de x están formados antes de s, así que en s se puede formar la unión de x con TE10 mediante $\varphi \equiv$ "$\exists w (w \in x \wedge z \in w)$":

$\exists y \forall z (z \in y \Leftrightarrow \exists w (w \in x \wedge z \in w) \wedge \exists t (zFt \wedge tAs))$

El conjunto y postulado por la fórmula anterior es el que se busca.

Axioma de las Partes o del Conjunto Potencia.

ZF4: $\forall x \exists y \forall z (z \in y \Leftrightarrow \forall w (w \in z \Rightarrow w \in x))$

"Para cualquier conjunto x, la colección de todos los subconjuntos de x es un conjunto"; o bien, "hay un conjunto cuyos elementos son todos los subconjuntos de x ".

Sea s' el estrato inmediato posterior a s, aquel donde x se formó; si $\forall w (w \in z \Rightarrow w \in x)$,abreviado "$z \subseteq x$", por TE8 todo miembro de z está formado en un estrato t anterior a s, entoncesz está formado en s o antes; así que en s' se puede formar lacolección de todos los subconjuntos de s através de la aplicación al estrato s' de TE10 con $\varphi \equiv$ "$\forall w (w \in z \Rightarrow w \in x)$"; es decir,aplicando

$\forall s' \exists y \forall z (z \in y \Leftrightarrow \forall w (w \in z \Rightarrow w \in x) \wedge \exists t (zFt \wedge tAs'))$

o bien

$\forall s' \exists y \forall z (z \in y \Leftrightarrow z \subseteq x \wedge \exists t (zFt \wedge tAs'))$

Axioma de Infinitud.

ZF5: $\exists y (\exists x' (x' \in y \wedge \forall z (z \in x')) \wedge \forall y' (y' \in y \Rightarrow \forall w (\forall z (z \in w \Leftrightarrow z \in y' \vee z=y') \Rightarrow w \in y)))$

"Hay un conjunto que tiene al conjunto vacío y siempre que tiene a un conjunto y' tiene a su sucesor w ($z \in w \Leftrightarrow z \in y' \vee z=y'$) ".

Sea s el estrato cuya existencia está postulada por TE6; se verá que si un conjunto w está formado en un estrato anterior a s, su sucesor también está en un estrato anterior a s.

Sean w, t, y' tales que $y'Ft \wedge tAs \wedge \forall z (z \in w \Leftrightarrow z \in y' \vee z=y')$; por TE6 $\exists r (tAr \,\&\, rAs)$ y por TE5 r puede ser el estrato que sigue a t; ya que $y'Ft \wedge tAr$ y todo miembro de y' está formado antes de t (y por tanto antes que r) en r puede formarse un conjunto w cuyos elementos son exactamente los de y' junto con el mismo y' através del empleo de TE10 (aplicado al estrato s) mediante

$\varphi \equiv$"$\exists x' (x' \in y \wedge \forall z (z \in x')) \wedge \forall y' (y' \in y \Rightarrow \forall w (\forall z (z \in w \Leftrightarrow z \in y' \vee z=y') \Rightarrow w \in y))$

es decir, usando

$\forall s \exists y \forall x (x \in y \Leftrightarrow \varphi \wedge \exists t (tAs \wedge xFt))$

Esquema de Comprensión o de Separación o de Subconjuntos.

ZF6: $\forall x \exists y \forall z\ (z \in y \iff z \in x \wedge \psi)$, donde ψ es una fórmula en que la ocurrencia de la variable y no es libre.

"Para cualquier conjunto x hay un conjunto cuyos elementos son todos los elementos de x a los que ψ se aplica ".

Todos los elementos de x están construidos en estratos anteriores a aquel en que x se formó, en particular, aquellos a los cuales ψ se aplica. Así que apliquemos , a este estrato, el esquema TE10 con $\varphi \equiv$"$z \in x \wedge \psi$":

$$\forall s \exists y \forall z(\ z \in y \iff z \in x \wedge \varphi \wedge \exists t(\ zFt \wedge tAs\ ))\ .$$

Esquema de Regularidad.

Sean φ y φ' fórmulas donde en φ no ocurre la variable y y son iguales excepto porque en φ' ocurre y en aquellos lugares en que x ocurre libre, entonces

ZF7: $\exists x(\ \varphi\ ) \Rightarrow \exists x(\ \varphi \wedge \forall y\ (y \in x \Rightarrow \neg\varphi')\ )$

"Si existe un conjunto con una propiedad φ entonces existe un conjunto "minimal" respecto a esa propiedad; es decir, existe un conjunto con la propiedad φ tal que sus elementos ya no la tienen."

Si $\exists x(\varphi)$ entonces el estrato s tal que xFs no está cubierto por $\neg\varphi$ (véase la definición de *estar cubierto por* en la página 3), pero el principio de inducción para estratos y conjuntos dice que si un estrato se cubre por un predicado (fórmula) siempreque se cubra todo estrato anterior a él entonces todo estrato se cubre por ese predicado; la contrapositiva de esta afirmación establece que si algún estrato no se cubre por una formula entonces hay un estrato tal que todo estrato anterior a él se cubre por ella pero él mismo no se cubre por la fórmula. Esto quiere decir que en este estrato hay un conjunto al cual la fórmula no se aplica pero a sus elementos (formados en estratos anteriores) sí se aplica. Si esa fórmula es $\neg\varphi$ de ZF7 entonces se ha probado este esquema.

Formalmente:

El principio de inducción aplicado a $\neg\varphi$:

$\forall s(\ \forall t(tAs \Rightarrow \forall x(xFt \Rightarrow \neg\varphi)) \Rightarrow \forall x(xFs \Rightarrow \neg\varphi)\ ) \Rightarrow \forall s \forall x\ (xFs \Rightarrow \neg\varphi)$

la contrapositiva:

$\neg\forall s \forall x(xFs \Rightarrow \neg\varphi) \Rightarrow \neg\forall s(\ \forall t(tAs \Rightarrow \forall x(xFt \Rightarrow \neg\varphi)) \Rightarrow \forall x(xFs \Rightarrow \neg\varphi))$

o bien:

$\exists s \exists x\ (xFs \wedge \varphi) \Rightarrow \exists s(\ \forall t\ (tAs \Rightarrow \forall x\ (xFt \Rightarrow \neg\varphi\ )) \wedge \exists x\ (xFs \wedge \varphi)$

que es equivalente a:

$\exists s \exists x\ (xFs \wedge \varphi) \Rightarrow \exists s(\ \forall t\ (tAs \Rightarrow \forall y\ (yFt \Rightarrow \neg\varphi'\ )) \wedge \exists x\ (xFs \wedge \varphi)$

Usando la equivalencia lógica de que $(A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \wedge B \Rightarrow C)$

$\exists s \exists x\ (xFs \wedge \varphi) \Rightarrow \exists s((\forall t \forall y(\ tAs \wedge yFt\ ) \Rightarrow \neg\varphi') \wedge \exists x(\ xFs \wedge \varphi))$

O bien

$\exists s \exists x\ (xFs \wedge \varphi) \Rightarrow \exists s(\ \exists x(xFs \wedge \varphi) \wedge \forall t \forall y(\ tAs \wedge yFt\ ) \Rightarrow \neg\varphi')$

Por otro lado, la hipótesis de ZF7 y TE7 implican

$$\exists s \exists x(\ xFs \wedge \varphi\ )$$

así, tenemos

$$\exists s(\ \exists x(\ xFs \wedge \varphi\ ) \wedge \forall t \forall y(\ tAs \wedge yFt\ ) \Rightarrow \neg\varphi')$$

en particular

$$\exists s(\ \exists x((\ xFs \wedge \varphi\ ) \wedge \forall y(\ y \in x \Rightarrow \neg\varphi')))$$

en particular

$$\exists x(\ \varphi \wedge \forall y(\ y \in x \Rightarrow \neg\varphi')$$

Se ha probado que

$$\exists x(\ \varphi\ ) \Rightarrow \exists x(\ \varphi \wedge \forall y(\ y \in x \Rightarrow \neg\varphi'))$$

Esquema de Reemplazo o Sustitución.

ZF8: $\forall x \forall y \forall z(\ \varphi(x,y) \wedge \varphi(x,z) \Rightarrow y=z\ ) \Rightarrow \forall x \exists y \forall z(\ z \in y \Leftrightarrow \exists w(\ w \in x \wedge \varphi(w,z)\ )\ )$

"Para todo conjunto hay un conjunto cuyos miembros son las imágenes bajo la 'funcional' φ de algún elemento de aquel conjunto".

Intuitivamente, de acuerdo a la segunda de las dos últimas observaciones sobre la descripción intuitiva de la Teoría de Estratos (ver la página 2), para cada elemento $w \in x$ puede pensarse en un estrato R_w asociado a w que es aquel donde se construyó el único conjunto z (si es que existe) tal que $\varphi(w,z)$, la observación a que se hace referencia postula la existencia de un estrato s que es posterior a todos los R_w para $w \in x$; entonces, en s se puede formar el conjunto que tiene a la *imagen de* x *bajo* φ.

Para derivar formalmente el esquema de reemplazo necesitamos pues, extender la Teoría de Estratos para que incluya nuevos axiomas que permitan lo que se acaba de discutir; es decir, añadir los que podríamos llamar los *principios de cofinalidad:*

Si cada conjunto esta asociado con algún estrato (no importa como), entonces para cada conjunto z *existe un estrato* s *tal que para cada miembro* w *de* z, s *es posterior a algún estrato asociado a* w.

Con este principio aceptado como axioma pueden demostrarse (aparentemente) los axiomas de reemplazo; sin embargo, no está garantizado que todas las asociaciones de estratos a conjuntos puedan escribirse en el lenguaje $\mathfrak{C}$. Mas específicamente, la justificación intuitiva para el esquema de reemplazo que se enuncia tres párrafos más arriba habla de una asociación entre conjuntos y estratos en términos de la propiedad (funcional) φ pero la generalidad de ésta puede en algún momento requerir una asociación que no pueda escribirse en el lenguaje $\mathfrak{C}$.

Así pues, parece que no todos los axiomas de reemplazo pueden derivarse de la Teoría de Estratos, pero dada la importancia que pronto sobre ellos se observará, se aceptan como parte de la Teoría de Conjuntos de Zermelo-Fraenkel.

Axioma de Extensionalidad.

ZF9: $\forall x \forall y(\ \forall z(\ z \in x \Leftrightarrow z \in y\ ) \Rightarrow x=y\ )$.

"Si dos conjuntos tienen los mismos elementos entonces son iguales".

La negación de este axioma diría que hay dos conjuntos diferentes que tienen los mismos elementos. Dado que lo único que interesa de los conjuntos son sus elementos (de hecho, en la descripción intuitiva de la formación de conjuntos, se parte de una colección de objetos y con ellos se construyen los conjuntos) parece ser que este axioma es cierto en virtud únicamente de lo que dice y de nuestro interés en cuanto a los conjuntos. Así, este axioma tampoco se sigue de la Teoría de Estratos pero también se incluye porque a partir de él puede probarse, entre otras cosas, la unicidad del conjunto vacío, de la unión, etc. . . .

Se han introducido los axiomas sobre conjuntos que se necesitarán durante los capítulos siguientes; ahora se introducen algunas propiedades y algo de notación sobre conjuntos.

En ZF1 se postula la existencia incondicional de al menos un conjunto, el conjunto vacío, si hay más de uno con estas propiedades el axioma de extensionalidad dice que son iguales; es decir, el conjunto

vacio es único y se denota con el simbolo ø.

Si x,y son dos conjuntos cualesquiera, hay un conjunto que los tiene como elementos (ZF2) y por ZF9 éste es único, dado que está definido en términos de sus elementos. Este conjunto se denota por {x,y}.

En ZF3 la *union* de un conjunto x está definido en términos de los elementos que lo forman, también resulta único por extensionalidad y la unión de x se denota como $\bigcup x$. Si a y b son conjuntos se define la unión de a y b, denotada a∪b, como

$$a \cup b = \bigcup\{a, b\}$$

Obsérvese que esta definición requiere además del axioma del par.

En ZF4 el conjunto de los subconjuntos de un conjunto x se llama la *Potencia* de x ,por extensionalidad, solo hay un conjunto cuyos elementos son todos los subconjuntos de x y se denota como $P(x)$.

El *sucesor* de un conjunto x es un conjunto w tal que

$$z \in w \Leftrightarrow z \in x \vee z = x$$

así, el sucesor de un conjunto es único puesto que

$$w = x \cup \{x\} = \bigcup\{x, \{x\}\}.$$

El conjunto y de los elementos de un conjunto dado x que satifacen una propiedad ψ cuya existencia se postula en ZF6 se denota como

$$y = \{z \mid z \in x \wedge \psi(z)\}$$

o bien

$$y = \{z \in x \mid \psi(z)\} .$$

El llamado Axioma de Regularidad es un caso particular del esquema de regularidad ZF8 en que $\varphi(x,z) \equiv$"$x \in z$" es la relación de pertenencia entre conjuntos. Así, el axioma de regularidad dice que todo conjunto tiene un elemento que es minimal respecto a la pertenencia. Consecuencia de esto es que $\neg\exists x(x \in x)$; es decir, no se presentan situaciones como la que se muestra enseguida:

$$x = \{------, x, ------\}$$

porque entonces se tendría

$$x = \{------, \{------, x, ------\}, ------\}$$

y así sucesivamente. En el contexto de la construcción intuitiva de conjuntos esto significa que todos los conjuntos comenzaron a construirse alguna vez.

Ahora bien, aun cuando el axioma de regularidad se ha derivado de la Teoría de Estratos, en los capítulosque siguen no se hará uso de él porque, como se verá, realmente no es necesario.

Por último se verá que aun cuando ZF1-ZF9 se han obtenido directamente de la Teoría de Estratos en realidad no son independientes; es decir, algunos pueden obtenerse a partir de otros; a saber:

Afirmación 1. ZF6 (comprensión) implica ZF1 (vacio).

Prueba:

Sea $\varphi \equiv "z \neq z"$, por hipótesis,

$$\forall x \exists y \forall z (z \in y \Leftrightarrow z \in x \wedge z \neq z) \quad \text{--------(1)}$$

por otro lado, y dado que la fórmula $\exists x(x=x)$ es universalmente válida, resulta que, por razones lógicas debe haber al menos un conjunto.

Así, al aplicar (1) a cualquier conjunto x y en vista de que $z \neq z$ siempre es falso se tiene que

$$\exists y \forall z (z \in y)$$

esto es ZF1.

∎

Afirmación 2. ZF1 (vacio) , ZF8 (reemplazo) y ZF4 (potencia) implican ZF2 (par).

Prueba:

Se debe probar que

$$\forall x \forall y \exists w \forall z (z \in y \Leftrightarrow z=x \vee z=y).$$

Por ZF1 y ZF4 $P(\varnothing)= \{ \varnothing \}$ es un conjunto, por ZF4 $P(P(\varnothing))=P(\{\varnothing\})=\{\varnothing,\{\varnothing\}\}$ también es un conjunto.

Sean x,y dos conjuntos y una fórmula dada como

$$\varphi(w,z) \equiv "(w=\varnothing \wedge z=x) \vee (w=\{\varnothing\} \wedge z=y)$$

es claro que φ define una 'función' del conjunto $\{\varnothing,\{\varnothing\}\}$ en el universo y su imagen, que por ZF8 es un conjunto, es el conjunto $\{x,y\}$.

∎

Afirmación 3. ZF8 (reemplazo) implica ZF6 (comprensión).

Prueba:

Sea x un conjunto, $\psi(z)$ una fórmula donde la ocurrencia de la variable y no es libre y una fórmula φ dada por

$$\varphi(w,z) \equiv "(\psi(z) \wedge w=z)"$$

esta φ satisface el antecedente de ZF8 y aplicando el consecuente al conjunto x se tiene que

$$\exists y \forall z (z \in y \Leftrightarrow \exists w(w \in x \wedge \varphi(w,z))$$

es decir,

$$\exists y \forall z (z \in y \Leftrightarrow \exists w(w \in x \wedge \psi(z) \wedge w=z))$$

que implica que

$$\exists y \forall z (z \in y \Leftrightarrow z \in x \wedge \psi(z)) .$$

∎

Hasta aquí solo quedan 6 axiomas independientes; puede demostrarse que, efectivamente, los axiomas que se enuncian enseguida son independientes

ZF3. Axioma de Unión.
ZF4. Axioma de Partes o del Conjunto Potencia.
ZF5. Axioma de Infinitud.
ZF7. Esquema de Regularidad.
ZF8. Esquema de Reemplazo o de Sustitución.
ZF9. Axioma de Extensionalidad.

2. LOS NUMEROS NATURALES

El objetivo de este capítulo es dar una definición conjuntista, que parezca natural, de los Números Naturales; para ello, se incluyen las definiciones (también en términos conjuntistas) de algunos objetos de uso común en Matemáticas como son el de par ordenado, función, relación, etc., que se usarán en los desarrollos subsecuentes. Para que estos conceptos queden expresados en una forma mas general que la de conjuntos, se introducirá la notación de *clases* pero solo con la intención de facilitar la escritura de sus definiciones formales; todos los conjuntos resultarán ser clases pero no toda clase será un conjunto, así que los axiomas ZF1-ZF9 del capítulo anterior no nos dicen como manipular clases, de aquí que estos objetos solo se emplean para simplificar la notación.

Dado que, desde ahora, no se hablará de estratos *y/o* sus relaciones, todo lo que sigue se escribirá (o al menos será claro que puede hacerse) en el lenguaje 3 de la Teoría de Conjuntos de Zermelo-Fraenkel que ya se ha descrito antes y que además se simplifica para agilizar su escritura siempre que tal simplificación sea obvia, por ejemplo:

$$\forall x,y,z\ (\varphi) \quad \text{abrevia a} \quad \forall x\forall y\forall z\ (\varphi)$$
$$\exists x,y,z\ (\varphi) \quad \text{abrevia a} \quad \exists x\exists y\exists z\ (\varphi)$$
$$\forall x{\in}y\ (\varphi(x)) \quad \text{abrevia a} \quad \forall x(\ x{\in}y \Rightarrow \varphi(x)\ )$$
$$\exists x{\in}y\ (\varphi(x)) \quad \text{abrevia a} \quad \exists x(\ x{\in}y \wedge \varphi(x)\ )\ .$$

Con todo esto, para llegar a la descripción de los Números Naturales, se define lo que es un *Sistema de Peano*, se muestra que, en un sentido específico, todos son *semejantes* y se adopta una representación de ellos que es la usual para describir a los Números Naturales.

2.1 CLASES, SISTEMAS DE PEANO Y CONJUNTOS INDUCTIVOS.

Las variables recorren conjuntos y si φ es una fórmula que tiene libre a la variable **y**, resulta que, en general

$$\neg\exists x\forall y(\ y{\in}x \Leftrightarrow \varphi(y)\ )$$

por ejemplo

$\varphi{\equiv}$"$y{\in}y$" ó
$\varphi{\equiv}$"$y{=}y$"

Para ayuda a la intuición y a la escritura usaremos la notación

$$\{\ y \mid \varphi(y)\ \}$$

leído como *la clase de todos los conjuntos y tales que $\varphi(y)$.*

Todo conjunto es una clase pues si b es un conjunto

$$b{=}\{\ y \mid y{\in}b\ \}$$

No toda clase es un conjunto, a estas se les llama *clases propias* y para ellas se usarán metavariables A,B,C,... .

Si $A=\{ x \mid \varphi(x) \}$ y $B=\{ y \mid \psi(y) \}$, al escribir

i) $A=B$ significa
$$\forall w(\varphi(w) \Leftrightarrow \psi(w))$$
ii) $w\in A$ significa
$$\varphi(w)$$
iii) $A\subseteq B$ significa
$$\forall w(\varphi(w) \Rightarrow \psi(w))$$
iv) $A\in B$ no tiene sentido a menos que A sea un conjunto.

Una vez que se ha entendido lo anterior surge una pregunta natural

¿Cuándo una clase es un conjunto?

Una clase A es un conjunto si con la ayuda de los axiomas ZF1-ZF9 se puede probar que
$$\exists x(x=A) \quad \text{o bien}$$
$$\exists x\forall w(w\in x \Leftrightarrow w\in A) \quad \text{o bien}$$
$$\exists x\forall w(w\in x \Leftrightarrow \varphi(w))$$
pero contando con el esquema de Comprensión ZF6 es suficiente con que
$$\exists x(A\subseteq x) \quad \text{o bien}$$
$$\exists x\forall w(w\in A \Rightarrow w\in x) \quad \text{o bien}$$
$$\exists x\forall w(\varphi(w) \Rightarrow w\in x)$$
pues en tal caso sería
$$A=\{ w \mid w\in x \wedge \varphi(w) \}$$

Ejemplos.

1) Sea $V=\{ x \mid x=x \}$ entonces V es la clase propia de todos los conjuntos.
   Notación: $a\in V$ ó $A\in V$ es una abreviatura para indicar que a ó A es un conjunto.

2) i) Si A y B son clases, la *diferencia* entre A y B es
$$A\setminus B=\{ x \mid x\in A \wedge x\notin B \}$$
   ii) Observación: Si $a\in V$ entonces $V\setminus a\in V$ pues si $V\setminus a\in V$ por el axioma de unión $V=(V\setminus a)\cup a \in V$ lo cual es falso.

3) Sea A una clase,
   i) la *unión* de A, denotada $\bigcup A$, está definida como
   $$\bigcup A=\{ x \mid \exists y(y\in A \wedge x\in y) \} = \{ x \mid \exists y(\varphi(y) \wedge x\in y \}$$
   ii) la *intersección* de A, denotada $\bigcap A$, se define como
   $$\bigcap A=\{ x \mid \forall y(y\in A \Rightarrow x\in y) \} = \{ x \mid \forall y(\varphi(y) \Rightarrow x\in y) \}.$$
   Por ejemplo $\bigcap \emptyset = V$.
   Observacion. Si A no es vacía entonces $\bigcap A\in V$.
   Prueba:
   Como $A\neq\emptyset$ existe $x_0\in A$; ahora, sea $x\in\bigcap A$ entonces $\forall y\in A\ (x\in y)$ en paticular $x\in x_0$, por lo tanto $\bigcap A\subseteq x_0$ y como $x_0\in V$ ZF6 implica que $\bigcap A\in V$. ∎

Notacion. Dados dos conjuntos x,y la *interseccion* de a y b denotada $a\cap b$, es el conjunto
$$a\cap b=\bigcap\{a,b\} .$$

DEFINICION 1. Dados x,y dos conjuntos, el *par ordenado* $\langle x,y\rangle$ es el conjunto
$$\langle x,y\rangle=\{\{x\},\{x,y\}\}$$

Aplicando tres veces el axioma del par se concluye que el par ordenado $\langle x,y\rangle$ es, efectivamente, un conjunto; además, puede verse que esta definición dota a los pares ordenados de la propiedad que se desea posean:

$$\langle x,y\rangle=\langle z,w\rangle \iff x=z \wedge y=w \ .$$

En lo que sigue, se abreviará $w=\langle x,y\rangle$ como

$$\forall z(z\in w \iff \forall u(u\in z \iff u=x) \vee \forall u(u\in z \iff u=x \vee u=y))$$

con lo cual, obviamente, se simplifica la escritura.

Por otro lado, se puede definir una *terna ordenada* como

$$\langle x,y,z\rangle=\langle\langle x,y\rangle,z\rangle \ .$$

DEFINICION 2. Dados a y b dos conjuntos, el *producto cartesiano* axb de a y b es

$$axb=\{w|w=\langle x,y\rangle \wedge x\in a \wedge y\in b \}$$

o bien

$$\forall w(w\in axb \iff \exists x,y(x\in a \wedge y\in b \wedge w=\langle x,y\rangle)) \ .$$

Puede verse que $axb\subseteq P(P(a\cup b))$, con lo que la aplicación de los axiomas de Unión, Potencia (dos veces) y comprensión el producto cartesiano resulta ser, en efecto, un conjunto.

DEFINICION 3. (1) Una clase R es una *relacional* si sus elementos son pares ordenados.

(2) Una relacional F es una *funcional* si

$$\forall x,y,z((\langle x,y\rangle\in F \wedge \langle x,z\rangle\in F) \Rightarrow y=z)$$

Notacionalmente, para una relacional se escribe xRy para decir $\langle x,y\rangle\in R$. Además se definen los conceptos de *dominio* de R, *imagen* de R y y *campo* de R como

$$\text{Dom } R =\{ x| \exists y(\langle x,y\rangle\in R \}$$
$$\text{Im } R = \{ y| \exists x(\langle x,y\rangle\in R \}$$
$$\text{Cam } R =\{ z| z\in\text{Dom } R \vee z\in\text{Im } R \} = \text{Dom } R \cup \text{Im } R \ .$$

o bien

$$\forall x(x\in\text{Dom } R \iff \exists y(\langle x,y\rangle\in R))$$
$$\forall y(y\in\text{Im } R \iff \exists x(\langle x,y\rangle\in R))$$
$$\forall z(z\in\text{Cam } R \iff z\in\text{Dom } R \vee z\in\text{Im } R)$$

Cuando la relacional R es un conjunto se le llama *relación* y usamos la correspondiente letra minúscula r para denotarla, analogamente, si una funcional F es un conjunto, le llamaremos *función* f; en tal caso, y dado que resulta Dom $r\subseteq\bigcup\bigcup r$ y Im $r\subseteq\bigcup\bigcup r$, el dominio, la imagen y el campo de una relación son conjuntos.

Por otro lado, para una funcional F se escribe

$$F: A\longrightarrow B$$

para indicar que F es una funcional donde Dom F=A y Im $F\subseteq B$, además, se denota por F(x) al único conjunto tal que $\langle x,F(x)\rangle\in F$, conjuntistamente

$$F(x)=\bigcap\{ y| \langle x,y\rangle\in F \}$$

Se aceptan como conocidas las definiciones de funcional *inyectiva*, *suprayectiva* y *biyectiva* así como su formulación en términos puramente conjuntistas.

Ahora continuamos con el material principal de este capitulo.

DEFINICION 4. Una terna ordenada <p,s,e> es un *sistema de Peano* si
s:p⟶p, e∈p y además
(i) e∉Im s : ∀x(s(x)≠e),
(ii) s es inyectiva: ∀x,y(s(x)=s(y) ⇒ x=y)
(iii) El único subconjunto de p que tiene a e y que es cerrado bajo s es el mismo p:
∀x(x⊆p ∧ e∈x ∧ ∀y∈x(s(y)∈x) ⇒ x=p)

Enseguida se construye un sistema de Peano en concreto y se hará ver que cualquier otro es isomorfo a éste; es decir, solo hay un Sistema de Peano salvo isomorfismo.

En general, dos objetos a y b son *isomorfos* si existe una función biyectiva entre ellos que es compatible con la estructura, en particular:

DEFINICION 5. Dos sistemas de Peano <p1,s1,e1>, <p2,s2,e2> son *isomorfos* si existe una función f:p1⟶p2 biyectiva tal que
(i) f preserva la operación sucesor:
∀x∈p1(f(s1(x))=s2(f(x)))
(ii) f preserva los elementos distinguidos:
f(e1)=e2 .

Lo que sigue va encaminado a construir la forma que tendrán todos los sistemas de Peano.

DEFINICION 6. Para cualquier conjunto x, su sucesor x^ es
x^=x∪{x}

Por los axiomas del Par y de Unión el sucesor de un conjunto es, en si mismo, un conjunto.

DEFINICION 7. Un conjunto a es *inductivo* si
∅∈a ∧ ∀x∈a(x^∈a)
El axioma de infinitud ZF5 postula la existencia de un conjunto inductivo; en términos de clases, esto quiere decir que la clase de conjuntos inductivos es no vacía. En su momento vimos que la intersección de una clase no vacía es un conjunto. Así pues, se puede hablar del más pequeño, en el sentido de contención, de los conjuntos inductivos y que se denota como w :
∀x(x∈w ⟺ ∀z((∅∈z ∧ ∀y∈z(y^∈z)) ⇒ x∈z))
O bien

DEFINICION 8. Sea A la clase de todos los conjuntos inductivos, abusando de la notación
w=⋂A

Es claro que w es un conjunto inductivo:
∅∈w pues ∅ pertenece a todo conjunto inductivo entonces ∅∈⋂A
y si x∈w entonces x pertenece a todo conjunto inductivo z y así x^∈z, es decir, x^∈⋂A .

Por caracteristicas propias del "operador" intersección sucede que si $x \in A$ entonces $\bigcap A \subseteq x$, asi se tiene que si $x \subseteq w$ y x es inductivo entonces $w \subseteq x$ y por tanto $x=w$. Esto es un "principio de inducción" para w, que puede expresarse así:

Si x es un subconjunto de w descrito por una propiedad φ $(y \in x \Leftrightarrow \varphi(y))$ y si $\varphi(\varnothing) \wedge \forall y(\varphi(y) \Rightarrow \varphi(y^+))$ entonces $x=w$.
En este punto w se parece a los números naturales que ya se conocen.

Otra característica que tendrán los números naturales:

DEFINICION 9. Un conjunto a es *transitivo* si
$\forall y \in a(y \subseteq a)$ ó equivalentemente $\forall x,y(x \in y \wedge y \in a \Rightarrow x \in a)$

Observación: El conjunto a es transitivo si y solo si $\bigcup a \subseteq a$.
Prueba:
Sea $x \in \bigcup a$, entonces $\exists y \in a$ tal que $x \in y$, por transitividad, $x \in a$.
Inversamente, si $x \in y$ & $y \in a$ entonces $x \in \bigcup a$, pero $\bigcup a \subseteq a$, entonces $x \in a$.

2.2 UNICIDAD DE LOS SISTEMAS DE PEANO.

Una opción para establecer la unicidad de los sistemas de Peano es obtener uno de ellos y mostrar que todos son isomorfos a él, esto es lo que se hará en esta sección.

PROPOSICION 1. $\varnothing \in W$.
Prueba:
Esta es la observación a la definición 8.

PROPOSICION 2. El conjunto $^+=\{ z \mid \exists x,y \in w(z=\langle x,y\rangle \wedge y=x^+=x \cup \{x\}) \}$ es una función, es decir,
$$^+ : w \longrightarrow w$$
$$^+(x)=x^+$$
Prueba:
Claramente el conjunto $^+$ es una relación y si $\langle x,y_1\rangle$, $\langle x,y_2\rangle$ estan en $^+$ entonces
$y_1=x^+$ y $y_2=x^+$
es decir $y_1=y_2$,
con lo que la relación es una función.

PROPOSICION 3. El conjunto vacío no es sucesor de ningún conjunto:
$\forall x(x^+ \neq \varnothing)$
Prueba:
Supóngase que $\exists x(x^+=\varnothing)$ entonces
$\exists x(x \cup \{x\}=\varnothing)$, o bien
$\exists x(x \in x \cup \{x\}=\varnothing)$, pero entonces
$\exists x(x \in \varnothing)$, lo cual es absurdo.

PROPOSICION 4. La función $^\frown$ es inyectiva:
$\forall x,y\in w(\ x\neq y \Rightarrow x^\frown \neq y^\frown\ )$

Prueba:

Es equivalente hacer ver que si $x^\frown=x\cup\{x\}=y\cup\{y\}=y^\frown$ entonces $x=y$.

Fijémonos en que

$$\bigcup a^\frown=\bigcup(a\cup\{a\})=\bigcup a\cup\bigcup\{a\}=\bigcup a\cup a\ .$$

Es decir,

$$\bigcup a^\frown=\bigcup a\cup a$$

Si además a es transitivo, por la observación a la definición 9 $\bigcup a\subseteq a$ y con esto

$$\bigcup a^\frown=a\ .$$

Por otro lado, se afirma que todo elemento de w es transitivo; esto será cierto si se prueba que el conjunto $T=\{\ x\in w|\ x$ es transistivo$\}$ es inductivo.

Es claro que $\varnothing\in T$, y si $x\in T$ por el resultado inmediato anterior $\bigcup x^\frown=x$, esto sirve para ver que $x^\frown\in T$:

De acuerdo a la definición 9 sean $z\in y\ \wedge\ y\in x^\frown$, esto significa que $z\in\bigcup x^\frown$ entonces

$$z\in\bigcup x^\frown=x\subseteq x\cup\{x\}=x^\frown$$

así, $z\in x^\frown$ con lo cual $x^\frown\in T$; por lo tanto T es inductivo y $T=w$.

Ahora concluimos la prueba de la proposición 4 si $x,y\in w$ tales que $x^\frown=y^\frown$ entonces $x=\bigcup x^\frown=\bigcup y^\frown=y$ y por lo tanto $^\frown$ es inyectiva. ∎

PROPOSICION 5. Si $x\subseteq w\ \wedge\ \varnothing\in x\ \wedge\ \forall y\in x(\ y^\frown\in x\ )$ entonces $x=w$.

Prueba:

La hipótesis dice que x es un subconjunto inductivo de w, en tal caso, $x=w$. ∎

Las proposiciones 3 – 5indican que la terna ordenada $\langle w,^\frown,\varnothing\rangle$ es un Sistema de Peano; de hecho, las proposiciones 1 a 5 son, como se indicará mas adelante, una reformulación conjuntista de los axiomas de Peano, retomando a ø como 0 y a w como los números naturales.

Si se quiere probar que cualquier sistema de Peano $\langle p,s,e\rangle$ es isomorfo a $\langle w,^\frown,\varnothing\rangle$ debe establecerse una función biyectiva $f:w\longrightarrow p$ que preserve la estructura; es decir, ha de satisfacerse

$f(\varnothing)=e$ y con esto
$f(\varnothing^\frown)=s(f(\varnothing))=s(e)$
$f(\varnothing^{\frown\frown})=s(f(\varnothing^\frown))=s(s(e))$
$f(\varnothing^{\frown\frown\frown})=s(s(s(e)))$
etc.

Estos cuantos ejemplos bastan para que se sepa, intuitivamente, como es esta función; sin embargo, debe garantizarse formalmente que se puede definir en todo w, que tal función existe.

TEOREMA 1. (Recursión en w). Sea a un conjunto, $a_0\in a$ y $f:a\longrightarrow a$ entonces existe una única función $h:w\longrightarrow a$ tal que
(1) $h(\varnothing)=a_0$
(2) $h(x^\frown)=f(h(x))$

Prueba:

Se formará h mediante funciones que satisfacen lo que interesa, es decir, si $x \in w$, $\langle x,y\rangle \in h$ $(h(x)=y)$ si existe alguna función v tal que $v(x)=y$, $dom\ v \subseteq w$, $Im\ v \subseteq a$ y además

1) Si $\emptyset \in Dom\ v$ entonces $v(\emptyset)=a_0$
2) Si $y^\frown \in Dom\ v$ entonces $y \in Dom\ v \wedge v(y^\frown)=f(v(y))$

Def. Si una función v satisface todo lo anterior, se le llamará *aproximada*.

Con esto, definimos la función $h=\bigcup\{ v \mid v$ es aproximada$\}$
Observemos primero que la colección de funciones aproximadas es un conjunto, pero esto es cierto porque

$$v \subseteq Dom\ v \times Im\ v \subseteq w \times a$$

y entonces la colección de funciones aproximadas es un subconjunto de $P(w \times a)$.
Veamos que h, así definida, es una función; para ello, basta ver que el conjunto

$$a=\{x \in w \mid \text{a lo mas un } y \in w\ \langle x,y\rangle \in h\ \}=\{\ x \in w \mid \forall y,z \in w(\ \langle x,y\rangle \in h \wedge \langle x,z\rangle \in h \Rightarrow y=z\ )\}$$

es inductivo, aunque aún no se garantiza que $Dom\ h = w$:

$\emptyset \in a$ porque si $\langle \emptyset, y_1\rangle \in h$ y $\langle \emptyset, y_2\rangle \in h$ entonces existen funciones v_1, v_2 aproximadas tales que $v_1(\emptyset)=y_1 \wedge v_2(\emptyset)=y_2$ pero v_1 y v_2 cumplen (1), entonces $y_1=v_1(\emptyset)=a_0=v_2(\emptyset)=y_2$

Supóngase que $x \in a$ y que $\langle x^\frown, y\rangle \in h \wedge \langle x^\frown, z\rangle \in h$ entonces existen funciones aproximadas u,v tales que $u(x^\frown)=y \wedge v(x^\frown)=z$, en tal caso $x^\frown \in Dom\ u \wedge x^\frown \in Dom\ v$, entonces por (2) x está en ambos dominios y además

$$y=u(x^\frown)=f(u(x)) \wedge z=v(x^\frown)=f(v(x))$$

pero $x \in a$ implica $u(x)=v(x)$, o sea, $y=z$, con lo cual $x^\frown \in a$, por lo tanto a es inductivo y h es una función.

Ahora, h debe satisfacer la conclusión del teorema; es decir, h debe ser aproximada:
— Supóngase que $\emptyset \in dom\ h$ entonces $h(\emptyset)$ se calcula através de una función aproximada v, así $h(\emptyset)=v(\emptyset)$, pero v satisface (1) entonces $h(\emptyset)=v(\emptyset)=a_0$ con lo que h cumple (1).
— Para (2), sea $x^\frown \in dom\ h$ entonces existe una función aproximada v tal que $x \in dom\ v$, $(\Rightarrow)$ $x \in Dom\ h$, $h(x)=v(x)$ y además $h(x^\frown)=v(x^\frown)$,y $v(x^\frown)=f(v(x))$, entonces

$$h(x^\frown)=v(x^\frown)=f(v(x))=f(h(x))$$

por lo tanto h satisface (2).

Falta var que h esta definida para todo $x \in w$, como $dom\ h \subseteq w$ es suficiente probar que $Dom(h)$ es inductivo, pues entonces

$$Dom(h)=\bigcup\{Dom(v) \mid v \text{ es aproximada }\}=w\ .$$

Claramente, $\{\langle \emptyset, a\rangle\}$ es una función aproximada, con lo que $\emptyset \in Dom(h)$. Supóngase que $x \in Dom(h)$, para que $x^\frown \in Dom(h)$ basta verificar que el conjunto v definido por

$$v=h \cup \{\langle x^\frown, f(h(x))\rangle\}$$

sea una función aproximada.
El conjunto v es una función dado que h lo es, el único problema se presentaría con el par que se le ha agregado pues si $x^\frown$ ya estaba en $Dom(h)$ entonces existe una función aproximada v_0 tal que $h(x^\frown)=v_0(x^\frown)=f(v_0(x))=f(h(x))$

y en tal caso, el par $\langle x^{\wedge}, f(h(x))\rangle$ ya estaba en h.
Veamos que esta v es aproximada:
v satisface (1) porque $\langle \emptyset, a_0\rangle \in h$ y $v(\emptyset)=h(\emptyset)=a_0$.
Para (2) sea $y \in Dom(v)$, entonces (a) $y \in Dom(h)$ ó (b) $x^{\wedge}=y$.
(a) Si $y \in Dom(h)$ como h es aproximada $y \in Dom(h)$ y
$$v(y^{\wedge})=h(y^{\wedge})=f(h(y))=f(v(y))$$
(b) Si $y^{\wedge}=x^{\wedge}$ por la proposición 4 $y=x \in Dom(h)$ (estamos en el caso $x \in Dom(h)$ para probar $x^{\wedge} \in Dom(h)$), entonces $y \in Dom(v)$ y
$$v(y^{\wedge})=v(x^{\wedge})=f(h(x))=f(h(y))=f(v(y))$$
entonces v satisface (2) y $\therefore$ es aproximada. Esto prueba que $x^{\wedge} \in Dom(h)$ y entonces Dom(h) es inductivo
$$\therefore h: w \longrightarrow a .$$

Por último, solo resta probar que h es la única función que cumple (1) y (2), para esto sea $h': w \longrightarrow a$ que cumple la conclusión del teorema y sea
$$s=\{\, x \in w \mid h(x)=h'(x) \,\}$$
(a) $\emptyset \in s$ pues por (1)
$$h(\emptyset)=a_0=h'(\emptyset)$$
(b) Supóngase que $x \in s$, entonces $h(x)=h'(x)$ y por (2)
$$h(x^{\wedge})=f(h(x))=f(h'(x))=h'(x^{\wedge})$$
entonces $x^{\wedge} \in s$.
(a) y (b) prueban que s es inductivo, por lo tanto $s=w$ y $h=h'$, con lo cual h es única. ∎

LEMA. $\forall x \in w(\, x=\emptyset \vee \exists z \in w(\, z^{\wedge}=x \,))$
Prueba:
Sea $a=\{\, x \in w \mid x=\emptyset \vee \exists z \in w(\, z^{\wedge}=x \,) \,\}$
Claramente $\emptyset \in a$ y si $\emptyset \neq x \in a$ entonces $\exists z \in w(\, z^{\wedge}=x \,)$, entonces $x^{\wedge}=z^{\wedge\wedge}$, así $x^{\wedge} \in a$.
Entonces $a \subseteq w$ es inductivo y esto prueba el lema. ∎

Con todo esto ya puede establecerse el resultado buscado,

TEOREMA 2. Sea $\langle p, s, e\rangle$ un Sistema de Peano, entonces el Sistema de Peano $\langle w, ^{\wedge}, \emptyset\rangle$ es isomorfo al primero.
Prueba:
Por el Teorema de Recursión, para $e \in p$ y $s: p \longrightarrow p$ existe una función $f: w \longrightarrow p$ tal que
$$f(\emptyset)=e$$
$$y \quad f(x^{\wedge})=s(f(x))$$
Veamos que
(1) f es inyectiva:
Sea $a=\{\, x \in w \mid \forall y \in w(\, f(x)=f(y) \Rightarrow x=y \,) \,\}$, se afirma que a es inductivo:
1) $\emptyset \in a$:
Sea $y \in w$ tal que $f(\emptyset)=f(y) \wedge \emptyset \neq y$, por el lema anterior $\exists z \in w(\, y=z^{\wedge} \,)$, entonces
$e=f(\emptyset)=f(y)=f(z^{\wedge})=s(f(z))$
lo cual es absurdo pues e no pertenece a la imagen de s.
2) $x \in a \Rightarrow x^{\wedge} \in a$
Sea $x \in a$ & $y \in w$ tales que
$f(x^{\wedge})=f(y)$, si $y=\emptyset$
$f(x^{\wedge})=f(\emptyset)=e$, entonces

e=f(x⁺)=s(f(x)) lo cual es absurdo, entonces debe ser y≠ø
entonces existe z∈w tal que y=z⁺ y
f(x⁺)=f(y)=f(z⁺), entonces
s(f(x))=s(f(z)), pero s es inyectiva, entonces
f(x)=f(z), pero x∈a, entonces para este z
x=z, entonces
x⁺=z⁺=y, entonces x⁺∈a.

Por lo tanto a es inductivo y entonces f es inyectiva.

(ii) Im(f)=p
a)Como f(ø)=e, e∈Im(f)
b)Sea n∈Im(f), entonces existe x∈w tal que
n=f(x), entonces
s(n)=s(f(x))=f(x⁺), entonces
s(n)∈Im(f),
Por (a) y (b) Im(f) tiene a e y es cerrado bajo s, por
(iii) para el sistema de Peano <p,s,e>, se tiene que Im(f)=p

Por lo tanto <w,⁺,ø> es isomorfo a <p,s,e> .

Ahora ya puede darse una descripción de los elementos del conjunto w del sistema de Peano <w,⁺,ø> y por tanto de cualquier otro.
Al elemento ø∈w se le llama *cero* y se le denota como

$$0:=\emptyset$$

por aplicaciones sucesivas de la función ⁺ se obtiene el resto de los elementos (principio de inducción):

$$1:=0^+=\emptyset^+=\{\emptyset\}$$
$$2:=1^+=\{\emptyset\}^+=\{\emptyset,\{\emptyset\}\}=\{0,1\}$$
$$3:=2^+=\{\emptyset,\{\emptyset\}\}^+=\{\ \emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\ \}=\{0,1,2\}$$
$$4:=3^+=\{0,1,2,3\}$$
$$\vdots$$
$$n=(n-1)^+=\{0,1,2,\ldots,n-1\}$$

esta imagen de w se denota como

$$\mathbb{N}=\{0,1,2,3,\ldots,n,\ldots\}$$

Obsérvese que la definición de estos símbolos hace uso de los axiomas de vacío, del par y de unión y, por otro lado, a simple vista, se les nota la propiedad de ser conjuntos transistivos; sin embargo, no cualquier conjunto transitivo está en ℕ, por ejemplo el conjunto

$$\{\emptyset,\{\emptyset\},\{\{\emptyset\}\}\}$$

es transitivo pero no está en ℕ, el candidato natural sería el conjunto 3, esto porque ambos conjuntos tienen "tres" elementos, pero no son iguales pues {{ø}}∉3.

Entonces, la propiedad de ser un conjunto transitivo no es suficiente para establecer una caracterización de los elementos (números naturales) de ℕ, para completar esa caracterización se requieren algunos conceptos adicionales.

2.3 RELACIONES DE ORDEN

DEFINICION 10. Sean a un conjunto y r una relación, se dice que r es una *relacion sobre* a si r⊆axa.

DEFINICION 11. Sean a un conjunto y r una relación sobre a

(a) r es *reflexiva* si $\forall x \in a(\ \langle x,x\rangle \in r\ )$
(b) r es *irreflexiva* si $\forall x \in a(\ \langle x,x\rangle \notin r\ )$
(c) r es *simetrica* si $\forall x,y \in a(\langle x,y\rangle \in r \Rightarrow \langle y,x\rangle \in a)$
(d) r es *asimetrica* si $\forall x,y \in a(\ xry \Rightarrow \neg yrx\ )$
(e) r es *antisimetrica* si $\forall x,y \in a(\ xry \wedge yrx \Rightarrow x=y\ )$
(f) r es *transitiva* si $\forall x,y,z \in a(\ xry \wedge yrz \Rightarrow xrz\ )$
(g) r es *dicotomica* si $\forall x,y \in a(\ xry \vee yrx\ )$
(h) r es *tricotomica* si $\forall x,y \in a(\ xry \vee x=y \vee yrx\ )$
(i) r es *de equivalencia* si r es reflexiva, simétrica y transitiva.

A continuación, la definición de un objeto que permitirá, mas adelante, construir nuevos objetos de otros ya construidos.

DEFINICION 12. Sean a un conjunto y $p \subseteq P(a)$. se dice que p es una *particion* de a si

(i) $\cup p = a$
(ii) $\forall x,y \in p(\ x \cap y = \emptyset\ )$
(iii) $\forall x \in p(\ x \neq \emptyset\ )$

La proposición siguiente es una relación importante entre las particiones y las relaciones de equivalencia.

PROPOSICION 6. Sea r una relación de equivalencia sobre un conjunto a, para cada $y \in a$ sea $y_r := \{\ x \in a \mid \langle x,y\rangle \in r\ \}$ entonces $p := \{\ y_r \mid y \in a\ \}$ es una partición de a . Inversamente, si $p \subseteq P(a)$ es una partición del conjunto a entonces $r \subseteq a \times a$ dado por

$$\langle x,y\rangle \in r \Leftrightarrow \exists u \in p(\ x,y \in u\ )$$

es una relación de equivalencia sobre a.

Prueba:

Cada y_r es un subconjunto de a, entonces $p \subseteq P(a)$; así, $\cup p \subseteq a$.
Sea $y \in a$, como r es reflexiva $y \in y_r = \{\ x \in a \mid \langle x,y\rangle \in r\ \} \in p$ entonces $y \in \cup p$, por lo tanto $a = \cup p$, que es la primera parte de la definición 12. Además, para toda $y \in a$ sucede que $y \in y_r$, con lo cual $\forall y_r \in p(\ y_r \neq \emptyset\ )$.
Sean ahora, $y_r, z_r \in p$ tales que $y_r \neq z_r$, supóngase además que $y_r \cap z_r \neq \emptyset$ y tómese $x \in y_r \cap z_r$, entonces $\langle x,y\rangle \in r$ & $\langle x,z\rangle \in r$ pues $y \in y_r$ & $z \in z_r$.
Si $z' \in z_r$ entonces, como r es simétrica

$$\langle z',z\rangle \in r \ \&\ \langle z,x\rangle \in r \ \&\ \langle x,y\rangle \in r$$

como r es transitiva se tiene que $\langle z',y\rangle \in r$; es decir,

$$z' \in y_r, \text{ o bien}$$
$$z_r \subseteq y_r.$$

Analogamente, si $y' \in y_r$ entonces

$$\langle y',y\rangle \in r \ \&\ \langle y,x\rangle \in r \ \&\ \langle x,z\rangle \in r, \text{ en tal caso}$$
$$\langle y',z\rangle \in r \text{ ó } y' \in z_r; \text{ es decir}$$
$$y_r \subseteq z_r.$$

Por tanto, $y_r = z_r$, lo cual es una contradicción, así que debe ser $x_r \cap y_r = \emptyset$. Esto pueba que p es una partición de a.

Sea ahora, $p \subseteq P(a)$ una partición de a, veamos que r, especificada como en la proposición, es una relación de equivalencia.

i) r es reflexiva:

Sea $x \in a$, entonces $\exists u \in p(\ x \in u\ )$ entonces $\langle x,x\rangle \in r$.

ii) r es simétrica:
Sean $x,y\in a$ tales que $\langle x,y\rangle\in r$, por definición, $\exists u\in p(x,y\in u)$, entonces $\exists u\in p(y,x\in u)$; o sea, $\langle y,x\rangle\in r$.
iii) r es transitiva:
Sean $x,y,z\in a$ tales que $\langle x,y\rangle\in r$ & $\langle y,z\rangle\in r$, entonces existen elementos u y v en p tales que $x,y\in u$ & $y,z\in v$, de lo cual se sigue que $u\cap v\neq\emptyset$, como p es una partición de a usamos (ii) de la definición 12 para decir que $u=v$; así, $x,y,z\in u$, de aquí, $\langle x,z\rangle\in r$. ∎

Observación: $\forall x,y\in a(\ x\in r=y_r \iff \langle x,y\rangle\in r\ )$
Prueba:
Supóngase que $\langle x,y\rangle\in r$ y sea $z\in x_r$ entonces $\langle z,x\rangle\in r$ y por transitividad $\langle z,y\rangle\in r$; es decir, $z\in y_r$, con lo cual $x_r\subseteq y_r$:
Para que $y_r\subseteq x_r$ basta invertir los papeles de x & y en la deducción anterior. ∎

Continuamos definiendo una tipo especial de relaciones que se manejarán continuamente en el resto de este trabajo.

DEFINICION 13: Sea r una relación sobre un conjunto *a*,
1. r es un *orden parcial reflexivo* en *a* si r es reflexiva, antisimétrica y transitiva sobre *a*.
2. r es un *orden parcial estricto* en *a* si r irreflexiva, y transitiva (por lo tanto asimétrica) sobre *a*.
3. r es un *orden total* (ó *lineal*) *reflexivo* en *a* si es un orden parcial reflexivo y r es dicotómica sobre *a*.
4. r es un *orden total* (ó *lineal*) *estricto* en *a* si es un orden parcial estricto y r es tricotómica sobre *a*.

Si r es un orden parcial (ó total) reflexivo en *a* y e es un orden parcial (ó total) estricto puede decirse simplemente que r ó e son ordenes parciales en *a* en base a:

$$(r)_e:=\{\langle x,y\rangle\mid \langle x,y\rangle\in r\ \wedge\ x\neq y\ \}\quad y$$
$$(e)_r:=\{\langle x,y\rangle\mid \langle x,y\rangle\in e\ \vee\ x=y\ \}$$

porque resulta que $(r)_e$ es un orden parcial (ó total) estricto en *a*, $(e)_r$ es un orden parcial (ó total) reflexivo en *a* y además $((r)_e)_r=r$ & $((e)_r)_e=e$. Tradicionalemente se usan los símbolos $<$ para el orden estricto y $\leq$ para el orden reflexivo.

DEFINICION 14: Sean a y b conjuntos, *r* una relación sobre a, $b\subseteq a$ y $m\in a$.
1. m es r-*minimal* para b si $m\in b\ \wedge\ \neg\exists x\in b(\ xrm\ \wedge\ x\neq m\ )$.
2. m es r-*maximal* para b si $m\in b\ \wedge\ \neg\exists x\in b(\ mrx\ \wedge\ x\neq m\ )$.
3. m es r-*mínimo* para b si $m\in b\ \wedge\ \forall x\in b(\ mrx\ \vee\ m=x\ )$, en tal caso se denota $m=\min_r b$.
4. m es r-*máximo* para b si $m\in b\ \wedge\ \forall x\in b(\ xrm\ \vee\ m=x\ )$, en tal caso se denota $m=\max_r b$.

Observación: i) Todo r-mínimo (maximo) es r-minimal (maximal).
ii) Si b tiene un r-minimal (r-maximal) m y r es tricotómica sobre a entonces m es r-mínimo (r-máximo).

DEFINICION 15: Sean r una relación y a un conjunto, r es un *buen orden* en a si

i) r es un orden parcial en a.

ii) Todo subconjunto no vacio de a tiene un r-mínimo:
$\forall x \subseteq a(x \neq \emptyset \Rightarrow \exists y \in x \forall z \in x(yrz \vee y=x).$

Obsérvese que si r es un buen orden en a entonces r es tricotómica sobre a y, por lo tanto, r es un orden total en a. Esto es así porque si $x,y \in a$ entonces $\emptyset \neq \{x,y\} \subseteq a$ tiene un r-mínimo, entonces xry si x es el mínimo o yrx si el mínimo es y.

Con todo lo anterior, se puede continuar la caracterización de los elementos de $\mathbb{N}$. Primero, la pertenencia ordena parcialmente a los conjuntos; es decir, si x,y son conjuntos $x<y \Leftrightarrow x \in y$ define un orden parcial y además en cada elemento $n \in \mathbb{N}$ la relación $\in_n$ dada por $x<_n y$ ó $x \in_n y$ si $x \in y$ & $x,y \in \mathbb{N}$ define un buen orden. Ahora, si x es un conjunto, $\in_x$ es un buen orden en x y x es transitivo, no ocurre necesariamente que x es un número natural; por ejemplo, sabemos que el conjunto $\mathbb{N}$ es bien ordenado y es transitivo pero él mismo no es un número natural, aquí, el problema es que $\mathbb{N}$ es "demasiado grande", que es "infinito" e intuitivamente, todos los elementos de $\mathbb{N}$ son "finitos"; de hecho, puede definirse un conjunto *finito* como aquel que es equipotente a algún elemento de $\mathbb{N}$; es decir, que existe alguna función biyectiva de aquel conjunto en algún elemento de $\mathbb{N}$. Así pues, la propiedad que hace falta pedir es que los conjuntos sean finitos, o un poco menos:

DEFINICION 16: Un conjunto x es un *numero natural*, denotado como $x \in \mathbb{N}$, si

i) x es transitivo.

ii) $\in_x$ es un buen orden en x.

iii) Todo subconjunto no vacio de x tiene un elemento $\in_x$-maximal:
$\forall y \subseteq x(y \neq \emptyset \Rightarrow \exists z(z \in y \wedge \neg \exists w(z \in_x w))$

Esta definición de número natural los dota de todas las propiedades que se les conoce, la veracidad de esta afirmación es lo que tratarán las secciones siguientes.

2.4 ORDEN EN LOS NUMEROS NATURALES

Esta sección expone dos resultados principales, uno es que el conjunto de números naturales (como apenas se definieron) es igual a ω y el otro es que es un conjunto bien ordenado.

Puede verificarse facilmente que se ha definido a $\mathbb{N}$ para que cumpla la propiedad de que siempre que un elemento $x \in \mathbb{N}$ entonces $x^+ \in \mathbb{N}$; es decir, $\mathbb{N}$ es inductivo.

PROPOSICION 7. $\emptyset \in \mathbb{N} \wedge \forall x(x \in \mathbb{N} \Rightarrow x^+ \in \mathbb{N})$

Prueba:

Primero, que $\emptyset \in \mathbb{N}$ es trivial porque las propiedades

i) $\emptyset$ es transitivo.

ii) La pertenencia $\in$ restringida a $\emptyset$ es un buen orden.

iii) Si $\emptyset \neq y \subseteq \emptyset$ entonces y tiene un elemento máximo respecto al orden de ii).

se cumplen por vacuidad.

Sea ahora $x \in \mathbb{N}$, habrá que probar que se cumplen las tres condiciones de la definición 16 para x^+:

i) x^+ es transitivo:

Sea $y \in x^- = x \cup \{x\}$, entonces $y \in x$ ∨ $y = x$

Si $y \in x$ entonces $y \subseteq x$ dado que x es transitivo;
entonces $y \in x \subseteq x^-$, así $y \subseteq x^-$.

Si $y = x$ entonces $y = x \subseteq x^-$; o sea $y \subseteq x^-$.

En cualquier caso, $\forall y \in x^- (y \subseteq x^-)$; es decir, x^- es transitivo.

ii) $\in_{x^-}$ es un buen orden:

a) P.D: $\in_{x^-}$ es un orden parcial irreflexivo:

1) P.D. $\in_{x^-}$ es una relación irreflexiva:

Sea $n \in x^-$, si $n \in x$ entonces, como $\in_x$ es irreflexiva, $n \notin n$ por tanto, $n \notin x^-$.

si $n = x$ y fuera $x = n \in_{x^-} n = x$ entonces $n \in n$ y el conjunto bien ordenado $\langle x, \in_x \rangle$ tiene al elemento $n = x$ tal que $n \in_x n$, lo cual va contra la irreflexividad de $\in_x$. Por tanto debe ser $n \neq n$ y entonces $n \notin_{x^-} n$.

En cualquier caso, $\forall n \in x^- (n \notin_{x^-} n)$; es decir, $\in_{x^-}$ es irreflexiva.

2) P.D. $\in_{x^-}$ es una relación transitiva.

Sean $u \in_{x^-} v \wedge v \in_{x^-} w$, donde $u, v, w \in x^-$.

Obsérvese primero que $u \neq x$ pues si $u = x$ entonces $x = u \in v \in x \cup \{x\}$, aquí hay dos posibilidades,

— si $v \in x$ entonces $x = u \in v \in x$ y como x es un conjunto transitivo se tiene $x \in x$, lo cual va contra la irreflexividad de $\in_x$.

— si $v = x$ entonces $x = u \in v = x$ y también se dá $x \in x$, lo cual no es posible.

Por lo tanto, efectivamente, $u \neq x$. Analogamente se prueba $v \neq x$, con lo cual se tiene

$u, v, w \in x$ ó $u, v \in x \wedge w = x$.

En el primer caso $u \in_x v$ & $v \in_x w$, entonces $u \in_x w$ porque $\in_x$ es transitiva, así $u \in_{x^-} w$.

En el segundo caso, $u \in v$ & $v \in w = x$ y como x es un conjunto transitivo resulta $u \in x = w$; o sea, $u \in_{x^-} w$.

Por lo tanto $\in_{x^-}$ es transitiva.

b) P.D. Si $\emptyset \neq y \subseteq x^-$ entonces y tiene un $\in_{x^-}$-mínimo.

Si $y \cap x \neq \emptyset$ entonces $y \cap x$ tiene un elemento n $\in_x$-mínimo.

Sea ahora cualquier $m \in y$,

si $m \in x$ entonces $m \in y \cap x$, como n es el mínimo de este conjunto, $n \in_x m$ y de aquí $n \in_{x^-} m$.

si $m = x$ entonces, como $n \in y \cap x \Rightarrow n \in x \Rightarrow n \in x = m \Rightarrow n \in_{x^-} m$ en cualquier caso $\forall m \in y (n \in_{x^-} m)$; o sea, n es el $\in_{x^-}$-mínimo del conjunto $y \subseteq x^-$.

Si $y \cap x = \emptyset$, como $y \subseteq x \cup \{x\}$ entonces $y \subseteq \{x\}$ como además $y \neq \emptyset$ resulta que $y = \{x\}$ en tal caso x es el $\in_{x^-}$-mínimo de $y \subseteq x^-$.

Habiendo probado (a) y (b) resulta que $\in_{x^-}$ es un buen orden.

iii) P.D. Si $\emptyset \neq y \subseteq x$ entonces y tiene un $\in_{x^-}$-máximo.

Si $x \in y$ entonces x es el $\in_{x^-}$-máximo de y.

Debe probarse que $\forall m \in y (m \in_{x^-} x \vee m = x)$.

Pero esto es inmediato porque si $m \in y \subseteq x^-$ entonces, por definición, $m \in x$ ∨ $m = x$; es decir, $m \in_{x^-} x \vee m = x$.

Si $x \notin y$ entonces $y \subseteq x$ & el $\in_x$-máximo de y, llamémosle n, es también $\in_{x^-}$-máximo.

Primero, que $y \subseteq x$ es porque si $z \in y \subseteq x^{\wedge}$ entonces $z \in y$ v $z=y$, como $x \in y$ & $z \in y$ no puede ser $z=x$, entonces $z \in x$ y por tanto, efectivamente, $y \subseteq x$.
Sea pues n el $\in_x$-máximo de y & tómese cualquier $m \in y \subseteq x^{\wedge}$, nuevamente, $m \neq x$, entonces $m \in x$ y como $n \in y \subseteq x \Rightarrow n \in x$ se tiene que
$m \in y$, $n \in y$ & $m, n \in x$ entonces
$m \in x n$ pues n es el máximo, por tanto $m \in x^{\wedge} n$.
Por lo tanto n es el $\in x^{\wedge}$-máximo de $y \subseteq x^{\wedge}$.
Después de probar (i), (ii) y (iii) se concluye que
$x^{\wedge} \in N$.

∎

PROPOSICION 8: $\forall x \in N(x=\in_{x^{\wedge}}\text{-}\max(x^{\wedge}))$
Prueba:
Sea $x \in N$, entonces $x^{\wedge} \in N$ y, por definición, $x^{\wedge}$ tiene un $\in_{x^{\wedge}}$-maximal x_0 y como $\in_{x^{\wedge}}$ es un orden total, x_0 es $\in_{x^{\wedge}}$-máximo. Además, $x_0 \in x^{\wedge} = \{x\} \cup x$, entonces $x_0 \in x$ ó $x_0 = x$, pero si $x_0 \in x$ sucede que $x_0 \in_{x^{\wedge}} x$ lo cual no es posible porque x_0 es máximo en $x^{\wedge}$, así que, $x=x_0=\in_{x^{\wedge}}\text{-}\max(x)$.

∎

PROPOSICION 9: $\forall x \in N(x \neq \emptyset \Rightarrow (\in_x\text{-}\max(x))^{\wedge} = x)$
Prueba:
Sea x_0 el $\in_x$-máximo de x, quiere probarse que $x_0^{\wedge} = x$.
Como $x_0 \in x$ y x es transitivo $x_0^{\wedge} \subseteq x$. Si $x \setminus x_0^{\wedge} \neq \emptyset$ tomamos $u \in x \setminus x_0^{\wedge}$, entonces $u \notin x_0^{\wedge} = x$, esto significa que $u \notin x_0$ & $u \neq x_0$, pero $u, x_0 \in x$, entonces $u \notin x x_0$ & $u \neq x_0$, por tricotomía de $\in_x$, $x_0 \in_x u$, lo cual es una contradicción, pues x_0 es el máximo de x.
Así que debe ser, $x \setminus x_0^{\wedge} = \emptyset$, por lo tanto
$x = x_0^{\wedge} = (\in_x\text{-}\max(x))^{\wedge}$.

∎

La siguiente proposición establece que N es, hasta ahora, una clase transitiva. Mas adelante se verá que, de hecho, es un conjunto.

PROPOSICION 10. $\forall x, y(x \in y \wedge y \in N \Rightarrow x \in N)$
Prueba:
Sean x,y tales que $x \in y$ & $y \in N$
i) x es transitivo:
Sean z,w tales que $z \in w$ & $w \in x$, como $y \in N$, y es transitivo, así que,
$w \in x \wedge x \in y \Rightarrow w \in y$
y también
$z \in w \wedge w \in y \Rightarrow z \in y$;
en resumen,
$z \in w \wedge w \in x$ & $z, w, x \in y$,
con esto,
$z \in y$ & $w \in y x$,
pero $\in_y$ es un buen orden (por lo tanto orden total y en particular, relación transitiva), entonces $z \in_y x$; es decir, $z \in x$, por lo tanto, x es transitivo.
ii) $\in_x$ es un buen orden en x:
Como $x \in y$ & y es transitivo, $x \subseteq y$; así, $\in_x = \in_y | x$ (la restricción de $\in_y$ a x: $\in_x = \in_y \cap x x$) y entonces $\in_x$ cumple (ii) porque $\in_y$ lo cumple.

iii) Todo subconjunto no vacío de x tiene un elemento $\in_x$-maximal:
En virtud del argumento dado en (ii), x satisface (iii).

Por lo tanto, habiendo probado (i), (ii) y (iii) para x, se tiene que $x \in \mathbb{N}$.

∎

Ya se sabe que $\mathbb{N}$ es una clase inductiva, enseguida, se prueba que $\mathbb{N} \subseteq \omega$, con lo que, usando el Esquema de Comprensión, será un conjunto y por ser inductivo será $\mathbb{N} = \omega$.

PROPOSICION 11. $\mathbb{N} \subseteq \omega$, o bien, todo conjunto inductivo contiene a $\mathbb{N}$.

Prueba:

Supóngase que $\mathbb{N}$ no está contenido en ω; es decir, existe $n \in \mathbb{N}$ tal que $n \notin \omega$. Por definición de ω, existe un conjunto inductivo a tal que $n \notin a$; de aquí, es claro que

$$n^- \setminus a = \{ x \mid x \in n^- \wedge x \notin a \} \neq \emptyset \quad \text{(pues } n \in n^- \setminus a\text{)}$$

y $n^- \setminus a \subseteq n^-$

Como $n^- \in \mathbb{N}$, $\in_{n^-}$ es un buen orden en n^- y entonces, $n^- \setminus a$ tiene un elemento m que es $\in_{n^-}$-mínimo, es decir,

(-) $m \in n^- \setminus a$

(--) $\forall x \in n^- \setminus a (m \in_{n^-} x \vee m = x)$

Ahora, $m \neq \emptyset$ pues en caso contrario, y como a es inductivo, $m = \emptyset \in a$ lo cual contradice (-). Además, $m \subseteq n$ puesto que $m \in n^- = n \cup \{n\}$ implica $m \in n$, en cuyo caso $x \in m \wedge m \in n \Rightarrow x \in n$ (pues n es transitivo); o sea, que, efectivamente, $m \subseteq n$; o puede ser que $m = n$ y en este caso $m \subseteq n$ trivialmente.

Sea p el $\in_m$-máximo de m, por la proposición 8 $p^- = m$; pero también $p \in p^- = m$, esto obliga a que $p \notin a$ porque si no fuera así, se tendría (dado que $p \in m \wedge m \in n^- \Rightarrow p \in n^-$) que $p \in n^- \setminus a$ y como m es el mínimo, entonces $m \in_{n^-} p \vee m = p$, lo cual es absurdo. Así que $p \notin a$, pero a es inductivo, entonces $m = p^- \in a$, lo cual contradice (-).

En vista de esta contradicción, lo que debe ocurrir es que $\mathbb{N} \subseteq \omega$.

∎

COROLARIO. $\mathbb{N} = \omega$

A partir de este punto, se puede hablar de $\mathbb{N}$ y ω (y sus propiedades indistintamente; es lo que se hará en los siguientes teoremas.

Pero antes se definirá un orden en $\omega (= \mathbb{N})$ y se establecerá explícitamente el principio de inducción en ω.

DEFINICION 18. $\forall x, y \in \omega (x < y \Leftrightarrow x \in y)$.

PROPOSICION 12. (Principio de Inducción en ω)

(1) $\forall x (x \text{ inductivo} \Rightarrow \omega \subseteq x)$

(2) $\forall x \subseteq \omega (x \text{ inductivo} \Rightarrow \omega = x)$

(3) Sea φ un fórmula conjuntista. Si

i) $\varphi(0)$

ii) $\forall x \in \omega (\varphi(x) \Rightarrow \varphi(x^-))$

entonces $\forall x \in \omega (\varphi(x))$.

Prueba:

(1) y (2) son inmediatos de la definición de ω.
Se probará (3) a partir de (2).
Sea $a=\{ x\in\omega \mid \varphi(x) \}\subseteq\omega$, por (1) y (ii) a es inductivo y por (2) $\omega=a$; es decir, $\forall x\in\omega(\ \varphi(x)\ )$.

■

En cuanto al principio de inducción, en (1), (2) y (3) de la proposición anterior se dice que *se aplica* inducción sobre x; en (3), $\varphi(0)$ es la *base* de la inducción y $\varphi(x)$ es la *hipótesis* de inducción.

LEMA. La pertenencia es una relación creciente en ω:
$\forall x,y\in\omega(\ y\in x \Rightarrow y^{+}\in x^{+}\ )$.

Prueba:
Sea $c(x)\equiv \forall y\in\omega(\ y\in x \Rightarrow y^{+}\in x^{+}\ )$. Usemos inducción sobre x.
i) $c(0)\equiv \forall y\in\omega(\ y\in 0 \Rightarrow y\in 0^{+}\ )$.
Esto es cierto por vacuidad.
ii) $c(x) \Rightarrow c(x^{+})\equiv \forall y\in\omega(\ y\in x^{+} \Rightarrow y^{+}\in x^{++}\ )$
Sea $\delta(y)\equiv y\in x^{+} \Rightarrow y^{+}\in x^{++}$. Inducción sobre y:
$\delta(0)$: $0\in x^{+} \Rightarrow 0^{+}\in x^{++}$.
Si $0\in x^{+}=x\cup\{x\}$, entonces se tienen dos casos:
1) $0\in x$:
Por $c(x)$ para $y=0$ se tiene
$0^{+}\in x^{+}$, pero $x^{+}\in x^{++}$, entonces $0^{+}\in x^{++}$; o sea, $\delta(0)$.
2) $0=x$
$0^{+}=x^{+}<x^{++}$, entonces, $\delta(0)$.
$\delta(y) \Rightarrow \delta(y^{+})\equiv y^{+}\in x^{+} \Rightarrow y^{++}\in x^{++}$:
Si $y^{+}\in x^{+}=x\cup\{x\}$, entonces $y^{+}\in x \vee y^{+}=x$
1) $y^{+}\in x$
por $c(x)$ para y^{+}, $y^{++}\in x^{+}$, además, $x^{+}\in x^{++}$; así, $\delta(y^{+})$
2) $y^{+}=x$
$y^{++}=x^{+}\in x^{++}$, entonces $y^{++}\in x^{++}$, entonces $\delta(y^{+})$.
Por tanto, $\forall y\in\omega(\ \delta(y)\ )$
Por tanto, $c(x) \Rightarrow c(x^{+})$,
Por tanto, $\forall x\in\omega(\ c(x)\ )$. Y esto prueba el lema.

■

PROPOSICION 13. La relación $<$ es un buen orden en ω.
Prueba:
I) $<$ es un orden total estricto:
i) $<$ es irreflexiva sobre ω:
Sea $x\in\omega$, $x<x \Longleftrightarrow x\in x$, pero por definición de $\mathbb{N}(=\omega)$
$x\in x \Longleftrightarrow x\in x^{+}x$, pero $\in^{+}$ es un orden total estricto en x^{+}, así, $x\notin x^{+}x$ y esto significa $\neg(x<x)$.
ii) $<$ es transitiva sobre ω:
Se quiere ver que $\forall x,y,z\in\omega(\ x<y \wedge y<z \Rightarrow x<z\ )$, esto es cierto si y solo si $\forall x,y,z\in\omega(\ x\in y \wedge y\in z \Rightarrow x\in z\ )$, pero esto es cierto porque $z\in\omega=\mathbb{N}$, o sea, porque z es transitivo.
iii) $<$ es tricotómica sobre ω: $\forall x,y\in\omega(\ x<y \vee x=y \vee y<x\ )$:
Sea $\varphi(x)\equiv\forall y\in\omega(\ x<y \vee x=y \vee y<x\ )$. Usamos inducción sobre x
1) $\varphi(0)\equiv\forall y\in\omega(\ 0<y \vee 0=y \vee y<0\ )$:
Sea $\psi(y)\equiv(0<y \vee 0=y \vee y<0\ )$. Ahora usamos inducción so-

bre y.
a)$\psi(0)$ es universalmente válido.
b)Sea $y\in\omega$ tal que $\psi(y)$, se desea $\psi(y^+)$:
$\psi(y)$ implica tres casos:
caso $0<y$:
como $y\in y^+$ se tiene $y<y^+$ y por transitividad $0<y^+$, entonces, en este caso, $\psi(y^+)$.
caso $y=0$:
$y^+=0^+=1 \Rightarrow y=0<1=y^+ \Rightarrow 0<y^+$, así, $\psi(y^+)$.
caso $y<0$:
Este caso no puede darse pues $y<0 \iff y\in 0=\emptyset$.
En los tres casos, $\psi(y^+)$.
Por lo tanto, $\forall y\in\omega(\ \psi(y)\ )$
Por lo tanto $\varphi(0)$.
2) Sea $x\in\omega$ y supóngase $\varphi(x)$, quiere probarse
$\varphi(x^+)\equiv\forall y\in\omega(\ x^+<y \vee x^+=y \vee y<x^+\ )$
Sea $\chi(y)\equiv x^+<y \vee x^+=y \vee y<x^+$. Inducción sobre y:
a) $\chi(0)$: $x^+<0 \vee x^+=0 \vee 0<x^+$
De $\varphi(x)$ para $y=0$ se presentan otros tres casos,
caso $x<0$:
como antes, este caso no puede darse.
caso $x=0$:
$0=x\in x^+$, entonces, $0<x^+$, así, en este caso, $\chi(0)$.
caso $0<x$:
$0<x\in x^+$ entonces, $0<x<x^+$ y por transitividad $0<x^+$ y también en este caso $\chi(0)$.
b) $\forall y\in\omega(\ \chi(y) \Rightarrow \chi(y^+)\ )$:
Sea $y\in\omega$ tal que $\chi(y)$, por probar
$\chi(y^+)\equiv x^+<y^+ \vee x^+=y^+ \vee y^+<x^+$
Nuevamente, de $\chi(y)$ se presentan tres casos:
caso $x^+<y$:
$x^+<y\in y^+ \Rightarrow x^+<y<y^+$, por transitividad $x^+<y^+$; es decir, $\chi(y^+)$.
caso $x^+=y$:
$x^+=y\in y^+$, entonces $x^+<y^+$; así, $\chi(y^+)$
caso $y<x^+$:
$y<x^+ \Rightarrow y\in x^+=x\cup\{x\}$, entonces $y\in x \vee y=x$; es decir, $y<x \vee y=x$. Si $y=x$ entonces $y^+=x^+$; es decir, $\chi(y^+)$.
Si $y<x$ por el lema anterior $y^+<x^+$.
Por lo tanto $\chi(y^+)$ y vale (b) de (2).
Por lo tanto $\varphi(x^+)$ entonces $\forall x\in\omega(\ \varphi(x)\ )$.
Y, finalmente, esto prueba que $<$ es tricotómica.

II) Todo subconjunto no vacío de ω tiene un elemento $<$-mínimo.
Sea $\emptyset\neq X\subseteq\omega$ y $n\in$, es claro que $n\in n^+\cap X$, así que $\emptyset\neq n^+\cap X\subseteq n^+$, pero $n\in\omega$ implica $n^+\in\omega$ y así, $n^+\cap X$ tiene un $\in_{n^+}$-mínimo pues $\in_{n^+}$ es un buen orden en n^+, sea m ese mínimo. Se afirma que m es $<$-mínimo en X; es decir, que $m\in X \wedge \forall p\in X(\ m<p \vee m=p\ )$.
Es inmediato que $m\in X$ y, por otro lado, si $p\in X\subseteq\omega$ y, dado que $<$ es tricotómica se tiene que
i) $n\subseteq p$ ($n<p \vee n=p$)
Como $n\in n^+\cap X$ y m es el mínimo, resulta que $m\in n^+ \vee m=p$, pero esto es lo mismo que decir $m\subseteq p$ ya que $\in_{n^+}$ es la restricción de $\in_\omega$ a n^+ y $\in_\omega$ es restricción de $\in(=<)$ a ω.
ii) $p<n$
Aquí, $p\in n\in n^+$, así, $p\in n^+$ y $p\in n\cap X$, pero $m=\min^+(n\cap X)$ entonces $m\in n^+ \vee m=p$; es decir, $m\subseteq p$.

Así, $m=<\text{-}\min(x)$.
Por lo tanto, $<$ es un buen orden en ω.

Ahora que ω es un conjunto bien ordenado se puede inducir esta característica en cualquier otro Sistema de Peano $<N,s,e>$ vía el isomorfismo que existe con $<\omega,^,0>$ para que todo Sistema de Peano sea como ω incluso en su orden.

2.5 AXIOMAS DE PEANO Y LA ARITMETICA DE LOS NUMEROS NATURALES.

Un curso estándar en que se estudian la propiedades de los Números Naturales es el desarrollo de una teoría axiomática. De los axiomas de Peano, se deducen esta propiedades, pero aquí, esos "axiomas" se derivan como teoremas de la Teoría de Conjuntos y solo refrasean las clausulas de los Sistemas de Peano.

PROPOSICION 14. El sistema $<\omega,^,0>$ es un modelo para los Axiomas de Peano:

P1. $0\in\omega$
P2. $\forall x\in\omega(\ x^\in\omega\ )$
P3. $\forall x\in\omega(\ x^\neq 0\ )$
P4. $\forall x,y\in\omega(\ x^=y^ \Rightarrow x=y\ )$
P5. $\forall a(\ a\subseteq\omega \wedge 0\in a \wedge \forall x(\ x\in a \Rightarrow x^\in a\ ) \Rightarrow a=\omega\ )$

Prueba:
P1 y P2 dicen que ω en un conjunto inductivo.
P3 dice que $0\notin Im(^)$
P4 establece que $^$ es una función inyectiva, lo cual es así por la definición de $<\omega,^,0>$.
P5 es el principio de inducción dado en la definición de $<\omega,^,0>$.

También el Teorema de Recursión es una herramienta sumamente importante en el estudio axiomático de los números naturales, pues permite establecer la aritmética.

LA SUMA EN ω.

Sean $A=\omega$, $m\in\omega$, $a=m$ y $F:\omega\longrightarrow\omega$ dada por $F(x)=x^$.
Por el Teorema de Recursión (sección 2.2) existe una única función $\sum_m:\omega\longrightarrow\omega$

tal que $\sum_m(0)=m$

y $\sum_m(n^)=(\sum_m(n))^$

La función $\sum_m$ es la "tabla de sumar del número m" y con ellas se puede definir la suma de dos números naturales cualesquiera como:

$+:\omega\times\omega\longrightarrow\omega$
$+(m,n)=\sum_m(n)$.

El teorema de recursión garantiza que la suma de números naturales esta bien definida, así por ejemplo:

$3+2:=+(3,2)=\sum_3(2)=\sum_3(1^)=(\sum_3(1))^=\sum_3(0^))^=((\sum_3(0))^)^=$

$=((3)^)^=4^=5$.

EL PRODUCTO EN ω.

Sea $A=\omega$, $a=0$, $G:\omega \longrightarrow \omega$ dada por $G(x)=x+m$ $(G=\sum_m)$ donde $m\in\omega$.

Nuevamente por el teorema de Recursión, existe una única función

$$\prod_m:\omega \longrightarrow \omega$$

tal que $\prod_m(0)=0$

y $\prod_m(n^+)=G(\prod_m(n))=\prod_m(n)+m$

La función $\prod_m$ es la "tabla de multiplicar del número m" y en base a ella se define el producto de dos números naturales como:

$$\cdot:\omega \times \omega \longrightarrow \omega$$
$$\cdot(m,n)=\prod_m(n)$$

También, el teorema de recursión garantiza que el producto de numeros naturales esta bien definido. Por ejemplo:

$3\cdot 2=\cdot(3,2)=\prod_3(2)=\prod_3(1^+)=\prod_3(1)+3=\prod_3(0^+)+3=(\prod_3(0)+3)+3=((0+3)+3)=$
$3+3=6$

Obsérvese que el cálculo anterior hace uso de algunas de las propiedadades de la suma, a saber, $0+3=3$. Enseguida se justifica esta y algunas otras propiedades.

PROPOSICION 15. El neutro aditivo. $\forall n\in\omega(\ n+0=0+n=n\ )$

Prueba:

Sea $\varphi(n)\equiv n+0=0+n \wedge 0+n=n$. Hagamos inducción sobre n.

$\varphi(0)$:

$0+0=\sum_0(0)$,por la base recursiva para $\sum_0$, $\sum_0(0)=0$.

Así, $0+0=0+0 \wedge 0+0=0$; es decir, $\varphi(0)$.

$\varphi(n) \Rightarrow \varphi(n^+)$:

Sea $n\in\omega$ tal que $\varphi(n)$

$n^++0=\sum_{n^+}(0)=n^+$., por otro lado

$0+n^+=\sum_0(n^+)=(\sum_0(n))^+=(0+n)^+$ y por hipótesis de inducción $(0+n)^+=n^+$.

Por lo tanto, $n^++0=0+n^+ \wedge 0+n^+=n^+$; esto es, $\varphi(n^+)$.

LEMA. Si $m\in\omega$ está fijo, entonces $\forall n\in\omega(\ m^++n=(m+n)^+\ )$.

Prueba:

Sea $\varphi(n)\equiv m^++n=(m+n)^+$

$\varphi(0)$:

$m^++0=\sum_{m^+}(0)=m^+$. Por la proposición anterior

$(m+0)^+=m^+$. Así, $m^++0=(m+0)^+\equiv\varphi(0)$.

$\varphi(n) \Rightarrow \varphi(n^+)$:

Sea $n\in\omega$ tal que $\varphi(n)$, quiere probarse $\varphi(n^+)\equiv m^++n^+=(m+n^+)^+$

$m^++n^+=\sum_{m^+}(n^+)=(\sum_{m^+}(n))^+=(m^++n)^+$, pero por $\varphi(n)$

$(m^++n)^+=(m+n)^{++}$. Por otro lado,

$(m+n^+)^+=(\sum_m(n^+))^+=(\sum_m(n))^{++}=(m+n)^{++}$. Por lo tanto,

$m^++n^+=(m+n^+)^+\equiv\varphi(n^+)$.

PROPOSICION 16. Conmutatividad de la suma. $\forall m,n\in\omega(\ m+n=n+m\ )$

Prueba:

Sea $\varphi(m)\equiv \forall n\in\omega(\ m+n=n+m\ )$. Inducción sobre m.

$\varphi(0)\equiv m+0=0+m$ es cierto por la proposición 14.

$\varphi(m)\Rightarrow\varphi(m^+)\equiv \forall n\in\omega(\ m^++n=n+m^+)$:

Sea ahora, $\psi(n)\equiv m^++n=n+m^+$. Inducción sobre n:

$\psi(0)\equiv m^++0=0+m^+$ es válido otra vez por la proposición 14.

$\psi(n)\Rightarrow\psi(n^+)\equiv m^++n^+=n^++m^+$:

pero $m^++n^+=\sum_{n^+}(n^+)=(\sum_{n^+}(n))^+=(m^++n)^+$, por $\psi(n)$

$$(m^++n)^+=(n+m^+)^+=(\sum_n(m^+))^+=(\sum_n(m))^{++}=(n+m)^{++}.$$

Así, $m^++n^+=(n+m)^{++}$.

Por otro lado,

$$n^++m^+=\sum_{n^+}(m^+)=\sum_{n^+}(m)^+=(n^++m)^+$$

por el lema anterior

$(n^++m)^+=(n+m)^{++}$; es decir, $n^++m^+=(n+m)^{++}$.

Por lo tanto, $m^++n^+=n^++m^+\equiv\psi(n^+)$.

Por lo tanto $\forall m,n\in\omega(\ m+n=n+m\ )$. ∎

Entre otras, la suma en $\mathbb{N}$ tiene la propiedad de ser asociativa ($\forall m,n,p\in\omega(\ (m+(n+p)=(m+n)+p)\ )$; no se incluye la prueba de este hecho, pero se establecen otros mas interesantes.

PROPOSICION 17. $\forall m,n\in\mathbb{N}(\ m+n=0\Rightarrow m=0\ \wedge\ n=0\ )$

Prueba:

Supóngase que $m+n=0$ y que $m\neq0\ \vee\ n\neq0$.

Si $m\neq0$ entonces hay un $p\in\mathbb{N}$ tal que $m=p^+$, entonces

$0=m+n=n+m=p^++n=(p+n)^+$; o sea,

$0=(p+n)^+$, lo cual es absurdo.

Si $n\neq0$ entonces $n=q^+$ con $q\in\mathbb{N}$ y, con esto,

$0=m+n=m+q^+=(m+q)^+$, donde $m+q\in\mathbb{N}$, lo cual también es una contradicción. ∎

Antes de estudiar las propiedades de la multiplicación de números naturales necesitaremos un resultado auxiliar, que es intuitivamente muy claro, pero que no se había establecido hasta ahora.

LEMA. $\forall n\in\mathbb{N}(\ n+1=n^+\ )$.

Prueba:

Sea $n\in\mathbb{N}$, $n+1=\sum_n(1)=\sum_n(0^+)=\sum_n(0)^+=n^+$.

Entonces $n+1=n^+$. ∎

PROPOSICION 18. El neutro multiplicativo. $\forall n\in\mathbb{N}(\ n\cdot1=1\cdot n=n\ )$

Prueba:

Sea $n\in\mathbb{N}$, $n\cdot1=\prod_n(1)=\prod_n(0^+)=\prod_n(0)+n=00+n=n$.

Para probar que $1\cdot n=n$ usamos inducción sobre n.

i) $1\cdot0=\prod_1(0)=0$

ii) Supóngase que $1\cdot n=n$, queremos ver que $1\cdot n^+=n^+$.

Pero

$$1\cdot n^+=\prod_1(n^+)=\prod_1(n)+1=1\cdot n+1$$

por hipótesis de inducción $=n+1$

por el lema anterior $=n^+$.

Por lo tanto $\forall n\in\mathbb{N}(\ n\cdot 1=1\cdot n \wedge 1\cdot n=n\ )$.

PROPOSICION 19. $\forall n\in\mathbb{N}(\ n\cdot 0 = 0\cdot n = 0\ )$

Prueba:

Sea $n\in\mathbb{N}$, $n\cdot 0=\prod_n(0)=0$,

Probamos que $0\cdot n=0$ empleando inducción sobre n.

1) $0\cdot 0=\prod_0(0)=0$.

11) Supóngase que $0\cdot n=0$, quiere probarse que $0\cdot n^{\wedge}=0$.

pero

$$0\cdot n^{\wedge}=\prod_0(n^{\wedge})=\prod_0(n)+0=0\cdot n+0,$$

por hipótesis de inducción $=0+0$

por la proposición 14 $=0$.

Por lo tanto, $\forall n\in\mathbb{N}(\ n\cdot 0 = 0 \wedge 0\cdot n = 0\ )$.

Puede verificarse, de manera igualmente laboriosa que el producto de números naturales tiene las propiedades de conmutatividad $(n\cdot m=m\cdot n)$, asociatividad $(m\cdot(n\cdot p)=(m\cdot n)\cdot p)$ y distributividad respecto a la suma $(m\cdot(n+p)=m\cdot n+m\cdot p)$. Si se prueban otras propiedades interesantes del producto en $\mathbb{N}$.

PROPOSICION 20. $\forall m,n\in\mathbb{N}(\ m\cdot n=0 \Rightarrow m=0 \vee n=0\ )$.

Prueba:

Supóngase que $m\cdot n=0$ y que $m\neq 0 \wedge n\neq 0$, entonces se pueden encontrar elementos p y q de $\mathbb{N}$ tales que $p^{\wedge}=m$ y $q^{\wedge}=n$, entonces

$$0=m\cdot n=p^{\wedge}\cdot q^{\wedge}=p^{\wedge}\cdot(q+1)=p^{\wedge}\cdot q+p^{\wedge}.$$

Pero dada la igualdad $0=p^{\wedge}\cdot q+p^{\wedge}$, se tiene, por la proposición 16 que $p^{\wedge}=0$, lo cual no es posible.

Esta contradicción prueba la proposición.

En adelante, cuando no haya confusión, se escribira $m\cdot n$ como mn, para facilitar la lectura.

PROPOSICION 21. $\forall m,n\in\mathbb{N}(\ mn=1 \Rightarrow m=1 \wedge n=1\ )$

Prueba:

Supóngase $mn=1$, de hecho, ocurre $m\neq 0$ y $n\neq 0$, entonces $m=p^{\wedge}=p+1$ & $n=q^{\wedge}=q+1$ con $p,q\in\mathbb{N}$, entonces

$$1=(p+1)(q+1)=pq+p\cdot 1+1\cdot q+1\cdot 1=pq+p+q+1=(pq+p+q)^{\wedge}$$

esto significa, usando P4 de la proposición 13, que $pq+p+q=0$, aplicando dos veces la proposición 16 se llega a que

$p=0$ & $q=0$, por lo tanto

$m=p^{\wedge}=0^{\wedge}=1$ y

$n=q^{\wedge}=0^{\wedge}=1$.

Algo que también es importante es observar las relaciones que existen entre las operaciones y el orden en un conjunto. Las siguientes proposiciones prueban algunas de las compatibilidades entre las operaciones y el orden en $\mathbb{N}$ establecido en la definición 18.

PROPOSICION 22. $\forall m,n,p\in N(\ m<n \Rightarrow m+p<n+p\ )$

Prueba:

Supondremos m y n fijos y probaremos $\varphi(p)\equiv m<n \Rightarrow m+p<n+p$ por inducción sobre p.

$\varphi(0)$:

Sea m<n, como m=m+0 y n=n+0 se tiene m+0<n+0: es decir, $\varphi(0)$.

$\varphi(p) \Rightarrow \varphi(p+1)$:

Sea m<n entonces , debido a $\varphi(p)$, m+p<n+p. Ahora, por el lema previo a la proposición 12 (m+p)+1<(n+p)+1, o bien,

$$m+(p+1)<n+(p+1)$$

que es $\varphi(p+1)$.

COROLARIO. $\forall m,n,p,q\in N(\ m<n \wedge p<q \Rightarrow m+p<n+q\ )$.

Prueba:

De m<n y la proposición anterior m+p<n+p.

Analogamente, de p<q se tiene, p+n<q+n.

Por conmutatividad de + y transitividad de <, resulta

$$m+p<n+q\ .$$

PROPOSICION 23. $\forall m,n,p\in N(\ m<n \Rightarrow mp\leq np\ )$.

Prueba:

Otra vez, supondremos m y n fijos y aplicamos inducción sobre p para probar $\varphi(p)\equiv \forall p\in N(\ m<n \Rightarrow mp\leq np\ )$.

$\varphi(0)$:

Sabemos que $n\cdot 0=0=m\cdot 0$, asi, $m\cdot 0\leq n\cdot 0\equiv\varphi(0)$.

$\varphi(p) \Rightarrow \varphi(p+1)$:

Sea m<n, por $\varphi(p)$ $mp\leq np$. Ahora, si mp<np entonces, por el corolario a la proposición anterior

$$mp+m<np+n, \quad \text{o bien,}$$
$$m(p+1)<n(p+1)$$

Falta el caso en que mp=np, aqui empleamos directamente la proposición anterior para obtener, junto con m<n, que

$$m+mp<n+mp=n+np\ ,$$

entonces $m(p+1)<n(p+1)$.

En cualquier caso se satisface, en particular

$$m(p+1)\leq n(p+1) \equiv \varphi(p+1).$$

COROLARIO. $\forall m,n,p,q\in N(\ m<n \wedge p<q \Rightarrow mp<nq\ )$

Prueba:

$m<n \Rightarrow mp<np$ y

$p<q \Rightarrow pn<qn$, por transitividad y conmutatividad

$$mp<nq.$$

Todos los resultados de esta sección y otros que ya no se incluyen (por ejemplo, "leyes de cancelación") se prueban de los Axiomas de Peano y de la definición del orden , pero estos conceptos e ideas han sido derivados directamente de la Teoria de Conjuntos; asi que, en última instancia, todas las propiedades de los Números Naturales son consecuencia de la Teoria de Estratos ya que de ahi se han obtenido las relaciones y propiedades de los conjuntos.

Una vez que lo anterior ha quedado claro, debe reflexionarse en que en la Teoria de Conjuntos se modelan muy bien los Números Naturales,

pero no debe afirmarse que cada uno de ellos sea, realmente, un conjunto; de hecho, la noción intuitiva con que de ellos se cuenta no tiene nada que ver con los conjuntos.

Por último, como se observó al principio de este capítulo, el conjunto $\omega=N$ es un conjunto inductivo, de hecho, el menor de todos ellos; si se desea ubicar este conjunto en alguno de los estratos construidos en el capítulo anterior, debe recordarse que el Axioma de Infinitud ZFS, postula la existencia de un conjunto inductivo que se localiza en un estrato cuya existencia se garantiza por TE6; además, observemos que el elemento $0=\emptyset$ se encuentra en el estrato cero, el $1=0^+$ se ecuentra en el estrato uno, y sucesivamente: el número n se encuentra en el n-ésimo estrato; por inducción, puede verse que el conjunto ω se encuentra en el estrato que en su momento fue denotado, precisamente, como ω.

La primera forma en que conocimos los números enteros indica que ellos son los números positivos (los números naturales) junto con los negativos; la forma estándar para representarlos es un símbolo, digamos 1, y el mismo símbolo precedido de un *menos* para el negativo correspondiente, -1. Que mejor que tomar esta concepción para usarla como base para dar una definición formal y natural de los Números Enteros: ya se cuenta con los números naturales, ahora habrá que añadirles los negativos.

Primero, se hace un paréntesis para definir la *diferencia* o *resta* de números naturales; esto permitirá, mas adelante, construir los números negativos y la operaciones para los enteros.

3.1 ALGUNAS PROPIEDADES ADICIONALES DE $\mathbb{N}$.

PROPOSICION 1. $\forall m,n\in\mathbb{N}(\ m\leq n \Rightarrow \exists d\in\mathbb{N}(\ n=m+d\ )\ )$

Prueba:

Sea $\varphi(n)\equiv \forall m\in\mathbb{N}(\ m\leq n \Rightarrow \exists d\in\mathbb{N}(\ n=m+d\ )\ )$, se probará $\forall n\in\mathbb{N}(\ \varphi(n)\ )$ por inducción sobre n.

$\varphi(0)$:

Si $m\leq 0$ entonces $m=0$ y $d=0$ hace que $\varphi(0)$ se válida.

$\varphi(n) \Rightarrow \varphi(n+1)$:

Supóngase $m\leq n+1$; si $m<n+1$ entonces $m\leq n$ y $\varphi(n)$ dice que hay un elemento $d\in\mathbb{N}$ tal que $n=m+d$ y entonces

$$n+1=m+d+1,$$

así, $d'=d+1$ satisface $\varphi(n+1)$.

Ahora, si $m=n+1$, con $d=0$ se cumple $\varphi(n+1)$.

∎

COROLARIO. $\forall m,n\in\mathbb{N}(\ m\leq n \Rightarrow \exists d\in\mathbb{N}(\ n=m+d \wedge \forall d'\in\mathbb{N}(\ n=m+d' \Rightarrow d=d')\ )\ )$.

Prueba:

Este corolario solo dice que el número $d\in\mathbb{N}$ de la proposición anterior es único, lo cual es cierto gracias a la ley de la cancelación en la suma de $\mathbb{N}$:

$$m+d=m+d' \Rightarrow d=d' .$$

∎

DEFINICION 1. Sea $D=\{\langle n,m\rangle \mid m,n\in\mathbb{N} \wedge n\leq m\} = \{x \mid \exists m,n\in\mathbb{N}(\ x=\langle n,m\rangle \wedge n\leq m\ )\}$, entonces se define

$$-:D \longrightarrow \mathbb{N}$$

$$-(\langle n,m\rangle)=d, \text{ donde d es tal que } m=n+d.$$

O bien, $\langle\langle n,m\rangle,d\rangle\in- \Leftrightarrow m=n+d$.

En virtud del corolario anterior, la relación - es, efectivamente, una función, y el elemento $d\in\mathbb{N}$ se denota como

$$d=m-n$$

y se llama de *resta* o *diferencia* entre m y n.

3.2 LOS NUMEROS ENTEROS Y SU ORDEN

La siguiente definición recoge las ideas expuestas en los primeros párrafos de este capitulo.

DEFINICION 2. Sea $\mathbb{N}^+=\mathbb{N}\setminus\{0\}$, $\mathbb{N}^-=\{<0,n>\mid n\in\mathbb{N}^+\}=\{x\mid \exists n\in\mathbb{N}(\ n\neq 0 \wedge x=<0,n>)\}$
y sea $\mathbb{Z}=\mathbb{N}^+\cup\mathbb{N}^-\cup\{0\}=\mathbb{N}\cup\mathbb{N}^-$

Por el axioma de unión, $\mathbb{Z}$ es un conjunto, el conjunto de los *Números Enteros*, $\mathbb{N}^+$es el conjunto de *enteros positivos* y $\mathbb{N}^-$ es el conjunto de *enteros negativos*.

Enseguida se define el *opuesto* de un número entero mediante una función de un argumento, se abusa de la notación y se denota con el mismo simbolo que el empleado para la diferencia entre números naturales.

DEFINICION 3. La función $-:\mathbb{Z}\longrightarrow\mathbb{Z}$ dada por
i) $-(n)=<0,n>$ si $n\in\mathbb{N}^+$
ii) $-(<0,n>)=n$ para $n\in\mathbb{N}^+$
iii) $-(0)=0$
O mas correctamente,
$<x,y>\in -\iff (\exists w\in\mathbb{N}[(\ n\neq 0 \wedge x=n \wedge y=<0,n>) \vee (n\neq 0 \wedge x=<0,n> \wedge y=n)] \vee (x=0 \wedge y=0)\ )$.
define al *opuesto* de un número entero.

Algunas observaciones sobre esta definición: primero, puede desecharse la notación <0,n> sustituyéndola por -n (inciso i), con lo que ii) queda como
$$-(-n)=n\ .$$
También, la función - es inyectiva, pues si $-x=-y$ entonces:
i) si $-x,-y\in\mathbb{N}$ entonces $x=<0,n>$, $y=<0,m>$ con $m,n\in\mathbb{N}$, así $n=-x=-y=m$ $\therefore$ $x=y$
ii) si $-x,-y\in\mathbb{N}^-$ entonces $<0,x>=-x=-y=<0,y>$ $\Rightarrow$ $x=y$.

A su vez, el orden en $\mathbb{Z}$ es una extensión del orden en $\mathbb{N}$. Por el momento, $<'$ denotará al orden en $\mathbb{Z}$, después de caracterizarlo, se le denotará de la misma forma que el orden de $\mathbb{N}$.

DEFINICION 4. Sean $x,y\in\mathbb{Z}$, definimos $x<'y$ si y solo si
$(\ x,y\in\mathbb{N} \wedge x<y\ ) \vee (\ x,y\in\mathbb{N}^- \wedge -y<-x\ ) \vee (\ x\in\mathbb{N}^- \wedge y\in\mathbb{N}\ )$.

Ejemplos:
1) $\forall y\in\mathbb{N}^-(\ x<'0\ )$: Todos los enteros negativos son menores que cero.
2) $\forall y\in\mathbb{N}^+(\ 0<'y\ )$: Todos los enteros positivos son mayores que cero.
3) $\forall y\in\mathbb{N}^-\forall x\in\mathbb{N}^-(\ x<'y\ )$: Todos los negativos son menores que todos los positivos.

PROPOSICION 2. La relación $<'$ es un orden total estricto.
Prueba:
a) $<'$ es irreflexiva: $\forall x\in\mathbb{Z}(\neg(\ x<'x\ ))$.
Sea $x\in\mathbb{Z}$, si $x\in\mathbb{N}$ entonces $\neg(\ x<'x\ )$ pues $\neg(\ x<x\ )$.
Si $x\in\mathbb{N}^-$ entonces $-x\in\mathbb{N}^+\subseteq\mathbb{N}$ y $x<'x \iff -x<-x$.
Como $\neg(\ -x<-x\ )$ entonces $\neg(\ x<'x\ )$.
b) $<'$ es transitiva: $\forall w,x,y\in\mathbb{Z}(\ w<'x \wedge x<'y \Rightarrow w<'y\ )$.
Supónganse $w,x,y\in\mathbb{Z}$ tales que $w<'x$ & $x<'y$
aquí hay, en principio, varios casos:
i) $w,x,y\in\mathbb{N}$, entonces $w<'x$ por transitividad de $<$.
ii) $w,x\in\mathbb{N}$ $\wedge$ $y\in\mathbb{N}^-$, este caso no puede darse (ejemplo 3).
iii) $w,y\in\mathbb{N}$ $\wedge$ $x\in\mathbb{N}^-$, este caso no puede darse (ejemplo 3).
iv) $x,y\in\mathbb{N}$ $\wedge$ $w\in\mathbb{N}^-$, entonces $w\in\mathbb{N}^-$ $\wedge$ $y\in\mathbb{N}$, entonces $w<'y$.
v) $w\in\mathbb{N}$ $\wedge$ $x,y\in\mathbb{N}^-$, este caso no puede darse.

vi) $x\in\mathbb{N} \wedge w,y\in\bar{\mathbb{N}}$, este caso no puede darse.
vii) $y\in\mathbb{N} \wedge w,x\in\bar{\mathbb{N}}$, entonces $w<y$ por el caso (iv).
viii) $w,x,y\in\bar{\mathbb{N}}$, entonces $-w,-x,-y\in\mathbb{N}$, luego, $-x<-w \wedge -y<-x$,
por transitividad de $<$, $-y<-w$,
esto significa $w<'y$.

c) $<'$ es tricotómica sobre $\mathbb{Z}$: $\forall x,y\in\mathbb{Z}(\ x<'y \vee x=y \vee y<'x\ )$.
Sean $x,y\in\mathbb{Z}$, se presentan tres casos:
i) $x,y\in\mathbb{N}$, por tricotomía de $<$ se tiene $x<'y \vee x=y \vee y<'x$.
ii) $x,y\in\bar{\mathbb{N}}$, entonces $-x,-y\in\mathbb{N}$ y por tanto,
$-x<-y \vee -x=-y \vee -y<-x$
así, respectivamente,
$y<'x \vee x=y \vee x<'y$.
iii) $x\in\mathbb{N} \wedge y\in\bar{\mathbb{N}}$, directamente, por definición, $y<'x$.

Por supuesto, este orden tiene asociado un orden reflexivo como se observa inmediatamente después de la definición 13 de la sección 2.3 . Se resalta este hecho, porque en lo que sigue puede hacerse referencia al orden reflexivo si es necesario.

Antes de establecer la aritmética de $\mathbb{Z}$, se presentan algunas propiedades que caracterizan a una estructura como la que se le ha dado a los números enteros.

En adelante, el símbolo $<$ denotará indistintamente a los órdenes de $\mathbb{N}$ y $\mathbb{Z}$ a menos que se especifique alguna otra cosa.

TEOREMA 1. La estructura $\langle\mathbb{Z},<,-\rangle$ satisface
(1) $<$ es on orden total en $\mathbb{Z}$.
(2) $\mathbb{N}\subseteq\mathbb{Z}$ y $<|_{\mathbb{Z}}$ es el orden usual en $\mathbb{N}$.
(3) $\forall x\in\mathbb{Z}(\ x\in\mathbb{N} \iff 0<x$.
(4) $\forall a\in\mathbb{Z}(\ -(-a)=a\ )$ y, de hecho, $-0=0$.
(5) $\forall a,b\in\mathbb{Z}(\ a<b \iff -b<-a$
Además, si cualquier otra estructura $\langle\mathbb{Z},<',-\rangle$ satisface estas propiedades, entonces es posible hallar una función biyectiva $f:\mathbb{Z}\longrightarrow\mathbb{Z}$ que deja fijo a $\mathbb{N}$ y que cumple
$f(-a)=-f(a) \wedge a<b \iff f(a)<'f(b)$.
Es decir, $\langle\mathbb{Z},<,-\rangle$ es único salvo isomorfismo.

Prueba:
(1) es la proposición 2.
(2) Esto es cierto por las definiciones 2 y 4.
(3) Esto es el ejemplo 2 de la definición 4.
(4) Este hecho se mostró inmediatamente después de la definición 3 para el caso en que $a\in\bar{\mathbb{N}}$; si ahora $a\in\mathbb{N}$ entonces por definición
$-a=\langle 0,a\rangle$, entonces
$-(-a)=-\langle 0,a\rangle$, y nuevamente de la definición 3
$-\langle 0,a\rangle=a$.
Así, $-(-a)=a$.
(5) Suponga $a<b$ y que, de acuerdo a la definición 4, se dá: .

i) a,b∈N ∧ a<'b: entonces -a,-b∈N⁻ y, por la definición 4 -b<'-a y por (2) -b<-a.

ii)a,b∈N⁻ ∧ -b<'-a: de (2) -b<-a pues -a,-b∈N.

iii) b∈N ∧ a∈N⁻: entonces -b∈N⁺ ∧ -b∈N⁺, por la definición 4 -b<-a.

En cualquier caso, -b<-a.

Sea ahora, una estructura <Z,<',-) que satisface (1)-(5); (2) permite definir

f:Z⟶Z
f(x)=x si x∈N
f(x)=-x si x∈N⁺.

O mas correctamente:

<x,y>∈f ⇔ (x∈N ∧ y=x) ∨ (∃z∈N⁺(x=-z ∧ y=-z))

——Veamos que f es inyectiva

Sean x,y∈N tales que x≠y, se analizan los tres casos:

i) x,y∈N, entonces
f(x)=x
f(y)=y, por lo tanto f(x)≠f(y).

ii) x,y∈N⁻, entonces -x,-y∈N &
f(x)=f(--x)=--x .
f(y)=f(--y)=--y
Si fuera f(x)=f(y) se tendría
--x=--y, pero - es función, entonces
---x=---y, por (4) aplicado a -
-x=-y, como - es inyectiva
x=y lo cual es absurdo.

iii) x∈N, y∈N⁻, entonces
f(x)=x
f(y)=f(--y)--y
si fuera f(x)=f(y) sería
x=--y, pero x>0, entonces
--y>0, por (2)
--y∈N, otra vez por (2)
--y'>0, por(5)
---y<'- 0, por(4)
-y<'0 ----------(*)
pero y∈N⁻ implica -y∈N, o sea, 0<-y , por (2) 0<'-y que es lo contario de (*).

——Veamos que f es suprayectiva.

Sea z∈Z, como <' es total:

i) 0≤'z, entonces z∈N y así, z=f(z).

ii) z<'0, entonces 0=-0<'-z, o bien 0<-z, de aquí, -z=m∈N⁺ entonces f(-m)=-m=--z=z.

——Se afirma que f(-x)=-f(x):

i) si x=0∈N entonces f(-0)=f(0)=0
-f(0)=-0=0, por tanto, f(-0)=-f(0).

ii) si x∈N⁺ entonces f(-x)=-x=-f(x).

iii) si x∈N⁻ entonces -x∈N⁺ y
f(-x)=-x
-f(x)=-f(--x)=---x=-x, es decir,
f(-x)=-f(x).

——Probemos x<y ⇒ f(x)<'f(y):

i) si x,y∈N el resultado es inmediato.

ii) si x,y∈N⁻ entonces -x,-y∈N y por tanto,
f(x)=f(--x)=--x
f(y)=f(--y)=--y

por otro lado, como $x<y$
$-y<-x$, entonces
$0<-y<-x$, esto implica
$0<^{'}-y<^{'}-x$; así,
$--x<^{'}--y$ que es lo mismo que
$f(x)<^{'}f(y)$.

iii) si $x\in\mathbb{N}^{-}\ \wedge\ y\in\mathbb{N}$
$f(x)=f(--x)=--x$
$f(y)=y$
pero $x<0$ implica $-x>0$ entonces $0<^{'}-x \Rightarrow --x<^{'}0$,
por otro lado, $y\in\mathbb{N} \Rightarrow y\geq 0 \Rightarrow 0\leq y$,
por transitividad $--x<^{'}y$
o bien $f(x)<^{'}f(y)$.

∎

El teorema anterior es una caracterización de la estructura $\langle \mathbb{Z}, <, - \rangle$, donde el orden es tal que extiende al de $\mathbb{N}$ y además es un orden total. Mas adelante, se establecerá otro resultado de unicidad de $\mathbb{Z}$ que involucra propiedades adicionales del orden; primero se hablará un poco de la aritmética de $\mathbb{Z}$. Temporalmente se denotarán los signos para la suma y resta en $\mathbb{N}$ con negritas (+,-) para diferenciarlos de los correspondientes para $\mathbb{Z}$.

3.3 LA ARITHETICA DE LOS NUMEROS ENTEROS

DEFINICION 5. La suma de números enteros es la función

$$+:\ \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$$

$$+(a,b)=\begin{cases} a+b & \text{si } a,b\in\mathbb{N}^{-} & \text{----(+1)}\\ -(-a+-b) & \text{si } a,b\in\mathbb{N}^{-} & \text{----(+2)}\\ a-(-b) & \text{si } a\in\mathbb{N}\ \wedge\ b\in\mathbb{N}^{-}\ \wedge\ -b\leq a & \text{----(+3)}\\ -(-b-a) & \text{si } a\in\mathbb{N}\ \wedge\ b\in\mathbb{N}^{-}\ \wedge\ a\leq -b & \text{----(+4)}\\ b-(-a) & \text{si } a\in\mathbb{N}^{-}\ \wedge\ b\in\mathbb{N}\ \wedge\ -a\leq b & \text{----(+5)}\\ -(-a-b) & \text{si } a\in\mathbb{N}^{-}\ \wedge\ b\in\mathbb{N}\ \wedge\ b\leq -a & \text{----(+6)} \end{cases}$$

Por supuesto, se escribe a+b en lugar de +(a,b).

Esta definición cumple las propiedades que ya se conocen sobre ella y que se enuncian enseguida; como las pruebas son tediosas, aunque sencillas, solo se dan algunas de ellas.

PROPOSICION 3. $\forall x,y\in\mathbb{Z}$ se cumple
(S1) $x+y=y+x$
(S2) $x+(y+z)=(x+y)+z$
(S3) $x+0=x$
(S4) $x+(-x)=0$

Prueba:
(S1) Solo en algunos casos
i) Supóngase $x\in\mathbb{N}$, $y\in\mathbb{N}^{-}$, $-y\leq x$; por (+3)
$x+y=x-(-y)$
calculamos y+x por otro lado, usando (+5)
$y+x=x-(-y)$.
Así, $x+y=y+x$.
ii) Supóngase $x,y\in\mathbb{N}^{-}$; por (+2)

$x+y=-(-x+-y)=-(-y+-x)=y+x.$

(S3) i) Sea $x\in\mathbb{N}$, como $0\in\mathbb{N}$

$x+0=x+0=x$

ii) Sea $x\in\mathbb{N}^-$, por el ejemplo 1 de la definición 4

$x<0$, o bien

$0<-x$ y como $0\in\mathbb{N}$ usamos (+6) para calcular $x+0$:

$x+0=-(-x-0)=-(-x)=x$

(S4) i) Sea $x\in\mathbb{N}$; si $x=0$ por (+1) y usando $-0=0$

$x+(-x)=0+(-0)=0+0=0+0=0$

si $x\in\mathbb{N}^-$ entonces $-x\in\mathbb{N}^-$ y por (+3)

$x+(-x)=x-(--x)=x-x=0$

ii) Sea $x\in\mathbb{N}^-$, entonces $-x\in\mathbb{N}$ y por (+5)

$x+(-x)=-x-(-x)=0$

Con objeto de definir la multiplicación de números enteros, se denota, por el momento, el producto de dos números naturales a y b como ab, empleando la cruz x para el producto de enteros.

DEFINICION 6. El producto de números enteros es la función

$$x:\mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$$

$$x(a,b)=\begin{cases} ab & \text{si } a,b\in\mathbb{N}^- \quad \text{---------(x1)} \\ (-a)(-b) & \text{si } a,b\in\mathbb{N}^- \quad \text{---------(x2)} \\ -(a(-b)) & \text{si } a\in\mathbb{N},\ b\in\mathbb{N}^- \quad \text{-------(x3)} \\ -((-a)b) & \text{si } a\in\mathbb{N}^-,\ b\in\mathbb{N}. \quad \text{-------(x4)} \end{cases}$$

Análogamente, la notación axb abrevia a x(a,b) y se tienen las propiedades usuales de la multiplicación de números enteros, de las cuales se muestran algunas de ellas.

PROPOSICION 4. $\forall r,s,t\in\mathbb{Z}$ se cumple

(P1) $rxs=sxr$

(P2) $rx(sxt)=(rxs)xt$

(P3) $rx1=r$

(P4) $rx0=0$

(P5) $rx(s+t)=rxs+rxt$

(P6) $rxs=0 \iff r=0 \vee s=0$

(P7) $rxs=1 \iff (r=1 \wedge s=1) \vee (r=-1 \wedge s=-1)$

Prueba:

(P1) Cuando $r\in\mathbb{N}$ & $s\in\mathbb{N}^-$:

Por (x3)

$rxs=-(r(-s))$,

Por (x4)

$sxr=-((-s)r)$,

como $r(-s)=(-s)r$ resulta que $rxs=sxr$.

(P3) i) Sea $r\in\mathbb{N}$, como $1\in\mathbb{N}$ usamos (x1)

$rx1=(r)(1)=r$

ii) Si $r\in\mathbb{N}^-$ usamos (x4)

$rx1=-((-r)(1))=-(-r)=r$

En cualquier caso, $r\times 1=r$.

(P4) i) $r\in\mathbb{N}$:
por (x1) $\quad r\times 0=(r)(0)=0$

ii) $r\in\mathbb{N}$:
por (x4) $\quad r\times 0=-((-r)(0))=-0=0$.

En cualquier caso $r\times 0=0$.

(P6) i) $r\in\mathbb{N}$, $s\in\mathbb{N}$:
Del hecho de que $0=r\times s=-(r(-s))$
se tiene $r(-s)=0$,
como esta última igualdad ocurre en $\mathbb{N}$, se cumple
$r=0 \vee -s=0$, y de aquí
$r=0 \vee s=0$.

ii) $r,s\in\mathbb{N}$:
$0=r\times s=(-r)(-s)$, nuevamente, como $-r,-s\in\mathbb{N}$
$-r=0 \vee -s=0$, o bien
$r=0 \vee s=0$.

(P7) La implicación de derecha a izquierda es trivial. Para la otra supóngase $r\in\mathbb{N} \wedge s\in\mathbb{N} \wedge r\times s=1$, entonces
$1=-(r(-s))$
como la función - es inyectiva
$r(-s)=-1$,
pero $r,-s\in\mathbb{N}$ implica $-1=r(-s)\in\mathbb{N}$, lo cual es absurdo, entonces este caso no puede darse. Analogamente, tampoco se dá el caso que $r\in\mathbb{N} \wedge s\in\mathbb{N} \wedge r\times s=1$
Por otro lado, el caso $r,s\in\mathbb{N}$ es trivial y la última posibilidad es $r,s\in\mathbb{N}$, en tal situación:
$1=r\times s=(-r)(-s)$
y como $-r,-s\in\mathbb{N}$ se tiene que
$-r=1 \wedge -s=1$
otra vez se usa la inyectividad de la función - para concluir
$r=-1 \wedge s=-1$

■

El orden, la suma y el producto de $\mathbb{Z}$ extienden a los de $\mathbb{N}$, es este hecho el que permite emplear los mismos signos para denotarlas.

PROPOSICION 5. El orden $<$ es compatible con la suma y el producto en $\mathbb{Z}$:
$\forall x,y,z\in\mathbb{Z}$
i) $x<y \Rightarrow x+z<y+z$
ii) $x<y \wedge z>0 \Rightarrow xz<yz$.

En la definición 1 se estableció la diferencia entre dos números naturales m, n y la exitencia del opuesto de cualquier entero permite definir la resta de cualesquiera dos números enteros: si $x,y\in\mathbb{Z}$
$x-y=x+(-y)$.

3.4 LA UNICIDAD DE LOS NUMEROS ENTEROS

Enseguida se presenta un resultado de unicidad para $\mathbb{Z}$, salvo isomorfismo, como un conjunto linealmente ordenado sin extremos donde cada subconjunto no vacío tiene un mínimo y un máximo.

TEOREMA 2. La estructura linealmente ordenada $\langle \mathbb{Z}, \leq \rangle$ satisface

(1) $\forall x \in \mathbb{Z}\ \exists y, z \in \mathbb{Z}(\ x<y \wedge z<x\ )$

(2) $\forall a \subseteq \mathbb{Z}(\ a \neq \emptyset \wedge \exists z, w \in \mathbb{Z}(\ \forall x \in a(\ z \leq x \wedge w \leq x\ )\ ) \Rightarrow \exists m, n \in a(\ \forall x \in a(\ x \leq m \wedge m \leq x\ )\ )\ )$

y si $\langle \mathbb{Z}, \leq \rangle$ satisface (1) y (2)entonces existe una función $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ biyectiva tal que $x<y \Rightarrow f(x)<f(y)$.

Prueba:

(1) Sea $x \in \mathbb{Z}$ y pongamos $y=x+1 \wedge z=x-1$, debe probarse $x<x+1 \wedge x-1<x$

esto es claro en el caso que $x \in \mathbb{N}$ pero puede probarse en general mediante la compatibilidad del orden con la suma en $\mathbb{Z}$: si ocurriese

$$\begin{array}{ll} x \geq x+1 \vee x-1 \geq x & \text{entonces} \\ x+(-x) \geq (x+1)+(-x) & \vee\ x-1+(-x) \geq x+(-x) \\ 0 \geq x+(-x)+1 & \vee\ (x+(-x))-1 \geq 0 \\ 0 \geq 0+1 & \vee\ 0-1 \geq 0 \\ 0 \geq 1 & \vee\ -1 \geq 0 \end{array}$$

lo cual es absurdo.

(2) Sea a un subconjunto no vacío y acotado de $\mathbb{Z}$. Como $\mathbb{Z}=\mathbb{N} \cup \mathbb{N}^-$ $a=(\mathbb{N} \cap a) \cup (\mathbb{N}^- \cap a)$

dividimos esta prueba en dos casos:

i) $\mathbb{N} \cap a \neq \emptyset \neq \mathbb{N}^- \cap a$.

por hipótesis $\{\ z \in \mathbb{Z} |\ \forall x \in a(\ x \leq z\ )\ \} \neq \emptyset$ entonces $S=\{\ z \in \mathbb{Z} |\ \forall x \in a \cap \mathbb{N}(\ x \leq z\ )\ \} \neq \emptyset$

entonces $S \subseteq \mathbb{N}$ tiene un mínimo; sea m ese mínimo. Ahora, si $m=0$ entonces debe ser $S=\{0\}$ & $m \in a$ y si $m \neq 0$ también $m \in a$ pues en caso contrario

$\forall x \in a \cap \mathbb{N}(\ x<m\ )$ y entonces

$\forall x \in a \cap \mathbb{N}(\ x \leq m-1\ )$ pero entonces

$m-1 \leq m$

esto significa que $m-1$ también es un mínimo de S, lo cual no es posible.

Así, se tiene que $m \in a$ y es máximo de $a \cap \mathbb{N}$ como también lo es de a.

Por otro lado, sea $N=\{\ y \in \mathbb{N} |\ \exists x \in \mathbb{N}^- \cap a(\ y=-x\ )\ \}$ o bien, $N=\{\ -x \in \mathbb{N} |\ x \in \mathbb{N}^- \cap a\ \}$.

Como antes, n tiene un máximo que denotamos n', sea $n=-n'$ entonces $\forall x \in \mathbb{N}^- \cap a(\ -x \leq n'\ )$ o bien, $\forall x \in \mathbb{N}^- \cap a(\ n \leq x\ )$;

es decir, n es el mínimo de $a \cap \mathbb{N}^-$ y consecuentemente de a.

ii) $a \cap \mathbb{N}^- = \emptyset \vee a \cap \mathbb{N} = \emptyset$

También en este caso se satisface la conclusión del teorema tomando como m al máximo y como n al mínimo (usando el proceso anterior) de $a \cap \mathbb{N}^-$ si este es no vacío o de $a \cap \mathbb{N}$ en otro caso. Por ejemplo, si $a \cap \mathbb{N}^- \neq \emptyset$ entonces $N'=\{\ -x |\ x \in a \cap \mathbb{N}^-\ \} \subseteq \mathbb{N}$ tiene un mínimo n por ser no vacío y de acuerdo a la primera parte del inciso (i) también tiene un máximo m.

Aquí hacemos un paréntesis para exponer un lema que ayudará a probar la seguda parte de este teorema.

LEMA. Sea $\langle X, \leq \rangle$ un conjunto linealmente ordenado que cumple

a) $\forall x \in X\ \exists m \in X(\ x \leq m\ )$

b) $\forall a \subseteq X(\ a \neq \emptyset \Rightarrow \exists n \in a(\ \forall x \in a(\ n \leq x \vee n = x\ )\ )\ )$

c) $\forall a \subseteq X(\ a \neq \emptyset \wedge \exists z \in X(\ \forall x \in a(\ x \leq z \vee x = z\ )\ ) \Rightarrow$

$\exists m\in a(\ \forall x\in a(\ x<m \vee x=m\ )\ )$

Entonces $\langle X,<\rangle$ es isomorfo a $\langle \mathbb{N},<\rangle$

Prueba:

La idea es asociar a 0 el menor elemento $x_0\in X$, a 1 el siguiente a x_0, a 2 el siguiente del siguiente a x_0, etc.; esto puede hacerse recursivamente.

Sea $x\in X$, por (a) $\{\ z\in X|\ x<z\ \}\neq\emptyset$ y por (b) tiene un mínimo; como el orden $<$ es total ese mínimo es único, entonces se puede definir

$$F: X\longrightarrow X \quad \text{dada por}$$
$$F(x)= <\text{-}min\{\ z\in X|\ x<z\ \}.$$

Usando el teorema de recursión estudiado en el capítulo 2 con $a= <\text{-}min(X)$ resulta que existe

$$h:\mathbb{N}\longrightarrow X$$
(1) $h(0)=a= <\text{-}min(X)$

(2) $h(n+1)= F(h(n))= <\text{-}min\{\ z\in X|\ h(n)<z\ \}$

Observemos que (2) implica $h(n)<h(n+1)$; esto prueba que h es inyectiva:

Sean $m,n\in\mathbb{N}$ y digamos, $m<n$, se usará inducción sobre n para ver que $h(m)<h(n)$.

i) Si $n=1$ entonces $m=0$, por la observación anterior $h(0)<h(1)$.

ii) Supóngase que $m<n$ implica $h(m)<h(n)$, ahora se verá que si $m<n+1$ entonces $h(m)<h(n+1)$.

Sea $m<n+1$, si $m<n$ entonces $h(m)<h(n)$ y además $h(n)<h(n+1)$, por tanto $h(m)<h(n+1)$.

Por otro lado, si $m=n$

$$h(m)=h(n)<h(n+1).$$

Es decir, en cualquier caso $m<n+1 \Rightarrow h(m)<h(n+1)$.

Esto prueba que $\forall m,n\in\mathbb{N}(\ m<n \Rightarrow h(m)<h(n))$ y solo falta probar que h es suprayectiva porque ya es compatible con el orden.

Supóngase que h no es suprayectiva entonces $X\setminus Im(h)\neq\emptyset$ y por (b) tiene un $<$-mínimo x_0 entonces x_0 acota al conjunto $Y=\{y\in X|\ y<x_0\ \}$. Si $Y=\emptyset$ se tendría $\forall y\in X(\ y>x_0 \vee y=x_0\ )$; es decir, $x_0=minX=a=h(0)$, así que $x_0\in Im(h)$ lo cual es absurdo; por tanto debe ser $Y\neq\emptyset$ y por (c) tiene un $<$-mínimo y_0.

Sea $y\in X$ con $y_0<y$, como $y_0=maxY$ resulta que $y\notin Y$, entonces $x_0\leq y$, esto significa que $x_0=<\text{-}min\{\ y\in X|\ y_0<y\ \}$.

Por otro lado, $y_0\in Y$ entonces $y_0<x_0=minX\setminus Im(h)$ entonces $y_0\notin X\setminus Im(h)$ o bien, $\exists m\in\mathbb{N}(\ h(m)=y_0\ )$ pero en tal caso,

$$x_0=<\text{-}min\{\ y\in X|\ y_0<y\ \}= <\text{-}min\{\ y\in X|\ h(m)=y\ \}= h(m+1)$$

lo cual significa que $x_0\in Im(h)$, pero, nuevamente, esto no es posible y esta contradicción prueba que h es suprayectiva.

■

Ahora ya se puede terminar la prueba del teorema 2; es decir, que $\langle Z,<\rangle$ es isomorfo a $\langle Z,<\rangle$.

Sea $z_0\in Z$ cualquier elemento, $Z^+=\{\ z\in Z|\ z_0<z \vee z_0=z\ \}$ y $Z^-=\{\ z\in Z|\ z<z_0 \vee z=z_0\ \}$. Se tiene que probar que $\langle Z^+,<\rangle$ es isomorfo a $\langle \mathbb{N},<\rangle$ cuidando que se cumplan las hipótesis del lema anterior.

(a) Sea $x\in Z^+\subseteq Z$, por la hipótesis (1) del teorema 2
$$\exists y\in Z(\ x<y\ )$$
y como $x\in Z^+$, $z_0\leq x<y$ entonces $z_0<y$ así, $y\in Z^+$.

(b) Sea $a\subseteq Z^+\subseteq Z$, por hipótesis 2 del teorema, el conjunto a tiene un mínimo.

(c) También, si $a\subseteq Z^+$ es no vacío y acotado, por hipótesis 2 del teorema a tiene un máximo.

Analogamente, ayudados del lema anterior puede verificarse

que el conjunto $\langle \mathbb{Z}^-, <' \rangle$ es isomorfo a $\langle \mathbb{N}, < \rangle$ donde $x<'y$ si y solo si $y<x$, pues esa estructura cumple (a), (b), (c) del lema usando las hipótesis (1) y (2) del teorema.

Así pues, existe una función biyectiva

$$f^+ : \mathbb{N} \longrightarrow \mathbb{Z}^+ \quad \text{tal que} \quad m<n \Leftrightarrow f^+(m)<f^+(n)$$

y una función

$$f^- : \mathbb{N} \longrightarrow \mathbb{Z}^- \quad \text{tal que} \quad m<n \Leftrightarrow f^-(m)<f^-(n).$$

Con estas dos funciones ya puede darse una $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ como

$$f(m) = \begin{cases} f^+(m) & \text{si } m \geq 0 \\ f^-(-m) & \text{si } m \leq 0 \end{cases}$$

i) f es suprayectiva pues f^+ y f^- lo son y además $\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^-$.

ii) Sean $m, n \in \mathbb{Z}$, si $m, n<0 \vee m, n \geq 0$ es claro que $m \neq n \Rightarrow f(m) \neq f(n)$ y si $m \geq 0 \wedge n<0$ observemos primero que z_0 es el primer elemento de $\mathbb{Z}^+$ así que $f^+(0)=z_0$ pues si no fuera así entonces

$$\exists z \in \mathbb{Z}(\ z<f^+(0)\ )$$

o bien $\exists m_0 \in \mathbb{N}(\ f^+(m_0)<f^+(0)\ )$ pero esto significa que $m_0<0$ lo cual es absurdo; ahora

$$f(n)=f^-(-n) \quad \& \quad f(m)=f^+(m)$$

y además $-n>0$, $m>0$ entonces $f^-(-n)>f(0)=z_0$ o bien $z_0>f^-(-n)$ y $f^+(m)>f^+(0)=z_0$ así que $f^-(-n)<f^+(m)$ es decir $f(n)<f(m)$. Esto significa que f es inyectiva y; de hecho, también establece la compa-compatibilidad del orden. ∎

3.5 LOS ENTEROS COMO CLASES DE EQUIVALENCIA

Para finalizar este capítulo, y a manera de comentario, se harán algunas comparaciones entre la definición 2 para los enteros (sus operaciones y el orden) y otra que se da a continuación.

Sea $i = \{ x \mid \exists a,b,c,d \in \mathbb{N}(\ x = \langle \langle a,b \rangle, \langle c,d \rangle \rangle \wedge a+d=b+c \}$; es decir, i es una relación de $\mathbb{N}\times\mathbb{N}$ en que $\langle a,b \rangle i \langle c,d \rangle \Leftrightarrow a+d=b+c$.

Puede verse que i es una relación de equivalencia e induce una partición de $\mathbb{N}\times\mathbb{N}$ en clases de equivalencia; de hecho, se puede pensar, en la clase de equivalencia de un par ordenado $\langle a,b \rangle$ denotada por $\overline{ab}$ y definida como

$$\overline{ab} = \{ x \mid \exists m,n \in \mathbb{N}\ (\ x = \langle m,n \rangle \wedge \langle m,n \rangle i \langle a,b \rangle\ )\ \}$$
$$= \{\ \langle m,n \rangle \in \mathbb{N}\times\mathbb{N} \mid \langle m,n \rangle i \langle a,b \rangle\ \}$$

realmente, una clase de equivalencia es un conjunto gracias al axioma de comprensión de Zermelo-Fraenkel pues,

$$\overline{ab} \subseteq \mathbb{N}\times\mathbb{N}, \text{ o bien, } \overline{ab} \in \mathcal{P}(\mathbb{N}\times\mathbb{N})$$

Esto también indica que la colección de todas las clases de equivalencia es un conjunto; de hecho es un subconjunto de $\mathcal{P}(\mathbb{N}\times\mathbb{N})$; sea $\mathbb{Z}$ ese conjunto, ayudados del orden en $\mathbb{N}$ se puede dar un orden a este $\mathbb{Z}$:

Definición. $\overline{ab} < \overline{cd} \Leftrightarrow a+d < b+c$.
Donde $<$ es el orden en $\mathbb{N}$ y $<$ es el orden para $\mathbb{Z}^+$.

Puede verse que este orden está bien definido; es decir, no depende de la elección de los representantes de la clase $\overline{ab}$ y que además es un orden lineal.

Por otro lado, las operaciones en $\mathbb{Z}^*$ se puede definir como

$$\overline{ab}+\overline{cd} = \overline{[a+c][b+d]} \quad y$$

$$\overline{ab}\times\overline{cd} = \overline{[ac+bd][ad+bc]}$$

donde $\overline{[a+c][b+d]}$ es la clase de equivalencia de los números a+c y b+d.

Con todas estas definiciones $\langle \mathbb{Z}^*, <, +, \times \rangle$ es isomorfo a $\langle \mathbb{Z}, <, +, \cdot \rangle$ por ejemplo a través de la función:

$$f: \mathbb{Z}^* \longrightarrow \mathbb{Z}$$

$$f(\overline{ab}) = a-b$$

No se pretende entrar en los detalles de las pruebas de todo lo que se ha dicho hasta aquí; las observaciones serán en relación a la primera definición que se dio para $\mathbb{Z}$. Por ejemplo, el conjunto $\mathbb{Z}$ extiende de una manera muy natural $\mathbb{N}$; de hecho, $\mathbb{N} \subseteq \mathbb{Z}$; es decir, tomando como base a los números naturales (los positivos y cero) solo se le agregaron nuevos objetos que tomarían el papel de los enteros negativos; igualmente el orden y las operaciones en $\mathbb{N}$ se mantienen exactamente igual (más que de manera isomorfa) que cuando estos se ven como números enteros. Las ventajas en la definición de $\mathbb{Z}^*$ son evidentes: es mucho más fácil establecer el orden y las operaciones, y también resulta más sencillo hacer las pruebas de las propiedades que cumplen estas relaciones, pero aquí se pierde la manera intuitiva en que se relacionan $\mathbb{N}$ y $\mathbb{Z}$; en este caso no sucede que $\mathbb{N} \subseteq \mathbb{Z}$, sino que $\mathbb{N}$ es isomorfo a un subconjunto de $\mathbb{Z}^*$, a saber, al subconjunto de los elementos de $\mathbb{Z}^*$ mayores que la clase $\overline{00}$ en el orden <.

En otro orden de ideas comentaremos que si bien este capítulo comenzó definiendo $\mathbb{Z}^*$ y no $\mathbb{Z}$ es porque aquí se trata de presentar a los objetos de los que se habla, de la manera mas natural posible pero sin que las propiedades sobre ellos sean demasiado complicadas de obtener.

Finalmente diremos que $\mathbb{Z}^*$ es la forma en que se presenta a los números enteros en un curso típico de álgebra; es muy precisay, sobre todo, elegante pero, al parecer, menos intuitiva que lapresentada al inicio de este capítulo.

Las definiciones que se exponen aquí para los números racionales, sus operaciones y su orden, son las que se pueden encontrar en casi cualquier texto relacionado a la materia; es muy elegante y fácil de enunciar, por lo cual es sencillo probar todas las propiedades.

También se incluye un resultado de unicidad que caracteriza a los números racionales como un conjunto totalmente ordenado, sin extremos y *numerable*, debido a esta última característica será necesario incluir los conceptos necesarios para poder hablar de *numerabilidad*; todo esto, desde luego, el los términos de la Teoría de los Conjuntos.

4.1 LOS NUMEROS RACIONALES COMO CLASES DE EQUIVALENCIA

PROPOSICION 1. Sea la relación $q\subseteq(\mathbb{Z}\times\mathbb{Z}\setminus\{0\})\times(\mathbb{Z}\times\mathbb{Z}\setminus\{0\})$ dada como
$\forall a,b,c,d\in\mathbb{Z}(\ \langle a,b\rangle q\langle c,d\rangle \leftrightarrow ad=bc\ )$
entonces q es una relación de equivalencia sobre $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$

Prueba:

i) q es reflexiva:
Sea $\langle a,b\rangle\in\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$
$\langle a,b\rangle q\langle a,b\rangle \leftrightarrow ab=ba$
lo cual es inmediato de la conmutatividad del producto en $\mathbb{Z}$.

ii) q es simétrica:
Sean $a,b,c,d\in\mathbb{Z}$ tales que $\langle a,b\rangle q\langle c,d\rangle$ entonces
$ad=bc$ por conmutatividad
$cb=da$ lo cual significa
$\langle c,d\rangle q\langle a,b\rangle$.

iii) q es transitiva:
Sean $a,b,c,d,e,f\in\mathbb{Z}$ tales que $\langle a,b\rangle q\langle c,d\rangle$ & $\langle c,d\rangle q\langle e,f\rangle$ entonces
$ad=bc$ & $cf=de$ por tanto
$(ad)f=(bc)f$
$(ad)f=b(cf)=b(de)$
$a(df)=b(de)$
$a(fd)=b(ed)$
$(af)d=(be)d$, ahora, como $d\neq 0$
$af=be$; es decir,
$\langle a,b\rangle q\langle e,f\rangle$.

∎

Obsérvese que si fuera $q\subseteq\mathbb{Z}\times\mathbb{Z}$, q no necesariamente es transitiva, pues en la prueba anterior se usa fuertemente el hecho de que $d\neq 0$.

De acuerdo a la proposición 6 del capítulo 2 esta relación de equivalencia permite definir una partición de $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ en subconjuntos de la forma

$$\langle a,b\rangle q=\{\ \langle x,y\rangle\in\mathbb{Z}\times\mathbb{Z}\setminus\{0\}\mid \langle x,y\rangle q\langle a,b\rangle\ \}$$

Para este caso, el conjunto $\langle a,b\rangle q$ se denota por a/b, así que la partición es

$$Q=\{\ z\in P(\mathbb{Z}\times\mathbb{Z})\mid \exists a,b\in\mathbb{Z}(\ b\neq 0\ \wedge\ z=a/b\ )\ \}$$

el elemento $a\in\mathbb{Z}$ se llama el *numerador* de $z\in\mathbb{Q}$ y el elemento $b\in\mathbb{Z}$ se llama el *denominador* de $z\in\mathbb{Q}$.

DEFINICION 1. El conjunto $\mathbb{Q}$ de clases (conjuntos) de equivalencia de $\mathbb{Z}\times\mathbb{Z}$ bajo la relación q se llama el conjunto de *Números Racionales.*

Antes de ordenar y establecer la aritmética de $\mathbb{Q}$ vale la pena hacer algunas observaciones sobre él. En el capítulo anterior se extendió el conjunto $\mathbb{N}$ de números naturales para llegar al conjunto $\mathbb{Z}$ de números enteros, de manera que resulta $\mathbb{N}\subseteq\mathbb{Z}$; aquí, la extensión de $\mathbb{Z}$ para llegar a $\mathbb{Q}$ es un poco diferente: no resulta $\mathbb{Z}\subseteq\mathbb{Q}$, pero sí hay una función inyectiva muy natural de $\mathbb{Z}$ en $\mathbb{Q}$, a saber,

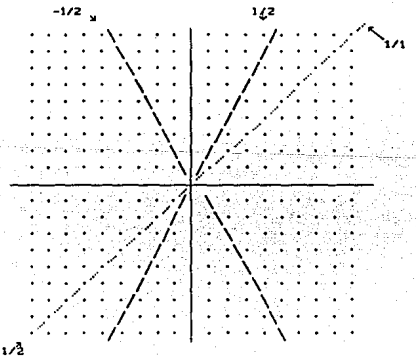
$$i:\mathbb{Z}\longrightarrow\mathbb{Q}$$
$$i(z)=z/1.$$

Efectivamente, i es inyectiva pues si $z/1=z'/1$, de acuerdo a la observación a la proposición 6 del capítulo 2

$$\langle z,1\rangle q\langle z',1\rangle; \qquad \text{es decir,}$$
$$z\cdot 1=z'\cdot 1, \qquad \text{o bien,}$$
$$z=z'.$$

En otras palabras, se puede abusar de la notación al escribir $\mathbb{Z}\subseteq\mathbb{Q}$ identificando a cada elemento $z\in\mathbb{Z}$ con el elemento $z/1\in\mathbb{Q}$.

Por otro lado, puede verse geométricamente la relación entre $\mathbb{Z}$ y $\mathbb{Q}$ en el plano $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$: el número racional p/q corresponde a la recta (discreta) de pendiente q/p que cruza por el origen.



4.2 EL ORDEN EN $\mathbb{Q}$

Por el momento se denotará con $<$ al orden de $\mathbb{Z}$ para definir un orden en $\mathbb{Q}$ que, como se verá mas adelante, si se restringe a $\mathbb{Z}$ coincidirá con el suyo propio, por lo que, en su momento, se escribirán con el mismo signo.

Primero observemos que, gracias a que $\mathbb{Q}$ es una partición de $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$, el denominador de un número racional es diferente de cero, de hecho,

siempre es posible tomar un representante con denominador positivo dado que

$$a/b=-a/-b \quad (\Leftrightarrow a(-b)=b(-a),\ \text{lo cual es válido en } \mathbb{Z})$$

y sucede que b ó -b es positivo. Así pues, en adelante se supondrá que cualquier (número) racional tiene denominador positivo. ¿Por qué este artificio?,... porque debe ocurrir

$$\frac{8}{-4} < \frac{-1}{2} \quad (\text{o sea } -2<-1) \Leftrightarrow 8=8\cdot 1 < -1\cdot -4=4$$

pero esto funciona correctamente representando 8/-4 como -8/4, con esto

$$-8/4 < -1/1 \iff -8<-4\ .$$

Lo anterior se puede evitar si se define a $\mathbb{Q}$ como clases de equivalencia de $\mathbb{Z}\times\mathbb{N}^*$.

DEFINICION 2. Definimos la relación $<\subseteq \mathbb{Q}\times\mathbb{Q}$ en $\mathbb{Q}$ dada por

$\forall a,c\in\mathbb{Z}\ \forall b,d\in\mathbb{N}(\ a/b<c/d \Leftrightarrow ad<bc\ )$ o bien

$\forall z,y\in\mathbb{Q}\ \forall a,c\in\mathbb{Z}\ \forall b,d\in\mathbb{N}(\ z<y \Leftrightarrow z=a/b \wedge y=c/d \wedge ad<bc\ ).$

PROPOSICION 3. La relación $<\subseteq \mathbb{Q}\times\mathbb{Q}$ define un orden total en $\mathbb{Q}$.

Prueba:

i) $<$ es irreflexiva: $\forall z\in\mathbb{Q}(\ \neg(z<z)\ )$

$a/b<a/b \Leftrightarrow ab<ba \Leftrightarrow ab<ab$

pero $<$ es irreflexiva entonces $\neg(ab<ab)$ ó $\neg(a/b<a/b)$.

ii) $<$ es transitiva: $\forall x,y,z\in\mathbb{Q}(\ x<y \wedge y<z \Rightarrow x<z\ )$

Supóngase $x=a/b$, $y=c/d$, $z=e/f$

si $x<y$ & $y<z$ entonces $ad<bc$ & $cf<de$

como $0<f$ $\quad adf<bcf$

como $o<b$ $\quad bcf<bde$

por transitividad de $<$ $\quad adf<bde$

o bien $\quad afd<bed$

por cancelación, para $d\neq 0$ $\quad af<be$

es decir, $\quad a/b<e/f$

iii) $<$ es tricotómica: $\forall x,y\in\mathbb{Q}(\ x<y \vee x=y \vee y<x\ )$

Sean $x=a/b$, $y=c/d$.

Como $<$ es tricotómica $\quad ad<bc \vee ad=bc \vee bc<ad.$

En el primer y tercer caso ocurre, respectivamente,

$a/b<c/d \vee c/d<a/b$

y si $ad=bc$ entonces $<a,b>q<c,d>$, por tanto $a/b=c/d$.

∎

En la definición 2 debe verificarse que $<$ es una relación bien definida, puesto que para definir $x<y$, donde $x=a/b$ & $y=c/d$, se ha tomado el par $<a,b>$ de la clase de equivalencia a/b; pero en esta clase puede haber (y de hecho los hay) más de un elemento, digamos $<p,q>\in a/b$, entonces debe suceder que $x<y \Leftrightarrow pd<cd$. Esto se verifica en la siguiente proposición.

PROPOSICION 2. Sean $a,b,c,d,p,q,r,s\in\mathbb{Z}$ tales que $b\neq 0\neq d$, $q\neq 0\neq s$ y $<p,q>\in a/b$, $<r,s>\in c/d$ entonces

$$ad<bc \Leftrightarrow ps<qr$$

Prueba:

$<p,q>\in a/b$ significa que $<p,q>q<a,b>$ lo cual, a su vez, quiere decir

$$pb=aq.$$

Análogamente, $<r,s>\in c/d \Leftrightarrow rd=sc$.

De $pb=aq$ se tiene $pbd=aqd=adq$, como $q>0$

pbd=adq<bcq, como s>0
pbds<bcqs=bqsc, de rd=sc
pbds<bqrd o bien
psbd<qrbd finalmente, b≠0≠d entonces
ps<qr.

La implicación en sentido contrario se obtiene invirtiendo el orden de la secuencia de los pasos anteriores.

Dado que se ha identificado a un elemento x∈Z con el elemento x/1∈Q puede decirse que el orden de Q extiende al orden de Z, porque si x,y∈Z & x<y entonces

x·1<y·1 es decir x/1<y/1.

4.3 LA ARITMETICA DE Q

En Z existen elementos distinguidos 0 y 1 con propiedades especiales, sus correspondientes imágenes 0/1 y 1/1 se denotan con los mismos simbolos (cuando no haya confusión), tendrán propiedades análogas y, desde ahora, se les pueden ver algunas particularidades fáciles de verificar:

i) si <x,y>∈0/1 entonces x=0.
ii) si <x,y>∈1/1 entonces x=y.

Las propiedades de estos elementos están descritas dentro de las operaciones entre números racionales.

Sean + y · las operaciones de suma y producto, respectivamente en Z.

DEFINICION 3. Definimos la función ⊕: Q×Q⟶Q como
⊕(a/b, c/d)=(ad+bc)/bd
Se escribe a/b⊕c/d en lugar de ⊕(a/b, c/d) y se abusa de la notación para emplear el signo + en vez de ⊕.

Obsérvese que el elemento (ad+bc)/bd realmente esta en Q pues b≠0 & d≠0 y, realmente, la suma ⊕ no define correctamente una función (ni siquiera una relación) mientras no se pruebe que no importan los elementos de los conjuntos a/b y c/d empleados para definirla.

PROPOSICION 3. Si el <m, n>∈a/b & <p, q>∈c/d entonces
<mq+np, nq>∈(ad+bc)/bd

Prueba:
Según como están definidos los elementos de Q, quiere probarse que si mb=na y pd=cq entonces (mq+np)bd=nq(ad+bc).
Pero, por conmutatividad de la multiplicación en Z
(mq+np)bd=mqbd+npbd
=mbqd+pdnb,
como mb=na y pd=cq =naqd+cqnb
=nq(ad+bc)
es decir, (mq+np)bd=nq(ad+bc).

Otra manera de establecer la proposición anterior es emplear la observación a la proposición 6 del capitulo 2 que indica que las clases de equivalencia (ad+bc)/bd y (mq+np)/nq son iguales si y solo si sus

representantes <ad+bc, bd> y <mq+np, nq> están en la relación que define a $\mathbb{Q}$; esto es lo que se probó en la proposición 3.

Una vez que se ha verificado que la suma de números racionales es una función bien definida, se procede a mostrar algunas de sus propiedades.

PROPOSICION 4. i) $\forall x \in \mathbb{Q}(\ x+0=x=0+x\ )$.
ii) $\forall x \in \mathbb{Q}\ \exists z \in \mathbb{Q}(\ x+z=0\ )$.
iii) $\forall x, y \in \mathbb{Q}(\ x+y=y+x\ )$.
iv) $\forall x, y, z \in \mathbb{Q}(\ x+(y+z)=(x+y)+z\ )$.

Prueba:

i) Sea $x=a/b$, entonces $a/b+0/1=(a\cdot 1+b\cdot 0)/b\cdot 1=a/b$.

ii) Sea $a/b \in \mathbb{Q}$, entonces $-a/b \in \mathbb{Q}$ y
$a/b+(-a)/b=(ab+b(-c))/bb=(ab-ab)/bb=0/bb=0$.

iii) Sean $x=a/b$, $y=c/d$
$x+y=a/b+c/d=(ad+bc)/bd=(bc+ad)/db=(cb+da)/db=$
$=c/d+a/b=y+x$.

∎

DEFINICION 4. Se define la función $o: \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}$ como
$o(a/b, c/d)=ac/bd$
Por notación: $o:(a/b, c/d)=a/b \circ c/d=a/b\cdot c/d$

Realmente el elemento ac/bd está en $\mathbb{Q}$ pues $b\neq 0\neq d$ entonces $bd\neq 0$ y, así como en la suma, hay un resultado que implica que o define correctamente una función.

PROPOSICION 5. Si $\langle m, n\rangle \in a/b$ & $\langle p, q\rangle \in c/d$ entonces $\langle mp, nq\rangle \in ac/bd$.

Prueba:

Quiere probarse que $mb=na$ & $pd=qc$ implica $mp\cdot bd=nq\cdot ac$.
Pero esto es fácil:
$mp\cdot bd = mb\cdot pd = na\cdot qc = nq\cdot ac$.

∎

El producto en $\mathbb{Q}$ tiene propiedades semejantes a las de la suma.

PROPOSICION 6 i) $\forall x \in \mathbb{Q}(\ x\cdot 1=x=1\cdot x\ )$.
ii) $\forall x \in \mathbb{Q}(\ x\neq 0 \Rightarrow \exists z \in \mathbb{Q}(\ x\cdot z=1\ )\ )$.
iii) $\forall x, y \in \mathbb{Q}(\ x\cdot y=y\cdot x\ )$.
iv) $\forall x, y, z \in \mathbb{Q}(\ x\cdot(y\cdot z)=(x\cdot y)\cdot z\ )$.

Prueba:

i) Sea $x=a/b \in \mathbb{Q}$ y $m \in \mathbb{Z}$ diferente de cero
$x\cdot 1=a/b\cdot m/m=am/bm=a/b=x$.

ii) Sea $0\neq x=a/b \in \mathbb{Q}$, de acuerdo al análisis hecho en el primer párrafo de esta sección, debe ocurrir $a\neq 0$; con esto $z=b/a \in \mathbb{Q}$ y
$x\cdot z=a/b\cdot b/a=ab/ba=ab/ab=1/1=1$.

∎

Por supuesto, también vale la propiedad distributiva en $\mathbb{Q}$; es decir, si $x, y, z \in \mathbb{Q}$ entonces $x\cdot(y+z)=x\cdot y+x\cdot z$.

Por otro lado, la propiedad $x\cdot y=0 \Leftrightarrow x=0$ v $y=0$ debe probarse a partir de la definición de $\mathbb{Z}$ y de su producto; en $\mathbb{Q}$ esta propiedad se obtiene de algunas de las derivadas en la proposición 6:

Sean $x, y \in \mathbb{Q}$ tales que $x \cdot y = 0$, si $x = 0$ el resultado es evidente; en caso contrario, por (ii) de la proposición 6 existe un elemento $z \in \mathbb{Q}$ tal que $x \cdot z = 1$, entonces de

$$0 = x \cdot y \quad \text{se tiene}$$
$$0 \cdot z = xy \cdot z = xz \cdot y = 1 \cdot y \quad \text{por(1)}$$
$$= y$$

Por lo tanto $y = 0 \cdot z$, el hecho de que $0 \cdot z = 0$ es consecuencia de las leyes de cancelación para la suma y de la propiedad distributiva.

Aun cuando no se enunciaron las leyes de cancelación, su verdad debe ser clara:

$0 \cdot z = (0+0) \cdot z = 0 \cdot z + 0 \cdot z$ entonces
$0 = 0 \cdot z$.

También se enuncian, sin demostración, algunas de las propiedades del orden en $\mathbb{Q}$ relacionadas con la suma y el producto:

PROPOSICION 7. Sean $x, y, z, w \in \mathbb{Q}$ entonces
i) $x < y \iff x+z < y+z$
ii) $x < y \wedge z > 0 \Rightarrow x \cdot z < y \cdot z$
iii) $x < y \wedge z < 0 \Rightarrow x \cdot z > y \cdot z$
iv) $x < y \wedge 0 < z < w \Rightarrow xz < yw$.

Prueba:
Se prueba esta proposición solo en los casos más interesantes.
iii) Supónganse $x = a/b$, $y = c/d$, $z = m/n$.
Quiere probarse que
$a/b < c/d \wedge m/n < 0/1 \Rightarrow am/bn > cm/dn$ o bien
$ad < bc \wedge m < 0 \Rightarrow am \cdot dn > bn \cdot cm$
Pero esta propiedad se desprende de la análoga para $\mathbb{Z}$:
Primero, hemos elegido $n \in \mathbb{Z}$ tal que $n > 0$, de tal suerte que
$mn < 0$ además
$ad < bc$ entonces
$admn > bcmn$ o bien
$amdn > cmbn$.
La otras afirmaciones de esta proposición se prueban de manera igualmente sencilla y el interesado puede realizarlas sin ninguna dificultad.

■

4.4 CONJUNTOS NUMERABLES

Al inicio del presente capitulo se indicó que uno de los objetivos del mismo es obtener una caracterización del conjunto $\mathbb{Q}$ de números racionales como un conjunto *numerable*, totalmente ordenado, denso y sin extremos. En vista de lo anterior, esta sección es un paréntesis para introducir los conceptos necesarios para llegar a la noción de *numerabilidad* ; si bien este último es el concepto principal de esta sección, habrá otras ideas que permitirán una visión mas completa de su significado intuitivo.

Es útil retomar la idea de número natural como un conjunto: $0 = \emptyset \wedge \forall n \neq 0 (n = \{0, 1, 2, \ldots, n-1\})$; esto permitirá establecer fácilmente las ideas que se requieren.

DEFINICION 5. Un conjunto a es *finito* si existe una función biyectiva de él sobre algún número natural. Si FIN es la clase de los conjuntos finitos entonces puede decirse

$$\forall a(a\in FIN \Leftrightarrow \exists n\in N \exists f[\ f: a \longrightarrow n \wedge \forall x,y\in a(\ f(x)=f(y) \Rightarrow x=y\ ) \wedge \forall m\in n \exists z\in a(\ m=f(z)\ )]).$$

Además, decimos que a es *infinito* si no es finito, en términos de clases

$$INFIN=\{\ a \mid a\notin FIN\ \}$$

Lo único que dice la definición anterior es que un conjunto a es finito si es *equipotente* al (existe una función biyectiva de a en el) conjunto formado por los primeros n números naturales; en este caso, se dice que a tiene n *elementos* o que el *cardinal* de a es n, esto escrito como $|a|=n$.

Observación: 1. $\forall n\in N(\ |n|=n\ )$
2. $\forall a,b(\ a\in FIN \wedge b$ equipotente a $a \Rightarrow b\in FIN\ )$.

PROPOSICION 8. $\forall a(\ a\in FIN \Rightarrow \forall x(\ a\cup\{x\}\in FIN\ )$

Prueba:

Se dará un bosquejo de la prueba.

Sean $a\in FIN$ y x un conjunto, si $x\in a$ entonces $a=a\cup\{x\}$ es finito y si $x\notin a$ la función

$$g: a\cup\{x\} \longrightarrow n^{\cdot} \quad \text{dada por}$$

$$g(y)=\begin{cases} f(y) & \text{si } y\in a \\ n & \text{si } y=x \end{cases}$$

es biyectiva.

PROPOSICION 9. i) $a\in FIN \wedge b\subseteq a \Rightarrow b\in FIN$
ii) $\forall n\in N \forall x(\ x\subseteq n \Rightarrow x\in FIN\ )$

Prueba:

Que (ii) $\Rightarrow$ (i) es claro, para probar (ii) úsese inducción sobre n.

i) Si $x\subseteq 0=\emptyset$ entonces $x=0=\emptyset \Rightarrow x\in FIN$.

ii) Si $x\subseteq n^{\cdot}=n\cup\{n\}$ y n es finito entonces
si $n\notin x \Rightarrow x\subseteq n$ y, por hipótesis de inducción $x\in FIN$.
si $n\in x \Rightarrow x=z\cup\{n\}$ donde $z\subseteq n$ (de hecho, $z=x\setminus\{n\}$); por hipótesis de inducción z es finito y, por la proposición 8 $x=z\cup\{n\}$ es finito.

∎

PROPOSICION 10. (a) Ningún número natural es equipotente a alguno de sus subconjuntos propios.
(b) Ningún conjunto finito es equipotente a alguno de sus subconjuntos propios.

Prueba:

Se probará (a) por inducción.

Denotemos, por ahora, como $\approx$ la relación (de equivalencia) de ser equipotentes.

Debe probarse $\varphi(n)\equiv\forall x(\ x\subseteq n \wedge x\neq n \Rightarrow \neg(n\approx x)\ )$ por inducción sobre n.

$\varphi(0) \equiv \forall x(\ x \subseteq 0 \wedge x \neq 0 \Rightarrow \neg(0 = x)\ )$ lo cual es cierto porque el antecedente es falso.

$\varphi(n) \Rightarrow \varphi(n^{+}) \equiv \forall x(\ x \subseteq n^{+} \wedge x \neq n^{+} \Rightarrow \neg(n^{+} = x)\ ).$

Supóngase que hay un subconjunto propio x de n^{+} que es equipotente a n^{+}; es decir, existe una función biyectiva f de x sobre n^{+}.

Como x es un subconjunto propio de n^{+} consideremos dos casos:

1) $n \notin x$

En este caso $x \subseteq n$, ahora, $n \in n^{+}$ entonces hay único $z \in x$ tal que $f(z)=n$. Sean $y=x\setminus\{z\}$ & $m \in y$ entonces $m \in x$ & $f(m) \in n^{+}$, pero $f(m) \neq n$ pues en caso contrario

$$f(m)=n=f(z)$$

y entonces, como f es inyectiva $m=z \in y=x\setminus\{z\}$, lo cual es absurdo. Esto quiere decir que

$$f|_y : y \longrightarrow n$$

Además, $f|_y$ es inyectiva y si $a \in n$ entonces $s \in n^{+}$ por lo cual $\exists k \in x(\ f(k)=a\ )$, pero $a \neq n$ implica $k \neq z$, por lo tanto $k \in y$, lo cual quiere decir que $f|_y$ wes suprayectiva y entonces $y=n$ con $y \subseteq x$, $x \subseteq n$ & $y \neq x$, lo cual contadice la hipótesis de inducción.

Por lo tanto, en este caso, $\varphi(n^{+})$ se satisface.

2) $n \in x$

Aqui tomaremos en cuenta dos subcasos.

i) $f(n)=n$

Igual que en el caso anterior, para $y=x\setminus\{n\}$ resulta que $f|_y$ es biyevtiva.

Además, $y \subseteq n$ y si sucediera $y=n$ entonces

$$n^{+}=n \cup \{n\}=y \cup \{n\}=(x\setminus\{n\}) \cup \{n\}=x$$

lo cual contradice el que x es subconjunto propio de n^{+}.

Entonces $y \neq n$ & $y \subseteq n$ &$y=n$ que contadice le hipótesis de inducción.

ii) $f(n) \neq n$

Sea $z \in x$ tal que $f(z)=n$, entonces $z \neq n$.

Por otro lado, sea $y=x\setminus\{n\}$; igual que en el caso 1

$$f|_y : y \longrightarrow n$$

es inyectiva y si $m \in n$ entonces $m \in n^{+}$, sea $w \in x$ tal que $f(w)=m$; como $m \in n$ se tiene $m \neq n$ y de aqui $w \neq z$ pues si $w=z$ entonces $n=f(z)=f(w)=m \in n$, lo cual es absurdo. Así, $f|_y$ es suprayectiva; o sea, $y=x\setminus\{z\} \ni n$.

Ahora bien, estamos en el caso $n \in x$ y hemos obtenido $z \neq n$, esto fuerza a que $n \in y$, entonces pongamos

$$x_o=(y\setminus\{n\}) \cup \{n\}$$

Es claro que $y \neq x_o$, también $x_o \subseteq n$ y si fuera $x_o=n$ entonces

$$n=(y\setminus\{n\}) \cup \{z\}=[(x\setminus\{z\})\setminus\{n\}] \cup \{z\}=(x\setminus\{z,n\}) \cup \{z\}=$$
$$=x\setminus\{n\}; \qquad \text{por lo tanto}$$

$n^{+}=n \cup \{n\}=(x\setminus\{n\}) \cup \{n\}=x$, lo cual es falso.

Así que $x_o \neq n$ & $x_o \subseteq n$ & $x_o=y \ni n$ lo cual, nuevamente, contradice la hipótesis de inducción.

Por lo tanto, $\varphi(n^{+})$ se cumple también en el caso 2.

Finalmente; $\forall n \in \mathbb{N},\ \varphi(n^{+}) \equiv \forall n \in \mathbb{N} \forall x(\ x \subseteq n \wedge x \neq n \Rightarrow \neg(x=n)\ ).$

La parte (b) de la proposición 10 dice que si un conjunto es finito entonces no es equipotente a ninguno de sus subconjuntos propios. Esto tiene una consecuencia interesante.

COROLARIO. El conjunto de números naturales es infinito.

Prueba:

Para probarlo basta dar un subconjunto propio de $\mathbb{N}$ que sea equipotente; esto es fácil. Sea

$$f:\mathbb{N}\longrightarrow\mathbb{N}\setminus\{0\} \qquad \text{dada por}$$
$$f(n)=n.$$

Ya se ha probado (capítulo 2) que esta f es inyectiva y que f es suprayectiva es uno de los axiomas de Peano y, además, es obvio que

$$\mathbb{N}\setminus\{0\}\subseteq\mathbb{N} \wedge \mathbb{N}\setminus\{0\}\neq\mathbb{N}$$

Por la proposición 10, $\mathbb{N}$ no es finito; es decir, $\mathbb{N}$ es infinito. ∎

DEFINICION 6. 1) Un conjunto *a* es *dominado por* un conjunto *b*, denotado $a\preceq b$ si existe una función inyectiva de *a* en *b*.

2) Un conjunto *a* es *dominado estrictamente* por un conjunto *b*, denotado $a\prec b$ si *a* es dominado por b pero a no es equipotente a *b*.

PROPOSICION 11 (Teorema de Cantor). $\forall x(\ x\prec P(x)\ )$: Todo conjunto es dominado estrictamente por su potencia.

Prueba:

Es fácil ver que $x\preceq P(x)$ pues

$$f:x\longrightarrow P(x)$$
$$f(y)=\{y\}$$

es inyectiva.

Para probar que la dominancia es estricta veremos que no puede haber una función suprayectiva de x sobre $P(x)$.

Sea $g:x\longrightarrow P(x)$ y considérese $b=\{\ a\in x\mid a\notin g(a)\ \}$.

Es claro que $b\in P(x)$, pero $b\notin Im(g)$ pues es ese caso habría $a_0\in x$ tal que $g(a_0)=b$ y aquí hay dos posibilidades.

i) $a_0\in b$

entonces $a_0\notin g(a_0)=b$; es decir, $a_0\notin b$.

ii) $a_0\notin b$

entonces $a_0\in g(a_0)=b$; es decir, $a_0\in b$.

Esta contradicción implica que g no es suprayectiva pues $b\notin Im(g)$. ∎

Para facilitar la escritura en el teorema que sigue, se introduce la siguiente notación:

Si $h:x\longrightarrow y$ & $z\subseteq x$ el conjunto denotado $h[z]$ es

$$h[z]=\{w\in y\mid \exists r\in x(\ h(r)=w\ )\}=\{h(r)\mid r\in z\ \}$$

Enseguida un resultado se suma importancia en este contexto.

TEOREMA 1. (Cantor, Schröeder, Berstein). Si $a\preceq b$ & $b\preceq a$ entonces $a\approx b$.

Prueba:

Sean $f:a\longrightarrow b$ y $g:b\longrightarrow a$ funciones inyectivas.

Si $Im(g)=a$ entonces $a\approx b$.

Si $Im(g)\neq a$ podemos definir en forma recursiva

$$C_0=a\setminus Im(g)$$

$$\forall n\in\mathbb{N}\ C_{n+1}=g[f[C_n]]$$

Si denotamos $D_n=f[C_n]$ se tiene

$$\forall n\in\mathbb{N}\ C_{n+1}=g[D_n]$$

Construyamos ahora una función biyectiva de a en b. Sea

$$h: a\longrightarrow b \qquad \text{dada por}$$

$$h(x)=\begin{cases} f(x) & \text{si } x\in\cup\{\, C_n \mid n\in\mathbb{N}\,\} \\ g^{-1}(x) & \text{si } x\notin\cup\{\, C_n \mid n\in\mathbb{N}\,\} \end{cases}$$

donde $g^{-1}(x)$ es el único elemento $y\in b$ (si existe) tal que $g(y)=x$. En este caso, ese elemento $y\in b$ existe porque si $x\notin\cup\{\, C_n \mid n\in\mathbb{N}\,\}$ entonces $\forall n\in\mathbb{N}\ (x\notin C_n)$ en particular, $x\notin C_0=a\setminus Im(g)$, lo cual significa que $x\in Im(g)$.

Ahora, que h es inyectiva es porque si x & y son elementos distintos de a &

i) $x,y\in\cup\{\, C_n \mid n\in\mathbb{N}\,\}$
entonces $f(x)\neq f(y)$ porque f es inyectiva, razón por la cual $h(x)\neq h(y)$.

ii) $x,y\notin\cup\{\, C_n \mid n\in\mathbb{N}\,\}$

$h(x)=g^{-1}(x)\neq g^{-1}(y)=h(y)$ porque g es inyectiva.

iii) $x\in\cup\{\, C_n \mid n\in\mathbb{N}\,\}$, $y\notin\cup\{\, C_n \mid n\in\mathbb{N}\,\}$

aquí, $h(x)=f(x)$

$h(y)=g^{-1}(y)$

Como $x\in C_m$ (para algún $m\in\mathbb{N}$) entonces $h(x)=f(x)\in f[C_m]=D_m$.

Ahora, $g^{-1}(y)\notin D_m$ pues en caso contario: $g^{-1}(y)\in f[C_m]$ implica que $y=g(g^{-1}(y))\in g[f[C_m]]=C_{m^+}$, lo cual no es posible pues $y\notin\cup\{\, C_n \mid n\in\mathbb{N}\,\}$.

Por tanto, $h(x)\in D_m$ & $h(y)\notin D_m$; consecuentemente,

$$h(x)\neq h(y).$$

Veamos que h es suprayectiva.

Sea $z\in b$

si $z\in\cup D_n$ entonces $z\in D_m=f[C_m]$ entonces hay un $x_0\in C_m\subseteq a$ tal que $z=f(x_0)=h(x_0)$.

Por otro lado, si $z\in b\setminus\cup D_n$ observemos primero que $g(z)\notin\cup C_n$, esto es así porque si n=0, entonces $g(z)\notin C_0=a\setminus Im(g)$ y, además, si sucediera $g(z)\in C_{n^+}=g[f[C_n]]=g[D_n]$ entonces habría un $z'\in D_n$ tal que $g(z)=g(z')$, pero entonces $z=z'\in D_n$ que contradice el supuesto de que $z\notin\cup D_n$. Así, por definición,

$$h(g(z))=g^{-1}(g(z))=z.$$

Por tanto, h es suprayectiva y, en conclusión,

$$a\approx b.$$

∎

DEFINICION 7. Un conjunto *a* en *numerable* si existe una función $f: a\longrightarrow\mathbb{N}$ biyectiva.

Con el Teorema 1 ya es fácil probar que $\mathbb{Q}$ es numerable. Como preámbulo, digamos que, con el matelal desarrollado para los números enteros puede desarrollarse la llamada Teoría de los Números y ahí se sabe que un número racional $(p/q,\ q>0)$ se respresenta de manera única, por ejemplo, tomando p y q como primos relativos. Como el camino para obtener ese resultado es muy largo, lo aceptaremos verdadero para escribir las siguientes funciones inyectivas:

$$\mathbb{N} \xrightarrow{f} \mathbb{Q} \xrightarrow{g} \mathbb{Z}\times\mathbb{Z} \xrightarrow{h} \mathbb{N}\times\mathbb{N} \xrightarrow{i} \mathbb{N}$$

$$n \xrightarrow{f} n/1$$

$$p/q \xrightarrow{g} \langle p,q\rangle$$

$$\langle m,n\rangle \xrightarrow{i} 2^m(2n+1)-1$$

Efectivamente, i es inyectiva pues si $2^{m'}(2n'+1)-1=2^m(2n+1)$ entonces $2^{m'}(2n'+1)=2^m(2n+1)$, ahora, si $m'>m$ entonces $2^{m'-m}\in\mathbb{N}$ y $2^{m'-m}(2n'+1)=2n+1$ lo cual indica que $2n+1$ es par; analogamente, $m'<m$ implica $2n'+1$ es par; por tanto, solo queda la posibilidad de que $m'=m$, en cuyo caso ocurre $2n'+1=2n+1$, de donde resulta $n=n'$ y se conluye que i es inyectiva.

Por otro lado, para completar el anterior esquema de funciones resta dar una función $h:\mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{N}\times\mathbb{N}$ inyectiva, para lo cual es suficiente dar una $h':\mathbb{Z}\longrightarrow\mathbb{N}$, por ejemplo, sea

$$h'(z)=\begin{cases} 2z & ,z\geq 0 \\ 2(-z)-1 & ,z<0 \end{cases}$$

De hecho, la cadena de funciones y el Teorema 1 prueba que todos los conjuntos involucrados son numerables.

DEFINICION 8. Un conjunto *a* es *contable* si es finito o numerable.

Si *a* es un conjunto contable e infinito (numerable) entonces la proposición 11 dice que $P(a)$ no es contable. Mas adelante surgirán otros conjuntos no contables.

4.5 LA UNICIDAD DE LOS NUMEROS RACIONALES

Ahora se necesitan otros conceptos de interés respecto al tipo de orden de los números racionales.

DEFINICION 8. Un conjunto *a* ordenado por una relación $<$ es *denso* si tiene al menos dos elementos en la relación $<$ y sucede

$$\forall x,y\in a(\ x<y \Rightarrow \exists z\in a(x<z \wedge z<y)\ )$$

Si *a* tiene un elemento $<$-máximo y uno $<$-mínimo los llamamos *extremos* de *a*.

PROPOSICION 12. El orden $<$ de $\mathbb{Q}$ es un orden denso sin extremos.

Prueba:

Que $\mathbb{Q}$ no tiene extremos es fácil pues si $x\in\mathbb{Q}$ entonces

$$x<x+1 \quad y \quad x-1<x\ .$$

También es sencillo ver que el orden es denso; sean $a/b, c/d\in\mathbb{Q}$ con $a/b<c/d$, entonces

$$a/b<(ad+bc)/2bd \quad y \quad (ad+bc)/2bd<c/d$$

esto es cierto porque

$a/b<c/d$ implica

$a/b+a/b < a/b+c/d$ y $a/b+c/d < c/d+c/d$ o bien
$2(a/b) < a/b+c/d$ y $a/b+c/d < 2(c/d)$ entonces
$a/b < (1/2)(a/b+c/d)$ y $(1/2)(a/b+c/d) < c/d$ es decir
$a/b < (ad+bc)/2bd$ y $(ad+bc)/2bd < c/d$

∎

Ahora ya se puede establecer la unicidad del conjunto de números racionales que se ha definido. Al mismo tiempo se introduce un poco de terminología usual. Por ejemplo, si un conjunto A es numerable, por definición existe una función $a:\mathbb{N}\longrightarrow A$ biyectiva; esta función permite "identificar" cada elemento de A con uno, digamos n, de $\mathbb{N}$ por medio de a. Si se escribe a_n en lugar de a(n) resulta que

$$A=\{\, a_n \mid n\in\mathbb{N} \,\}$$

la expresión del lado derecho se dice que es una *enumeración* del conjuto numerable A.

Sean pues, dos conjuntos numerables A y B y

$$A=\{\, a_n \mid n\in\mathbb{N} \,\} \quad y \quad B=\{\, b_n \mid n\in\mathbb{N} \,\}$$

enumeraciones para ellos. Si A y B además son conjuntos totalmente ordenados por $\ll$ y $<$ respectivamente, densos y sin extremos podemos definir, vía el teorema de Recursión, funciones, de hecho enumeraciones $c:\mathbb{N}\longrightarrow A$, $d:\mathbb{N}\longrightarrow B$ como sigue:

i) $c(0)=c_0=a_0$, $d(0)=d_0=b_0$.

ii) Si $0<k$ y

1) k es impar

Definimos $d_k=b_j\in B$ donde j es el mínimo natural tal que $b_j\neq d_m\ \forall m<k$ y $c_k=a_i\in A$ donde i es el mínimo natural tal que a_i guarda la misma relación en el orden $\ll$ con respecto a $\{c_0,\ldots,c_{k-1}\}$ que la relación que mantiene d_k en el orden $<$ con respecto a $\{d_0,\ldots,d_{k-1}\}$.

2) k es par

Como, en particular A es infinito y, obviamente, el conjunto $C_j=\{\, c_j\in A \mid j<k \,\}$ es finito, habrá elementos a_i que no están ahí, así, el conjunto $\{\, n\in\mathbb{N} \mid c_n\notin C \,\}\neq\emptyset$ tiene un primer elemento i pues $\mathbb{N}$ es bien ordenado. Entonces definimos

$$c_k=a_i$$

Por otro lado, para definir d_k nos ayudamos de los elementos $c_0,c_1,\ldots,c_k$; como el orden $\ll$ es total, estos elementos están totalmente ordenados; así, c_k está entre dos elementos, digamos c_l,c_m $(c_l\ll c_k,\ c_k\ll c_m)$ con $l,m<k$. Además, el orden $<$ de B es denso y no tiene primero ni último elemento, así que entre d_l y d_m habrá elementos de B; es decir, $\{\, b_j\in B \mid d_l<b_j \wedge b_j<d_m \,\}\neq\emptyset$, consecuentemente $\{\, n\in\mathbb{N} \mid d_l<b_n \wedge b_n<d_m \,\}\neq\emptyset$ y tiene un primer elemento, si j es ese primer elemento definimos

$$d_k=b_j$$

En pocas palabras, $c_k=a_i$ donde i es el mínimo número natural tal que $a_i\neq c_m\ \forall m<k$ y $d_k=b_j$ donde j es el mínimo natural tal que b_j se encuentra en la misma relación de orden $<$ con $\{d_0,\ldots,d_{k-1}\}$ que la relación que guarda d_k con $\{c_0,\ldots,c_{k-1}\}$ en el orden $\ll$.

Las anteriores son enumeraciones para A y para B que servirán para establecer una biyección entre ellos que respete el orden. Ahora bien, intuitivamente debe ser claro que

$$\{\, c_n \mid n\in\mathbb{N} \,\}=A \quad y \quad \{\, d_n \mid n\in\mathbb{N} \,\}=B$$

debido a la manera en que se van eligiendo los elementos; de cualquier forma, esto puede probarse formalmente usando inducción sobre n:

Si n=0

como $a_0=c_0$ entonces $a_0 \in \{ c_n \mid n \in \mathbb{N} \}$

Supóngase que $a_0, \ldots, a_k$ están todos en $\{ c_n \mid n \in \mathbb{N} \}$; es decir,

$$\forall i \leq k \; \exists n \in \mathbb{N}(a_i = c_n)$$

Sea n_0 el máximo de todos esos $n \in \mathbb{N}$

si $a_{k+1}=c_n$ para algún $n \leq n_0$ entonces $a_{k+1} \in \{ c_n \mid n \in \mathbb{N} \}$

en caso contrario $a_{k+1} \neq c_n \; \forall n \leq n_0$ y si n_0 es impar entonces n_0+1 será par y por tanto

$$a_{k+1}=c_{n_0+1} \in \{ c_n \mid n \in \mathbb{N} \}$$

pero si n_0+1 es impar y $a_{k+1}=c_{n_0+1}$ entonces, nuevamente

$$a_{k+1} \in \{ c_n \mid n \in \mathbb{N} \}$$

por último, si $a_{k+1} \neq c_{n_0+1}$ entonces $a_{k+1} \neq c_n \; \forall n \leq n_0+1$ o bien

$$a_{k+1} \neq c_n \; \forall n < n_0+2$$

y como n_0+2 es par, por definición

$$a_{k+1}=c_{n_0+2}$$

y también en este caso, $a_{k+1} \in \{ c_n \mid n \in \mathbb{N} \}$.

Así que, efectivamente, $\{ c_n \mid n \in \mathbb{N} \}=A$; análogamente se prueba que $\{ d_n \mid n \in \mathbb{N} \}=B$.

Finalmente, la función

$$h: A \longrightarrow B \quad \text{dada por} \quad h(c_n)=d_n$$

establece un isomorfismo de orden entre A y B; de hecho, $\{ c_n \mid n \in \mathbb{N} \}$ y $\{ d_n \mid n \in \mathbb{N} \}$ están definidos para que h preserve el orden.

En resumen, se ha probado el último resultado de esta sección.

TEOREMA 2. (CANTOR) Cualesquiera dos conjuntos totalmente ordenados, densos, sin extremos y numerables son isomorfos.

∎

En virtud de la proposición 12, el conjunto $\mathbb{Q}$ es totalmente ordenado, denso y sin extremos; por otro lado, el comentario que sigue al teorema 1 (CSB) dice que $\mathbb{Q}$ es numerable; así, el conjunto de números racionales es el único (salvo isomorfismo) linealmente ordenado, denso, sin extremos y numerable.

También debe ser intuitivamente claro que un orden como el de $\mathbb{Q}$ "absorbe" a cualquier conjunto numerable totalmente ordenado; de cualquier forma, para terminar este capítulo, se incuye este resultado:

PROPOSICION 13. Sea X un conjunto numerable tal que $\langle X, <' \rangle \in$ COTO entonces existe una función inyectiva $f: X \longrightarrow \mathbb{Q}$ tal que

$$\forall x, y \in \mathbb{Q}(x <' y \Rightarrow f(x) < f(y))$$

Es decir, f es una *inmersión* de $\langle X, <' \rangle$ en $\langle \mathbb{Q}, < \rangle$.

Prueba:

Sean $X=\{ c_n \mid n \in \mathbb{N} \}$, $\mathbb{Q}=\{ q_n \mid n \in \mathbb{N} \}$ enumeraciones para X y $\mathbb{Q}$ respectivamente y $q_0 \in \mathbb{Q}$ cualquiera.

Se define $p: \mathbb{N} \longrightarrow \mathbb{Q}$ recursivamente como

$$p(0) := p_0 = q_0$$

y si $n>0$

$$p(n) := p_n = q_i$$

donde $i \in \mathbb{N}$ es el primero tal que q_i guarda la misma relación de orden con respecto a $p_0, p_1, p_2, \ldots, p_{n-1}$ que la que guarda c_n con $c_0, c_1, c_2, \ldots, c_{n-1}$. Es decir,

si $c_0 <' c_1$ entonces $p_1 = q_i$ donde $i \in \mathbb{N}$ es el primero tal que

$p_0=q_0<q_1$; así,

$$p_0<p_1$$

y si $c_1<'c_0$ entonces $p_1=q_i$, donde $i\in N$ es el primero tal que $q_i<q_0=p_0$; así,

$$p_1<p_0.$$

Obsérvese que este primer paso siempre es posible gracias a que Q no tiene extremos.
Ahora, supóngase sin pérdida de generalidad que $c_0<'c_1$ entonces $p_0<p_1$ y si

i) $c_0<'c_1<'c_2$
entonces $p_2=q_i$ donde i es el primero tal que $p_0<p_1<q_i$; así,

$$p_0<p_1<p_2$$

ii) $c_0<'c_2<'c_1$
entonces $p_2=q_i$ donde i es el primero tal que $p_0<q_1<q_i$; así,

$$p_0<p_2<p_1$$

iii) $c_2<'c_0<'c_1$
entonces $p_2=q_i$ donde i es el primero tal que $q_i<p_0<p_1$; así,

$$p_2<p_0<p_1$$

y así sucesivamente se definen $p_3, p_4, \ldots$
i) y iii) son posibles, nuevamente, porque Q no tiene extremos y ii) es posible porque Q es denso.
Ahora bien, es claro que $\{ p_n \mid n\in N \}\subseteq Q$ y que

$$f: X\longrightarrow Q$$
$$f(c_n)=p_n$$

es tal que

$$c_i<'c_j \Rightarrow f(c_i)=p_i<p_j=f(c_j)$$

o bien $\quad c_j<'c_i \Rightarrow f(c_j)=p_j<p_i=f(c_i)$.

Así que f es compatible con el orden entre X y Q y, por tanto, es inyectiva.

∎

Claramente esta prueba es una versión mas simple que la del teorema 2, donde se han mencionado explícitamente las propiedades de Q con objeto de ilustrar que en la prososición 13 puede colocarse cualquier $\langle Q,<\rangle\in COTO$ denso, numerable y sin extremos aún sin saber que resulta ser isomorfo a Q con el orden usual.

De las dos formas usuales de definir los números reales, que son sucesiones de Cauchy y cortaduras de Dedekind, se elige la segunda opción por parecer, intutivamente, mas clara y natural.

Para los números reales se desea un orden lineal, sin extremos, denso y sin "huecos". Los números racionales ya tienen las tres primeras de estas cuatro características así que solo falta "rellenar los huecos" que aún permanecen. Para esto, se tomará el orden lineal de $\mathbb{Q}$ y se le "partirá" para completarlo y llegar a $\mathbb{R}$.

Se desea que las cortaduras definan, posiblemente, nuevos objetos además de los elementos de $\mathbb{Q}$, con esta idea en mente debe ser claro que las siguientes cuatro posibilidades se presentan al "cortar" un orden lineal cualquiera, las que pueden definir nuevos objetos son las de tipo 2 y 3 y las de tipo 4 (huecos).

1) ——— ——— salto
2) ——— ⟵———
3) ———⟶ ———
4) ———⟶ ⟵——— hueco

El caso 1 ya no se dá si el orden lineal también es denso.

De hecho, las cortaduras de tipo 2 y 3 (que solo difieren por la localización del extremo), pueden identificarse con el punto que las define pero las cortaduras de tipo hueco no están definidas por ningún elemento (ninguno del conjunto totalmente ordenado, denso y sin extremos del que se parte); ellos constituyen los "nuevos números", los números que llamaremos *irracionales*.

5.1 DEFINICION Y PROPIEDADES DE LOS NUMEROS REALES

DEFINICION 1. Un conjunto I es un *segmento inicial* de $\mathbb{Q}$ si

i) $I\subseteq\mathbb{Q}$, $I\neq\mathbb{Q}$, $I\neq\emptyset$

ii) $\forall q,r\in\mathbb{Q}(\ q<r\ \wedge\ r\in I\ \Rightarrow\ q\in I\ )$

iii) $\neg\exists r\in I\ \forall q\in\mathbb{Q}(\ q\leq r\ )$

El inciso (iii) de esta definición establece que un segmento inicial de $\mathbb{Q}$ no tiene un elemento máximo.

DEFINICION 2. Una *cortadura de Dedekind* es un conjunto $<I,\mathbb{Q}\setminus I>$ tal que I es un segmento inicial de $\mathbb{Q}$.

De la definición de segmento inicial de $\mathbb{Q}$ se observa que trabajando cortaduras del tipo 3 y de tipo hueco.

DEFINICION 3. El conjunto $\mathbb{R}$ de los *números reales* se define como
$\mathbb{R}=\{\ I\subseteq\mathbb{Q} \mid I$ es un segmento inicial de $\mathbb{Q}\ \}$

Obsérvese que $\mathbb{R}$ se ha definido como el conjunto de segmentos iniciales de $\mathbb{Q}$ y no como el conjunto de cortaduras de Dedekind; aun cuando puede emplearse cualquiera de las dos opciones, en realidad no son muy diferentes pues solo hay diferencia cuando se definen y se prueban características y propiedades de $\mathbb{R}$.

Por otro lado, que $\mathbb{R}$ efectivamente es un conjunto, se debe al axioma de comprensión y de potencia de ZF, pues resulta obvio que $\mathbb{R}\subseteq\mathcal{P}(\mathbb{Q})$.

Si bien un número racional no es un número real en sentido estricto, si se le puede identificar con uno de ellos de una manera muy natural; a saber

$$\forall r\in\mathbb{Q},\ I_r=\{\ q\in\mathbb{Q} \mid q<r\ \}\in\mathbb{R}$$

Es claro que I_r cumple la definición 1; el inciso (i) es inmediato, el (ii) se cumple por la transitividad del orden de $\mathbb{Q}$ y (iii) se satisface porque $\mathbb{Q}$ es denso.

5.2 EL ORDEN DE LOS NUMEROS REALES

DEFINICION 4. Si $x,y\in\mathbb{R}$ se dice que $x<y$ si $x\subseteq y$ & $x\neq y$.

Se abusa de la notación al usar el mismo símbolo para el orden en $\mathbb{R}$ y en $\mathbb{Q}$, si hubiera posibilidad de confusión se emplearán subíndices r y q para distinguirlos.

PROPOSICION 1. $\langle\mathbb{R},<\rangle\in$COTO ($\mathbb{R}$ es un conjunto totalmente ordenado por $<$)

Prueba:

La parte de interés es probar que la relación $<_r$ cumple la propiedad de tricotomía.

Sean $x,y\in\mathbb{R}$ y supóngase $x\neq y$ & $\neg(x<y)$. Una sencilla propiedad en el álgebra de conjuntos dice que $\neg(a\subseteq b)\ \Rightarrow\ a\backslash b\neq\emptyset$; sea pues $r\in x\backslash y$. Queremos ver que $y\subseteq x$, tómese entonces $q\in y$, como el orden en $\mathbb{Q}$ es total, sucede $q<r$ ó $r\leq q$, pero $r\leq q$ no puede ocurrir pues en tal caso, como y es un segmento inicial, por el inciso ii) de la definción 1 se tiene $r\in y$, lo cual es absurdo; así que debe ser $q<r$, pero $r\in x$ & x es un segmento inicial, por tanto $q\in x$, así pues $y\subseteq x$ & $y\neq x$; o bien, $y<x$.

∎

Establezcamos las propiedades adicionales que tendrá $\langle\mathbb{R},<\rangle$.

DEFINICION 5. Si A es un conjunto y $<$ es una relación sobre A, se dice que $<$ es un *orden continuo* o simplemente un *continuo* para A si

i) $\langle A,<\rangle\in$COTO, A es $<$-denso y A no tiene $<$-extremos.

ii) A es $<$-*completo*; es decir, todo subconjunto no vacío de A acotado superiormente tiene una mínima cota superior o *supremo*.

iii) A es $<$-*separable*; es decir, A tiene un subconjunto numerable *denso en* A.

Resta escribir explícitamente las propiedades de completud y separabilidad en el lenguaje 3 de la Teoría de Conjuntos de Zermelo-Fraenkel que se ha venido empleando.

- A es <-*completo*:
  $\forall B \subseteq A[\ B \neq \emptyset \wedge \exists y \in A\ \forall x \in B(\ x<y \vee x=y\ ) \Rightarrow \exists w \in A\{\ \forall x \in B(\ x<w \vee x=w\ ) \wedge \forall z \in A(\ \forall x \in B(\ x<z \vee x=z\ ) \Rightarrow w<z \vee w=z\ )\ \}\ ]$
  Si B es no vacío y tiene una cota superior entonces hay una cota superior w tal que toda cota superior z es mayor o igual a ella (w).

- A es <-*separable*:
  $\exists B \subseteq A[\ B \approx \mathbb{N} \wedge \forall x,y \in A(\ x<y \Rightarrow \exists z \in B[\ x<z \wedge z<y\ ]\ )\ ]$
  Existe un subconjunto B numerable de A tal que entre cualesquiera dos elementos de A existe uno de B.

PROPOSICION 2. El orden < es continuo para $\mathbb{R}$.

Prueba:

Veremos que se cumple i), ii) y iii) de la definición 5.

i) Por la proposición 1 $<\mathbb{R},<> \in COTO$; además, si se prueba que $\mathbb{R}$ es separable automáticamente se tendrá su densidad; así pues se posterga esta prueba y ahora veremos que $\mathbb{R}$ no tiene extremos. Pero esto es fácil pues si $x \in \mathbb{R}$ bastará encontrar un elemento $y \in \mathbb{R}$ tal que $x<y$, sea $y=x^{\frown}=\{\ p+q \in \mathbb{Q} |\ p \in x \wedge q<1\ \}$. Claramente $x \subseteq x^{\frown}$ y si fuera $x=x^{\frown}$ podríamos tomar $p=r/s \in x$ tal que para cualquier $m/n \in \mathbb{Q}$ sucede lo siguiente: si $0<p$ entonces $0 \in x=x^{\frown}$ (pues $x \in \mathbb{R}$) y así $0+1/n \in x^{\frown}$, repitiendo este proceso a lo más m veces resulta que $0+m/n=m/n \in x^{\frown}=x$, por tanto $x=x^{\frown}=\mathbb{Q}$. Ahora, si $p \leq 0$ y $p=r/s$ entonces a lo más en $|r|$ pasos se tiene $0 \in x^{\frown}$ y en otros $|m|$ pasos $m/n \in x^{\frown}$ entonces, nuevamente $x=x^{\frown}=\mathbb{Q}$. Esta contradicción implica $x \subseteq x^{\frown}$ & $x \neq x^{\frown}$; es decir, $x<x^{\frown}$. Sin embargo también debe probarse que $x^{\frown} \in \mathbb{R}$, *i.e* cumple la definición 1.

   - Es inmediato que $\emptyset \neq x^{\frown} \subseteq \mathbb{Q}$; para ver que $x^{\frown} \neq \mathbb{Q}$, sea $r \in \mathbb{Q}/x$, se afirma que $r+1 \notin x^{\frown}$ pues si $r+1=p+q$ con $p \in x$ y $q<1$ entonces $p=r+1-q \in x$. Ahora, como $q<1$ se tiene $r<r+1-q=p$ pero $p \in x$ y $x \in \mathbb{R}$ entonces $r \in x$, lo cual es absurdo. Así, $r+1 \notin x^{\frown}$ y finalmente $x^{\frown} \neq \mathbb{Q}$.
   - Sean $r,s \in \mathbb{Q}$ tales que $r<s$ y $s \in x^{\frown}$ entonces $s=p+q$ con $p \in x$ y $q<1$ entonces $r<p+q \Rightarrow r-q<p$ y $p \in x$ implica $r-q \in x$ por tanto
     $$r=(r-q)+q \in x^{\frown}$$
   - Supóngase que $x^{\frown}$ tiene un máximo y sea m ese máximo, entonces $m=p_0+q$ con $p_0 \in x$ & $q<1$. Sea ahora $p \in x$, se afirma que $p \geq p_0$ no puede ocurrir pues en tal caso
     $$p+q \geq p_0+q=m$$
     pero $p+q \in x^{\frown}$ y m es el máximo; así, el $\geq$ no se dá, entonces se tiene que $p<p_0$, pero esto quiere decir que p_0 es máximo para x, lo cual es absurdo pues $x \in \mathbb{R}$. Por tanto $x^{\frown}$ no puede tener máximo.
     De manera análoga se tiene que $x^{\sim}=\{\ p+q \in \mathbb{Q} |\ p \in x \wedge q<-1\ \}<x$ con lo cual queda establecido que $\mathbb{R}$ no tiene extremos.

ii) Sea $\emptyset \neq B \subseteq \mathbb{R}$ acotado superiormente, hallaremos la mínima cota superior para B; como los elementos de B son segmentos iniciales y como la unión de segmentos iniciales también es un segmento inicial y además $\cup B$ es el mínimo conjunto que contiene a B; el candidato natural para el supremo (mínima cota superior) de B es $\cup B$, solo resta probar que $\cup B \in \mathbb{R}$:
   - Es inmediato que $\emptyset \neq \cup B \subseteq \mathbb{Q}$. Supóngase que $\cup B = \mathbb{Q}$ y sea $y \in \mathbb{R}$

una cota superior para B, como y es un segmento inicial, $y \leq \mathbb{Q} = \bigcup B$; por otro lado, el que sea una cota implica que $\forall x \in B(\ x \leq y\ )$ y entonces $\bigcup B \leq y$. Así, $y = \mathbb{Q} = \bigcup B$, lo cual contradice el inciso (i) de la definición 1 para $y \in \mathbb{R}$.

–Sea $p, q \in \mathbb{Q}$ tales $p<q$ y $q \in \bigcup B$, entonces $\exists x \in B(\ q \in x\ )$, como x es un segmento inicial, se tiene que $p \in x$ y de aquí que $p \in \bigcup B$.

– Supóngaseque $\bigcup B$ tiene un máximo m, entonces hay un elemento $x \in B$ tal que $m \in x$ pero $\forall y \in \bigcup B(\ y \leq m\ )$; en particular, $\forall y \in x(\ y \leq m\ )$; o sea, m es máximo para x, lo cual no es posible.

iii) Para ver que $\mathbb{R}$ es separable, habrá que hallar un subconjunto numerable denso en $\mathbb{R}$. Intuitivamente, conocemos un conjunto con esa propiedad: los racionales.

Sea $\mathbb{Q} = \{\ I_r \mid r \in \mathbb{Q}\ \}$ donde $I_r = \{\ q \in \mathbb{Q} \mid q < r\ \}$, claramente $\mathbb{Q} \subseteq \mathbb{R}$ y la función $f: \mathbb{Q} \longrightarrow \mathbb{Q}$ dada por $f(r) = I_r$ establece una biyección, así $\mathbb{Q}$ es numerable porque $\mathbb{Q}$ lo es; es inmediato que f es suprayectiva y si $I_r = I_{r'}$ veremos que no es posible que $r<r'$ pues en tal caso, $r \in I_{r'} = I_r$ entonces $r<r$, lo cual es absurdo; análogamente $\neg(r'<r)$, así solo queda que $r'=r$.

Sean ahora $x, y \in \mathbb{R}$ tales que $y<x$; como x es subconjunto propio de y, sean $r \in y \setminus x$, aquí podria decirse que $x<I_r<y$, pero no puede garantizarse que x sea un subconjunto propio de I_r; de hecho, puede suceder que $x = I_r$. Pero r no es el último elemento de y, así que hay un $t \in y$ tal que $r<t$. Ahora si afirmamos que $x \leq I_t < y$. Veamos que $x \leq I_t$ & $x \neq I_t$: si $p \in x$ no puede darse $t \leq p$ pues en tal caso sería $t \in x$, lo cual es falso; así $p<t$, por tanto $p \in I_t$ o bien, $x \leq I_t$. Además si $x = I_t$ y, dado que, $r<t$ se tiene que $r \in I_t = x$ lo cual es una contradicción; es decir, $x \neq I_t$.

Comprobemos que $I_t \subseteq y$ & $I_t \neq y$, si $p<t$ entonces $p \in y$ pues $t \in y$, entonces $I_t \subseteq y$; por otro lado, $t \in y$ y como $\neg(t<t)$ sucede que $t \notin I_t$; así, $I_t \neq y$.

Por lo tanto, $x<I_t<y$ y desde luego, $I_t \in \mathbb{Q}$.

∎

En la concepción común de $\mathbb{Q}$ y $\mathbb{R}$ sucede que $\mathbb{Q} \subseteq \mathbb{R}$, por la forma en que se los ha definido aquí no resulta esto directamente, pero un resultado intuitivamente claro es que $\mathbb{Q}$ es isomorfo a un subconjunto de $\mathbb{R}$. Si denotamos momentáneamente por $<$ al orden de $\mathbb{Q}$ y por $<$ al de $\mathbb{R}$ se puede enunciar la siguiente afirmación.

PROPOSICION 3. Existe una *inmersión* de $\langle \mathbb{Q}, < \rangle$ en $\langle \mathbb{R}, < \rangle$. Es decir, existe una función $i: \mathbb{Q} \longrightarrow \mathbb{R}$ inyectiva tal que
$\forall s, s' \in \mathbb{Q}(\ s<s' \Rightarrow i(s)<i(s')\ )$

Prueba:

Sea $i: \mathbb{Q} \longrightarrow \mathbb{R}$ dada por
$i(s) = I_s = \{\ q \in \mathbb{Q} \mid q<r\ \}$.

Las observaciones hechas al final de la sección 5.1 muestran que, efectivamente, $I_s \in \mathbb{R}$ para cada $s \in \mathbb{Q}$.

Supóngase que $s, s' \in \mathbb{Q}$ son tales que $s<s'$, si se prueba que $I_s \subseteq I_{s'}$ y $I_s \neq I_{s'}$ automáticamente resultará la inyectividad de la inmersión i.

Es claro que $I_s \subseteq I_{s'}$ pues si $q \in I_s$ entonces $q<s$ y como $s<s'$ se tiene que $q<s'$, con lo cual $q \in I_{s'}$.

Ahora, de que $s<s'$ y de la densidad de $\mathbb{Q}$, tomamos $s'' \in \mathbb{Q}$ tal que

s<s"<s'; por definición s"∈I$' pero s"∉I$ puers en caso contrario sería s"<s' lo cual es absurdo. Así, I$≠I$'; es decir, I$<I$'.

5.3 UNICIDAD DE LOS NUMEROS REALES

Ahora ya se puede caracterizar al conjunto $\mathbb{R}$ de números reales como el único conjunto que satisface la definición 5; es decir, $\langle \mathbb{R}, < \rangle$ es el único conjunto con un orden continuo; único en el siguiente sentido:

PROPOSICION 4. Si $\langle A, < \rangle$ y $\langle B, <' \rangle$ son conjuntos tales que su orden es continuo, entonces ellos son isomorfos; es decir, existe una función $f: A \longrightarrow B$ biyectiva tal que

$$\forall a_1, a_2 \in A\,(\, a_1 < a_2 \iff f(a_1) <' f(a_2)\,)$$

Prueba:

En particular, A y B son separables; sean pues, D_A y D_B los subconjuntos numerables de A y B respectivamente, tales que D_A es denso en A y D_B es denso en B. Por supuesto, D_A y D_B no tienen extremos; así, de acuerdo al teorema 2 (Cantor) del capítulo 4, existe una función $h: D_A \longrightarrow D_B$ biyectiva tal que

$$\forall r, r' \in D_A\,(\, r < r' \iff h(r) <' h(r')\,)$$

Ahora, para cada $a \in A$ considérese el conjunto

$$\{\, h(r) \mid r \in D_A \wedge r \leq a\,\} \leq A$$

es claro que este conjunto es no vacío y que cualquier $h(r')$ con algún $r' \in D_A$ tal que $a \leq r'$ es una cota para él; como A es completo, el conjunto en cuestión tiene una mínima cota superior; es decir, un supremo. Con esto definimos

$$f: A \longrightarrow B \quad \text{como}$$
$$f(a) = <'\text{-sup}\{\, h(r) \mid r \in D_A \wedge r \leq a\,\}$$

Observemos primero que f coincide con h en D_A; o sea,

$$\forall r \in D_A\,(\, f(r) = h(r)\,)$$

Sea $r' \in D_A$, $f(r') = \sup\{\, h(r) \mid r \in D_A \wedge r \leq r'\,\}$

Como h es isomorfismo $\forall r \in D_A\,(\, r \leq r' \Rightarrow h(r) \leq' h(r')\,)$ entonces $h(r')$ es cota superior de $\{\, h(r) \mid r \in D_A \wedge r \leq r'\,\}$.

Si t es cota superior de este conjunto, y si $r \in D_A$ es tal que $r \leq r'$ se tiene que $h(r) \leq' t$, en particular, para $r = r'$ $h(r') \leq' t$.

Por tanto, $h(r') = \sup\{\, h(r) \mid r \in D_A \wedge r \leq r'\,\} = f(r')$.

—Veamos ahora que f es inyectiva probando directamente que preserva el orden.

Sean $a_1, a_2 \in A$ tales que $a_1 < a_2$, Como D_A es denso en A podemos tomar $r_1, r_2 \in D_A$ tales que $a_1 < r_1 < r_2 < a_2$; entonces $h(r_1)$ es cota de $\{\, h(r) \mid r \in D_A \wedge r \leq a_1\,\}$, así, $\sup\{\, h(r) \mid r \in D_A \wedge r \leq a_1\,\} \leq' h(r_1)$ además $h(r_1) <' h(r_2)$ y $h(r_2) \leq' \sup\{\, h(r) \mid r \in D_A \wedge r \leq a_2\,\}$; i.e, $\sup\{\, h(r) \mid r \in D_A \wedge r \leq a_1\,\} <' \sup\{\, h(r) \mid r \in D_A \wedge r \leq a_2\,\}$; entonces

$$f(a_1) <' f(a_2).$$

Por tanto, f preserva el orden y, como el orden $<$ de A es total, también f es inyectiva.

—Para ver que f es suprayectiva, tómese $b \in B$ y considérese

$$A_b = \{\, r \in D_A \mid h(r) \leq' b\,\}$$

Primero, si $b \in D_B$ entonces $\exists a \in D_A$ tal que $h(a) = b$ y como h coincide con f en D_A se tiene $f(a) = b$.

Supóngase pues que $b \notin D_B$, ello prmite escribir

$$A_b = \{\, r \in D_A \mid h(r) <' b\,\}$$

Sea cualquier $s_0 \in D_b$ tal que $b <' s_0$, como $s_0 = h(r_0)$ para algún $r_0 \in D_a$, $b <' h(r_0)$. Así que si $r \in A_b$ entonces $h(r) <' b <' h(r_0)$, de lo cual $r < r_0$ pues h preserva el orden; todo esto ha sido para afirmar que A_b es acotado superiormente y poder referirnos a su supremo.

Se afirma que

$$b = f(\sup A_b) = \sup\{\, h(r) \mid r \in D_a \wedge r \leq \sup A_b \,\}. \qquad \text{----------(I)}$$

Para probar esto será útil recordar una propiedad del supremo: En un COTO X, $\forall x \in X(\ x < \sup A \Rightarrow \exists x_0 \in A(\ x < x_0\ )\ )$, esta implicación es obvia porque la contrapositiva lo es:

$$\forall x \in X(\ \forall x_0 \in A(\ x_0 \leq x\ ) \Rightarrow \sup A \leq x\ ).$$

Se usa la primera forma de este enunciado para ver que si $r' \in D_a$ es tal que $r' < \sup A_b$ entonces $\exists r_0 \in A_b(\ r' < r_0\ )$, pero $r_0 \in A_b$ significa que $h(r_0) <' b$ entonces

$h(r') <' h(r_0) <' b$, así $h(r') <' b$, por tanto, $r' \in D_a$.

En pocas palabras

$$r \in D_a \wedge r < \sup A_b \Rightarrow r \in A_b \qquad \text{----------(II)}$$

lo cual debió ser intuitivamente claro.

Ahora si probemos (I), lo cual implica probar que:

i) b es cota superior de $\{\, h(r) \mid r \in D_a \wedge r \leq \sup A_b \,\}$:

Sea $r \in D_a$ tal que $r \leq \sup A_b$:

-) Si $r = \sup A_b$ entonces $h(r) = h(\sup A_b) \leq' b$ pues si fuera $b <' h(\sup(a_b))$ podríamos tomar $s_0 \in D_b$ tal que

$$b <' s_0 <' h(\sup(A_b)) \qquad \text{----------(III)}$$

entonces, para algún $r_0 \in D_a$

$b <' h(r_0) <' h(\sup A_b) = h(r)$, entonces $r_0 < \sup A_b = r$ y por (II) $r_0 \in A_b$, por tanto, $h(r_0) <' b$, o bien

$s_0 <' b$, lo cual contradice (III).

=) Si $r < \sup A_b$, por (II) $r \in A_b$ entonces $h(r') <' b$.

Con lo cual queda probado que b es cota superior.

ii) b es la mínima cota superior de $\{h(r) \mid r \in D_a \wedge r \leq \sup A_b\}$:

Supóngase que b' es un cota superior del mismo conjunto, entonces

$$\forall r(\ r \in D_a \wedge r \leq \sup A_b \Rightarrow h(r) \leq' b'\ ) \qquad \text{----------(IV)}$$

Supóngase también que $b' <' b$ y sea $s \in D_b$ tal que

$$b' <' s <' b \qquad \text{----------(V)}$$

entonces, para algún $r \in D_a$,

$b' <' h(r) <' b$, entonces $r \in A_b$ y

$r \leq \sup A_b$ y, por (IV)

$h(r) \leq' b'$, o bien

$s \leq' b$, lo cual contadice (V).

Por tanto, lo que debe ocurrir es que $b \leq' b'$.

O sea que, por i) y ii) $b = \sup\{\, h(r) \mid r \in D_a \wedge r \leq \sup A_b \,\}$, i.e, $b = f(\sup A_b)$.

Por tanto f es suprayectiva.

Lo cual prueba la proposición. ∎

La proposición 2 dice que $\langle R, < \rangle$ es un continuo así que, de acuerdo a la proposición 4, ha quedado establecido que $\langle R, < \rangle$ es el único orden continuo salvo isomorfismo.

5.4 LA ARITMETICA EN LOS NUMEROS REALES

Con objeto de leer fácilmente la presente sección, se empleará aquí la siguiente convención, se reservan las últimas letras del alfabeto,

w,x,y,z, para denotar números reales, dejando las intermedias, m,n,p,q,r,s para números racionales; de esta forma, el abuso de notación que se hará al denotar con los mismos símbolos a las operaciones no causará confusión; por ejemplo, xy significa el producto de los números reales x & y, mientras que r+s es la suma de los números racionales r & s, también -p denota al inverso aditivo del racional p y -x será el inverso aditivo del real x. Algo parecido sucede con los elementos distinguidos; por ejemplo, 0 es el cero de $\mathbb{R}$ y 0 el de $\mathbb{Q}$.

DEFINICION 6. Para $x,y\in\mathbb{R}$ definimos la *suma* de x & y como

$$x+y:=\{\ p+q\in\mathbb{Q}\mid p\in x\ \wedge\ q\in y\ \}$$

Obsérvese que x+y es un conjunto gracias al Axioma de Separación y al hecho de que $\mathbb{Q}$ es un conjunto.

Por supuesto que la suma de números reales disfruta de las propiedades esperadas; es decir, es conmutativa y asociativa. Aunque sencillo, es muy tedioso probarlas, mejor las damos por ciertas y probaremos otras propiedades mas interesantes.

PROPOSICION 5. $\forall x,y\in\mathbb{R}(\ x+y\in\mathbb{R}\ )$

Prueba:

i) Que $x+y\subseteq\mathbb{Q}$ & $x+y\neq\emptyset$ es inmediato. Probemos ahora que x+y es un subconjunto propio de $\mathbb{Q}$.
Sin pérdida de generalidad podemos suponer
$$x\subseteq y\ \&\ y\subseteq\mathbb{Q}\ \wedge\ y\neq\mathbb{Q}$$
sean $r\in\mathbb{Q}\setminus y$ & $p\in x, q\in y$, como x & y son segmentos iniciales
$$p<r\ ,\ q<r$$
entonces $p+q<r+r$
por tanto $r+r\notin x+y$ $\therefore\ x+y\neq\mathbb{Q}$.

ii) Sean $r,s\in\mathbb{Q}$ tales que $r<s\ \wedge\ s\in x+y$ entonces
$$r<s=p+q\quad\text{con } p\in x\ \&\ q\in y$$
$$r-p<q\ \Rightarrow\ r-p\in y$$
$$r=p+(r-p),\ p\in x,\ r-p\in y$$
entonces $r\in x+y$.
Se ha probado $\forall r,s\in\mathbb{Q}(\ r<s\ \wedge\ s\in x+y\ \Rightarrow\ r\in x+y\ )$

iii) Sean cualesquiera $p\in x$, $q\in y$, veremos que p+q no es máximo de x+y hallando $p_0+q_0\in x+y$ tal que $p+q<p_0+q_0$.
Como p no es máximo de x $\exists p_0\in x(\ p<p_0)$, igualmente,
como q no es máximo de y $\exists q_0\in y(\ q<q_0)$ entonces
$$p+q<p_0+q_0.$$

Los tres incisos anteriores prueban que $x+y\in\mathbb{R}$. ∎

La definición anterior debe disfrutar de las propiedades que de ella se esperan; para ello se necesitan algunos otros objetos.

DEFINICION 7. 1) Para $x\in\mathbb{R}$ su *inverso aditivo* se denota -x y se define como: $-x:=\{\ p\in\mathbb{Q}\mid \exists s>p(\ -s\in x\ )\ \}$

2) También se denota al *cero* como 0, y se le define por
$$0:=\{\ q\in\mathbb{Q}\mid q<0\ \}.$$

Debe ser claro que $0\in\mathbb{R}$; de hecho, según las obervaciones que siguen a la definición 3, $0=1_0$.

PROPOSICION 6. $\forall x\in\mathbb{R}(\ x+0=x\ )$

Prueba:

Por definición

$$x+0=\{\ p+q|\ p\in x\ \wedge\ q\in 0\ \}=\{\ p+q|\ p\in x\ \wedge\ q<0\ \}$$

Sean pues $p\in x\ \wedge\ q<0$, i.e. $p+q\in x+0$, de

$$q<0 \quad \text{se sigue}$$

$$p+q<p+0=p$$

pero $p\in x$ & x es segmento inicial, entonces $p+q\in x$

$$\therefore\ x+0\subseteq x.$$

Sea ahora $p\in x$, como x no tiene máximo $\exists p_0\in x(\ p<p_0)$ entonces $p-p_0<0$, luego

$$p=p_0+(p-p_0) \quad \text{con } p_0\in x \text{ \& } p-p_0<0$$

esto significa que $p\in x+0$

$$\therefore\ x\subseteq x+0.$$

Junto con la conclusión anterior se tiene

$$x=x+0.$$

■

PROPOSICION 7. $\forall x\in\mathbb{R}(\ -x\in\mathbb{R}\ )$.

Prueba:

i) a) $-x\subseteq 0$ es inmediato.

b) Sea $p\in 0\setminus x$ y $q\in 0$ tal que $p<q$, entonces $-q<-p$ y como $-(-p)=p\notin x$ el elemento $-p$ evidencia que $-q\in -x$. Por tanto

$$-x\neq\emptyset.$$

c) Sea $p\in x$, se afirma que $-p\notin -x$. Esto será cierto si y solo si $\forall s>-p(\ -s\in x\ )$

pero esto es cierto porque si $s>-p$ entonces $-s<p$ y como $p\in x$ & x es segmento inicial se sigue que $-s\in x$.

Por lo tanto

$$-x\neq 0.$$

ii) Sean $p,q\in 0$ tales que $p<q$ & $q\in -x$,

entonces $\exists s>q(\ -s\notin x\ )$,

pero $q>p$ entonces

$\exists s>p(\ -s\notin x\ )$,

esto prueba que $p\in x$. Por lo tanto,

$$\forall p,q\in 0(\ p<q\ \wedge\ q\in -x\ \Rightarrow\ p\in -x\ )$$

iii) Enseguida se prueba que $-x$ no tiene máximo:

Existen elementos $q\in 0$ tales que $\forall p\in -x(\ p<q\ )$, si se prueba que ninguno de ellos pertenece a $-x$ se habrá probado lo que se desea. Si un q de ellos perteneciera a $-x$ entonces $\exists s>q(\ -s\in x\ )$.

Afirmamos que $-q$ es máximo de x pues si no fuera así $\exists r\in x(\ -q<r\ )$, de que $-s<-q$ se sigue $-s<r$ y como $r\in x$ también $-s\in x$, lo cual es absurdo; por tanto, efectivamente, $-q$ es máximo de x, lo cual, a su vez, es una contradicción. Entonces, $q\notin -x$, lo cual prueba que $-x$ no tiene máximo.

Ya se puede concluir que

$$-x\in\mathbb{R}.$$

■

Para probar que $x+(-x)=0$ se necesitan algunos resultados previos.

LEMA 1. Si $x>0$ entonces $-x<0$.

Prueba:

Sea $p\in -x$, por definición $\exists s>p(\ -s\in x\ )$.

$-s\notin x$ implica $-s\in 0$ gracias a que $0\subseteq x$, así $-s\geq 0$, o bien $s\leq 0$, entonces

$p<s\leq 0$ entonces $p<0$; es decir, $p\in 0$. Por lo tanto
$$-x\leq 0.$$
P.D. $-x\neq 0$.
Como $x\neq 0$ $\exists p_0\in x\setminus 0$, entonces $0\leq p_0\in x$. Dado que x no tiene máximo se puede hallar $p\in x$ tal que $0\leq p<p$, entonces $-p\in 0$. Se afirma que $-p\notin -x$.
Si $s\in Q$ es tal que $s>-p$ y $-p<s\leq p$ entonces
$-p\leq -s<p$, entonces $-s\in x$ pues $p\in x$.
si se da la otra posibilidad, i.e.
$s>p>0$ entonces $s>0$ ó
$-s<0$ luego $-s\in 0\leq x$, entonces $-s\in x$.
En cualquier caso se ha probado
$$\forall s\in Q(\ s>-p \Rightarrow -s\in x\ ).$$
Por tanto
$-p\notin -x$ y como $-p\in 0$, se tiene en consecuencia que $-x\neq 0$.
Finalmente
$$-x<0.$$
∎

LEMA 2. $\forall p\in Q(\ -I_p=I-p \wedge I_p+(-I_p)=0\ )$. Donde $I_p:=\{\ q\in Q \mid q<p\ \}$
Prueba:
Sea $q\in -I_p$, entonces $\exists s>q(\ -s\notin I_p\ )$, luego $q<s$ y por definición de I_p, $-s\geq p$ entonces $q<s$ & $s\leq -p$, de aqui, $q<-p$, por tanto $q\in I-p$; es decir,
$$-I_p\subseteq I-p.$$
Sea ahora $q\in I-p$, entonces $q<-p$ y quiere probarse que $\exists s>q(\ -s\notin I_p\ )$, i.e. $\exists s>q(\ p\leq s\ )$.
Sea $s\in 0$ cualquiera entre q y $-p$; o sea, $q<s<-p$, entonces $q<s$ & $p<-s$, en particular, $q<s$ & $p\leq s$, por lo tanto $q\in -I_p$; es decir,
$$I-p\subseteq -I_p.$$
Por lo tanto,
$$I-p=-I_p.$$
Veamos ahora que $I_p+I-p=0$.
Probaremos que $0\subseteq I_p+I-p$.
Supóngase primero $p<0$.
Sea $q\in 0$, entonces $q<0$ y como $p<0$ siempre existe el mínimo $0\neq n\in N$ tal que
$nq\in I_p$ y como $n-1\in N$ $(n-1)q\notin I_p$, i.e. $nq<p$ & $(n-1)q\geq p$ entonces $-(n-1)q\leq -p$.
Si $-(n-1)q<-p$ entonces $-(n-1)q\in I-p$, por tanto
$$q=nq+(-(n-1)q)\in I_p+I-p.$$
Si $-(n-1)q=-p$, sea $r\in 0$ tal que $nq<r<p=(n-1)q$, entonces
$-nq>-r$, sumando q
$-nq+q>q-r$ entonces $(1-n)q>q-r$ y si fuera
$q-r\geq -p$ ..... (*)
entonces $(1-n)q>-p$ o bien $(n-1)q<p$, lo cual significa que $(n-1)q\in I_p$, pero esto es absurdo, así que (*) no se cumple, es decir,
$q-r<-p$, luego $q-r\in I-p$. Por lo tanto
$$q=r+(q-r)\in I_p+I-p.$$
Supóngase ahora $p=0$ y $q\in 0$, cualquier $r\in 0$ tal que $0<r<-q$ hace que $q=(q+r)-r$ com $q+r\in 0$ & $-r\in 0=I-0$
$$\therefore\ q\in 0+I-0.$$
El caso $p>0$ es análogo al caso $p<0$ intercambiando p por $-p$, pues $-p<0$.

En cualquier caso ha quedado probado que

$$0 \leq I_p + I_{-p}.$$

Para probar $I_p + I_{-p} \leq 0$ tómese $q \in I_p + I_{-p}$, entonces $q = r + s$ con $r < p$ & $s < -p$, pero entonces

$q = r + s < p + (-p) = 0$; es decir,

$$q \in 0.$$

Por lo tanto, se puede concluir que

$$I_p + I_{-p} = 0.$$

∎

PROPOSICION 8. $\forall x \in R(\ x + (-x) = 0\ )$.

Prueba:

Sea $r \in x + (-x)$, $\Rightarrow r = p + q$ con $p \in x$ & $q \in -x \Rightarrow \exists s > q(\ -s \notin x\ )$. Pero $-s \notin x$ y $p \in x$ implica $p \geq -s$ y junto con $q < s$ resulta $r = p + q < -s + s = 0$, entonces $r \in 0$, o bien $x + (-x) \leq 0$.

Sea ahora $t \in 0$, entonces $t < 0$.

Si primero suponemos $x < 0$ puede hallarse el mínimo $0 \neq n \in N$ tal que $nt \in x$, entonces $(n-1)t \notin x$.

Si $\exists s < (n-1)t$ tal que $s \notin x$ entonces $-s > -(n-1)t$ & $-(-s) = s \notin x$, luego $-s$ evidencia que $-(n-1)t \in -x$

$\therefore\ t = nt + (-(n-1)t) \in x + (-x)$.

Si $\forall s < (n-1)t$ ocurre que $s \in x$ entonces $x = I_{(n-1)t}$.

Esto es cierto porque

Si $p \in I_{(n-1)t}$ entonces $p < (n-1)t$, lo cual implica $p \in x$

$\therefore\ I_{(n-1)t} \leq x$.

Si $p \in x$ como $(n-1)t \notin x$ se tiene $p \geq (n-1)t$, pero es claro que $p = (n-1)t$ no puede ocurrir, entonces $p < (n-1)t$; es decir, $p \in I_{(n-1)t}$.

$\therefore\ x \leq I_{(n-1)t}$.

Por tanto, el caso $x = I_{(n-1)t}$ queda probado por el lema 2.

Por otro lado, si $x = 0$ entonces $x = I_0$, en cuyo caso el lema 2 prueba, nuevamente, la proposición.

Si $x > 0$ por el lema 1 $-x < 0$ y la demostración es análoga:

Sea $r \in 0$; o sea $r < o$ y sea el mínimo $0 \neq n \in N$ tal que $nr \in -x$, entonces $(n-1)r \in -x$.

Se afirma que $-(n-1)r \in x$ pues en caso contrario, y si se puede tomar $p < -(n-1)r$ tal que $p \notin x$ entonces $-p > (n-1)r$ y $-p$ evidencia que $(n-1)r \in -x$, lo cual no es posible.

entonces $r = -(n-1)r + nr \in x + (-x)$.

Si no se puede tomar $p \notin x$ con las propiedades mencionadas, otra vez ocurre que $x = I_{-(n-1)t}$, en cuyo caso el lema 2 se encarga de la veracidad de la proposición.

A fin de cuentas se ha probado que

$$0 \leq x + (-x).$$

Por lo tanto

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

∎

Es muy útil el concepto de *valor absoluto* de un número real para establecer el producto de números reales de una manera sencilla.

DEFINICION 8. Para $x\in\mathbb{R}$ el *valor absoluto* de x se denota como $|x|$ y se define como $|x|:=x\cup -x=\max\{x,-x\}$.

Obsérvese que gracias al hecho de que se dá $x\leq -x$ ó $-x\leq x$, la igualdad $x\cup -x=\max\{x,-x\}$ es obvia. Además, como $\max\{x,-x\}$ es igual a x o a -x también resulta claro que $|x|\in\mathbb{R}$.

DEFINICION 9. Si $x,y\in\mathbb{R}$ el *producto* entre ellos, denotado xy ó $x\cdot y$ se define como

$$x\cdot y=\begin{cases} 0\cup\{\, pq\in\mathbb{Q}\mid 0\leq p\in x\ \wedge\ 0\leq q\in y\,\} & \text{si } x\geq 0\ \wedge\ y\geq 0\\ |x|\cdot|y| & \text{si } x\leq 0\ \wedge\ y\leq 0\\ -(|x|\cdot|y|) & \text{si } x\leq 0,\ y>0\ \ \vee\ x>0,\ y\leq 0.\end{cases}$$

Igualmente solo se probarán las propiedades de mayor interés para el producto y, como se notará en su momento, las pruebas utilizan exactamente la mismas ideas que las que se manejaron para la suma, solo que, por ejemplo, en lugar de múltiplos naturales de números racionales se usarán potencias.

PROPOSICION 9. $\forall x,y\in\mathbb{R}(\ x\cdot y\in\mathbb{R}\ )$.

Prueba:

Obsérvese que basta hacer la prueba cuando $x,y\geq 0$ pues los otros casos se reducen a éste por medio del valor absoluto y el inverso aditivo que son "operaciones" sobre $\mathbb{R}$.

Sean pues $x,y\in\mathbb{R}$ tales que $x,y\geq 0$.

i) Que $xy\leq\mathbb{Q}$ & $xy\neq\emptyset$ es inmediato.
Por otro lado, sean $p_0\in\mathbb{Q}\backslash x$ & $q_0\in\mathbb{Q}\backslash y$ entonces
$\forall p\in x(\ p<p_0)$ & $\forall q\in y(\ q<q_0)$.
Sea cualquier $pq\in\{\, pq\mid 0\leq p\in x\ \wedge\ 0\leq q\in y\,\}$ entonces
$0\leq p<p_0$ & $0\leq q<q_0$, de aquí, $0\leq pq<p_0q_0$, entonces
$p_0q_0\notin 0$ & $p_0q_0\notin\{\, pq\mid 0\leq p\in x\ \wedge\ 0\leq q\in y\,\}$
$\therefore\ xy\neq\mathbb{Q}$.

ii) Sean $r,s\in\mathbb{Q}$ tales que $r<s\ \wedge\ s\in xy$ P.D. $r\in xy$.
Si $s\leq 0\Rightarrow r<0\Rightarrow r\in 0\Rightarrow r\in xy$.
Si $s>0\Rightarrow s=pq$ con $0<p\in x$ & $0<q\in y$
si $r\leq 0$ entonces $r\in xy$ trivialmente.
si $r>0$ entonces

$$r<pq\Rightarrow \frac{r}{p}<q\in y\Rightarrow \frac{r}{p}\in y\Rightarrow r=p\left(\frac{r}{p}\right)\Rightarrow r\in\{\, pq\mid 0\leq p\in x\ \wedge\ 0\leq q\in y\,\}$$

Por lo tanto, $r\in xy$.

iii) Sea el elemento $pq\in xy$, si $pq\in\mathbb{Q}$ entonces habrá un $r\in\mathbb{Q}$ tal que $pq<r$ & $r\in xy$; es decir, en este caso, xy no tiene máximo.
Si ahora $pq\in\{\, pq\mid 0\leq p\in x\ \wedge\ 0\leq q\in y\,\}$ entonces,
como x no tiene máximo $\exists p_0\in x$ tal que $p<p_0$ y
como y no tiene máximo $\exists q_0\in y$ tal que $q<q_0$, por lo tanto
$0\leq p<p_0$ y
$0\leq q<q_0$ entonces
$0\leq pq<p_0q_0$.
Por tanto, en cualquiera de los casos, xy no tiene máximo.

Los tres incisos anteriores prueban que $xy\in\mathbb{R}$. ∎

De igual forma damos por hecho que la multiplicación de números reales es asociativa y conmutativa para continuar con cosas como las que siguen.

DEFINICION 10. 1. El *neutro multiplicativo* se denota como 1 y se define por

$$1=\{\, p\in Q \mid p<1 \,\}.$$

2. Para $0\neq x\in R$ definimossu *inverso multiplicativo*, denotado como x^{-1}, a través de

$$x^{-1}=\{\, p\in Q \mid \exists s(\, s^{-1}>p \wedge s\in x \,)\,\} \quad \text{siempre que } x>0 \text{ y}$$

$$x^{-1}=-(|x|)^{-1} \quad \text{siempre que } x<0.$$

Como $1=1_1$ se obtiene que $1\in R$. Lo que puede no ser inmediato es que $x^{-1}\in R$.

PROPOSICION 10. $\forall x\in R(\, x\neq 0 \Rightarrow x^{-1}\in R \,)$

Prueba:

De acuerdo a la definición 1 deben probarse tres cosas; además, gracias a la proposición 6 y a la definción de x^{-1} para el caso en que $x<0$ basta hacer la prueba para $x>0$.

i) a) Es claro que $x^{-1}\subseteq 0$.

b) Veamos que $x^{-1}\neq\emptyset$.
Si $x>0$ sea $p<0$ tal que $p\in x$ entonces $p\in x^{-1}$ para probarlo basta con tomar cualquier $s\in x$ que sea $s>0$, lo cual siempre es posible; así que, efectivamente $x^{-1}\neq\emptyset$.

c) Sea $0<p\in x$, se afirma que $p^{-1}\notin x^{-1}$ pues si $p^{-1}\in x^{-1}$ entonces $\exists s(s^{-1}>p^{-1} \wedge s\in x)$, pero

$$s^{-1}>p^{-1} \wedge p>0 \quad \text{implica} \quad s^{-1}>p^{-1}>0$$

entonces $s>0$ y por tanto

$$s<p$$

de que $p\in x$ se sigue que $s\in x$, lo cual es absurdo. Así,

$$p^{-1}\notin x^{-1} \text{ ; es decir, } x^{-1}\neq 0.$$

ii) Sean $q,r\in Q$ tales que $q<r$ & $r\in x^{-1}$ entonces

$\exists s(\, s^{-1}>r \wedge s\in x \,)$, como $r>q$, por transitividad

$\exists s(\, s^{-1}>q \wedge s\in x \,)$, lo cual quiere decir que $q\in x^{-1}$.
Por lo tanto,

$$\forall q,r(\, q<r \wedge r\in x^{-1} \Rightarrow q\in x^{-1} \,).$$

iii) Sucede que x^{-1} no tiene máximo pues si $m\in x^{-1}$ fuera máximo entonces

$$\exists s(\, s^{-1}>m \wedge s\in x \,).$$

Pero entonces m^{-1}es máximo para x pues si no fuera así entonces

$$\exists s_0\in x \text{ tal que } m^{-1}<s_0$$

como $x>0$ entonces puede verse que $x^{-1}>0$, de lo cual, $m>0$ y consecuentemente $m^{-1}>0$, entonces

$s_0^{-1}<m$ y como $m<s^{-1}$, por tanto $s_0^{-1}<s^{-1}$ o bien
$s<s_0$, entonces
$s\in x$, lo cual no es posible.

Esta contradicción prueba que m^{-1}es máximo para x, pero como también esto es absurdo debe ocurrir que x^{-1}no tiene máximo.

Finalmente se puede concluir que

$$x^{-1} \in R.$$

Por problemas tipográficos en adelante se denotará, cuando sea conveniente, al inverso multiplicativo de un número racional p indistintamente con p' ó p^{-1} (de hecho, solo se usará esta notación cuando se utilize p^{-1} como subindice), manteniendo la notación que se ha venido empleando para el inverso multiplicativo de un número real.

LEMA 3. $\forall q \in Q (I_q^{-1} = I_{q'} \wedge I_q \cdot I_q^{-1} = 1^-)$.

Prueba:

Sea $p \in I_q^{-1}$, por definición $\exists s(s^{-1} > p \wedge s \notin I_q)$ entonces

$$s^{-1} > p \ \& \ s \geq q$$

si $q>0$, $s^{-1} \leq q^{-1}$ .....(*)

por transitividad $p<q^{-1}$,

lo cual signica que

$$p \in I_{q'};$$

por tanto,

$$I_q^{-1} \subseteq I_{q'}.$$

Sea ahora $p \in I_{q'}$ entonces $p<q$' P.D. $\exists s(s^{-1} > p \wedge s \notin I_q)$ i.e.

$$\exists s(s^{-1} > p \wedge s \geq q).$$

Sea $1/s=s'$ tal que $p<s^{-1}<q^{-1}$

si $q<0$ entonces $p, s^{-1}, q^{-1} < 0$ entonces

$$p<s^{-1} \ \& \ q<s$$

y así s evidencia que $p \in I_q^{-1}$.

si $q>0$ sea $s^{-1}>0$ tal que $p<s^{-1} \ \& \ s^{-1}<q^{-1}$ entonces

$$p<s^{-1} \ \& \ q<s,$$

luego $p \in I_{q'}$.

En cualquier caso, ($q<0$ ó $q>0$) resulta que

$$I_{q'} \subseteq I_q^{-1}.$$

Por otro lado, para ver que $I_q \cdot I_{q'} = 1$ se probarán también las dos contenciones.

Sea $t \in I_q \cdot I_{q'}$

si $t<0$ entonces, trivialmente, $t \in 1$.

si $t=rs$ con $0 \leq r \in I_q$ & $0 \leq s \in I_{q'}$ entonces

$$0 \leq r < q \ \& \ 0 \leq s < q^{-1}, \text{ de aquí}$$

$$t = rs < qq^{-1} = 1, \text{ entonces}$$

$$t \in 1.$$

Sea ahora $t \in 1$, i.e. $t<1$ y supóngase primero $0<q<1$. Si $t \leq 0$ el resultado buscado es trivial y si $t>0$ tomamos el mínimo $0 \neq n \in N$ tal que $t^n < q$, entonces $t^{(n-1)} \geq q$, entonces

$$t^{-(n-1)} \leq q^{-1} \quad \text{y} \quad q^{-1}$$

Si $t^{-(n-1)} < q^{-1}$ tómese $s \in Q$ tal que $t^{-(n-1)} < s^{-1} < q^{-1}$ entonces

$$t^{-(n-1)} < s^{-1} \wedge s > q$$

con lo anterior, s pone en evidencia que $t^{-(n-1)} \in I_q^{-1}$.

Por lo tanto,

$$t=t^{n}\cdot t^{-(n-1)}\in Iq\cdot I.q'$$

Si $t^{-(n-1)}=q^{-1}$ entonces $q=t^{n-1}$.

Sea $r\in Q$ tal que $t^{n}<r<t^{n-1}=q \Rightarrow t^{n}<r \Rightarrow t^{-n}>r^{-1} \Rightarrow t\cdot t^{-n}>t\cdot r^{-1} \Rightarrow t^{-(n-1)}>t\cdot r^{-1}$ y si fuera

$$t\cdot r^{-1}\geq q^{-1} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(**)$$

$\Rightarrow q^{-1}\leq t\cdot r^{-1}<t^{-(n-1)} \Rightarrow q^{-1}<t^{-(n-1)} \Rightarrow t^{n-1}<q=t^{n-1}$.

Como esta última desigualdad es una contradicción, no puede darse (**), i.e.

$t\cdot r^{-1}<q^{-1}$ entonces

$t\cdot r^{-1}\in Iq'$ por lo tanto

$$t=r\cdot(t\cdot r^{-1})\in Iq\cdot Iq'.$$

Es decir, en cualquier caso se ha probado que $1\leq Iq\cdot Iq'$. Con lo cual se puede concluir la igualdad

$$1=Iq\cdot Iq'.$$

Pero se está en el caso $q\geq 1$; ahora, si $q>1$ sucede que $q^{-1}<1$, entonces se repite la misma prueba intercambiando q por q^{-1} .

∎

Recuérdese que en la proposición anterior se trabajó siempre con $q>0$; de hecho, esto se empleó en la relación (*). Sin embargo, es suficiente considerar este caso pues si $q<0$ entonces $q^{-1}<0$ & $Iq\cdot Iq'=|Iq|\cdot|Iq'|$ y además $|Iq|=I|q|$, esto último se prueba en la siguiente observación.

Observación. $\forall q\in Q(\ |Iq|=I|q|\ )$. Donde $|q|$ también denota al valor absoluto de q.

Prueba:

Si $q\geq 0$ y

$p\in|Iq|=\max\{Iq, I-q\}=Iq=I|q|$ entonces $p\in I|q|$. Por otro lado, si

$p\in I|q|=Iq$, como $|Iq|=Iq$ se tiene $p\in|Iq|$.

La prueba para $q<0$ es análoga.

∎

LEMA 4. Para $x\in R$, si $x>1$ entonces $x^{-1}<1$.

Prueba:

Sea $p\in x^{-1}$, entonces $\exists s(\ s^{-1}>p \wedge s\in x\ )$. Como $1\leq x$ & $s\in x$ se tiene que $s>1$, entonces

$$p<s^{-1}<1, \quad \text{luego} \quad p<1 \quad \text{y así} \quad p\in 1.$$

Por lo tanto

$$x^{-1}\subseteq 1.$$

Habrá que hacer ver que $x^{-1}\neq 1$.

Como $1\neq x$ $\exists p_0\in x\setminus 1$, luego se puede tomar $p\in x$ tal que $p>1$, entonces $p^{-1}\in 1$ y además $p^{-1}\notin x^{-1}$ porque si $s\in Q$ es cualquiera tal que $s^{-1}>p^{-1}$ entonces $s<p$ y como $p\in x$ también resulta $s\in x$. Es decir, se ha probado

$$\forall s(\ s^{-1}>p^{-1} \Rightarrow s\in x\ ) \quad \text{i.e.}\ p^{-1}\notin x^{-1}.$$

∎

PROPOSICION 11. $\forall x\in\mathbb{R}(\ x\cdot x^{-1}=1\ )$

Prueba:

Sea $r\in x\cdot x^{-1}$, si $r\leq 0$ trivialmente $t\in 1$ y

si $r=pq$ con $p,q>0$ & $p\in x \wedge q\in x^{-1}$ entonces

$\exists s(\ s^{-1}>q \wedge s\in x\ )$,

pero $s\in x$ implica $s\geq p$ entonces

$$s^{-1}\leq p^{-1} \Rightarrow q<s^{-1}<p^{-1} \Rightarrow q<p^{-1} \quad \text{entonces}$$

$$r=pq<1.$$

Lo cual significa que

$$r\in 1.$$

Por tanto $x\cdot x^{-1}\subseteq 1$.

Para la segunda contención supóngase primero

— $x<1$

Sea $t\in 1$ entonces $t<1$ y existe el mínimo $0\neq n\in\mathbb{N}$ tal que

$$t^n\in x$$

entonces $t^{n-1}\notin x$.

Si se existe $p\in 0$ tal que $p<t^{n-1}$ y $p\in x$ entonces

$$t^{-(n-1)}<p^{-1}$$

entonces p evidencia que $t^{-(n-1)}\in x^{-1}$.

por tanto

$$t=t^n\cdot t^{-(n-1)}\in x\cdot x^{-1}\ .$$

Obsérvese que

si $\forall p<t^{n-1}(\ p\in x\ )$ entonces $x=I(t^{n-1})$

en cuyo caso el lema 3 prueba la proposición.

— Si ahora es $x>1$, por el lema 4 $x^{-1}<1$ entonces $\exists 0\neq n\in\mathbb{N}(\ t^n\in x^{-1})$

entonces $t^{n-1}\notin x^{-1}$ y se afirma que $t^{-(n-1)}\in x$ porque si no fuera

así tomo $p\in t^{-(n-1)}$ tal que $p\notin x$ entonces $t^{(n-1)}<p^{-1}$ y p evidencia que $t^{n-1}\in x^{-1}$, lo cual es absurdo. Por lo tanto

$$t=t^{-(n-1)}\cdot t^n\in x\cdot x^{-1}.$$

Nuevamente, si no se puede tomar tal $p<t^{-(n-1)}$ tal que $p\notin x$ entonces $x=I(t^{-(n-1)})$ y el lema 3 prueba la proposición.

Por lo tanto ha quedado probado que

$$1\subseteq x\cdot x^{-1}.$$

∎

Para terminar este capítulo se menciona que en este momento se han derivado los enunciados sobre los números reales que en un curso de Cálculo o de Análisis se llaman los axiomas de campo y los axiomas de orden para los Números Reales y se sabe que con ellos se logra alcanzar todas sus propiedades y, sobre todo, aquellos conceptos e ideas útiles en estas áreas; por ejemplo, los conceptos de *límite*, *continuidad*, etc. Así pues, se ha cumplido con el objetivo principal de este capítulo.

Es relativamente sencillo observar a las estructuras matemáticas que se revisarán aquí (grupos, campos, espacios vectoriales, topologías) desde el punto de vista de la Teoría de Conjuntos: directamente se toma un conjunto y se definen operaciones (funciones) entre sus elementos que proporcionan la estructura deseada. Así pues, este capítulo será, básicamente, una revisión de estas estructuras haciendo énfasis en las características conjuntistas de todos los objetos involucrados así como algunas variantes en la escritura de los axiomas presentando puntos interesantes.

6.1 GRUPOS, CAMPOS Y ESPACIOS VECTORIALES

Probablemente el concepto de grupo sea la estructura abstracta más elemental, pues muchas otras estructuras se definen a partir de él.

DEFINICION 1a. Si G es un conjunto, $e\in G$ y $*:G\times G\longrightarrow G$ entonces el conjunto $\langle G,e,*\rangle$ es un *grupo* respecto a $*$ si se cumplen

G1) $\forall x,y,z\in G(\ *(x,*(y,z))=*(*(x,y),z)\ )$
$x*(y*z)=(x*y)*z$

G2) $\forall x\in G(\ *(x,e)=*(e,x)=x\ )$
$x*e=e*x=x$

G3) $\forall x\in G\ \exists x'\in G(\ *(x,x')=*(x',x)=e\ )$
$x*x'=x'*x=e$

El axioma G3 establece que todo elemento x de G tiene un *inverso* respecto a la *operación* $*$, esto se puede decir a través del empleo de una función.

DEFINICION 1b. El conjunto $\langle G,e,*,i\rangle$ es un *grupo* si G es un conjunto, $e\in G$, $*:G\times G\longrightarrow G$, $i:G\longrightarrow G$ y se satisfacen las condiciones de la definición 1a donde G3 se cambia por

G3b) $\forall x\in G(\ *(x,i(x))=*(i(x),x)=e\ )$
$x*i(x)=i(x)*x=e$.

Los dos juegos de axiomas dicen exactamente lo mismo, sin embargo, presentan una diferencia importante.

G1, G2 y G3 implican que el inverso de cada $x\in G$ es único; es decir, $\forall x\in G(\ \exists x'\in G(\ x*x'=x'*x=e\ )\wedge\forall y,z\in G(\ x*y=y*x=e=x*z=z*x\Rightarrow y=z\ )\ )$ la veracidad de esto se deduce fácilmente:

si	$x*y=y*x=e\ \wedge\ x*z=z*x=e$
entonces	$y=x*e=y*(x*z)=(y*x)*z=e*z=z$.

Por otro lado, el hecho de que la definición 1b proporcione al inverso através de una función automáticamente lo hace único.

Otra estructura importante que se incluye es la de *campo*, es interesante por sí misma y se toma como base para desarrollar, entre otras cosas, los espacios vectoriales.

DEFINICION 2. Un conjunto $\langle K,+,\cdot,e_1,e_2\rangle$ es un *campo* si K es un conjunto tal que $e_1.e_2\in K$, $+:K\times K\longrightarrow K$, $\cdot:K\times K\longrightarrow K$, donde $\langle K,+,e_1\rangle$ es un grupo y se cumple

K1) $\forall x,y\in K(\ +(x,y)=+(y,x)\ )$
$x+y=y+x$

K2) $\forall x,y,z\in K(\ \cdot(x,\cdot(y,z))=\cdot(\cdot(x,y),z)$
$x\cdot(y\cdot z)=(x\cdot y)\cdot z$

K3) $\forall x,y\in K(\ \cdot(x,y)=\cdot(y,x)\ )$
$x\cdot y=y\cdot x$

K4) $\forall x\in K(\ \cdot(x,e_2)=\cdot(e_2,x)=x\ )$
$x\cdot e_2=e_2\cdot x=x$

K5) $\forall x\in K(\ x\neq e_1\Rightarrow \exists x'\in K(\ \cdot(x,x')=\cdot(x',x)=e_2\ ))$
$x\cdot x'=x'\cdot x=e_2$

K6) $\forall x,y,z(\ \cdot(x,+(y,z))=+(\cdot(x,y),\cdot(x,z))\ )$
$x\cdot(y+z)=x\cdot y+x\cdot z$

Igualmente pudimos definir un campo como el conjunto
$\langle K,+,\cdot,e_1,e_2,i_1,i_2\rangle$
donde i_1 e_i2 son funciones que calculan el inverso respecto a la operación + ($i_1:K\times K\longrightarrow K$) y respecto a $\cdot$ ($i_2:K\setminus\{e_1\}\times K\setminus\{e_1\}\longrightarrow K$), respectivamente. Por ejemplo (K5) cambiaría por

K5') $\forall x\in K(\ x\neq e_1\Rightarrow \cdot(x,i_2(x))=\cdot(i_2(x),x)=e_2\ )$
$x\cdot i_2(x)=i_2(x)\cdot x=e_2$

Ahora presentamos la definición típica de un espacio vectorial.

DEFINICION 3a. Si $\langle K,+,\cdot,e_1,e_2\rangle$ es un campo y $\langle V,\oplus,e\rangle$ es un grupo, se dice que $\langle V,K,\oplus,\cdot\rangle$ es un *K-espacio vectorial* si $\cdot:K\times V\longrightarrow V$ y se cumplen

V1) $\forall a,b\in V(\ \oplus(a,b)=\oplus(b,a)\ )$

V2) $\forall x\in K\ \forall a,b\in V(\ \cdot(x,\oplus(a,b))=\oplus(\cdot(x,a),\cdot(x,b))\ )$
$x\cdot(a\oplus b)=(x\cdot a)\oplus(x\cdot b)$

V3) $\forall x,y\in K\ \forall a\in V(\ \cdot(\oplus(x,y),a)=\oplus(\cdot(x,a),\cdot(y,a))\ )$
$(x\oplus y)\cdot a=(x\cdot a)\oplus(y\cdot a)$

V4) $\forall x,y\in K\ \forall a\in V(\ \cdot(\cdot(x,y),a)=\cdot(x,\cdot(y,a))\ )$
$(x\cdot y)\cdot a=x\cdot(y\cdot a)$

V5) $\forall a\in V(\ \cdot(e_2,a)=a\ )$
$e_2\cdot a=a$

En los espacios vectoriales hay dos tipos de objetos involucrados, los elementos de V, llamados *vectores*, y los elementos de K, llamados *escalares*; aquí hay una alternativa de definición, que un espacio vectorial sea un conjunto, dentro del cual habrá que distinguir los que serán vectores de los que serán escalares. Para esto necesitamos una lógica 2-variada o bien, una univariada con dos predicados, a saber, $v(x)$ entendido como x *es vector* y $e(x)$ entendido como x *es escalar*.

DEFINICION 3b. Si V es un conjunto decimos que $\langle V, \oplus, \odot, +, \cdot, e_1, e_2 \rangle$ es un *espacio vectorial* si $e_1, e_2 \in V$, $v(e_1), e(e_2)$ y también ocurre que $K=\{ x \in V \mid e(x) \}$ es tal que $\langle K, +, \cdot, e_2 \rangle$ es un campo, $G=\{ x \in V \mid v(x) \}$ es tal que $\langle G, \oplus, e_1 \rangle$ es un grupo y además se cumplen las siguientes propiedades:

V1') $\forall x, y \in V(v(x) \wedge v(y) \Rightarrow x \oplus y = y \oplus (x))$

V2') $\forall x, y, z \in V(e(x) \wedge v(y) \wedge v(z) \Rightarrow x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z))$

V3') $\forall x, y, z \in V(e(x) \wedge e(y) \wedge v(z) \Rightarrow (x \oplus y) \odot z = (x \odot z) \oplus (y \odot z))$

V4') $\forall x, y, z \in V(e(x) \wedge e(y) \wedge v(z) \Rightarrow (x \cdot y) \odot z = x \odot (y \odot z))$

V5') $\forall x \in V(v(x) \Rightarrow e_2 \odot x = x \odot e_2 = x)$.

La definición 3b es sumamente incómoda porque en cada uno de los enunciados que se presenten en el álgebra lineal habrá que especificar cuándo se habla de vectores y cuándo de escalares; sin embargo, desde el punto de vista de la Lógica es correcta.

6.2 ESPACIOS TOPOLOGICOS

DEFINICION 4. Si X es un conjunto y $T \subseteq P(X)$ entonces $\langle X, T \rangle$ es un *espacio topológico* cuando $\varnothing \in T$, $X \in T$ y

T1) $\forall T \subseteq T(\bigcup T \in T)$

T2) $\forall T \subseteq T(\exists n \in N(T \approx \{1, 2, \ldots, n\}) \Rightarrow \bigcap T \in T)$

El signo $\approx$ en (T2) es el de equipotencia, quiere decir que hay una función biyectiva de T sobre el conjunto $\{1, 2, \ldots, n\}$. Si se emplea la definición para N ($=\omega$) dada en el capítulo 2 puede escribirse (T2) de forma más compacta:

T2) $\forall T \subseteq T(\exists n \in N(T \approx n) \Rightarrow \bigcap T \in T)$

En cuanto a terminología, al conjunto T se le llama *topología* del espacio T y los elementos de T son los *T-abiertos* o simplemente *abiertos* cuando no hay posibilidad de confusión.

Alrededor del concepto de espacio topológico se presentan (igual que en otras áreas) ideas como la de *productos cartesianos generalizados*, que no son otra cosa que productos cartesianos de una cantidad infinita de conjuntos; no hay problema en convencerse de que el producto cartesiano generalizado de una familia de conjuntos es, en sí mismo, un conjunto, sino que el problema radica en derivar la no vacuidad del mismo a partir de la no vacuidad de los conjuntos que lo forman. De hecho, se sabe que este enunciado es equivalente al axioma de elección, mismo que no se ha tratado en este trabajo, por lo tanto, si se desea garantizar que los productos cartesianos generalizados son no vacíos habrá que incluir al axioma de elección agregándolo a los axiomas de Zermelo-Fraenkel.

En cualquier caso, se observan claramente las características conjuntistas de los espacios topológicos, los elementos del objeto T (llamado *topología* del *espacio* X) son algunos elementos de $P(X)$ y es, por tanto, un conjunto; igualmente, todo $T \subseteq T$ es un conjunto y así, $\bigcup T$ y $\bigcap T$ son conjuntos.

Para resaltar una relación interesante entre los espacios topológicos y la caracterización de $\mathbb{R}$ como un orden continuo se

definirá un *continuo topológico* y dos topologías para $\mathbb{R}$ que lo hacen continuo topológicamente.

La Topología del Orden (T1).
Aquí, los T1-abiertos son los conjuntos $a_r=\{ x\in\mathbb{R} \mid x<r \}$; es decir,
$$T1=\{ a_r \mid r\in\mathbb{R} \}.$$

La Topología Usual (T2).
Los T2-abiertos de esta topología son los conjuntos formados por uniones arbitrarias de intervalos abiertos; donde, conjuntistamente, un *intervalo* I es un subconjunto de $\mathbb{R}$ tal que
$$\forall x,y\in I \forall z\in\mathbb{R}(x<z<y \Rightarrow z\in I)$$
el intervalo será *abierto* si no tiene extremos inicial ni final.
Es claro que hay mas subconjuntos de $\mathbb{R}$ que intervalos abiertos, esto permite tomar un subconjunto I de $P(\mathbb{R})$ como conjunto de subindices para definir la topología T2 como
$$T2=\{ a\subseteq\mathbb{R} \mid a=\bigcup\{ I_i \mid i\in I\subseteq P(\mathbb{R})\} \}.$$
No es difícil verificar que T1 y T2 son, en efecto, topologías para $\mathbb{R}$.
Por otro lado, si $\langle X,T\rangle$ es un espacio topológico y $\langle X,\langle\rangle\in COTO$ se dice que X es un *T-continuo* si X es <-denso, no tiene <-extremos y es *T-separable*, esto último significa que X tiene un subconjunto numerable Q que es *T-denso en* X, lo cual a su vez significa que
$$\forall a\in T(a\cap Q\neq\emptyset).$$
Es sabido que en las topologías del orden T1 y usual T2 para $\mathbb{R}$, el conjunto $\mathbb{Q}$ de números racionales resulta ser T1 y T2-denso en $\mathbb{R}$; de hecho la T1-densidad se sigue de la T2-densidad puesto que $T1\subseteq T2$. Con esto resulta ser que $\mathbb{R}$ es <-continuo y T1,T2-continuo.

La última sección de este capítulo tiene por objeto mostrar algunas limitaciones de la Teoría de Conjuntos en el sentido de la consecusión de algunas estructuras matemáticas, através de su insuficiencia en la fundamentación de una estructura no muy familiar pero de uso cada vez más extendido.

6.3 CATEGORIAS

En esta sección se describen algunas dificultades lógico-conjuntistas que presenta la Teoría de Categorías, las cuales hacen ver la necesidad de una fundamentación para esta teoría basada en conceptos de mayor alcance que los que permite, formalmente, la Teoría de Conjuntos de Zermelo-Fraenkel.

Entre los objetivos mas importantes de la Teoría de Categorías se cuenta el de describir y analizar las propiedades de una totalidad de objetos matemáticos. Así se tienen, la Categoría de Conjuntos, la Categoría de Grupos, etc. Uno de los primeros problemas que, desde el punto de vista de la Teoría de Conjuntos, debe enfrentarse es el de esa "totalidad". Para empezar a resaltar este y otros problemas primero se presenta la definición mas popular de categoría, enseguida se discute esa definición desde el punto de vista conjuntista y después se exhiben dificultades mas serias que parece no pueden salvarse fácilmente.

DEFINICION 5. Una *Categoría* K consiste en

i) una clase K° de elementos llamados *objetos*.

ii) Para cada $a,b \in K^{\circ}$ se tiene un conjunto denotado hom(a,b) de elementos llamados *morfismos* de a en b. Cuando $f \in hom(a,b)$ se escribe $f: a \longrightarrow b$ en su lugar.

iii) Una operación llamada *composición* que, para objetos arbitrarios $a,b,c \in K^{\circ}$, asigna a morfismos arbitrarios $f: a \longrightarrow b$, $g: b \longrightarrow c$ un morfismo $g \circ f: a \longrightarrow c$ que cumple

- Axioma de Asociatividad
  $\forall f: a \longrightarrow b \; \forall g: b \longrightarrow c, \; \forall h: c \longrightarrow d \;\; (\; h \circ (g \circ f) = (h \circ g) \circ f \;)$
- Axioma de Morfismo Identidad
  $\forall a \in K^{\circ} \; \exists 1_a: a \longrightarrow a$ tal que
  $1_a \circ f = f \quad \forall f: b \longrightarrow a$
  $f \circ 1_a = f \quad \forall f: a \longrightarrow b.$

Hay varias observaciones que pueden hacerse sobre esta definición. Primero, la clase K° es una clase completamente arbitraria; es decir, sus objetos son elementos de cualquier tipo en contraposición con las clases descritas en la primera sección del capítulo 2 donde se describe una clase como una colección de conjuntos que tienen una propiedad determinada φ. En general, los objetos de una categoría no tienen porque ser conjuntos.

Ahora, por la forma en que está denotado, el conjunto hom(a,b) puede darse a través de una funcional, si V denota la clase de conjuntos,

$$hom: K^{\circ} \times K^{\circ} \longrightarrow V$$
$$(a,b) \longmapsto hom(a,b)$$

que significa que hom asocia a cada $(a,b) \in K^{\circ} \times K^{\circ}$ un conjunto hom(a,b) que satisface las condiciones del inciso iii) de la definición anterior. Obsérvese que las expresiones $K^{\circ} \times K^{\circ}$ y $(a,b) \in K^{\circ} \times K^{\circ}$ tienen sentido, al menos en este contexto, cuando K° es una clase de conjuntos. Otra observación importante es que aun si K° es un conjunto, hom(a,b) no deja de estar dada por una funcional que no está especificada explícitamente sino que es alguna funcional tal que su imagen sobre una par $(a,b) \in K^{\circ} \times K^{\circ}$ satisface (iii) de la definición 5. Recuérdese que una funcional es una subclase, en este caso, de $(K^{\circ} \times K^{\circ}) \times V$, por lo tanto, es escencialmente una fórmula conjuntista; así que, buscar una funcional con ciertas propiedades implica cuantificar sobre fórmulas, lo cual no es permitido en el lenguaje 3 de la Teoría de Conjuntos.

Una vez que hom(a,b) es un conjunto dado de alguna forma, la composición de morfismos tiene perfecto sentido, por ejemplo, si $a,b,c \in K^{\circ}$:

$$\circ: hom(a,b) \times hom(b,c) \longrightarrow hom(a,c) \qquad (*)$$
$$(f,g) \longmapsto g \circ f$$

Es decir, $\circ$ es una función del conjunto hom(a,b) x hom(b,c) en el conjunto hom(a,c) que asigna a cada par $(f,g) \in hom(a,b) \times hom(b,c)$ un elemento $g \circ f \in hom(a,c)$ con las propiedades especificadas en el inciso (iii) de la definición 5. Pero, ¿qué es la operación composición?, la discusión anterior dice qué es, conjuntistamente, la composición de dos morfismos para $a,b,c \in K^{\circ}$ fijos; sin embargo, la operación composición asigna a cada tres elementos $a,b,c \in K^{\circ}$ y a cada $f \in hom(a,b)$, $g \in hom(b,c)$

un elemento $g \circ f \in hom(a,c)$. Un primer intento para resolver este problema es observar que, dados $a,b,c \in K^{\circ}$, la función descrita en (*) cumple, por definición:

$$\circ \subseteq (hom(a,b) \times hom(b,c)) \times hom(a,c).$$

De aquí, $\circ \in P((hom(a,b) \times hom(b,c)) \times hom(a,c))$; así pues, la operación composición sería alguna funcional (y, por tanto, alguna fórmula) :

$$comp: K^{\circ} \times K^{\circ} \times K^{\circ} \longrightarrow \cup \{ P((hom(a,b) \times hom(b,c)) \times hom(a,c)) \mid (a,b,c) \in K^{\circ} \times K^{\circ} \times K^{\circ} \}$$

$$comp(a,b,c) = \left\{ \begin{array}{c} \circ : hom(a,b) \times hom(b,c) \longrightarrow hom(a,c) \\ (f,g) \longmapsto g \circ f \end{array} \right.$$

Igualmente, esta funcional está sujeta a las misma observaciones de carácter lógico que las que se hicieron sobre la funcional hom. Nótese que ambas funcionales se dan con objeto de establecer en forma conjuntista los enunciados de la definición de categoría: *para cada* $a,b,c \in K^{\circ}$ *y* $f \in hom(a,b)$ ..... De tal forma que las propiedades que deben cumplir cada uno de estos objetos están dadas sobre las imágenes, para $a,b,c \in K^{\circ}$ fijos, de las funcionales hom y comp.

Tratando de reunir todas las observaciones anteriores, se puede redefinir una Categoría K como una terna $\langle K^{\circ}, hom, comp \rangle$ donde K° es una clase arbitraria y hom y comp son cualesquiera dos funcionales descritas como antes y tales que sus imágenes sobre objetos $a,b,c \in K^{\circ}$ fijos satisfacen (iii) de la definición 5. Se insiste en que mucho de lo anterior no tiene sentido en la noción general de clase; es decir, en clases cuyos miembros no sean conjuntos.

Probablemente algunos de los problemas explicados anteriormente tengan una mejor solución empleando una teoría que, junto con los conjuntos, permita manipular formalmente a las clases, pero la respuesta a esta conjetura ya no es un objetivo de este trabajo.

Por otro lado, se dará enseguida un ejemplo de una categoría que ejemplifica algunos de los escollos de los que apenas se habló; este ejemplo, junto con las observaciones hechas pretende hacer ver que la Teoría de Categorías no puede estudiarse formalmente con la Teoría de Conjuntos, al menos no con la de Zermelo-Fraenkel. El ejemplo es, precisamente, la Categoría de Conjuntos, aquí la clase de objetos es la clase de todos los conjuntos y para cada par de conjuntos $a,b \in V$ el conjunto $hom(a,b)$ es el conjunto de todas las funciones de a en b; es decir,

$$hom(a,b) = \{ f \mid f : a \longrightarrow b \}$$

y para cada $a,b,c \in V$ y $f : a \longrightarrow b$, $g : b \longrightarrow c$ la composición $g \circ f$ es la composición usual:

$$g \circ f : a \longrightarrow c$$
$$g \circ f(x) = g(f(x))$$

es de todods conocido que esta operación satisface el axioma de asociatividad

$$h \circ (g \circ f) = (h \circ g) \circ f$$

y que para cada $a \in V$ la función 1_a definida como

$$1_a : a \longrightarrow a$$
$$1_a(x) = x$$

cumple con el axioma de morfismo identidad.

Con esta categoría se muestra el hecho de que su clase de objetos no es un conjunto aunque sus objetos mismos sí lo son. Es

decir, la clase de conjuntos no es un conjunto, o bien, no hay un conjunto cuyos elementos sean todos los conjuntos, o dicho de otra forma, para cada conjunto existe otro que no le pertenece:

PROPOSICION. $\forall a \exists b(b \notin a)$

Prueba:

Sea a un conjunto y pongamos

$$b=\{ x \in a \mid x \notin x \} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (*)$$

Obsérvese que, gracias al Axioma de Comprensión, b es, efectivamente, un conjunto: un subconjunto de a.

Se afirma que $b \notin a$ pues de no ser así; es decir, si

$$b \in a \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (**)$$

entonces se presenta alguna de las dos siguientes posibilidades:

i) $b \in b$,

tiene sentido esta posibilidad porque (**) es el primer requisito para que se dé; pero en tal caso debe cumplir la segunda de las condiciones que definen a b, que es

$$b \notin b$$

Es decir,

$$b \in b \Rightarrow b \notin b .$$

ii) $b \notin b$,

En este caso, debido a (**), puede decirse que b es un elemento de a que, por no pertenecer al conjunto b, cumple la condición que lo define; o sea

$$b \in b.$$

Es decir,

$$b \notin b \Rightarrow b \in b.$$

Los resultados de cada uno de los dos casos anteriores hacen una contradicción, con lo cual se concluye que

$$b \notin a.$$

∎

Este es un ejemplo, entre muchos otros, de una categoría que "no cabe" en la Teoría de Conjuntos.

Hay un concepto muy ligado al de categoría que parece tener problemas tan importantes como los que ya se han descrito. Se lo presenta a continuación en su forma usual.

DEFINICION 6. Un *funtor* $F: K \longrightarrow L$ de una categoría K en una categoría L es una aplicación tal que

i) $F: K^{0} \longrightarrow L^{0}$; i.e, F asigna a cada objeto $a \in K^{0}$ un elemento $F(a) \in L^{0}$.

ii) Dados $a, b \in K^{0}$ y $f \in hom(a,b)$, F asigna un morfismo $F(f) \in hom(F(a),F(b))$ de tal forma que si $c \in K^{0}$ y $g \in hom(b,c)$ se tiene

1) $F(g \circ f)=F(g) \circ F(f) : F(a) \longrightarrow F(c)$

2) $F(1_a)=1_{F(a)}$.

Un funtor es como una doble función, ó mas precisamente, una doble funcional pues actúa sobre los objetos y sobre los morfismos de la categoría K. Esto sugiere que, conjuntistamente, un funtor F sea un par

$$F=<F_o, F_m>$$

notación que sugiere que F_o es la parte que actúa sobre los objetos:

$$F_o: K^o \longrightarrow L^o$$
$$a \longmapsto F_o(a)$$

y F_M actúa sobre los morfismos:

$$F_m: K^m \longrightarrow L^m$$
$$f \epsilon hom(a,b) \longmapsto F(f) \epsilon hom(F(a),F(b))$$

donde

$$K^m = \cup\{\ hom(a,b) \mid\ (a,b) \epsilon K^o \times K^o\ \}$$
$$L^m = \cup\{\ hom(a,b) \mid\ (a,b) \epsilon L^o \times L^o\ \}$$

y además F_o es una funcional arbitraria y F_m cumple (1) y (2) de la definición anterior.

Nuevamente, lo anterior tiene sentido al menos si K^o y L^o son conjuntos pues en tal caso, F^o es una función y F^m también lo es pues K^m es un conjunto por ser la imagen de la funcional hom del conjunto $K^o \times K^o$ (véase el axioma ZF8 en la página 9). Así, el funtor F es el conjunto $F=\langle F_o, F_m \rangle$ quedando aún el problema de que los hom(a,b) siguen estando dados por una funcional.

Con todo lo anterior queda en evidencia la necesidad de una Teoría de Clases con urielementos para la fundamentación formal de la Teoría de Categorías.

En esta sección se presenta una lista de algunos textos que pueden consultarse si se desea profundizar en los temas a que se hace referencia en la cita de cada uno de ellos.

El articulo *The Iterative Conception of Set*, escrito por Goerge Boolos, que es la base del capitulo 1 sobre la Teoria de Estratos puede encontrarse en el siguiente libro, el cual es una colección de articulos sobre diversos temas de la Filosofia de las Matemáticas. También puede hallarse otro articulo, este de Hao Wang llamado *The Concept of Set*, que expone un punto de vista muy intuitivo de la llamada Jerarquia Acumulativa aunque no la llama con este nombre.

- Benacerraf F, Paul. (Ed).
  Philosophy of Matehematics: Selected Readings.
  Cambridge; Cambridge University, 1983.

Un texto que muestra los temas tipicos de la Teoria de Conjuntos desde un punto de vista axiomático, que es de fácil y amena lectura:

- Hamilton A.G.
  Numbers, Sets and Axioms: The Aparatus of Mathematics.
  Cambridge, Cambridge University, 1982.

Dos textos de uso corriente en los cursos de Teoria de Conjuntos , cuya existencia no debe ignorarse. Fueron material de amplia referencia en los capitulos 2, 3 y 4.

- Hrbaceck, Karel; and Jech, Tomas.
  Introduction to Set Theory.
  M.Dekker, 1978.

- Enderton, Herbert B.
  Elements of Set Theory.
  Academic Press, 1977.

Para una discusión interesante de los axiomas de Regularidad y de Elección y, en general, de los axiomas de Zermelo-Fraenkel puede consultarse:

- Fraenkel, Abraham A.; Bar-Hillel, Yehoshua; Levy, Azriel.
  Foundations of Set Theory.
  North Holland Publishing Co., 1973.

Una descripción completa de los conjuntos no bien fundados puede encontarse en:

- Aczel, Peter.
  Non-Well-Founded Sets.
  C.S.L.I.(Center for The Study of Language and Information), 1988.

Un tratamiento diferente de los axiomas de la Teoría de Conjuntos que combina muy bien la lógica se encuentra en:

- Morse, A.P.
  A Theory of Sets.
  Second Edition.
  Academic Press, Inc. 1986.

Un tratamiento sencillo pero preciso sobre los números racionales definidos como fracciones y de los números reales definidos como sucesiones de Cauchy:

- Suppes Patrick.
  Axiomatic Set Theory.
  Dover Publications, Inc. 1972.

Un texto que desarrolla un tipo especial de espacios topológicos junto con la Teoría de Conjuntos y la discusión concerniente del axioma de Elección entre otros:

- Kaplansky, Irving.
  Set Theory and Metric Spaces.
  Chelsea Publishing Co. 1977.

Una exposición histórica, típica e intuitiva que desarrolla los sistemas numéricos y los objetos relacionados con ellos. Utiliza conceptos y terminología que prácticamente ya no se emplean. Al autor se debe el método de construcción de los números reales através de cortaduras.

- Dedekind, Richard.
  Essays on the Theory of Numbers.
  Dover Publications Inc.

El siguiente combina de una manera muy agradable la Teoría de Conjuntos, los órdenes y la Topología.

- Kuratowsky, Kazimierz.
  Introduction to Set Theory and Topology.
  Addison-Wesley Publishing Co. Inc. 1962.

Una exposición de los números reales y complejos como conjuntos partiendo, desde luego, de la Teoría de Conjuntos. Presenta a los

números reales como cortaduras de Dedekind.

- Zuckerman, Martin M.
  Sets and Transfinite Numbers.
  Macmillan Publishing Co. Inc.

Un típico texto de consulta que incuye una gran variedad de ejercicios útiles para familiarizarse con las propiedades de los conjuntos y de los sistemas numèricos. Además presenta un enfoque bastante estandarizado.

- Potter, Michael D.
  Sets. An Introduction.
  Oxford Science Publications, 1990.

Un estudio clásico e intuitivo de la Teoría de Categorías se encuentra en:

- Mac Lane, Saunders.
  Categories for the Working Mathematician.
  Springer-Verlag.

En el siguiente texto se discuten formalmente los conceptos de categoría y funtor presentando bonitos e interesantes ejemplos.

- Adámek, Jirí.
  Theory of Mathematical Structures.
  D. Reidel Publishing Co.

Exposición típica de la Teoría de categorías con una gran variedad de aplicaciones.

- Mitchell, Barry.
  Theory of Categories.
  Academic Press.