T E O R I A S   C A T E G O R I C A S

JOAN BAGARIA PIGRAU

Tesis de Licenciatura en Filosofía

Director : Dr. D. JESUS MOSTERIN

V° B°
Jesús Mosterín

UNIVERSIDAD DE BARCELONA

FACULTAD DE FILOSOFIA Y CIENCIAS DE LA EDUCACION

SECCION DE FILOSOFIA

Febrero, 1984

INDICE

INTRODUCCION

Uno de los problemas fundamentales que se ha planteado la filosofía de la matemática ya desde Platon y Aristoteles es el de la determinación del tipo de existencia que poseen los objetos matemáticos tales como los números o las figuras geométricas.

El tema ha sido tratado de muy diferentes maneras a lo largo de la historia de la filosofía y ha recibido también, cómo no, soluciones muy diversas.

En la actualidad, mediante el potente instrumento que constituye la lógica matemática moderna, es posible abordar esta cuestión de un modo mucho más preciso. Efectivamente, la mayor parte de las teorías matemáticas pueden ser formalizadas y axiomatizadas en los lenguajes lógicos de primer o segundo orden. Así, la teoría de grupos, la aritmética, la geometría euclídea,etc. Esto nos permite considerar dichas teorías como un conjunto de sentencias en uno de estos lenguajes.

Estas teorías formalizadas se interpretan sobre las estructuras, entendiendo por estructura una entidad conjuntista constituída por un conjunto de elementos o universo de la estructura y por un conjunto de relaciones y funciones definidas entre ellos. Las variables que aparecen en las sentencias de la teoría se refieren a elementos del universo de la estructura, mientras que los relatores y functores de la teoría hacen referencia a las relaciones y funciones de aquella.

No todas la teorías, sin embargo, pueden ser consideradas del mismo modo. En efecto, algunas de ellas determinan unívocamente una estructura; lo que significa que todo lo que es preciso decir de esa estructura para distinguirla de todas las demás, lo dice dicha teoría. Otras, por el contrario, no caracterizan unívocamente ninguna estructura; con lo cual, existen estructuras distintas descritas por la misma teoría y que no obstante son indistinguibles para ella.

Al primer tipo de teorías, eso es, a las teorías que determinan unívocamente una estructura, las llamamos teorías categóricas. Así, por ejemplo, la teoría de los números naturales de segundo orden, la de los números reales de segundo orden y la geometría euclídea de segundo orden. Por tanto, las estructuras correspondientes, unívocamente caracterizadas por dichas teorías, a saber : los números naturales, los números reales y el espacio euclídeo, pueden ser consideradas como entidades concretas, perfectamente determinadas, como si poseyeran existencia propia.

El presente trabajo constituye un análisis del concepto de categoricidad así como una exposición de algunas de las teorías matemáticas más relevantes para las que probamos que son categóricas. Esto se realiza en tres secciones :

En la primera, previa exposición de la sintaxis de un lenguaje lógico de primer orden, se introducen los conceptos básicos de "estructura","modelo" y "teoría". A continuación se define la "completud" de teorías y la "equivalencia elemental" entre estructuras y se prueba que una teoría es completa si y sólo si todos sus modelos son elementalmente equivalentes. Finalmente se define el concepto de "categoricidad" y se analiza su relación con la completud.

La sección segunda podemos considerarla dividida en tres apartados: en el primero se muestran varios ejemplos de teorías categóricas de primer orden. Estas teorías son poco interesantes dado que sus modelos deben ser necesariamente finitos (ello es una consecuencia del teorema de Löwenheim-Skolem-Tarski enunciado al final de la primera sección). En el segundo apartado se prueba la α-categoricidad de algunas teorías de orden, de ciertas teorías de grupos y cuerpos, para terminar con las álgebras de Boole, de gran interés en lógica y teoría de conjuntos. El tercer apartado está formado por una serie de conclusiones y ejemplos basados en los resultados anteriores. Se prueban también algunos teoremas que permiten extender dichos resultados a otras teorías.

En la tercera sección, después de introducir un lenguaje lógico de segundo orden, se prueba que la Aritmética de Peano no es categórica si la formulamos en el lenguaje lógico de primer orden. Para ello se muestra que existen modelos no-standard, eso es, modelos no isomorfos al modelo $\langle \mathbb{N} , + , \cdot , S , 0 \rangle$. Se prueba a continuación que la Aritmética formulada en segundo orden sí es categórica. Pasamos luego a la teoría de los números reales de primer orden donde probamos que no es categórica. La prueba es parecida a la de la Aritmética : mostramos que existen modelos no-standard (el modelo standard es, naturalmente, $\langle \mathbb{R} , + , \cdot , \leq , 0 , 1 \rangle$) construyendo para ello un cuerpo ordenado completo no arquimediano. Seguidamente vemos que la teoría de los números reales de segundo orden sí es categórica. Probamos finalmente la categoricidad de la Geometría Euclídea de segundo orden. La prueba consiste básicamente en mostrar que existe un isomorfismo entre los puntos del espacio euclídeo y $\mathbb{R}^3$.

Se encuentran al final varios anexos y notas a fin de aclarar algunos detalles.

No se ha pretendido con este trabajo tratar exhaustivamente el tema de las teorías categóricas, aunque sí dar una visión general de la cuestión, al tiempo que exponer algunas de las teorías fundamentales en matemáticas para las que es posible probar su categoricidad. Aunque los resultados aquí expuestos no son nuevos, su dispersión y ausencia de pruebas detalladas en muchos casos hace que su recopilación y demostración completa pueda ser de utilidad no sólo para entender mejor lo que es una teoría categórica, sino también para ayudar a comprender la naturaleza de ciertas entidades matemáticas.

Deseo expresar mi agradecimiento al Dr. Jesús Mosterín por su ayuda y estímulo constantes, así como al Dr. Ignacio Jané por sus valiosas sugerencias en la realización de las pruebas.

Joan Bagaría . Febrero 1984

EL LENGUAJE DE LA LOGICA DE PRIMER ORDEN :

TEORIAS Y MODELOS

Este lenguaje tiene la ventaja de ser el más potente para el que es posible disponer de un cálculo deductivo correcto y suficiente. También es el lenguaje más potente que satisface los teoremas de compacidad y el de Löwenheim-Skolem. Así, este lenguaje ocupa un lugar privilegiado, pues es posible además formalizar en él una gran parte de las argumentaciones matemáticas. No obstante, su capacidad para caracterizar unívocamente estructuras es relativamente escasa. La mayoría de las teorías formalizadas en este lenguaje que son categóricas son triviales. No así, en cambio, las teorías que son α-categóricas para alguna cardinalidad α. De todos modos, éste es el lenguaje lógico mejor estudiado, así como su correspondiente teoría de modelos.

Suponemos al lector familiarizado con los lenguajes lógicos de primer orden. No obstante, para fijar la notación, vamos a exponer a continuación cuáles son los símbolos y expresiones del lenguaje lógico de primer orden que utilizaremos aquí y que llamaremos L .

El alfabeto del lenguaje L constará de un conjunto de símbolos que dividiremos en los siguientes grupos:

a- Símbolos para constantes individuales: utilizaremos letras minúsculas a,b,c,...con subíndices si es necesario $a_1, a_2, a_3, \ldots$

b- Símbolos para variables individuales: utilizaremos también letras minúsculas x,y,z,... con subíndices si es necesario $x_1, x_2, x_3, \ldots$

c- Símbolos para functores n-ádicos: utilizaremos letras minúsculas a partir de la f con n como superíndice: $f^n, g^n, h^n, \ldots$.con subíndices si es necesario $f_1^n, f_2^n, f_3^n, \ldots$.

d- Símbolos para relatores n-ádicos: utilizaremos letras mayúsculas con n como superíndice $P^n, Q^n, R^n, \ldots$ con subíndices si es necesario $P_1^n, P_2^n, P_3^n, \ldots$

e- Símbolos lógicos:

Conectores: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.

Cuantificadores: $\bigwedge, \bigvee$.

Descriptor: ι .

f- Un símbolo para el igualador: $\doteq$

Escribimos $\doteq$ en lugar de = como es habitual para distinguirlo de la igualdad en el metalenguaje.

Las expresiones de L son los términos y las fórmulas. Vamos a ver a continuación cómo se forman a partir de los símbolos anteriores los términos y las fórmulas de L :

1- Cualquier constante individual es un término de L.

2- Cualquier variable individual es un término de L.

3- Si $\tau_1, \ldots, \tau_n$ son términos de L y f^n es un functor n-ádico de L, entonces $f^n \tau_1, \ldots, \tau_n$ es un término de L.

4- Si $\tau_1, \ldots, \tau_n$ son términos de L y P^n es un relator n-ádico de L, entonces $P^n \tau_1, \ldots, \tau_n$ es una fórmula de L.

Puesto que el igualador es en realidad un relator diádico, un caso especial será: si τ_1, τ_2 son términos de L, $\tau_1 \doteq \tau_2$ es una fórmula de L . Escribimos como es habitual $\tau_1 \doteq \tau_2$ en lugar de $\doteq \tau_1 \tau_2$.

5- Si α es una fórmula de L, entonces $\neg\alpha$ es una fórmula de L.

6- Si α y β son fórmulas de L, entonces, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ y $(\alpha \leftrightarrow \beta)$ son fórmulas de L.

7- Si α es una fórmula de L, entonces (para cualquier variable x) $\bigwedge x \alpha$ y $\bigvee x \alpha$ son fórmulas de L. (Diremos que x está cuantificada).

8- Si α es una fórmula de L, entonces (para cualquier variable x) $\iota x \alpha$ es un término de L. (Diremos que x está descrita)

9- Sólo son expresiones de L los términos y las fórmulas formadas de acuerdo con las reglas anteriores 1-8.

Una variable puede estar libre o ligada en una expresión de L . Los cuantificadores y el descriptor son signos ligadores. Por tanto, si en una expresión de L, todas las variables que aparecen en ella están cuantificadas o bien descritas, diremos que dicha expresión no tiene variables libres. Un término en el que no aparecen variables libres es un designador y una fórmula en la que no aparecen variables libres es una sentencia.

Interpretar un conjunto Γ de expresiones de L consiste fundamentalmente en indicar un conjunto o universo no vacío de elementos a los que se referirán las constantes y las variables individuales del lenguaje de Γ y un conjunto de funciones y relaciones definidas entre dichos elementos a las que se referirán respectivamente los functores y relatores del lenguaje de Γ . Las descripciones impropias deberán ser atribuídas a un elemento concreto del universo a fin de que todo designador designe efectivamente un individuo de dicho universo. A un conjunto no vacío de elementos junto con un conjunto de funciones y relaciones definidas en este conjunto lo llamamos una estructura. Así pues, las expresiones de L pueden ser interpretadas sobre las estructuras. Definimos a continuación estos conceptos de forma más precisa:

$\mathcal{A}$ es una estructura si y sólo si :

$$\mathcal{A} = \langle A \ , \langle f_i \rangle_{i \in I}, \langle R_j \rangle_{j \in J} \rangle$$

con dos funciones asociadas μ, δ (μ: I $\longrightarrow \mathbb{N}$,
δ : J $\longrightarrow \mathbb{N} - \{0\}$) tal que :

i- $A \neq \emptyset$

ii- I es un conjunto de índices (que puede ser vacío).
para cada $i \in I$, $f_i : A^{\mu(i)} \longrightarrow A$

iii- J es un conjunto de índices (que puede ser vacío).
para cada $j \in J$, $R_j \subset A^{\delta(j)}$

Es conveniente que las funciones y relaciones de $\mathcal{A}$ estén ordenadas : 0-arias, monarias, binarias,etc...
Para ello pedimos que μ y δ sean crecientes:
si $i,k \in I$ y $i \leq k$ entonces $\mu(i) \leq \mu(k)$
si $j,l \in J$ y $j \leq l$ entonces $\delta(j) \leq \delta(l)$

Sea Γ un conjunto de expresiones de L . Sea L(Γ) su lenguaje, eso es, el conjunto de functores, relatores, constantes y variables que aparecen en las expresiones de Γ . Una interpretación de Γ es una función $\mathcal{F}$ tal que a cada elemento de L(Γ) le asigna un elemento de una estructura $\mathcal{A} = \langle A , \langle f_i \rangle_{i \in I}, \langle R_j \rangle_{j \in J} \rangle$ de la manera siguiente:
Para cada constante individual c de L(Γ) : $\mathcal{F}(c) = a$ donde $a \in A$. No obstante, para mayor comodidad, consideraremos aquí las constantes como funciones 0-arias; eso es, $a = f_k$ donde $k \in I$ y $\mu(k) = 0$.
Para cada variable individual x de L(Γ) : $\mathcal{F}(x) = y$ donde y es un elemento de A.
Para cada functor n-ádico f^n de L(Γ) : $\mathcal{F}(f^n) = f_k$ donde $k \in I$ y $\mu(k) = n$.
Para cada relator n-ádico R^n de L(Γ) : $\mathcal{F}(R^n) = R_k$, donde $k \in J$ y $\delta(k) = n$.

Dada una interpretación $\mathcal{F}$ de Γ sobre $\mathcal{A}$, cada término de Γ denota un elemento de A y cada fórmula de Γ es satisfecha o no satisfecha por $\mathcal{F}$. Para indicar que τ denota x en A escribiremos $\mathcal{F}(\tau) = x$. Para indicar que $\mathcal{F}$ satisface α escribiremos $\mathcal{F}$ sat α .
Vamos a definir a continuación por inducción semiótica la denotación de un término y la satisfacción de una fórmula de Γ por $\mathcal{F}$ en $\mathcal{A}$:

$\mathcal{F}(x) = \mathcal{F}(x)$

$\mathcal{F}(c) = \mathcal{F}(c)$

$\mathcal{F}(f^n \tau_1, \ldots, \tau_n) = \mathcal{F}(f^n)\ \mathcal{F}(\tau_1), \ldots, \mathcal{F}(\tau_n)$

$\mathcal{F}$ sat $P^n \tau_1, \ldots, \tau_n$ si y sólo si $\langle \mathcal{F}(\tau_1), \ldots, \mathcal{F}(\tau_n) \rangle \in \mathcal{F}(P^n)$

$\mathcal{F}$ sat $\tau_1 = \tau_2$ si y sólo si $\mathcal{F}(\tau_1) = \mathcal{F}(\tau_2)$

$\mathcal{F}$ sat $\neg\alpha$ si y sólo si no $\mathcal{F}$ sat α .

$\mathcal{F}$ sat $\alpha \wedge \beta$ si y sólo si $\mathcal{F}$ sat α y $\mathcal{F}$ sat β

$\mathcal{F}$ sat $\alpha \vee \beta$ si y sólo si $\mathcal{F}$ sat α o $\mathcal{F}$ sat β

$\mathcal{F}$ sat $\alpha \rightarrow \beta$ si y sólo si, si $\mathcal{F}$ sat α entonces $\mathcal{F}$ sat β

$\mathcal{F}$ sat $\alpha \leftrightarrow \beta$ si y sólo si, $\mathcal{F}$ sat α si y sólo si $\mathcal{F}$ sat β

$\mathcal{F}$ sat $\bigwedge x\, \alpha$ si y sólo si, para todo $x \in A$: $\mathcal{F}^x_y$ sat α

donde $\mathcal{F}^x_y$ es la interpretación que coincide con $\mathcal{F}$ absolutamente en todo con la excepción de que asigna a la variable y el elemento x de A . Para toda variable z de L(Γ) : $\mathcal{F}^x_y(z) = \mathcal{F}(z)$ si $z \neq y$

$\mathcal{F}^x_y(z) = x$ si $z = y$

$\mathcal{F}$ sat $\bigvee x\, \alpha$ si y sólo si para algún $x \in A$: $\mathcal{F}^x_y$ sat α

$$\mathcal{F}(\iota x \alpha) = \begin{cases} \text{el único } x \in A \text{ tal que } \mathcal{F}^x_y \text{ sat } \alpha \text{ si hay un tal } x \text{ y sólo uno .} \\ a \text{, si no. Donde } a \text{ es un elemento concreto de } A \text{ (siempre el mismo) .} \end{cases}$$

Sea Γ un conjunto de fórmulas de L . $\mathcal{A}$ es una estructura homóloga a Γ syss en $\mathcal{A}$ hay tantas relaciones n-arias como relatores n-arios hay en Γ , para cada $n \geqslant 1$; hay tantas funciones n-arias como functores n-arios hay en Γ , para cada $n \geqslant 1$; y hay tantas funciones 0-arias como constantes individuales hay en Γ .Sea una interpretación $\mathcal{F}$ de Γ sobre $\mathcal{A}$. Si toda fórmula de Γ es satisfecha por $\mathcal{F}$ en $\mathcal{A}$, decimos que $\mathcal{A}$ es un modelo de Γ . (abreviado $\mathcal{A}$ Mod Γ). Así pues, dado un conjunto Γ de fórmulas de L y dada una estructura $\mathcal{A}$ homóloga a Γ , diremos que $\mathcal{A}$ es modelo de Γ si y sólo si existe una interpretación $\mathcal{F}$ de Γ en $\mathcal{A}$ tal que $\mathcal{F}$ satisface toda fórmula φ de Γ .

Sea Γ un conjunto de fórmulas de L . Sea φ una fórmula de L. Decimos que φ es una consecuencia lógica de Γ si y sólo si toda interpretación que satisface Γ satisface también φ . O lo que es lo mismo, si y sólo si todo modelo de Γ lo es también de φ . (abreviado $\Gamma \models \varphi$).

Sea Γ un conjunto de sentencias de L clausurado respecto de la relación de consecuencia lógica (o de deducibilidad, pues son relaciones equivalentes en L, ya que existe un cálculo deductivo correcto y suficiente para L). Eso es, si ocurre que : si $\Gamma \models \varphi$ entonces $\varphi \in \Gamma$, diremos que Γ es una teoría.

Naturalmente, exigimos de las teorías que sean consistentes, es decir, que dada una teoría Γ y una sentencia φ, si $\varphi \in \Gamma$ entonces $\neg\varphi \notin \Gamma$ y si $\neg\varphi \in \Gamma$ entonces $\varphi \notin \Gamma$. De lo contrario cualquier sentencia pertenecería a Γ dado que sería deducible de Γ. Además no tendría ningún modelo. En efecto: Una teoría Γ será consistente si y sólo si tiene al menos un modelo.

Prueba: si Γ no es consistente habrá una sentencia φ tal que $\varphi \in \Gamma$ y tal que $\neg\varphi \in \Gamma$. Pero φ y $\neg\varphi$ no pueden ser satisfechas en una misma estructura. Luego, Γ no tendrá ningún modelo. Sea Γ consistente y supongamos que Γ no tiene ningún modelo. Luego, dada una sentencia cualquiera φ de Γ, para toda estructura $\mathcal{A}$, si $\mathcal{A}$ Mod $\Gamma - \{\varphi\}$ entonces no $\mathcal{A}$ Mod φ pues de lo contrario $\mathcal{A}$ Mod Γ. Pero si no $\mathcal{A}$ Mod φ entonces $\mathcal{A}$ Mod $\neg\varphi$. Por tanto, todo modelo de $\Gamma - \{\varphi\}$ lo es de $\neg\varphi$. De donde se sigue que $\Gamma \models \neg\varphi$ y de ahí que $\neg\varphi \in \Gamma$. Luego, Γ no es consistente.

Así pues, una teoría Γ será un conjunto consistente de sentencias tal que toda consecuencia lógica de Γ pertenece a Γ.

Un conjunto de sentencias Δ es un conjunto de axiomas para una teoría Γ si y sólo si Δ y Γ tienen las mismas consecuencias lógicas. O lo que es equivalente, si y sólo si Δ tiene exactamente los mismos modelos que Γ. Eso es, si y sólo si para toda estructura $\mathcal{A}$, $\mathcal{A}$ Mod Γ si y sólo si $\mathcal{A}$ Mod Δ. Será, pues, indiferente hablar de los modelos de una teoría que hablar de los modelos de un conjunto de axiomas de dicha teoría.

Dada una teoría Γ de L. todo teorema de Γ puede ser deducido a partir de un conjunto de axiomas de Γ pues en L disponemos de un cálculo deductivo correcto y suficiente. Γ, puesto que suponemos que es consistente, tendrá un modelo $\mathcal{A}$. Pero puede ocurrir que exista una sentencia $\varphi \in L(\Gamma)$ tal que $\mathcal{A}\,\mathrm{Mod}\,\varphi$ y $\varphi \notin \Gamma$. Esto significa que dicha teoría es insuficiente para describir completamente la estructura $\mathcal{A}$ ya que habrá una sentencia de $L(\Gamma)$ que puede ser satisfecha en $\mathcal{A}$ y que no será un teorema de la teoría. O lo que es lo mismo, que no podrá ser deducida a partir de un conjunto de axiomas de la teoría. Esto no se da en las teorías completas.

Una teoría Γ es completa si y sólo si para toda sentencia φ de $L(\Gamma)$ o bien $\varphi \in \Gamma$ o bien $\neg\varphi \in \Gamma$. Una teoría completa Γ es un conjunto máximamente consistente de sentencias de $L(\Gamma)$.

Puesto que dada una estructura $\mathcal{A}$, tal que $\mathcal{A}$ es modelo de Γ y una sentencia φ de $L(\Gamma)$, o bien $\mathcal{A}\,\mathrm{Mod}\,\varphi$ o bien $\mathcal{A}\,\mathrm{Mod}\,\neg\varphi$, tenemos que una teoría completa es el conjunto de todas las sentencias de L que son satisfechas en una estructura dada.

Dos estructuras son elementalmente equivalentes en L si y sólo si son modelos de exactamente las mismas sentencias de L. (Abreviado $\mathcal{A} \equiv \mathcal{B}$: $\mathcal{A}$ es elementalmente equivalente a $\mathcal{B}$).

Teorema : Sea Γ una teoría de L. Γ es completa si y sólo si todos sus modelos son elementalmente equivalentes.

Prueba: Sea Γ completa. Luego, para cada sentencia φ de $L(\Gamma)$ ocurrirá que o bien $\Gamma \models \varphi$ o bien $\Gamma \models \neg\varphi$. Sean $\mathcal{A}$ y $\mathcal{B}$ dos modelos cualesquiera de Γ y sea φ una sentencia de $L(\Gamma)$. O bien $\mathcal{A}$ y $\mathcal{B}$ serán ambos modelos de φ o no (depende de si $\Gamma \models \varphi$ o si $\Gamma \models \neg\varphi$). Por consiguiente $\mathcal{A}$ y $\mathcal{B}$ son elementalmente equivalentes.

Prueba: (continuación)

Sean todos los modelos de Γ elementalmente equivalentes. Luego, para cada sentencia φ de $L(\Gamma)$ y para todo modelo $\mathscr{A}$ de Γ, o bien $\mathscr{A}$ Mod φ o bien $\mathscr{A}$ Mod $\neg\varphi$. Pero si $\mathscr{A}$ Mod φ todos los demás modelos de Γ también serán modelos de φ. Y lo mismo ocurrirá si $\mathscr{A}$ Mod $\neg\varphi$. Por tanto, o bien $\Gamma \models \varphi$ o bien $\Gamma \models \neg\varphi$. Luego, Γ es completa.

Dos estructuras elementalmente equivalentes en L son totalmente indistinguibles para L ; aunque eso no quiere decir que sean idénticas, como veremos.

Así pues, una teoría Γ completa tiene la ventaja de que para toda sentencia φ de $L(\Gamma)$ o bien φ es un teorema de Γ o bien $\neg\varphi$ es un teorema de Γ. Eso es, que o bien φ o bien $\neg\varphi$ es deducible de un conjunto de axiomas de Γ. Además, toda sentencia de L que es satisfacible en un modelo de Γ, es satisfacible en todo modelo de Γ.

CATEGORICIDAD

Puede ocurrir, no obstante, que una teoría completa Γ tenga como modelos a dos estructuras $\mathscr{A}$ y $\mathscr{B}$ distintas, eso es, no isomórficas. Vamos a definir la relación de isomorfía entre estructuras:

Sean $\mathscr{A}$ y $\mathscr{B}$ dos estructuras del mismo tipo. Eso es, que para cada n, haya tantas funciones y relaciones n-arias en $\mathscr{A}$ como en $\mathscr{B}$.

Sean $\mathscr{A} = \langle A , \langle f_i \rangle_{i\in I} , \langle R_j \rangle_{j\in J} \rangle$ y $\mathscr{B} = \langle B , \langle g_i \rangle_{i\in I} , \langle S_j \rangle_{j\in J} \rangle$

Una función h es un isomorfismo entre $\mathscr{A}$ y $\mathscr{B}$ si y sólo si:

i- $h: A \longrightarrow B$ es biyectiva.

ii- para cada $i \in I$, $x_1, \ldots, x_{\mu(i)} \in A$:

$$h(f_i(x_1, \ldots, x_{\mu(i)})) = g_i(h(x_1), \ldots, h(x_{\mu(i)}))$$

iii- para cada $j \in J$, $x_1, \ldots, x_{\delta(j)} \in A$:

$$\langle x_1, \ldots, x_{\delta(j)} \rangle \in R_j \text{ si y sólo si } \langle h(x_1), \ldots, h(x_{\delta(j)}) \rangle \in S_j$$

Diremos que dos estructuras son isomórficas si y sólo si existe un isomorfismo entre ellas. (Abreviadamente $\mathscr{A} \cong \mathscr{B}$: $\mathscr{A}$ y $\mathscr{B}$ son isomórficas).

La relación de isomorfía entre estructuras es claramente una relación de equivalencia. (Véase el Anexo 1)

Dos estructuras isomórficas son de hecho la misma estructura, pues son completamente indistinguibles no sólo para L, ya que como veremos si $\mathscr{A} \cong \mathscr{B}$ entonces $\mathscr{A} \equiv \mathscr{B}$, sino incluso para todo lenguaje lógico de orden superior.

Luego, a pesar de que una teoría completa de L, es el conjunto de todas las sentencias de L que son satisfechas en una estructura dada $\mathscr{A}$, es posible que sea también a la vez el conjunto de todas las sentencias de L que son satisfechas en otra estructura $\mathscr{B}$ tal que $\mathscr{A} \not\cong \mathscr{B}$. Lo que significa que aunque $\mathscr{A}$ y $\mathscr{B}$ son distintas, son indistinguibles para L. ¿En qué casos ocurre eso?. Veamos el teorema siguiente:

Teorema : Si $\mathscr{A} \cong \mathscr{B}$ entonces $\mathscr{A} \equiv \mathscr{B}$. Lo contrario de cumple solamente en el caso de que $\mathscr{A}$ sea **finito.**

(Véase la prueba en el Anexo 2).

Así pues, si Γ es una teoría de L completa y tiene un modelo finito, entonces Γ tiene exactamente un único modelo (aparte los isomórficos). Así, Γ describe unívoca y completamente una estructura; eso es, todas las sentencias de L que son satisfacibles en esa estructura pertenecen a Γ y no existe otra estructura distinta (no isomórfica) que satisfaga exactamente las mismas sentencias (que sea modelo de Γ).

Por otra parte, si Γ es una teoría completa de L y tiene un modelo infinito, entonces puede ocurrir que tenga dos modelos distintos, eso es, no isomórficos .

Decimos que una teoría es categórica si y sólo si tiene todos sus modelos isomórficos.

Luego, si Γ es una teoría completa de L y tiene sólo modelos finitos, Γ será categórica. Así, en el caso finito, la completud y la categoricidad son propiedades equivalentes de las teorías. No obstante, si Γ tiene modelos infinitos, dichas propiedades ya no son equivalentes. En este caso, Γ describirá unívocamente una estructura si y sólo si es categórica.

Sin embargo, para el lenguaje de la lógica de primer orden esto no ocurre nunca, es decir, que no existe ninguna teoría en este lenguaje que tenga un modelo infinito y que sea categórica. Ello es una consecuencia del teorema siguiente:

Teorema : (Löwenheim-Skolem-Tarski). Si Γ es una teoría de L y tiene modelos infinitos, entonces Γ tiene modelos infinitos en cada cardinalidad $\alpha \geqslant \|L\|$ .Donde $\|L\| = \omega \cup |L|$.

(Véase una prueba de este teorema en Chang-Keisler: "Model Theory" Pág.67).

Así pues, en L, una teoría que tenga un modelo infinito de cardinalidad α numerable o no, tendrá también otro modelo infinito de cardinalidad $\alpha' \neq \alpha$. Luego, estos dos modelos no serán isomorfos, pues no serán biyectables y por tanto dicha teoría no será categórica.

Luego, en L no existen teorías categóricas que tengan modelos infinitos. Lo que significa que una estructura cuyo universo es infinito no puede ser unívocamente caracterizada por el lenguaje de la lógica de primer orden.

Sin embargo, dada una teoría Γ de L, podemos considerar sólo los modelos de Γ de una cardinalidad dada α finita o infinita. Entonces sí que puede ocurrir que todos los modelos de Γ de cardinalidad α sean isomorfos. Si ello ocurre diremos que Γ es α-categórica.

Una teoría Γ es α-categórica si y sólo si tiene al menos un modelo de cardinalidad α y todos sus modelos de cardinalidad α son isomórficos.

Si una teoría es α-categórica para un α finito, $\alpha = n$, entonces la teoría que resulta de añadir a la anterior la sentencia que afirma la existencia de exactamente n elementos, sentencia que puede ser expresada en el lenguaje L, es categórica, pues sólo tendrá modelos de cardinalidad α los cuales serán todos isomórficos.

Por otra parte, si una teoría Γ de L es α-categórica para un α infinito y sólo tiene modelos infinitos, entonces es completa. Efectivamente: Basta ver que dos modelos $\mathcal{A}$ y $\mathcal{B}$ cualesquiera de Γ son elementalmente equivalentes. Por el teorema de Löwenheim-Skolem-Tarski existirán modelos $\mathcal{A}'$ y $\mathcal{B}'$ de cardinalidad α tales que $\mathcal{A} \equiv \mathcal{A}'$ y $\mathcal{B} \equiv \mathcal{B}'$. Puesto que Γ es α-categórica, $\mathcal{A}' \cong \mathcal{B}'$ y por tanto, $\mathcal{A} \equiv \mathcal{B}$.

Veremos a continuación algunos ejemplos de teorías de L que son categóricas. Estas teorías, como puede suponerse son poco interesantes o aún triviales, dado que las teorías realmente interesantes en matemáticas tienen modelos infinitos y por tanto, no son categóricas.

Ejemplos de Teorías categóricas

1- La teoría cuyo único axioma es la sentencia que afirma la existencia de exactamente n elementos.

Claramente es una teoría categórica: Todos sus modelos tienen cardinalidad n.

2- La teoría cuyos axiomas son:

$$\bigwedge x \, Px$$
$$\bigwedge xy \; x \doteq y$$

Fácilmente se comprueba que esta teoría es categórica.

i) Todos los modelos de esta teoría tienen un solo elemento. Luego, dados dos modelos cualesquiera $\mathcal{A}$ y $\mathcal{B}$ existe una biyección h: A $\longrightarrow$ B .

ii) Debe cumplirse que : $\langle x \rangle \in P \longleftrightarrow \langle h(x) \rangle \in P'$
Efectivamente, pues h(x) es el único elemento de B y según el axioma 1 todo elemento del universo tiene la propiedad P.

(Nótese que si consideramos sólo el segundo axioma la teoría es también categórica, no así en cambio si consideramos sólo el primero).

3- La teoría cuyos axiomas son:

$$\bigwedge xyz \, (x \doteq y \vee y \doteq z \vee x \doteq z)$$
$$\bigvee xy \, (x \not\doteq y \wedge Px \wedge \neg Py)$$

Según estos axiomas todos los modelos de esta teoría tienen dos elementos. Vamos a ver que dados dos modelos cualesquiera $\mathcal{A}$ y $\mathcal{B}$ de la teoría, existe un isomorfismo entre ellos.

i) Puesto que todos los modelos de la teoría tienen dos elementos, existirán dos biyecciones h: A $\longrightarrow$ B y h`: A $\longrightarrow$ B .

ii) Sean $\mathcal{A} = \langle A , P \rangle$ y $\mathcal{B} = \langle B , R \rangle$ dos modelos de la teoría.

Luego debe cumplirse que para todo $x \in A$:

$\langle x \rangle \in P \longleftrightarrow \langle h(x) \rangle \in R$

Es claro que al menos una de las dos biyecciones lo cumplirá pues sólo uno de los dos elementos de A tiene la propiedad P y sólo uno de los elementos de ~~X~~ B tiene la propiedad R . Simplemente debemos escoger la biyección que relaciona estos dos elementos.

TEORIAS α - CATEGORICAS

Veremos ahora algunos ejemplos de teorías de L que sí son importantes desde un punto de vista matemático : teorías de orden, grupos, cuerpos y álgebras de Boole; las cuales, como se probará son α-categóricas en alguna cardinalidad α .

Aquellas de estas teorías que sean α-categóricas para algún α finito, pueden convertirse en teorías categóricas añadiendo simplemente un axioma que establezca la existencia de exactamente α elementos. De otro lado, aquellas de estas teorías que tengan sólo modelos infinitos y que sean α-categóricas para algún α infinito, serán completas; además de caracterizar unívocamente un modelo suyo de cardinalidad α .

Volveremos a tratar estos temas con mayor detalle después de haber visto dichos ejemplos y demostrado su α-categoricidad.

Se ha procurado que las pruebas sean lo más claras posible. Para ello se ha intentado no omitir ningún paso; lo que hace que algunas de ellas sean un poco extensas. Casi tan importantes como los mismos resultados son los distintos métodos algebraicos y de teoría de modelos utilizados en las pruebas, por lo que es interesante que el lector se fije en ellos.

Antes de empezar con las teorías de orden conviene aclarar algunas convenciones sobre notación.

Así, por ejemplo, en las teorías de orden utilizamos el signo $\leq$ en lugar de un relator binario R^2. En las teorías de grupos utilizamos el signo $+$ en lugar de un functor binario f^2; así como el signo 0 en lugar de una constante individual c para indicar el elemento neutro.

En las álgebras de Boole utilizamos los signos $+$, $\cdot$, también como functores binarios, así como el signo $-$ en lugar de un functor monario. También utilizamos los signos 0 y 1 como constantes.

Los signos $+$, $\cdot$, 0 , 1 , también son utilizados en la teoría de cuerpos en el sentido anterior.

También variamos el orden de la notación. Así, en lugar de escribir $\leq xy$, escribimos $x \leq y$. En lugar de $+xy$, escribimos $x + y$, etc...

Todo ello se hace en vistas a una mayor simplicidad y naturalidad, pues de esta manera nos acercamos a la notación matemática tradicional. Sacrificamos así la elegancia de una presentación utilizando solamente símbolos de L en aras de una mayor facilidad de lectura e intuición.

Sea $\mathcal{L} = \{ \leqslant \}$ un lenguaje de primer orden donde $\leqslant$ es un relator binario. Escribimos $x \leqslant y$ en lugar de $\leqslant xy$. La teoría de Orden parcial tiene los tres axiomas siguientes :

1- $\bigwedge xyz \ (x \leqslant y \wedge y \leqslant z \longrightarrow x \leqslant z)$
2- $\bigwedge xy \ (x \leqslant y \wedge y \leqslant x \longrightarrow x = y)$
3- $\bigwedge x \ (x \leqslant x)$

Que son respectivamente las propiedades : transitiva, antisimétrica y reflexiva.

Si añadimos el axioma siguiente, obtendremos la teoría de orden lineal (también llamada de orden total) . En lo que sigue, siempre que hablemos de " orden ", se entenderá " orden lineal ".

4- $\bigwedge xy \ (x \leqslant y \vee y \leqslant x)$

Un modelo de esta teoría es un conjunto ordenado. Luego, para todo α existe al menos un modelo de cardinalidad α .

Proposición : La teoría de orden lineal es α-categórica en cada cardinalidad α finita.

Prueba : Haremos la prueba por inducción aritmética, eso es, probaremos primero que es 1-categórica y luego que si es n-categórica también es n+1-categórica.

Que la teoría es 1-categórica se comprueba trivialmente.

Supongamos ahora que es n-categórica y veamos que también es n+1-categórica:

Prueba : (continuación)

Sean $\mathscr{A}'$ y $\mathscr{B}'$ modelos de la teoría de cardinalidad $n + 1$.

Puesto que $\mathscr{A}'$ es un orden lineal y es finito, existirá un elemento $a \in \mathscr{A}'$ tal que para todo $x \in \mathscr{A}'$, ocurre que $a \geqslant x$.

Lo mismo ocurrirá en $\mathscr{B}'$. Sea este elemento b.

Sean ahora $\mathscr{A} = \mathscr{A}' - \{a\}$ y $\mathscr{B} = \mathscr{B}' - \{b\}$

$\mathscr{A}$ será un orden lineal y $\mathscr{B}$ también y ambos serán de cardinalidad n . Luego, según lo supuesto, $\mathscr{A} \cong \mathscr{B}$.

Sea h el isomorfismo entre $\mathscr{A}$ y $\mathscr{B}$.

Sea ahora h' una función de $\mathscr{A}'$ en $\mathscr{B}'$ tal que $h'(a) = b$, y para todo $x \in \mathscr{A}'$ tal que $a \neq x$, $h'(x) = h(x)$.

Veamos que h' es un isomorfismo entre $\mathscr{A}'$ y $\mathscr{B}'$.

i) Claramente h' es biyectiva, pues h lo es.

ii) Para cualesquiera $a_1, a_2 \in \mathscr{A}'$ debe cumplirse que :

$$a_1 \leqslant a_2 \longleftrightarrow h'(a_1) \leqslant h'(a_2)$$

Si $a_1 \neq a$ y $a_2 \neq a$, esto se cumple necesariamente, pues $h'(a_1) = h(a_1)$ y $h'(a_2) = h(a_2)$ y h es un isomorfismo entre $\mathscr{A}$ y $\mathscr{B}$.

Prueba : (continuación)

Sea $a_1 = a$.

Si $a_1 \leq a_2$, entonces $a_2 = a$. Pues para todo $x \in \mathscr{A}'$, $a \geq x$.

Pero si $a_1 = a$, $h'(a_1) = h'(a) = b$ y si $a_2 = a$, $h'(a_2) = h'(a) = b$. De donde $h'(a_1) = h'(a_2)$. Se cumple pues, que :

$$a_1 \leq a_2 \longrightarrow h'(a_1) \leq h'(a_2)$$

Dado que $a_1 = a$, $h'(a_1) = b$ y entonces, si $h'(a_1) \leq h'(a_2)$, se sigue que $h'(a_2) = b$ pues para todo $y \in \mathscr{B}'$, $b \geq y$.
Luego, $a_2 = a$. De donde $a_1 \leq a_2$. Se sigue pues, que :

$$h'(a_1) \leq h'(a_2) \longrightarrow a_1 \leq a_2$$

Tendremos entonces :

$$a_1 \leq a_2 \longleftrightarrow h'(a_1) \leq h'(a_2).$$

Un razonamiento análogo vale si $a_2 = a$.

h' es, pues, un isomorfismo entre $\mathscr{A}'$ y $\mathscr{B}'$.
Y por inducción aritmética sobre la cardinalidad de sus modelos, tenemos que la teoría de orden lineal es α -categórica para todo α finito.

Si a los axiomas de al teoría de orden les añadimos los axiomas 5 y 6, obtendremos la teoría de orden denso.

5- $\bigwedge xy\ ((x \leqslant y \wedge x \neq y) \longrightarrow \bigvee z\ (x \leqslant z \wedge z \neq x \wedge z \leqslant y \wedge z \neq y))$

6- $\bigvee xy\ (x \neq y)$

Añadiendo los dos axiomas siguientes, tenemos la teoría de orden denso sin extremos :

7- $\bigwedge x\ \bigvee y\ (x \leqslant y \wedge x \neq y)$

8- $\bigwedge x\ \bigvee y\ (y \leqslant x \wedge y \neq x)$

La teoría de orden denso sin extremos es particularmente importante , pues tiene como modelos al conjunto de los números racionales con su orden natural, así como al conjunto de los números reales también con su orden natural. Como veremos a continuación, esta teoría es ω -categórica, eso es, todos sus modelos de cardinalidad ω son isomorfos.

Proposición : La teoría de orden lineal denso sin extremos es ω - categórica.

Prueba : Esta prueba está basada en el procedimiento de Cantor " back and forth " .

Sean $\mathcal{A} = \langle A , \leq \rangle$ y $\mathcal{B} = \langle B , \leq' \rangle$ dos modelos de la teoría de cardinalidad ω .
Sean $A_0 \subset A$ y $B_0 \subset B$.
Entonces diremos que una función f: $A_0 \longrightarrow B_0$ es un isomorfismo parcial entre A y B si y sólo si :

i) La función f es biyectiva.

ii) Para cualesquiera $a_0 , a_1 \in A_0$ ocurre que:

$$a_0 \leq a_1 \longleftrightarrow f(a_0) \leq' f(a_1)$$

Sean ahora A y B numerables.
Supongamos que tenemos una sucesión de isomorfismos parciales entre A y B $\langle f_u : u \in \omega \rangle$ tales que :

i) $f_0 \subseteq f_1 \subseteq f_2 \subseteq, \ldots, \subseteq f_u \subseteq, \ldots\ldots$
donde $f_i \subseteq f_j$ si y sólo si $i \leq j$.

ii) Para todo $a \in A$, existe un u tal que a pertenece al dominio de f_u .

iii) Para todo $b \in B$, existe un u tal que b pertenece al recorrido de f_u .

Entonces, $F = \bigcup_u f_u$ será un isomorfismo entre $\mathcal{A}$ y $\mathcal{B}$. Efectivamente :

Prueba : (continuación)

El dominio de F será A , según la condición ii) y el recorrido de F será B según la condición iii). Además F será una función, pues si no la fuera deberían existir dos elementos $\langle x,y\rangle$ y $\langle x,z\rangle$ de F , donde $y \neq z$. Pero $\langle x,y\rangle \in f_i$ y $\langle x,z\rangle \in f_j$ para algún $f_i, f_j \in \langle f_u : u \in \omega \rangle$. Entonces existirá un $k \geqslant i,j$ tal que $\langle x,y\rangle , \langle x,z\rangle \in f_k$. Lo que es absurdo, pues f_k es una función.
F es pues una biyección entre A y B y además es un isomorfismo, pues dados $a_0, a_1 \in A$ cualesquiera, ambos pertenecen al dominio de algún $f_i \in \langle f_u : u \in \omega\rangle$ y $f_i \subseteq F$.

Vamos a construir, pues, una sucesión de isomorfismos parciales $\langle f_u : u \in \omega \rangle$ entre $\mathcal{A}$ y $\mathcal{B}$ tal que cumpla las tres condiciones anteriores:

Puesto que A y B son numerables, sean:
$\{a_i : i \in \omega\}$ y $\{b_i : i \in \omega\}$
enumeraciones de los elementos de A y B .

Tomemos ahora, para empezar, el primer elemento de cada uno de estos dos conjuntos, eso es, a_0 y b_0 . Sea $f_0 = \langle a_0, b_0\rangle$

Tomemos a continuación el segundo elemento de $\{a_i : i \in \omega\}$, eso es, a_1 . Entonces, o bien $a_0 \leqslant a_1$ o bien $a_1 \lneqq a_0$ (Axiomas 2 y 4) Supongamos que $a_0 \lneqq a_1$. Luego existirá un $b_i \in \{b_i : i \in \omega\}$ tal que $b_0 \lneqq b_i$ (Axioma 7). Sea b_j el primero de tales b_i .

Sea $f_1 = f_0 \cup \langle a_1, b_j\rangle$.

Prueba : (continuación)

Consideremos ahora el primer b_i no utilizado de $\{b_i : i \in \omega\}$. Luego, o bien $b_i \leq b_0 \leq b_j$ o bien $b_0 \leq b_i \leq b_j$ o bien $b_0 \leq b_j \leq b_i$. En cualquiera de los tres casos existirá algún $a_i \in \{a_i : i \in \omega\}$ tal que a_i se encontrará en la misma relación con a_0 y a_1 . (Axiomas 8,7,5 respectivamente) . Sea a_j el primero de tales a_i .

Sea $f_2 = f_1 \cup \langle a_j , b_i \rangle$

El paso siguiente consistiría en tomar el primer a_i no utilizado de $\{a_i : i \in \omega\}$, y buscar el primer b_i de $\{b_i : i \in \omega\}$ tal que esté en la misma relación de orden con los b_i ya utilizados que a_i con los a_i ya utilizados.

Prosiguiendo de este modo, eso es, para cada f_u , cuando u es par, formamos el isomorfismo parcial f_u añadiendo al isomorfismo parcial f_{u-1} el par ordenado formado a partir del primer $a_i \in \{a_i : i \in \omega\}$ no utilizado; y para cada u, cuando u es impar, formamos el isomorfismo parcial f_u añadiendo al isomorfismo parcial f_{u-1} el par ordenado formado a partir del primer $b_i \in \{b_i : i \in \omega\}$ no utilizado, obtenemos una sucesión de isomorfismos parciales que cumplen las tres condiciones del principio de la prueba . Luego, $F = \bigcup_u f_u$ será un isomorfismo entre $\mathscr{A}$ y $\mathscr{B}$.

Puesto que $\mathscr{A}$ y $\mathscr{B}$ son modelos cualesquiera de la teoría de orden lineal denso sin extremos de cardinalidad ω , dicha teoría es ω -categórica.

Sea $\mathcal{L} = \{ + , 0 \}$ un lenguaje de primer orden donde $+$ es un functor binario y 0 es una constante individual. Escribimos $x + y$ en lugar de $+ xy$. La teoría de Grupos tiene los tres axiomas siguientes :

1- $\bigwedge xyz \; (x + (y + z) = (x + y) + z)$
2- $\bigwedge x \; (x + 0 = x \wedge 0 + x = x)$
3- $\bigwedge x \bigvee y \; (x + y = 0 \wedge y + x = 0)$

Puesto que las congruencias módulo n de los números enteros son modelos de la teoría, ésta tiene modelos en cada cardinalidad finita. También tiene modelos infinitos, numerables y no-numerables, por ejemplo $\langle \mathbb{Z} , + , 0 \rangle$ y $\langle \mathbb{R} , + , 0 \rangle$.

Sea $\mathcal{A}$ un grupo. Decimos que $\mathcal{B}$ es un subgrupo de $\mathcal{A}$ si y sólo si $\mathcal{B} \sqsubseteq \mathcal{A}$ y $\mathcal{B}$ es un grupo. (Véase la Nota 1).

En todo subgrupo $\mathcal{B}$ de $\mathcal{A}$ estará el elemento neutro 0 de $\mathcal{A}$; y para cualquier $x \in \mathcal{A}$, si $x \in \mathcal{B}$ entonces también $-x \in \mathcal{B}$ (donde $-x$ es el elemento simétrico de x) . Evidentemente, la intersección de un conjunto de subgrupos de un grupo $\mathcal{A}$ es un subgrupo de $\mathcal{A}$.

Los subgrupos de un grupo $\mathcal{A}$ pueden obtenerse de la forma siguiente :

Sea S un subconjunto de A . Luego, la intersección de todos los subgrupos que incluyen los elementos de S será un subgrupo que incluye los elementos de S . Llamamos a este subgrupo el subgrupo generado por S .

El subgrupo generado por un elemento $a \in A$ consiste en todos los productos na, donde n es un entero positivo y $na = a + a +, \ldots, + a$ n veces; $0a$ es el elemento neutro y $n(-a)$ es el simétrico de na.

Decimos que un grupo $\mathscr{A}$ es cíclico si y sólo si tiene un elemento generador.

Proposición: La teoría de Grupos es α-categórica para α primo.

Para probar que la teoría de grupos es α-categórica cuando α es un número primo, probaremos primero la siguiente proposición :

Proposición: Dos grupos cíclicos de orden n son isomorfos.

Prueba : Sean $\mathscr{A}$ y $\mathscr{B}$ dos grupos cíclicos de orden n (llamamos orden de un grupo al número de sus elementos) :

$$\mathscr{A} = \langle A , + , 0 \rangle \quad \mathscr{B} = \langle B , +' , 0' \rangle$$

Debemos probar que existe una función h de $\mathscr{A}$ en $\mathscr{B}$ tal que :

i) h es biyectiva.
ii) Para todo $a_0, a_1 \in A$ ocurre que :

$$h(a_0 + a_1) = h(a_0) +' h(a_1)$$

Puesto que $\mathscr{A}$ es cíclico, tendrá un elemento generador x tal que para todo $a_i \in A$ existirá un entero positivo m tal que $mx = a_i$.

Necesitamos ahora probar el teorema siguiente :

Teorema : El orden de un grupo cíclico es el orden de su elemento generador.

Llamamos orden de un elemento x de un grupo $\mathscr{A}$ al

Prueba : (continuación)
menor m tal que $mx = 0$.

Prueba : Sea $\mathcal{A}$ un grupo cíclico cuyo elemento generador es a .
Sea n el orden de a.
Consideraremos que $a \neq 0$ pues de lo contrario la prueba es trivial.
Sea $a' \in \mathcal{A}$ tal que $a' \neq a$.
Luego $a' = ma$ para algún m determinado tal que $m \leq n$ pues el orden de a es n .
Además, dados m_i y m_j menores o iguales a n y distintos , se sigue que $m_i a \neq m_j a$; pues de lo contrario $(m_i - m_j)a = 0$ con lo cual a no sería de orden n .
Así pues, en $\mathcal{A}$ hay tantos elementos distintos como enteros positivos menores o iguales a n . Luego $\mathcal{A}$ es de orden n .

Volviendo a la prueba inicial, sea x el elemento generador de $\mathcal{A}$ y sea y el elemento generador de $\mathcal{B}$.
Luego, $nx = 0$ y $ny = 0'$

Sea h una función de $\mathcal{A}$ en $\mathcal{B}$ y tomemos $h(0) = 0'$ y $h(x) = y$

Sean a_0, $a_1 \in \mathcal{A}$. Si $a_0 = 0$ o $a_1 = 0$, la condición ii) de isomorfía se cumple trivialmente . Sean pues a_0 y a_1 distintos de 0.

Para todo m_i ($i \leq n$) tomemos $m_i x = a_i$ y $m_i y = b_i$, y sea $h(a_i) = b_i$.

Luego, $h(a_0 + a_1) = h(m_0 x + m_1 x) =$
$= h((m_0 + m_1) x) = (m_0 + m_1) h(x) =$

Prueba : (continuación)

$= m_0 h(x) +' m_1 h(x) = m_0 y +' m_1 y =$

$= b_0 +' b_1 = h(a_0) +' h(a_1)$

Luego, la función h cumple la segunda condición de isomorfía.

Veamos ahora que h es biyectiva :

Para ello basta demostrar que para cualesquiera $a_i , a_j \in A$, $a_i = a_j$ si y sólo si $h(a_i) = h(a_j)$.

Sean a_i y a_j distintos de 0 y de x , pues en estos casos la demostración es trivial . Sea $a_i = a_j$. Entonces $m_i x = m_j x$ y luego $m_i = m_j$. Pues si $m_i \neq m_j$ uno de los dos sería mayor que el otro. Sea por ejemplo $m_i > m_j$. Puesto que $m_i x = m_j x$ tendremos $(m_i - m_j) x = 0$; y luego el orden de x será menor que n, contra lo supuesto .

Así pues, si $a_i = a_j$ entonces $m_i x = m_j x$ y $m_i = m_j$. Luego $m_i y = m_j y$. Pero $m_i y = b_i$ y $m_j y = b_j$. Además $b_i = h(a_i)$ y $b_j = h(a_j)$

Por tanto, si $a_i = a_j$ tenemos que $h(a_i) = h(a_j)$.

Sea ahora $h(a_i) = h(a_j)$. Entonces $h(m_i x) = h(m_j x)$ lo que equivale a $m_i h(x) = m_j h(x)$ y esto a $m_i y = m_j y$ de donde $m_i = m_j$. Luego, $m_i x = m_j x$ y por tanto $a_i = a_j$.

De este modo hemos probado que dos grupos cíclicos de orden n son isomorfos .

Probando ahora el teorema siguiente, habremos probado que la teoría de grupos es α-categórica cuando α es un número primo .

Teorema : Todo grupo de orden primo es cíclico .

Prueba : Sea $\mathcal{A}$ un grupo de orden primo p .

El teorema de Lagrange de la teoría de grupos dice :
El orden de un grupo finito $\mathcal{A}$ es múltiplo del orden de cualquiera de sus subgrupos.

Prescindimos aquí de su demostración, la cual puede encontrarse en la mayoría de los tratados de álgebra o de teoría de grupos. (véase, por ejemplo, G. Birkhoff-S. Maclane: "Algebra moderna". Pág. 152)

Sea $\mathcal{A}_0$ un subgrupo de $\mathcal{A}$ engendrado por un elemento a $\in \mathcal{A}$ distinto de 0.
$\mathcal{A}_0$ será cíclico, y según el teorema de Lagrange, el orden de $\mathcal{A}_0$ será un divisor del orden de $\mathcal{A}$.
Pero el orden de $\mathcal{A}$ es primo y por tanto sólo es divisible por sí mismo o por la unidad.
Luego $\mathcal{A}_0$ será de orden p , ya que en $\mathcal{A}_0$ hay como mínimo dos elementos : 0 y a . Luego, $\mathcal{A}_0 = \mathcal{A}$. Puesto que $\mathcal{A}_0$ es cíclico, también lo es $\mathcal{A}$.

Probadas las dos proposiciones anteriores, queda automáticamente probada la proposición inicial :

Proposición :La teoría de grupos es α-categórica cuando α es un número primo

(Claramente todos estos grupos son abelianos. Véanse los teoremas de las páginas 69-70).

Pero no son éstos los únicos grupos finitos en cuyas cardinalidades la teoría de grupos es categórica. Efectivamente :

Sea por ejemplo un grupo $\mathcal{G}$ de cardinalidad n, donde $n \in \mathbb{N}$.

Sea $n = pq$, donde p y q son números primos y $p < q$.

Llamamos p-grupo a un grupo finito cuyo orden es una potencia de p (es decir, p^n para cierto $n \geqslant 0$)

Sea $\mathcal{G}$ un grupo finito y H un subgrupo de $\mathcal{G}$. Llamaremos a H un p-subgrupo de $\mathcal{G}$ si y sólo si H es un p-grupo.

Diremos que H es un p-subgrupo de Sylow si el orden de H es p^n y si p^n es la mayor potencia de p que divide al orden de $\mathcal{G}$.

Un conocido teorema de la teoría de grupos, (Sylow) , establece que : " Si $\mathcal{G}$ es un grupo finito y p un número primo que divide el orden de $\mathcal{G}$, entonces existe un p-subgrupo de Sylow de $\mathcal{G}$ " Además, " el número de p-subgrupos de Sylow de un grupo $\mathcal{G}$ es congruente con 1 , módulo p , y divide al orden de $\mathcal{G}$". (Véase, por ejemplo, Lang : "Algebra" Pág. 26).

Luego, puesto que p divide al orden de $\mathcal{G}$ y q divide al orden de $\mathcal{G}$ y p y q son primos , existirá un p-subrupo de Sylow y un q-subgrupo de Sylow de $\mathcal{G}$.

Además, dado que p y q son primos y $pq = n$, un p-subgrupo de Sylow de $\mathcal{G}$ será de orden p y será por tanto cíclico. Y lo mismo ocurrirá con q .

Sea m el número de p-subgrupos de Sylow de $\mathscr{A}$. Luego, de acuerdo con la segunda parte del teorema anterior, $m \equiv 1 \pmod p$. Eso es $m = kp + 1$ para algún $k \in \omega$. Además, m dividirá a pq.

Pueden ocurrir sólo dos cosas: o bien $m = 1$, o bien $m = q$.

Supongamos que $m = 1$. Eso es, que $q \not\equiv 1 \pmod p$. Sea entonces H_p el <u>único</u> p-subgrupo de Sylow de $\mathscr{A}$. Puesto que $p < q$, sólo puede darse el caso de que el número de q-subgrupos de Sylow de $\mathscr{A}$ sea igual a 1. Sea éste H_q.

Definimos ahora el producto directo de dos grupos finitos $G_1 \times G_2$ de la manera siguiente:

Sea $G = G_1 \times G_2$

G estará formado por los pares ordenados $\langle g_i , g_j \rangle$ donde $g_i \in G_1$ y $g_j \in G_2$, entre los que se define una operación $*$ tal que:

$$\langle g_i , g_j \rangle * \langle g_k , g_l \rangle = \langle g_i * g_k , g_j * g_l \rangle$$

Claramente $*$ es asociativa. Si e es el elemento neutro de G_1 y e' es el elemento neutro de G_2, el par $\langle e , e' \rangle$ es el elemento neutro de G. Si g_i^{-1} es el simétrico de g_i y g_j^{-1} es el simétrico de g_j, entonces $\langle g_i^{-1} , g_j^{-1} \rangle$ es el simétrico de $\langle g_i , g_j \rangle$. Evidentemente, $\langle G , * \rangle$, es un grupo. Además,

$$|G| = |G_1| \cdot |G_2|$$

Sea ahora $H_p \times H_q$; el grupo resultante será de cardinalidad $pq = n$.

Sabemos por la teoría de grupos que: " Si m y n son primos entre sí, el producto directo de dos grupos cíclicos de órdenes m y n es también un grupo cíclico de orden mn ". (Véase , por ejemplo , G.Birkhoff - S. Maclane "Algebra Moderna " Pág. 161)

Luego el grupo producto $H_p \times H_q$ es cíclico y es de orden n. Pero según el teorema ya demostrado de que dos grupos cíclicos de orden n son isomórficos , tenemos que dos grupos de orden n donde n = pq, siendo $q \not\equiv 1$ (mod. p) son isomorfos. Así pues, la teoría de grupos también es categórica en las cardinalidades n = pq donde $q \not\equiv 1$ (mod. p) .

Si $q \equiv 1$ (mod. p) , la teoría de grupos tiene exactamente dos modelos no-isomorfos de cardinalidad n=pq. Uno de ellos es abeliano y el otro no . (Véase por ejemplo : M.I.Kargapolov-Ju.I.Merzljakov:"Fundamentals of the Theory of Groups" Pág.68).

Si a la teoría de grupos le añadimos el axioma siguiente, obtenemos la teoría de grupos abelianos:

$$4\text{-} \quad \bigwedge xy \; (x + y = y + x)$$

Según lo apuntado en el parágrafo anterior, esta teoría será categórica en toda cardinalidad n tal que n = pq donde $q \equiv 1$ (mod. p) . Además de en las cardinalidades en las que es categórica la teoría de grupos, naturalmente. (Véase el Teorema 1 de la Pág. 70).

Añadiendo el axioma 5_p a la teoría de grupos abelianos, tenemos la teoría de grupos abelianos con todos sus elementos de orden p :

$$5_p\text{-} \quad \bigwedge x \; (px = 0)$$

Donde p es un número primo determinado .

Proposición: Dos grupos abelianos con todos sus elementos de orden p y de la misma cardinalidad son isomorfos.

Prueba : Definición : Sea $\mathcal{F}$ un cuerpo (Véase Pág. 47)
Un espacio vectorial $\mathcal{V}$ sobre $\mathcal{F}$ es un grupo abeliano junto con una operación $*$ de $\mathcal{F}$ sobre $\mathcal{V}$ tal que para todo $a,b \in F$ y todo $x,y \in V$, se cumple :

$$(a + b) * x = (a * x) + (b * x)$$

$$a * (x + y) = (a * x) + (a * y)$$

$$(a * b) * x = a * (b * x)$$

$$1 * x = x$$

Sea el grupo abeliano $G_0 = \langle \mathbb{Z}_p, + , 0 \rangle$. Veamos que G_0 es un espacio vectorial sobre el cuerpo $\mathcal{F} = \langle \mathbb{Z}_p, + ,., 0 \rangle$. (O lo que es lo mismo, que G_0 es un $\mathcal{F}$-espacio vectorial). Para ello tomemos $a * x = a.x$
Entonces:

$$(a + b).x = x.(a + b) = (x.a) + (x.b) = (a.x) + (b.x)$$

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

$$(a.b).x = a.(b.x)$$

$$1.x = x$$

pues $a,b,x,y, \in \mathbb{Z}_p$ y $\langle \mathbb{Z}_p, + ,., 0 \rangle$ es un cuerpo. (Véanse los axiomas de la página 47).

Definiremos a continuación los conceptos de: combinación lineal, independencia lineal, base, y suma directa de grupos (en este caso

Prueba : (continuación)

de espacios vectoriales sobre un cuerpo $\mathcal{F}$); los cuales son imprescindibles para continuar con la prueba.

Definición: Sea $S \subset F$. Una combinación lineal de elementos de S (con coeficientes en $\mathbb{Z}_p$) es una suma $\sum_{x \in S} a_x x$ donde $\{a_x\}$ es un conjunto de elementos de $\mathbb{Z}_p$.

Definición: Un subconjunto S de F es linealmente independiente (sobre $\mathcal{F}$) si siempre que se tenga una combinación lineal $\sum_{x \in S} a_x x = 0$, entonces $a_x = 0$ para todo x elemento de S.

Definición: Decimos que un subconjunto S de F es una base de F si $S \neq \emptyset$, S engendra F y S es linealmente independiente.
S engendra F si para todo $x \in F$, x es igual a una combinación lineal de los elementos de S. Si S engendra F diremos que S es un conjunto de generadores de F.

Definición: Si G es un grupo, la suma directa $\sum_{i \in I} G_i$ es el subgrupo de $\prod_{i \in I} G_i$ que consiste en todos los elementos $\langle x_i \rangle_{i \in I}$ donde $x_i \in G_i$ tales que $x_i = 0$ para todos menos un número finito de índices i . Aquí, $\prod_{i \in I} G_i$ denota el producto directo de grupos, eso es, los elementos del producto cartesiano de G_i .

Continuando con la prueba, sea ahora :

Prueba : (continuación)

$\mathcal{G} = \sum_{i \in I} (\mathbb{Z}_p)_i$ .Para cada i $\in$ I, $(\mathbb{Z}_p)_i = \mathbb{Z}_p$ considerado como $\mathcal{F}$ -espacio vectorial.

$\mathcal{G}$ admite una base formada por los elementos g_i de $\mathcal{G}$ cuya componente i-ésima es el elemento unidad de $\mathcal{F}$, eso es, el 1 ; y cuyas restantes componentes son iguales a 0. Claramente, la cardinalidad de dicha base es $|I|$. (Nótese que $\mathcal{G}$ es un grupo abeliano con todos sus elementos de orden p y además es un $\mathcal{F}$ -espacio vectorial).

Sea $\mathcal{G}' = \langle G', +', 0' \rangle$ un grupo abeliano con todos sus elementos de orden p . $\mathcal{G}'$ será un $\mathcal{F}$ -espacio vectorial . Para comprobarlo basta tomar a.x = x $+'$,..., $+'$ x (a veces) y tener en cuenta que $\mathcal{G}'$ por ser un grupo, satisface la propiedad asociativa.

$\mathcal{G}'$ tendrá una base, efectivamente :

En $\mathcal{G}'$ existe un conjunto no vacío de elementos linealmente independientes : evidentemente, pues para cualquier x $\in$ $\mathcal{G}'$ distinto de 0' y para cualquier a $\in$ $\mathbb{Z}_p$, a.x = 0' si y sólo si a = 0 , pues todo elemento de $\mathcal{G}'$ es de orden p y todo elemento de $\mathbb{Z}_p$ es menor que p . Sea P tal conjunto.

Sea $\mathcal{T}$ el conjunto cuyos elementos son subconjuntos T de G' que contienen a P y son linealmente independientes. Luego, $\mathcal{T}$ no es vacío y contiene a P.

Prueba : (continuación)

Si $\{T_i\}$ es un subconjunto de $\mathscr{C}$ linealmente ordenado por la relación de inclusión, $\bigcup T_i$ será también linealmente independiente y contendrá a P .

El lema de Zorn establece que : Si X es un conjunto no vacío de conjuntos en el cual ocurre que, si $\emptyset \neq Y \subset X$ y Y es un orden lineal, entonces $\bigcup Y \in X$; luego X tiene un elemento maximal.

Así pues, existirá un elemento maximal B en $\mathscr{C}$ (eso es, un elemento B tal que si $x \in \mathscr{C}$ y $x \geqslant B$, se sigue que $x = B$) tal que B será linealmente independiente.

Veamos que B genera G'. Efectivamente:

Sea G'_o el subconjunto de G' generado por B. Si $G'_o \neq G$ existirá un elemento $x \in G'$ tal que $x \notin G'_o$. Puesto que $x \notin G'_o$ y B engendra a G'_o , se sigue que $x \notin B$.

Luego, $B \cup \{x\}$ deberá ser linealmente independiente, pues dada una combinación lineal

$$\sum_{y\in B} a_y . y +' b.x = 0' \quad \text{donde } a_y , b \in \mathbb{Z}_p$$

deberá ser b = 0 , pues de lo contrario,

$$x = - \sum_{y\in B} b^{-1} . a_y . y$$

con lo que x sería igual a una combinación lineal de B y por tanto, $x \in G'_o$, contra lo supuesto. Así pues, $B \cup \{x\}$ es linealmente independiente. Pero esto es absurdo, pues B es maximal linealmente independiente.

Prueba : (continuación)

Se sigue entonces que $G'_0 = G'$. Luego, B es una base de G'.

Dicha base será de cardinalidad k, donde $|G'| = p^k$ en el caso de que G' sea finito; pues dado que todo elemento de G' es igual a una única combinación lineal de los elementos de su base y dado que tenemos p coeficientes distintos, tendremos tantos elementos en G' como posibles combinaciones con repetición de p elementos tomados de k en k . Eso es, p^k .

Por lo que respecta a G , también en el caso finito, $|G| = p^{|I|}$; pues en el caso finito, la suma directa y el producto directo coinciden. (Por definición).

Así pues, si G y G' son finitos, y si $|G| = |G'|$ tendremos que $p^{|I|} = p^k$ de donde, $|I| = k$.

Definición: Decimos que dos espacios vectoriales $\mathcal{V}_1$ y $\mathcal{V}_2$ tienen la misma dimensión si existen bases B_1 de $\mathcal{V}_1$ y B_2 de $\mathcal{V}_2$ tales que $|B_1| = |B_2|$. Escribimos dim $\mathcal{V}_1$ en lugar de "dimensión de $\mathcal{V}_1$ " .

Luego, en el caso finito, si $|G| = |G'|$ entonces dim G = dim G' .

Si $G = \sum_{i\in I} (\mathbb{Z}_p)_i$ es infinito, $|G| = |I| \cdot p$. De donde, si $|G| = \alpha \geq \omega$ entonces $|I| = \alpha \geq \omega$, pues p es finito.

Prueba : (continuación)

Por otra parte, si G' es infinito, la cardinalidad de su base debe ser infinita, pues sólo existe un número finito de coeficientes distintos. Luego, si $|G'| = \beta \geq \omega$, se sigue que $k = \beta \geq \omega$.

(Nótese que en el caso infinito $|G'| \neq p^k$ pues en caso contrario, $|G'| = p^{\beta \geq \omega}$ de donde $|G'| = \beta' \geq \omega_1$) .

Luego, si $|G| = |G'| = \alpha \geq \omega$, entonces $|I| = k = \alpha \geq \omega$. Así pues, también en el caso infinito, si $|G| = |G'|$ tenemos que $\dim G = \dim G'$.

Para ver que $G \cong G'$ bastará probar la siguiente proposición :

Proposición: Dos espacios vectoriales sobre un cuerpo $\mathcal{F}$, de la misma dimensión son isomorfos.

Prueba : Sea $\mathcal{F}$ un cuerpo y sean $\mathcal{V}$ y $\mathcal{V}'$ espacios vectoriales sobre $\mathcal{F}$. Sea I un conjunto no vacío y sean $\{x_i\}_{i\in I}$ y $\{y_i\}_{i\in I}$ bases de $\mathcal{V}$ y $\mathcal{V}'$ respectivamente. Entonces existe un isomorfismo $h: V \longrightarrow V'$ tal que $h(x_i) = y_i$ para todo $i \in I$.

Efectivamente, sea $x \in V$. Luego existe un único conjunto de elementos de F , $\{a_i\}_{i\in I}$ tales que :

$$x = \sum_{i\in I} a_i . x_i$$

Prueba : (continuación)

pues todo elemento de V es igual a una combinación lineal de los elementos de una base de V . Además esta combinación lineal es única, pues de lo contrario los elementos de la base no serían linealmente independientes.

Definimos $h(x) = \sum_{i \in I} a_i . x_i$

Sean $x, y \in V$ y sean $x = \sum_{i \in I} a_i . x_i$ y $y = \sum_{i \in I} a_i' . x_i$. Entonces,

$$h(x + y) = h\left(\sum_{i \in I} a_i . x_i + \sum_{i \in I} a_i' . x_i \right) =$$
$$= h\left(\sum_{i \in I} (a_i + a_i') . x_i \right) = \sum_{i \in I} (a_i + a_i') . y_i =$$
$$= \sum_{i \in I} a_i . y_i +' \sum_{i \in I} a_i' . y_i = h(x) +' h(y)$$

Claramente h es biyectiva, pues todo elemento de V es igual a una única combinación lineal de los elementos de una base de V . Y lo mismo ocurre con V' .

Se sigue, pues, que $\mathcal{V} \cong \mathcal{V}'$. Lo que queríamos probar.

Siguiendo con la prueba inicial, puesto que G y G' son espacios vectoriales de la misma dimensión siempre y cuando $|G| = |G'|$ se sigue que si $|G| = |G'|$ entonces $G \cong G'$.

Hemos probado ahora que $G \cong G'$ considerados como espacios vectoriales sobre $\mathcal{F}$. Pero, ¿ son también isomorfos considerados únicamente como grupos abelianos con todos sus elementos de orden p ?. Para comprobar que

Prueba : (continuación)

sí lo son, probaremos antes la siguiente proposición :

Proposición: Sea $\mathcal{V}$ un espacio vectorial sobre $\mathcal{F}$. Considerado $\mathcal{V}$ como un grupo abeliano, $\mathcal{V}$ es isomorfo a una suma directa de $|B|$ copias de $\mathcal{F}$. Siendo B una base de $\mathcal{V}$.

Prueba : Sea $B = \{ x_k : k \in K \}$ una base de $\mathcal{V}$. Sea $\mathcal{V}_k$ el subespacio generado por x_k . Los elementos de $\mathcal{V}_k$ serán de la forma $r.x_k$, donde $r \in \mathcal{F}$. Claramente $\mathcal{V}_k$ será isomorfo a $\mathcal{F}$. Bastará tomar $h(r.x_k) = r$.

Veamos que el grupo abeliano $\mathcal{V}$, eso es, el espacio vectorial $\mathcal{V}$ considerado únicamente como grupo abeliano, es isomorfo a:

$$\sum_{k \in K} \mathcal{V}_k$$

Puesto que B genera $\mathcal{V}$, cada elemento $v \in \mathcal{V}$ es igual a una combinación lineal de los elementos de B con coeficientes en $\mathcal{F}$. Y esta combinación lineal es única, pues B es linealmente independiente.

$$v = \sum_{k \in K} r_k . x_k$$

Pero cada $r_k . x_k \in \mathcal{V}_k$, y sólo a $\mathcal{V}_k$, para cada $k \in K$.

Luego, $\mathcal{V} = \sum_{k \in K} \mathcal{V}_k \cong \sum_{k \in K} \mathcal{F}_k$

Lo que queríamos probar.

Prueba : (continuación)

Ahora, puesto que G y G' son espacios vectoriales sobre $\mathcal{F}$, si consideramos G y G' como grupos abelianos con todos sus elementos de orden p , serán isomorfos a una suma directa de $|B_1|$ y $|B_2|$ copias de $\mathcal{F}$ respectivamente, donde B_1 es una base de G y B_2 una base de G'. Pero como ya hemos visto, $|B_1| = |B_2|$ siempre y cuando $|G| = |G'|$. Por tanto, si $|B_1| = |B_2| = k$ tendremos que $G \cong \sum_{k \in K} \mathcal{F}_k$ y $G' \cong \sum_{k \in K} \mathcal{F}_k$ De donde $G \cong G'$ considerados como grupos abelianos.

Así pues, queda probada la proposición inicial: dos grupos abelianos con todos sus elementos de orden p y de la misma cardinalidad son isomorfos. De donde se sigue que la teoría de grupos abelianos con todos sus elementos de orden p es α-categórica para todo α . (Suponiendo que exista algún modelo de cardinalidad α , naturalmente).

Al añadir a los axiomas de la teoría de grupos abelianos los dos axiomas siguientes, se obtiene la teoría de grupos abelianos divisibles con todos sus elementos de orden ∞ (o también, la teoría de grupos abelianos divisibles sin torsión) .

5- $\bigwedge x \; (x \neq 0 \longrightarrow nx \neq 0)$ para cada $n \geqslant 1$

6- $\bigwedge x \bigvee y \; (ny = x)$ para cada $n \geqslant 1$

Proposición: La teoría de grupos abelianos divisibles sin torsión es α-categórica para todo α no-numerable.

Prueba : Sea el grupo abeliano divisible y sin torsión $G_0 = \langle \mathbb{Q}, +, 0 \rangle$

G_0 es un espacio vectorial sobre el cuerpo conmutativo $\mathcal{F} = \langle \mathbb{Q}, +, ., 0 \rangle$.

Efectivamente :

Sean a,b $\in \mathcal{F}$ y sean x,y $\in G_0$.

Tomemos $a * x = a.x$. Entonces:

$(a + b).x = x.(a + b) = (x.a) + (x.b) =$

$= (a.x) + (b.x)$

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

$(a.b).x = a.(b.x)$

$1.x = x$

pues a.b.x.y $\in \mathbb{Q}$ y $\langle \mathbb{Q}, +, ., 0 \rangle$ es un cuerpo. (Véanse los axiomas de la página 47).

Sea $G = \sum_{i \in I} \mathbb{Q}_i$ donde $\mathbb{Q}_i = \mathbb{Q}$, para cada $\mathbb{Q}$, considerado como $\mathcal{F}$-espacio vectorial.

G admite una base formada por los elementos $x_i \in G$ cuya componente i-ésima es el elemento unidad de $\mathcal{F}$, eso es, el 1; y cuyas restantes componentes son iguales a 0. La cardinalidad de dicha base es evidentemente $|I|$. (Nótese que G es un grupo

Prueba : (continuación)

abeliano divisible sin torsión y que además es un $\mathcal{F}$ -espacio vectorial).

Sea ahora G' un grupo abeliano divisible sin torsión cualquiera. Entonces G' es un $\mathcal{F}$ -espacio vectorial . Efectivamente:

Bastará tomar $a * x \doteq a.x$
Puesto que $a \in \mathbb{Q}$, a será de la forma a_1/a_2 para $a_1, a_2 \in \mathbb{Z}$. E igualmente, si $b \in \mathbb{Q}$ tendremos que $b = b_1/b_2$ para algún $b_1, b_2 \in \mathbb{Z}$. Luego,

$(a + b).x = (a_1/a_2 + b_1/b_2).x = ((a_1.b_2 + a_2.b_1)/a_2.b_2).x = (a_1.b_2.x + a_2.b_1.x)/a_2.b_2 = (a_1.x/a_2) + (b_1.x/b_2) = (a.x)$
$(b.x)$

$a.(x + y) = (a_1/a_2).(x + y) = (a_1.x + a_1.y)/a_2 = (a_1.x/a_2) + (a_1.y/a_2) = (a.x) + (a.y)$

$(a.b).x = (a_1.b_1.x/a_2.b_2) = (a_1/a_2).((b_1/b_2).x) = a.(b.x)$

$1.x = x$

Pues $a_1, a_2, b_1, b_2, 1 \in \mathbb{Z}$ y $\langle \mathbb{Z} , + , . , 0 \rangle$ es un cuerpo conmutativo.

G' tendrá una base. Efectivamente:

En G' existe un conjunto de elementos linealmente independientes , pues para cada $x \in G'$ distinto de $0'$ y para cualquier $a \in \mathbb{Q}$, $a.x = 0'$ si y sólo si $a = 0$;

Prueba : (continuación)

pues x es de orden ∞ . Sea P tal conjunto.

A partir de aquí , la prueba es análoga a la realizada al tratar de grupos abelianos con todos sus elementos de orden p. (Véase la página 36). Luego, G' tendrá una base.

Puesto que G' es divisible, para cada $x \in G'$ existen ω elementos $y_i : i \in \omega$, distintos, de G' tales que $n_i . y_i = x$. Es claro que existen ω de tales elementos, pues si $n_i \neq n_j$ y $n_i . y = x$, entonces $n_j . y \neq x$; para un x y un y determinados; ya que si, por ejemplo, $n_i \leq n_j$, $(n_j - n_i) . y = 0'$ con lo cual, y, sería de orden finito.

Luego, la cardinalidad de la base de G' será igual a k , donde $|G'| = k . \omega$.

Puesto que todos los modelos de la teoría de grupos abelianos divisibles sin torsión son infinitos, la cardinalidad de G y de G' deberá ser mayor o igual a ω .

Sea $|G| = |G'| = \omega$. Entonces, tanto k como $|I|$ pueden tener cualquier valor menor o igual a ω . Pues $|G| = |I| . \omega$ y $|G'| = k . \omega$.

Por tanto, si B_1 es una base de G y B_2 es una base de G' y si $|G| = |G'| = \omega$ entonces, no necesariamente $|B_1| = |B_2|$.

Si $|G| = |G'| \geq \omega_1$ se sigue que $k \geq \omega_1$ y que $|I| \geq \omega_1$ pues $|G| = |I| . \omega$ y

Prueba : (continuación)

y $|G'| = k.\,\omega$ de donde tenemos que si $|G| = |G'| \geq \omega_1$,entonces necesariamente $|B_1| = |B_2|$. Donde B_1 es una base de G y B_2 es una base de G' . Luego, dim G = dim G' .

Aplicando ahora el teorema ya demostrado (Véase la página 39) que dice que : dos espacios vectoriales sobre un cuerpo $\mathcal{F}$, de la misma dimensión son isomorfos; tendremos que $G \cong G'$.

Pero teniendo en cuenta ahora que todo espacio vectorial $\mathcal{V}$ sobre un cuerpo $\mathcal{F}$, considerando $\mathcal{V}$ como grupo abeliano es isomorfo a una suma directa de $|B|$ copias de $\mathcal{F}$, siendo B una base de $\mathcal{V}$ (Véase la página 41) ; tenemos que :

$$G \cong \sum_{k \in K} \mathcal{F}_k \quad \text{y} \quad G' \cong \sum_{k' \in K'} \mathcal{F}_{k'}$$

Pero como dim G = dim G' , tenemos que K = K' y entonces $G \cong G'$ considerados como grupos abelianos divisibles sin torsión. Con lo que queda probado que la teoría de grupos abelianos divisibles sin torsión es α -categórica para todo α no numerable.

Sea $\mathcal{L}: \{+ , . , 0 , 1\}$ un lenguaje de primer orden donde $+$ y $.$ son functores binarios y 0,1 son constantes individuales. Escribimos $x + y$ en lugar de $+ xy$ y $x.y$ en lugar de $.xy$. Los axiomas de la teoría de cuerpos son los siguientes:

1- $\bigwedge xyz\ (x + (y + z) = (x + y) + z)$
2- $\bigwedge x\ (x + 0 = x \land 0 + x = x)$
3- $\bigwedge x \bigvee y\ (x + y = 0 \land y + x = 0)$
4- $\bigwedge xy\ (x + y = y + x)$

Hasta aquí tenemos los axiomas de la teoría de grupos abelianos.

5- $\bigwedge xyz\ (x . (y . z) = (x . y) . z)$
6- $\bigwedge xyz\ (x . (y + z) = (x . y) + (x . z))$
7- $\bigwedge xy\ (x . y = y . x)$

Y hasta aquí los axiomas de la teoría de anillos conmutativos, los cuales, junto con el axioma siguiente, forman los axiomas de la teoría de anillos conmutativos con elemento unidad.

8- $\bigwedge x\ (1 . x = x \land x . 1 = x)$

Añadiendo el axioma 9 obtenemos la teoría de Dominios de integridad .

9- $\bigwedge xy\ (x . y = 0 \longrightarrow x = 0 \lor y = 0)$

Para tener los axiomas de la teoría de cuerpos debemos añadir aún dos axiomas más :

10- $0 \neq 1$
11- $\bigwedge x\ (x \neq 0 \longrightarrow \bigvee y\ (y . x = 1))$

Si para un número primo determinado p , añadimos el axioma siguiente, obtendremos la teoría de cuerpos de característica p :

12- $p1 = 0$

Donde $p1 = 1 + (1 + (1 + 1)\ldots\ldots)$ p veces.

Si en lugar del axioma 12 y para todo número primo p añadimos la negación de dicho axioma,

13- $p1 \neq 0$

obtenemos la teoría de cuerpos de carcterística 0. Nótese que 13 es en realidad un conjunto infinito de axiomas, uno para cada p.

Un cuerpo algebraico cerrado de característica 0 (o de característica p) es un modelo de los axiomas 1-12 (o 1-11 y 13) y además del axioma siguiente:

14- $\bigvee y\ (x_n \cdot y^n + x_{n-1} \cdot y^{n-1}, \ldots, + x_1 \cdot y + x_0 = 0\ ) \vee x_n = 0$

Donde $x^n = x \cdot (x \cdot (x \cdot x)\ldots\ldots)$ n veces

Nótese que también el axioma 14 es en realidad un conjunto infinito de axiomas, uno para cada $n \geqslant 1$. (Véase la Nota 2)

Vamos a probar a continuación que la teoría de cuerpos algebraicos cerrados de característica p (o 0) es α-categórica en cada cardinalidad α no numerable. Bastará probar la siguiente proposición.

Proposición : Dos cuerpos algebraicos cerrados no-numerables de la misma característica (0 o p) y cardinalidad son isomorfos.

Prueba : Definición: Decimos que K' es un cuerpo extensión de un cuerpo K si y sólo si:

i) $K \subseteq K'$

ii) K' es un cuerpo.

Definición: Sea K' un cuerpo extensión de un cuerpo K . Sea S un subconjunto de K'. S será algebraicamente independiente sobre K si y sólo si, si siempre que tengamos:

$$\sum_{r_1 \ldots r_n \geq 0} a_{r_1 \ldots r_n} \, x_1^{r_1} \ldots\ldots x_n^{r_n} = 0$$

entonces, todos los $a_{r_1 \ldots r_n} = 0$. Donde $r_1 \ldots r_n \in \mathbb{N}$ y casi todos son iguales a 0 , esto es, lo son todos excepto un número finito de ellos. $x_1 \ldots x_n \in S$ y $a_{r_1 \ldots r_n} \in K$.

Definición :Sea K' un cuerpo extensión de K. Sean $S_1 \ldots\ldots S_i$ conjuntos de elementos de K' algebraicamente independientes sobre K. Si los ordenamos por medio de la relación $\subseteq$, obtendremos sucesiones $S_j \subseteq, \ldots, \subseteq S_k \subseteq \ldots$ las cuales, según el Lema de Zorn, tendrán elementos maximales . Sea S_m uno de tales elementos. Si la cardinalidad de S_m es la mayor entre las cardinalidades de dichos elementos, diremos que $|S_m|$ es el grado de trascendencia de K' sobre K.

Definición: S es una base de trascendencia de K' sobre K si y sólo si S es un subconjunto de K' algebraicamente independiente

Prueba : (continuación)

sobre K y maximal respecto $\subseteq$.

Todo cuerpo K' algebraicamente cerrado de característica 0 y no-numerable, tiene un subcuerpo K de cardinalidad ω . Esto es, existe un cuerpo de cardinalidad ω tal que K' es una extensión de él. Efectivamente, tomemos el 0 y el 1 y todos los elementos resultantes de sumar n veces 1, donde $n \in \omega$. Añadamos a éstos los elementos inversos respecto $+$ y . . Claramente tendremos ω elementos que formarán un subcuerpo de K'. Sea éste K . Evidentemente, $K \cong \mathbb{Q}$.

Lo mismo ocurre con los cuerpos K' algebraicamente cerrados de característica p y no-numerables. Estos tienen un subcuerpo K de cardinalidad p . En efecto, tomemos el 1 y los elementos resultantes de sumar el 1 n veces, donde $n \leqslant p$. Tendremos p elementos, pues K' es de característica p. Cada elemento tendrá un inverso respecto $+$ y . . Claramente, estos p elementos forman un subcuerpo K de K' . Evidentemente, $K \cong \mathbb{Z}_p$.

Por tanto, todo cuerpo K' algebraicamente cerrado de característica 0 o p y de cardinalidad no-numerable, es un cuerpo extensión de un cuerpo K numerable . $K \cong \mathbb{Q}$ para los cuerpos de característica 0 y $K \cong \mathbb{Z}_p$ para los cuerpos de característica p .

El teorema siguiente es un resultado clásico de la teoría de cuerpos, el cual es necesario para continuar con la prueba:

Prueba : (continuación)

Teorema : Sea K' una extensión de un cuerpo K. Dos bases de trascendencia de K' sobre K tienen el mismo cardinal. Si Γ es un conjunto de generadores de K' sobre K (es decir, $K' = K(\Gamma)$) y S es un subconjunto de algebraicamente independiente sobre K, existe una base de trascendencia B de K' sobre K tal que $S \subset B \subset \Gamma$.

Prueba : (Véase Lang :"Algebra". Pág. 302)

Según el teorema anterior, K' tiene una base de trascendencia sobre K y dadas dos bases de trascendencia cualesquiera, éstas tienen la misma cardinalidad.

Veamos ahora que si tenemos dos cuerpos algebraicamente cerrados de característica 0 o p y de cardinalidad α no-numerable, su grado de trascendencia sobre un subcuerpo numerable es α no-numerable.

Efectivamente, sean K_0' y K_1' cuerpos algebraicos cerrados de característica 0 o p y sean S_0 y S_1 sus respectivas bases de trascendencia sobre los subcuerpos K_0 y K_1. Luego, $|K_0'| = |K_0| \cdot |S_0|$ y $|K_1'| = |K_1| \cdot |S_1|$ pues cada elemento de K_0' y K_1' es igual a una única combinación algebraica de S_0 y S_1 respectivamente con coeficientes en K_0 y K_1, respectivamente. Entonces, si $|K_0'| = \omega_{i \geq 1}$, se sigue que $|S_0| = \omega_{i \geq 1}$ pues K_0 es numerable. Igualmente, si $|K_1'| = \omega_{i \geq 1}$, $|S_1| = \omega_{i \geq 1}$, pues K_1 es numerable. Por tanto, si $|K_0'| = |K_1'| = \omega_{i \geq 1}$, entonces $|S_0| = |S_1| = \omega_{i \geq 1}$.

Para probar la proposición inicial, bastará probar ahora el lema siguiente:

Prueba : (continuación)

Lema : Si dos cuerpos K'_0 y K'_1 tienen el mismo grado de trascendencia sobre dos cuerpos K_0 y K_1 de los cuales son extensiones y si $K_0 \cong K_1$, entonces $K'_0 \cong K'_1$.

Prueba : Sean S_0 y S_0 bases de trascendencia de K'_0 y K'_1 respectivamente. Sea $|S_0| = |S_1|$ y Sea $S = \{x_1 \ldots x_i\}$ y $S_1 = \{y_1 \ldots y_i\}$
Sea $h: K'_0 \longrightarrow K'_1$ tal que si:

$$x = \sum_{r_1 \ldots r_i \geq 0} a_{r_1 \ldots r_i} x_1^{r_1} \ldots\ldots x_i^{r_i} \quad , \quad \text{entonces}$$

$$h(x) = \sum_{r_1 \ldots r_i \geq 0} a_{r_1 \ldots r_i} y_1^{r_1} \ldots\ldots y_i^{r_i}$$

Claramente h es un isomorfismo entre K'_0 y K'_1 . En efecto,

Sea $x = \sum_{r_1 \ldots r_i \geq 0} a_{r_1 \ldots r_i} x_1^{r_1} \ldots\ldots x_i^{r_i}$ y sea

$y = \sum_{r_1 \ldots r_i \geq 0} a'_{r_1 \ldots r_i} x_1^{r_1} \ldots\ldots x_i^{r_i}$. Entonces,

$$\begin{aligned} h(x+y) &= h\Big(\Big(\sum_{r_1 \ldots r_i \geq 0} a_{r_1 \ldots r_i} x_1^{r_1} \ldots\ldots x_i^{r_i}\Big) + \\ &\Big(\sum_{r_1 \ldots r_i \geq 0} a'_{r_1 \ldots r_i} x_1^{r_1} \ldots\ldots x_i^{r_i}\Big)\Big) = \\ &= h\Big(\sum_{r_1 \ldots r_i \geq 0} (a_{r_1 \ldots r_i} + a'_{r_1 \ldots r_i}) x_1^{r_1} \ldots\ldots x_i^{r_i}\Big) = \\ &= \sum_{r_1 \ldots r_i \geq 0} (a_{r_1 \ldots r_i} + a'_{r_1 \ldots r_i}) y_1^{r_1} \ldots\ldots y_i^{r_i} = \\ &= \sum_{r_1 \ldots r_i \geq 0} a_{r_1 \ldots r_i} y_1^{r_1} \ldots\ldots y_i^{r_i} + \sum_{r_1 \ldots r_i \geq 0} a'_{r_1 \ldots r_i} \\ &y_1^{r_1} \ldots\ldots y_i^{r_i} = h(x) + h(y) \end{aligned}$$

Análogamente con $h(x.y)$.

Además, h es biyectiva, pues $x = y$ si y sólo si $h(x) = h(y)$, dado que todo elemento de K'_0 es igual a una única combinación algebraica de S_0 y lo mismo con K'_1 . Así pues, $h: K'_0 \cong K'_1$. Con lo que queda probada la proposición inicial.

Sea $\mathscr{L} = \{ \wedge , \vee , ^{-} , 0 , 1 \}$ un lenguaje de primer orden donde $\wedge$ y $\vee$ son functores binarios, $^{-}$ es un functor monario y 0 y 1 son constantes individuales. Escribimos $x \wedge y$ en lugar de $\wedge xy$, $x \vee y$ en lugar de $\vee xy$ y $\bar{x}$ en lugar de $-x$. La teoría de Algebras de Boole tiene los axiomas siguientes:

1- $\bigwedge xyz\ (x \wedge (y \wedge z) = (x \wedge y) \wedge z)$

2- $\bigwedge xyz\ (x \vee (y \vee z) = (x \vee y) \vee z)$

3- $\bigwedge xy\ (x \wedge y) = (y \wedge x)$

4- $\bigwedge xy\ (x \vee y) = (y \vee x)$

5- $\bigwedge x\ (x \wedge x) = x$

6- $\bigwedge x\ (x \vee x) = x$

7- $\bigwedge xyz\ (x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

8- $\bigwedge xyz\ (x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

9- $\bigwedge xy\ (x \wedge (x \vee y) = x)$

10- $\bigwedge xy\ (x \vee (x \wedge y) = x)$

11- $\bigwedge xy\ (\overline{(x \wedge y)} = \bar{x} \vee \bar{y})$

12- $\bigwedge xy\ (\overline{(x \vee y)} = \bar{x} \wedge \bar{y})$

13- $\bigwedge x\ (x \vee 0 = x)$

14- $\bigwedge x\ (x \wedge 0 = 0)$

15- $\bigwedge x\ (x \vee 1 = 1)$

16- $\bigwedge x\ (x \wedge 1 = x)$

17- $0 \neq 1$

18- $\bigwedge x\ (x \vee \bar{x} = 1)$

19- $\bigwedge x\ (x \wedge \bar{x} = 0)$

20- $\bigwedge x\ (\bar{\bar{x}} = x)$

De hecho, sólo con los axiomas:3,4,7,8,13,16,18 y 19 sería suficiente,pues son independientes(Huntington,1904) y los demás puedendeducirse de ellos.

Proposición: La teoría de Algebras de Boole es α-categórica en cada cardinalidad α finita.

Prueba: Definición: Un elemento a de un álgebra de Boole $\mathcal{B}$ es un átomo si y sólo si $a \neq 0$ y si $b \in B$ y $b \leq a$ (donde escribimos $b \leq a$ en lugar de $b \wedge a = b$) se sigue que $b = 0$ o bien $b = a$.

Definición: Decimos que un álgebra de Boole es atómica si y sólo si para cada elemento $b \in B$ distinto de 0 existe un átomo $a \in B$ tal que $a \leq b$.

Probemos ahora la siguiente proposición:

Proposición: Si $\mathcal{B}$ es un álgebra de Boole finita, entonces $\mathcal{B}$ es atómica.

Prueba: Sea $\mathcal{B}$ un álgebra de Boole finita no atómica. Luego, $|\mathcal{B}| = m$ para algún $m < \omega$. Sea ahora una función h: $\mathcal{P}(B) - \{0\} \longrightarrow B$ tal que para todo $X \subseteq B$, $h(X) \in X$.
Dado que $\mathcal{B}$ no es atómica, existirá un elemento $b \in B$ distinto de 0 para el cual no existe ningún átomo $a \in B$ tal que $a \leq b$.
Sea la función f: $\mathbb{N} \longrightarrow B$ tal que $f(0) = b$ y $f(n+1) = h(\{X \in B - \{0\} : X < f(n)\})$.
Luego, como para todo X, $h(X) \in X$ y b no tiene átomos menores que b, se sigue que para todo $m,n \in \mathbb{N}$ $m \neq n$, $f(m) \neq f(n)$, lo que es imposible, pues B sólo tiene m elementos.

Probaremos a continuación que toda álgebra de Boole finita es isomórfica al álgebra de todos los subconjuntos del conjunto de sus átomos.

Teorema : Sea $\mathcal{B}$ un álgebra de Boole finita y sea A el conjunto de los átomos de $\mathcal{B}$. Luego, $\mathcal{B}$ es isomórfica al álgebra $\mathcal{A} = \langle \mathcal{P}(A), \cap, \cup, ', 0, 1 \rangle$. ($\cap$, $\cup$, y ' son respectivamente la intersección, la unión y "el complementario de" de la teoría de conjuntos; $0 = \emptyset$ y $1 = \mathcal{P}(A)$.) Utilizamos los símbolos $\cap$, $\cup$, ' , en lugar de los habituales $\wedge$, $\vee$, $^{-}$, por comodidad.

Prueba : Probaremos previamente cinco lemas (a)-(e).

(a) Si a es un átomo y $x \in B$, entonces, o bien $a \leq x$ o bien $a \cap x = 0$.

Prueba : Puesto que $a \cap x \leq a$, se sigue que o bien $a \cap x = a$ o bien $a \cap x = 0$. Ambos no pueden ser ciertos, pues $a \neq 0$.

(b) Para todo $x \in B$, sea $A(x)$ el conjunto de todos los átomos de B tales que $a \leq x$. Luego, $A(x \cap y) = A(x) \cap A(y)$ para todo $x,y \in B$.

Prueba : Supongamos que $a \in A(x \cap y)$. Luego, $a \leq x \cap y$ y por tanto, $a \leq x$ y $a \leq y$. Con lo que $a \in A(x) \cap A(y)$. Así pues, $A(x \cap y) \subseteq A(x) \cap A(y)$. Procediendo exactamente a la inversa tendremos que $A(x) \cap A(y) \subseteq A(x \cap y)$.

(c) $A(x') = A(1) - A(x)$

Prueba : $A(1)$ es el conjunto de todos los átomos de B.
Supongamos que $a \in A(x')$. Luego, por (a) tenemos que $a \notin A(x)$. Así pues, $a \in A(1) - A(x)$.
Por otra parte, si $a \in A(1) - A(x)$, luego

Prueba : (continuación)

$a \notin A(x)$; y por (a), $a \in A(x')$.

(d) $A(x) = A(y)$ si y sólo si $x = y$.

Prueba : Sea $x \neq y$. Luego, o bien $x \leq y$ o bien $y \leq x$ o bien los dos, serán falsos. Sea $x \not\leq y$. Entonces $x \cap y' \neq 0$. Luego, puesto que $\mathcal{B}$ es atómica, existe un átomo $a \leq x \cap y'$. Por (b) tenemos que $a \in A(x)$ y $a \in A(y')$. Entonces, $a \in A(x)$ y por (c) , $a \notin A(y)$. Luego, $A(x) \neq A\ y)$. (Análogamente si es el caso que $y \not\leq x$).

(e) Si $a_1, a_2, \ldots, a_i$ son átomos distintos, $A(a_1 \cup a_2 \cup, \ldots, \cup a_i) = \{a_1, a_2, \ldots, a_i\}$.

Prueba : Evidentemente $\{a_1, a_2, \ldots, a_i\} \subset$ $\subset A(a_1 \cup a_2 \cup, \ldots, \cup a_i)$.
Sea $a \in A(a_1 \cup a_2 \cup, \ldots, \cup a_i)$ y $a \neq a_i$ para todo i . Luego, por (a) , $a \cap a_i = 0$ para todo i ; y entonces, $a = a \cap (a_1 \cup$ $\cup a_2 \cup, \ldots, \cup a_i) = (a \cap a_1) \cup (a \cap a_2) \cup$ $\cup, \ldots, \cup (a \cap a_i) = 0$. Lo que es absurdo.

Sea ahora $h : B \longrightarrow \mathcal{P}(A)$ tal que $h(x) = A(x)$.

h es biyectiva, por (d) y (e).

(Puesto que $x \cup y = (x' \cap y')'$, basta sólo comprobar que h es un isomorfismo para $\cap$ y $'$).

Prueba : (continuación)

Por (b) , $h(x \cap y) = h(x) \cap h(y)$

y por (c) , $h(x') = (h(x))'$

Luego, h es un isomorfismo entre $\mathcal{B}$ y $\mathcal{A}$.

Nótese que si $\mathcal{B}$ es de cardinalidad n, el número de átomos de $\mathcal{B}$ es m, donde $n = 2^m$

Para probar el teorema inicial falta sólo demostrar que si $\mathcal{B}'$ es un álgebra de Boole de la misma cardinalidad de $\mathcal{B}$, sea ésta n , entonces $\mathcal{A} \cong \mathcal{A}'$ donde $\mathcal{A}' = \langle \mathcal{P}(A'), \cap , \cup , ' , 0, 1' \rangle$ y donde A' es el conjunto de los átomos de $\mathcal{B}'$.

Puesto que $|B| = |B'| = n$, $|A| = |A'| = m$, donde $n = 2^m$.

Sean $\{a_i : i \in m\}$ y $\{a'_i : i \in m\}$ enumeraciones de A y A' respectivamente.

Sea $f(a_i) = a'_i$

Sean m_0 y m_1 subconjuntos de m cualqesquiera. Luego, los elementos de $\mathcal{P}(A)$ serán de la forma $\{a_j\}_{j \in m_0}$.

Claramente, $\{a_j\}_{j \in m_0} \cap \{a_l\}_{l \in m_1} = \{a_k\}_{k \in m_0 \cap m_1}$. Igualmente para $\mathcal{P}(A')$.

Sea $h: \mathcal{P}(A) \longrightarrow \mathcal{P}(A')$ tal que :

$h(\{a_j\}_{j \in m_0}) = \{a'_j\}_{j \in m_0}$

Claramente h es biyectiva, pues f lo es. Además,

$$h(\{a_j\}_{j\in m_0} \cap \{a_\ell\}_{\ell\in m_1}) = h(\{a_k\}_{k\in m_0\cap m_1}) =$$

$$= \{a'_k\}_{k\in m_0\cap m_1} = \{a'_j\}_{j\in m_0} \cap \{a'_\ell\}_{\ell\in m_1} =$$

$$= h(\{a_j\}_{j\in m_0}) \cap h(\{a_\ell\}_{\ell\in m_1})$$

Y también, $h(\{a_j\}'_{j\in m_0}) = \{a'_j\}'_{j\in m_0} = \{a'_i\}_{i\in m} -$

$- \{a'_j\}_{j\in m_0} = h(\{a_i\}_{i\in m}) - h(\{a_j\}_{j\in m_0}) =$

$= (h(\{a_j\}_{j\in m_0}))'$

Así pues, h es un isomorfismo entre $\mathcal{A}$ y $\mathcal{A}'$. Con lo que queda probado el teorema inicial.

Si a la teoría de Algebras de Boole le añadimos el axioma siguiente, obtenemos la teoría de Algebras de Boole sin átomos:

$$21\text{-}\quad \neg \bigvee y\ (0 \neq y \wedge \bigwedge z\ (z \leq y \longrightarrow z = 0 \vee z = y))$$

Todos sus modelos son infinitos. (Véase la pág. 63). Como veremos, esta teoría es ω-categórica.

Proposición : La teoría de Algebras de Boole sin átomos es ω-categórica.

Prueba : Definición: Sean $\mathcal{A}$ y $\mathcal{B}$ álgebras de Boole sin átomos y numerables. Sean $A_0 \subset A$ y $B_0 \subset B$.

Diremos que una función $f: A_0 \longrightarrow B_0$ es un isomorfismo parcial entre $\mathcal{A}$ y $\mathcal{B}$ si y

Prueba : (continuación)

sólo si :

i) f es biyectiva

ii) Para cualesquiera $a_0, a_1 \in A$, ocurre:

$$f(a_0 \wedge a_1) = f(a_0) \wedge' f(a_1)$$

$$f(\bar{a}_0) = \overline{(f(a_0))}'$$

Definición: Decimos que $\mathcal{A}_0$ es una subálgebra de Boole de un álgebra de Boole $\mathcal{A}$ si y sólo si :

i) $\mathcal{A}_0 \sqsubseteq \mathcal{A}$

ii) $\mathcal{A}_0$ es un álgebra de Boole.

Supongamos ahora que tuviéramos una sucesión de isomorfismos parciales $\langle f_u : u \in \omega \rangle$ entre $\mathcal{A}$ y $\mathcal{B}$ tales que:

i) $f_0 \subseteq f_1 \subseteq f_2 \subseteq, \ldots, \subseteq f_u \subseteq, \ldots$

donde $f_i \subseteq f_j$ si $i \leq j$.

ii) Para todo $a \in A$, existe un u tal que $a \in \mathrm{Dom}\, f_u$

iii) Para todo $b \in B$, existe un u tal que $b \in \mathrm{Rec}\, f_u$.

iv) Para todo $f_i \in \langle f_u : u \in \omega \rangle$, el dominio de f_i es una subálgebra finita de $\mathcal{A}$ y el recorrido de f_i es una subálgebra finita de $\mathcal{B}$.

Entonces, $F = \bigcup_{u \in \omega} f_u$ será un isomorfismo entre $\mathcal{A}$ y $\mathcal{B}$. Efectivamente:

F es claramente una función, pues de lo contrario existirían dos elementos en F, $\langle x,y \rangle$ y $\langle x,z \rangle$ tales que $y \neq z$. Pero esto es

Prueba : (continuación)

imposible, ya que existirán f_i, f_j de $\langle f_u : u \in \omega \rangle$ tales que $\langle x,y \rangle \in f_i$ y $\langle x,z \rangle \in f_j$ y entonces existirá también un $k > i,j$ tal que $\langle x,y \rangle, \langle x,z \rangle \in f_k$, según la condición i) , con lo que f_k no será una función, contra lo supuesto.

Además, el dominio de F es A , según la condición ii) y el recorrido de F es B , según la condición iii). Luego, F es una biyección entre $\mathcal{A}$ y $\mathcal{B}$ y además es un isomorfismo, pues dados a_0 y a_1 cualesquiera de A, ambos pertenecen al dominio de algún f_i y $f_i \subseteq F$.

Para probar la proposición inicial bastará, pues, tener una sucesión de isomorfismos parciales entre $\mathcal{A}$ y $\mathcal{B}$ tal que cumpla las condiciones anteriores i)-iv).

Sean $\mathcal{A}$ y $\mathcal{B}$ álgebras de Boole sin átomos de cardinalidad ω . Construimos a continuación una sucesión de isomorfismos parciales entre $\mathcal{A}$ y $\mathcal{B}$ de la manera siguiente:

Sean $\{a_n : n \in \omega\}$ y $\{b_n : n \in \omega\}$ enumeraciones de los elementos de $\mathcal{A}$ y $\mathcal{B}$ respectivamente.

(Si $\mathbb{C}$ es una subálgebra de $\mathcal{A}$ y $a \in \mathcal{A} - \mathbb{C}$, entonces, la menor subálgebra de $\mathcal{A}$ que contiene a e incluye $\mathbb{C}$ es :

$$\mathcal{A}' = \{(c_0 \wedge a) \vee (c_1 \wedge \bar{a})\} \text{ donde } c_0, c_1 \in \mathbb{C}$$

$a \in \mathcal{A}'$, pues $a = (1 \wedge a) \vee (0 \wedge \bar{a})$

$\mathbb{C} \in \mathcal{A}'$, pues si $c \in \mathbb{C}$, $c = (c \wedge a) \vee (c \wedge \bar{a})$

$\mathcal{A}'$ es una subálgebra de $\mathcal{A}$. En efecto:

i) 0 y 1 pertenecen a $\mathcal{A}'$ pues pertenecen a $\mathbb{C}$.

ii) Sea $x \in \mathcal{A}$. Si $x \in \mathcal{A}'$, entonces $\bar{x} \in \mathcal{A}'$.

Prueba: Sea $x \in \mathcal{A}'$. Luego, $x = (c_0 \wedge a) \vee (c_1 \wedge \bar{a})$ donde $c_0, c_1 \in \mathbb{C}$. Por tanto,

$\bar{x} = \overline{(c_0 \wedge a) \vee (c_1 \wedge \bar{a})} = \overline{(c_0 \wedge a)} \wedge \overline{(c_1 \wedge \bar{a})} =$

$= (\bar{c}_0 \vee \bar{a}) \wedge (\bar{c}_1 \vee a) = (\bar{c}_0 \wedge a) \vee (\bar{c}_1 \wedge \bar{a})$

$\bar{c}_0, \bar{c}_1 \in \mathbb{C}$ pues $c_0, c_1 \in \mathbb{C}$ y $\mathbb{C}$ es un álgebra de Boole. Así pues, $\bar{x} \in \mathcal{A}'$.

iii) Sean $x,y \in \mathcal{A}$. Si $x,y \in \mathcal{A}'$ entonces $x \vee y \in \mathcal{A}'$.

Prueba: $x \vee y = ((c_0 \wedge a) \vee (c_1 \wedge \bar{a})) \vee ((d_0 \wedge a) \vee (d_1 \wedge \bar{a})) = ((c_0 \vee d_0) \wedge a) \vee ((c_1 \vee d_1) \wedge \bar{a})$ donde $c_0, c_1, d_0, d_1 \in \mathbb{C}$. Luego, $c_0 \vee d_0$, $c_1 \vee d_1 \in \mathbb{C}$ pues $\mathbb{C}$ es un álgebra de Boole. Así, $x \vee y \in \mathcal{A}'$.

Además, $\mathcal{A}'$ es la menor, pues de no ser así, existiría una subálgebra $\mathcal{A}''$ de $\mathcal{A}$ tal que contendría a , e incluiría $\mathbb{C}$ y existiría también un $x \in \mathcal{A}'$ tal que $x \notin \mathcal{A}''$. Luego, como $x \in \mathcal{A}'$, $x \in \{(c_0 \wedge a) \vee (c_1 \wedge \bar{a})\}$ donde $c_0, c_1 \in \mathbb{C}$. Pero $a \in \mathcal{A}''$ y por tanto, $\bar{a} \in \mathcal{A}''$, pues $\mathcal{A}''$ es un álgebra de Boole. Además, $c_0, c_1 \in \mathcal{A}''$, pues $\mathbb{C} \subset A''$. Luego, $\{(c_0 \wedge a) \vee (c_1 \wedge a)\} \subset A''$ y de ahí, $x \in \mathcal{A}'$, contra lo supuesto.) Continuemos ahora con la prueba inicial:

Prueba: (continuación)

Sea $\mathbb{D}_1'$ la menor subálgebra de $\mathcal{B}$ que contiene b_0.

$\mathbb{D}_1' = \{(d_0 \wedge b_0) \vee (d_1 \wedge \bar{b}_0)$ donde $d_0, d_1 \in \{0', 1'\}\}$

Sea $f_0 : \mathbb{C}_1' \longrightarrow \mathbb{D}_1'$ donde $\mathbb{C}_1'$ es la menor subálgebra de $\mathcal{A}$ que contiene un $a_i \in \{a_n : n \in \omega\}$ tal que para todo $x \in \mathbb{C}_1'$,

i) $x \leq a_i \longleftrightarrow f_0(x) \leq b_0$

ii) $a_i \leq x \longleftrightarrow b_0 \leq f_0(x)$

(En este caso, a_i es un elemento cualquiera distinto de 0 y 1).

Prueba: (continuación)

Tendremos que : $f_0(0) = 0'$, $f_0(1) = 1'$, $f_0(a_i) = b_0$, $f_0(\bar{a}_i) = \bar{b}_0$.

Sea ahora $\mathbb{C}_1$ la menor subálgebra de $\mathcal{A}$ que contiene a_0 e incluye $\mathbb{C}_1'$.
Sea $f_1 : \mathbb{C}_1 \longrightarrow \mathbb{D}_1$, donde $\mathbb{D}_1$ es la menor subálgebra de $\mathcal{B}$ que contiene un $b_i \in \{b_n : n \in \omega\}$ tal que para todo $x \in \mathbb{C}_1$:

i) $x \leq a_0 \longleftrightarrow f_1(x) \leq b_i$

ii) $a_0 \leq x \longleftrightarrow b_i \leq f_1(x)$

Prosiguiendo de este modo, tendremos en general que:

Para todo $a_n \in \{a_n : n \in \omega\}$, $a_n \in$ Dom f_{2n+1}

Para todo $b_n \in \{b_n : n \in \omega\}$, $b_n \in$ Rec f_{2n}

Además, $f_{2n+1} : \mathbb{C}_n \longrightarrow \mathbb{D}_n$.

Para cada f_u y cada $a_i \in$ Dom f_u , la existencia de un $b_i \in \{b_n : n \in \omega\}$ tal que:

i) $x \leq a_i \longleftrightarrow f_u(x) \leq b_i$

ii) $a_i \leq x \longleftrightarrow b_i \leq f_u(x)$

viene garantizada por la proposición que se prueba más abajo.

En efecto, nótese que si $a_i \in$ Dom f_u , los $x \in$ Dom f_u tales que $x > a$ tendrán un elemento mínimo, que será $\bigcap x = a_j$ y los $x' < a$, donde $x' \in$ Dom f_u tendrán un elemento máximo, que será $\bigcup x' = a_k$. Pero además puede existir un número finito de elementos del Dom f_u que

Prueba : (continuación)

sean incomparables con a_i . Llamamos Z a tal conjunto. Por tanto, no basta con comprobar que entre dos elementos cualesquiera de un álgebra de Boole sin átomos existe otro, por ejemplo entre $f_u(a_j)$ y $f_u(a_k)$. Deben tenerse en cuenta también los elementos incomparables.

Proposición : Si $\mathcal{B}$ es un álgebra de Boole sin átomos y $x,y \in B$ y $Z \subseteq B$, donde $|Z| < \omega$ y se cunple que : i) $x < y$, ii) Para todo $z \in Z$, $z \nleq x \wedge y \nleq z$, entonces existe un $b \in B$ tal que: i) $x < b < y$, ii) Para todo $z \in Z$, $b \nleq z \wedge z \nleq b$.

Prueba: Sea $Z = \{ z_1, \ldots, z_n \}$. Por los supuestos i) y ii), para cada i tal que $1 \leq i \leq n$, $z_i - x \neq 0$, $y - z_i \neq 0$ y $y - x \neq 0$. Necesitamos probar ahora el lema siguiente:

Lema : Si $\mathcal{B}$ es un álgebra de Boole sin átomos y $\{a_1, \ldots \ldots, a_n\} \subseteq B-\{0\}$, entonces existen n elementos $b_1, \ldots, b_n \in B-\{0\}$ tales que:

i) $0 \leq b_i \leq a_i$ donde $1 \leq i \leq n$

ii) $b_i \wedge b_j = 0$ donde $1 \leq i < j \leq n$

Prueba: Probamos por inducción sobre n. Si n = 1 no hay nada que probar.

Supongamos que sea cierto para n y veamos que también lo es para $n + 1$.

Dados $n + 1$ elementos distintos de 0 : $a_1, \ldots \ldots a_n, a_{n+1}$, existirán $c_1, \ldots, c_n$ elementos tales que $0 < c_i \leq a_i$ $(1 \leq i \leq n)$ y $c_i \wedge c_j = 0$ $(1 \leq i < j \leq n)$ pues suponemos que el lema vale para n.

Si $a_{n+1} \wedge (c_1 \vee, \ldots \vee c_n) = 0$, tomemos $b_{n+1} = a_{n+1}$ y $b_i = c_i$ $(1 \leq i \leq n)$. Si esto no

Prueba : (continuación)

ocurre, sea i_0 tal que $a_{n+1} \wedge c_{i_0} = x$, $x \neq 0$. Entonces existirán elementos y, z tales que $x = y \vee z$ y $y \wedge z = 0$. Tomemos entonces para j $(1 \leq j \leq n+1)$

$$b_j = \begin{cases} y & \text{si } j = i_0 \\ z & \text{si } j = n+1 \\ c_j & \text{si } j \neq i_0 \text{ y } j \neq n+1 \end{cases}$$

En cualquiera de los dos casos el lema vale para $n+1$, con lo que queda probado.

Volviendo a la prueba de la proposición tenemos que por el lema anterior existen $d_1, \ldots, d_n$, $e_1, \ldots, e_n, w$, elementos de B distintos de 0 y disjuntos dos a dos tales que:

$d_i \leq z_i - x$ donde $1 \leq i \leq n$

$e_i \leq y - z_i$ donde $1 \leq i \leq n$

$w \leq y - x$

Consideremos $b = x \vee (e_1 \vee, \ldots, \vee e_n)$. Luego,

i) $x < b < y$ ya que $x < b \leq y$ y $b \neq y$ pues $w \leq y - b$

ii) $b \not\leq z_i$ pues $e_i \leq b - z_i$ y $z_i \not\leq b$ ya que $d_i \leq z_i - b$.

Continuando con la prueba inicial, veamos que los f_u tal y como han sido construidos, son isomorfismos parciales entre $\mathcal{A}$ y $\mathcal{B}$.

Prueba : Que f_1 lo es se comprueba trivialmente. Supongamos que f_i lo es y veamos que también lo es f_{i+1} .

Prueba : (continuación)

Sea $f_i : \mathbb{C}' \cong \mathbb{D}'$ donde $\mathbb{C}'$ y $\mathbb{D}'$ son subálgebras finitas de $\mathcal{A}$ y $\mathcal{B}$ respectivamente. Luego, $f_{i+1} : \mathbb{C} \longrightarrow \mathbb{D}$, donde $\mathbb{C}$ es la menor subálgebra de $\mathcal{A}$ que contiene un a de $\{a_n : n \in \omega\} - \mathbb{C}'$ e incluye $\mathbb{C}'$, y donde $\mathbb{D}$ es la menor subálgebra de $\mathcal{B}$ que contiene un $b \in \{b_n : n \in \omega\} - \mathbb{D}'$ tal que para todo $x \in \mathbb{C}$:

i) $x \leq a \longleftrightarrow f_{i+1}(x) \leq b$

ii) $a \leq x \longleftrightarrow b \leq f_{i+1}(x)$

y $\mathbb{D}$ incluye $\mathbb{D}'$. Tendremos, pues, que:

$$\mathbb{C} = \{(x_0 \wedge a) \vee (x \wedge \bar{a})\} \quad \text{donde } x_0, x_1 \in \mathbb{C}'$$

$$\mathbb{D} = \{(y_0 \wedge b) \vee (y_1 \wedge \bar{b})\} \quad \text{donde } y_0, y_1 \in \mathbb{D}'$$

Tomemos $f_{i+1}((x_0 \wedge a) \vee (x_1 \wedge \bar{a})) =$
$= (f_i(x_0) \wedge b) \vee (f_i(x_1) \wedge \bar{b})$

Que esta función está bien definida se sigue del hecho de que f_i es un isomorfismo y de que para todo $x \in \mathbb{C}$, $x \leq a \longleftrightarrow f_{i+1}(x) \leq b$ y $a \leq x \longleftrightarrow b \leq f_{i+1}(x)$.

Claramente, $f_{i+1}(a) = b$ pues $f_{i+1}(a) =$
$= (1 \wedge a) \vee (0 \wedge \bar{a})$

Además, para todo $x \in \mathbb{C}'$, $f_{i+1}(x) = f_i(x)$ ya que $f_{i+1}(x) = (x \wedge a) \vee (x \wedge \bar{a})$.

Estos resultados se corresponden claramente

Prueba : (continuación)

nuestra construcción de los f_u .

Veamos que $f_{i+1} : \mathbb{C} \longrightarrow \mathbb{D}$ es un isomorfismo. Sean $z_0, z_1 \in \mathbb{C} - \mathbb{C}'$, pues si pertenecen a $\mathbb{C}'$ ya está probado.

i) $f_{i+1}(z_0 \vee z_1) = f_{i+1}(((x_0 \wedge a) \vee (x_1 \wedge \bar{a})) \vee ((x_2 \wedge a) \vee (x_3 \wedge \bar{a}))) = f_{i+1}(((x_0 \vee x_2) \wedge a) \vee ((x_1 \vee x_3) \wedge \bar{a})) = (f_i(x_0 \vee x_2) \wedge b) \vee (f_i(x_1 \vee x_3) \wedge \bar{b}) = ((f_i(x_0) \vee f_i(x_2)) \wedge b) \vee ((f_i(x_1) \vee f(x_3)) \wedge \bar{b}) = (f_i(x_0) \wedge b) \vee (f_i(x_2) \wedge b) \vee (f_i(x_1) \wedge \bar{b}) \vee (f_i(x_3) \wedge \bar{b}) = f_{i+1}((x_0 \wedge b) \vee (x_1 \wedge \bar{b})) \vee f_{i+1}((x_2 \wedge b) \vee (x_3 \wedge \bar{b})) = f_{i+1}(z_0) \vee f_{i+1}(z_1)$

ii) $f_{i+1}(\bar{z}_0) = f_{i+1}(\overline{((x_0 \wedge a) \vee (x_1 \wedge \bar{a}))}) = f_{i+1}((\bar{x}_0 \vee \bar{a}) \wedge (\bar{x}_1 \vee a)) = ((\overline{f_i(x_0)}) \bar{b}) \wedge ((\overline{f_i(x_1)}) \vee b) = \overline{(((f_i(x_0) \wedge b) \vee (f_i(x_1) \wedge \bar{b}))} = \overline{(f_{i+1}(z_0))}$

Todos los pasos enlas demostraciones anteriores quedan justificados por los axiomas de la teoría, así como por la definición de la función f_{i+1}.

iii) f_{i+1} es biyectiva, pues para todo $x, y \in \mathrm{Dom}\, f_{i+1}$,

$$x = y \longleftrightarrow f_{i+1}(x) = f_{i+1}(y)$$

por construcción de f_{i+1}.
Además, si $d \in \mathbb{D}$, existe un $c \in \mathbb{C}$ tal que $f_{i+1}(c) = d$; pues d será de la forma : $d = (d_0 \wedge b) \vee (d_1 \wedge \bar{b})$

Prueba : (continuación)

y entonces, $c = (f^{-1}(d_0) \wedge a) \vee (f^{-1}(d_1) \wedge \bar{a})$

Así pues, $f_{i+1} : \mathbb{C} \cong \mathbb{D}$

Luego, $\langle f_u : u \in \omega \rangle$ es un conjunto de isomorfismos parciales entre $\mathcal{A}$ y $\mathcal{B}$. Además, estos isomorfismos forman una sucesión que cumple las cuatro condiciones del principio de la prueba (Véase la página 59). Efectivamente, por construcción, $f_i \subseteq f_j$ si $i \leq j$. Para cada $a_i \in \{a_n : n \in \omega\}$, $a_i \in \mathrm{Dom}\, f_{2i+1}$. Para cada $b_i \in \{b_n : n \in \omega\}$ $b_i \in \mathrm{Rec}\, f_{2i}$. Además, para cada f_i , el dominio de f_i es una subálgebra finita de $\mathcal{A}$ y el recorrido de f_i es una subálgebra finita de $\mathcal{B}$.

Por tanto, $F = \bigcup_{u \in \omega} f_u$ será un isomorfismo entre $\mathcal{A}$ y $\mathcal{B}$. Con lo que queda probado que la teoría de álgebras de Boole sin átomos es ω-categórica, pues existe al menos un álgebra de Boole numerable y sin átomos. (Véase la Nota 3).

CONCLUSIONES . ALGUNOS TEOREMAS

Vistos todos los ejemplos anteriores de teorías α-categóricas, vamos a sacar algunas conclusiones:

Puesto que todas estas teorías tienen modelos infinitos, ninguna de ellas es categórica. (Véase Pág. 14). No obstante, algunas de ellas tienen también modelos finitos. Así, la teoría de orden lineal tiene modelos en cada cardinalidad α finita, pues todo conjunto ordenado de α elementos es un modelo suyo. La teoría de grupos tiene también modelos en cada cardinalidad α finita, pues $\langle \mathbb{Z}_n, +, 0 \rangle$ es un modelo de la teoría de cardinalidad n. También la teoría de grupos abelianos con todos sus elementos de orden p tiene modelos finitos, pues $\langle \mathbb{Z}_p, +, 0 \rangle$ es un modelo de la teoría de cardinalidad p.

Como hemos probado, la teoría de orden lineal es α-categórica en cada cardinalidad α finita. La teoría de grupos es α-categórica para eada α primo y para cada $\alpha = pq$ donde $q \neq 1 \pmod p$. La teoría de grupos abelianos con todos sus elementos de orden p es α-categórica en cada cardinalidad α en la que existe un modelo; en particular para $\alpha = p$. Estas teorías pueden convertirse en teorías categóricas con la simple adición de un axioma que determine la existencia de exactamente α elementos. Puesto que α es finito, dicho axioma puede expresarse en el lenguaje L.

Diremos que una teoría T_1 es una subteoría de otra teoría T_2 ($T_1 \subset T_2$) si y sólo si todo teorema (toda sentencia) de T_1 es también un teorema de T_2 . O lo que es equivalente, si y sólo si todo modelo de T_2 es un modelo de T_1 . Suponemos , naturalmente, que $L(T_1) = L(T_2)$.

Diremos que una teoría T_1 es distinta de uan teoría T_2 ($T_1 \neq T_2$) si y sólo si existe al menos un teorema φ de T_1 tal que φ no es un teorema de T_2 , o a la inversa. O lo que es equivalente, si y sólo si existe al menos un modelo de T_1 que no es modelo de T_2 , o a la inversa.

Veamos ahora el siguiente teorema:

Teorema : Sea Δ un conjunto de sentencias de L consistente. Sea φ una sentencia de L tal que $\Delta \cup \{\varphi\}$ es también consistente. Luego, la teoría que tiene como conjunto de axiomas a Δ , T(Δ), es una subteoría de la teoría que tiene como conjunto de axiomas a $\Delta \cup \{\varphi\}$, T($\Delta \cup \{\varphi\}$).

Prueba: Debemos probar que todo teorema de T(Δ) es un teorema de T($\Delta \cup \{\varphi\}$). Supongamos lo contrario. Sea s un teorema de T(Δ) tal que s no es un teorema de T($\Delta \cup \{\varphi\}$) . Luego, todo modelo de T(Δ) será modelo de s, pero no todo modelo de T($\Delta \cup \{\varphi\}$) será modelo de s. Sea $\mathcal{A}$ tal que $\mathcal{A}$ Mod T($\Delta \cup \{\varphi\}$) y tal que no $\mathcal{A}$ Mod s . Pero si $\mathcal{A}$ Mod T($\Delta \cup \{\varphi\}$) entonces $\mathcal{A}$ Mod T(Δ) y por tanto, $\mathcal{A}$ Mod s . Lo que es una contradicción.

Relacionando este teorema con los ejemplos de teorías vistos anteriormente, tenemos que:

i-La teoría de orden lineal es una subteoría de la teoría de orden lineal denso sin extremos. Además son distintas, pues esta última no tiene modelos finitos.
ii- La teoría de grupos es una subteoría de la teoría de grupos abelianos y ésta de la teoría de grupos abelianos con todos sus elementos de orden p. Además son distintas pues el grupo de las permutaciones de n elementos, n $>$ 2, no es abeliano y $\langle \mathbb{Z}_n, +, 0 \rangle$, n $\neq$ p es un grupo abeliano cuyos elementos no son de orden p.
Por otra parte, la teoría de grupos abelianos es una subteoría de la teoría de grupos abelianos divisibles sin torsión. Además son distintas, pues esta última no tiene modelos finitos.

iii- La teoría de anillos conmutativos con elemento unidad es una subteoría de la teoría de dominios de integridad y ésta de la de cuerpos y ésta de la de cuerpos de característica p y ésta a su vez de la de cuerpos algebraicamente cerrados de característica p. Además todas son distintas: $\langle \mathbb{Z}_4, +, \cdot, 0, 1 \rangle$ es un anillo conmutativo con elemento unidad aunque no es un dominio de integridad. $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ es un dominio de integridad y no es un cuerpo. $\langle \mathbb{Q}, +, \cdot, 0, 1 \rangle$ es un cuerpo y no es de característica p. $\langle \mathbb{Z}_p, +, \cdot, 0, 1 \rangle$ es un cuerpo de característica p que no está algebraicamente cerrado.

Por otra parte, la teoría de cuerpos de característica 0 es una subteoría de la teoría de cuerpos algebraicamente cerrados de característica 0. Además son distintas, pues $\langle \mathbb{R}, +, \cdot, 0, 1 \rangle$ es un cuerpo de característica 0 y no está algebraicamente cerrado.

iv- La teoría de álgebras de Boole es una subteoría de la teoría de álgebras de Boole sin átomos. Además son distintas, pues esta última no tiene modelos finitos.

Veamos ahora algunos teoremas:

Teorema 1 : Sea $T_1 \subset T_2$.
Supongamos que tanto T_1 como T_2 tienen al menos un modelo de cardinalidad α .
Luego, si T_1 es α-categórica, entonces T_2 también lo es.

Prueba: Supongamos que T_2 no sea α-categórica.
Luego tendrá como mínimo dos modelos de cardinalidad α , $\mathcal{A}$ y $\mathcal{B}$ tales que $\mathcal{A} \not\cong \mathcal{B}$.
Pero entonces, $\mathcal{A}$ Mod T_1 y $\mathcal{A}$ Mod T_2 ya que $T_1 \subset T_2$.
Luego, tendrá T_1 dos modelos de cardinalidad α no isomorfos y no será α-categórica, contra lo supuesto.

Teorema 2 : Sea $T_1 \subset T_2$ y sea $T_1 \neq T_2$.
Sea T_2 α -categórica.
Supongamos que exista una estructura $\mathcal{A}$ de cardinalidad α tal que $\mathcal{A}$ Mod T_1 y no $\mathcal{A}$ Mod T_2 .
Luego, T_1 no es α -categórica.

Prueba: Puesto que T_2 es α -categórica , tendrá todos sus modelos de cardinalidad α isomorfos.
Sea M el conjunto de todos los modelos de T de cardinalidad α.
Dado que $\mathcal{A}$ es de cardinalidad α , para que T_1 fuera categórica, $\mathcal{A}$ debería ser isomorfo a cualquier modelo $\mathcal{B}$ de M, pues dado que $T_1 \subset T_2$, todo modelo de T_2 es también modelo de T_1 .
Pero si $\mathcal{A} \cong \mathcal{B}$ entonces $\mathcal{A} \equiv \mathcal{B}$ y por tanto, $\mathcal{A}$ Mod T_2 . Lo que contradice lo supuesto.

Teorema 3 : Sea $T_1 \subset T_2$.
Supongamos que tanto T_1 como T_2 tienen al menos un modelo de cardinalidad α .
Luego, si T_2 no es α-categórica, entonces tampoco T_1 es α-categórica.

Prueba: Puesto que T_2 no es α -categórica debe tener como mínimo dos modelos $\mathcal{A}$ y $\mathcal{B}$ de cardinalidad α no isomórficos.
Pero puesto que $T_1 \subset T_2$ se sigue que $\mathcal{A}$ Mod T_1 y $\mathcal{B}$ Mod T_1 . Por tanto T_1 no es α-categórica.

Algunas consecuencias de estos teoremas en relación con los resultados anteriores son:

i-La teoría de orden lineal no es ω -categórica, pues lo es la teoría de orden lineal denso sin extremos. (Teorema 2). Ninguna subteoría de la teoría de orden lineal es ω -categórica. (Teorema 3).
ii-La teoría de grupos abelianos es α -categórica para

α primo o $\alpha = pq$ donde $q \neq 1 \pmod{p}$; pues lo es la teoría de grupos. (Teorema 1). Eso significa que todo grupo de orden α primo o de orden $\alpha = pq$ $q \neq 1 \pmod{p}$ es abeliano.

La teoría de grupos abelianos no es α-categórica para $\alpha \geqslant \omega_1$ puesto que lo es la teoría de grupos abelianos divisibles sin torsión (Teorema 2). Ninguna subteoría de la teoría de grupos abelianos es α-categórica para $\alpha \geqslant \omega_1$ (Teorema 3)

iii- Ninguna de las subteorías de la teoría de cuerpos algebraicamente cerrados de característica 0 (o p) es α-categórica para $\alpha \geqslant \omega_1$ pues ésta lo es. (Teoremas 2 y 3).

iv- La teoría de álgebras de Boole no es ω-categórica pues lo es la teoría de álgebras de Boole sin átomos. (Teorema 2). Ninguna subteoría de la teoría de álgebras de Boole es ω-categórica. (Teorema 3).

Un teorema importante sobre la α-categoricidad de las teorías de primer orden es el teorema siguiente:

Teorema : (Teorema de la categoricidad de Morley). Sea T una teoría completa en un lenguaje numerable. Si T es α-categórica para algún $\alpha \geqslant \omega_1$, entonces T es α-categórica para cada $\alpha \geqslant \omega_1$.

(Véase una prueba de este teorema en Chang-Keisler: "Model Theory" Pág. 413).

Por tanto, al probar la α-categoricidad para algún α de una teoría T, estamos probando indirectamente también la α-categoricidad o la no α-categoricidad de otras teorías que están en relación de subteoría con la teoría T. Además, por el teorema de Morley, si tenemos una teoría completa de L y probamos su α-categoricidad para algún $\alpha \geqslant \omega_1$ hemos probado indirectamente también su α-categoricidad para todo $\alpha \geqslant \omega_1$.

Naturalmente, la lista de teorías para las que hemos probado su α-categoricidad (o su no α-categoricidad) en alguna cardinalidad α no pretende ser exhaustiva ni muchísimo menos. No obstante, los teoremas anteriores contribuyen a aumentarla; y aún así, no hemos pretendido más que considerar aquellas teorías algebraicas más conocidas y de uso más frecuente en matemáticas. Sirvan, pues, como ejemplo.

A pesar de que las teorías que hemos estudiado no son categóricas, pues tienen modelos infinitos, algunas de ellas son completas.

Vimos (Pág. 15) que toda teoría que es α-categórica para algún α infinito y sólo tiene modelos infinitos es completa. Así, la teoría de orden lineal denso sin extremos, la teoría de grupos abelianos divisibles sin torsión, la teoría de cuerpos algebraicamente cerrados de característica 0 (o p) y la teoría de álgebras de Boole sin átomos son completas.

Por otra parte, las teorías de orden lineal, de grupos, de grupos abelianos, de anillos conmutativos con elemento unidad, de dominios de integridad, de cuerpos, de cuerpos de característica 0 (o p) y de álgebras de Boole no son ni tan siquiera completas. Efectivamente; ello es una consecuencia del siguiente teorema:

Teorema : Sea $T_1 \subset T_2$ y sea $T_1 \neq T_2$. Luego, T_1 no es completa. (Naturalmente suponemos que T_1 y T_2 son consistentes.)

Prueba: Puesto que $T_1 \subset T_2$ y $T_1 \neq T_2$ existirá una sentencia $\varphi \in L(T_1)$ tal que $\varphi \in T_2$ y

Prueba: (continuación)

y $\varphi \notin T_1$.
Supongamos que T_1 fuera completa. Luego, para toda sentencia $\psi \in L(T_1)$ ocurriría que o bien $\psi \in T_1$ o bien $\neg\psi \in T_1$.
Puesto que $\varphi \notin T_1$, tendríamos que $\neg\varphi \in T_1$ y dado que $T_1 \subset T_2$ se seguiría que $\neg\varphi \in T_2$.
Pero $\varphi \in T_2$. Por tanto, T_2 no sería consistente, contra lo supuesto. Luego, T_1 no es completa.

Hemos considerado, pues, un conjunto de teorías en el lenguaje L y hemos visto cuáles de ellas son categóricas o α -categóricas y también cuáles son completas y cuáles no.

Una teoría categórica tiene esencialmente un solo modelo, el cual queda unívocamente determinado por dicha teoría. Una teoría completa tiene todos sus modelos indistinguibles para el lenguaje de al teoría, aunque de hecho pueden ser modelos distintos. Una teoría no completa tiene modelos distintos incluso para el lenguaje de la teoría.

Por tanto, si lo que nos interesa es describir completamente una estructura entonces debemos exigir una teoría que tenga como modelo a esa estructura y que sea al menos completa, pues en este caso sabemos que todo lo que puede decirse de esa estructura en el lenguaje de la teoría es un teorema de dicha teoría. El caso óptimo es que la teoría, además de completa sea categórica, pues si el universo de la estructura es infinito, una teoría completa es insuficiente para describirla totalmente.

En este caso, lo más que se puede pedir es que la teoría sea α-categórica, donde α es infinito y es la cardinalidad del universo de la estructura, pues en L no existen teorías categóricas que tengan modelos infinitos.

Por tanto, podemos hablar de "el" grupo de 7 elementos, pues sólo existe uno (la teoría de grupos de 7 elementos es categórica) y no en cambio de "el" grupo, o de "el cuerpo", etc.... pues existen muchos grupos y muchos cuerpos distintos (las teorías de grupos y de cuerpos no son ni tan siquiera completas).

En algunas de las teorías que hemos visto, poníamos como ejemplos de modelos a los números enteros, los racionales, los reales, etc...

Si podemos hablar de ese modo es porque los números naturales, los números reales y el espacio euclídeo pueden ser unívocamente caracterizados; aunque no por medio de una teoría expresada en el lenguaje L. Veremos a continuación otro lenguaje, el lenguaje de la lógica de segundo orden que es más potente que L y que sí permite caracterizarlos unívocamente. Para que la diferencia entre ambos lenguajes se haga más patente, mostraremos que utilizando el lenguaje L es imposible caracterizar unívocamente tanto los números naturales como los números reales.

EL LENGUAJE DE LA LOGICA DE SEGUNDO ORDEN

Este lenguaje, al disponer de variables, que pueden ser cuantificadas, para propiedades y relaciones es más potente que el lenguaje de primer orden. En él se pueden formalizar argumentaciones más complejas, además, y aquí esto es lo que nos interesa, permite caracterizar unívocamente estructuras más importantes. Teorías fundamentales en matemáticas como la aritmética, la teoría de los números reales y la geometría euclídea son categóricas en dicho lenguaje. Pero tiene una limitación importante y es que no podemos disponer de un cálculo deductivo por medio del cual podamos encontrar todas y solas las fórmulas lógicamente válidas, en sentido standard (aunque sí podemos disponer de un cálculo suficiente si prescindimos de la noción standard de validez).

Vamos a definir a continuación, como ya hicimos para el lenguaje de primer orden, algunos conceptos básicos. Empezaremos como allí por lasintaxis para pasar a continuación a las interpretaciones sobre las estructuras.

En el lenguaje de la lógica de segundo orden disponemos de variables cuantificables para relaciones. Así, el alfabeto del lenguaje de segundo orden que utilizaremos aquí, además de símbolos para variables individuales, constantes individuales, functores y relatores y de los símbolos lógicos y el igualador (aunque aquí podemos prescindir de él como signo primitivo, pues es definible a partir de los demás) contendrá también los símbolos siguientes:

1- Símbolos para variables relacionales : para cada $n \in \mathbb{N}$ un conjunto infinito numerable de variables relacionales $X^n, Z^n, W^n, \ldots$.
2- Abstractor: λ , sirve para formar predicados a partir de fórmulas.

Las expresiones de la lógica de segundo orden son los términos, los predicados y las fórmulas:

A las reglas de formación de expresiones del lenguaje de primer orden ya dadas, deben añadirse las siguientes:

1- Cualquier variable relacional es un predicado.
2- Cualquier relator es un predicado.
3- Si $\tau_1,\dots,\tau_n$ son términos y Π^n es un predicado n-ádico entonces $\Pi^n \tau_1,\dots,\tau_n$ es una fórmula.
4- Si α es una fórmula, entonces $\bigwedge X^n \alpha$, $\bigvee X^n \alpha$, también son fórmulas .
5- Si α es una fórmula entonces $\lambda x_1,\dots,x_n$ es un predicado.

Las expresiones de la lógica de segundo orden, al igual que las de primer orden se interpretan sobre las estructuras. Una interpretación de un conjunto Γ de expresiones de la lógica de segundo orden sobre una estructura $\mathscr{A}$ se define del mismo modo que en primer orden, definición a la que debe añadirse:
Para cada variable relacional n-ádica X^n : $\mathcal{J}(X^n) \in A_n$ donde $A_n = \mathscr{P}A^n$.

Sea Δ un conjunto de expresiones de la lógica de segundo orden y sea $\mathcal{J}$ una interpretación de Δ sobre una estructura $\mathscr{A}$. La definición por inducción semiótica de la denotación de términos y predicados y la satisfacción de fórmulas de Δ por $\mathcal{J}$ en $\mathscr{A}$ es idéntica que la de primer orden, a la que debemos añadir:

$\mathcal{J}(X^n) = \mathcal{J}(X^n)$
$\mathcal{J}(R^n) = \mathcal{J}(R^n)$
$\mathcal{J}$ sat $\Pi^n \tau_1,\dots,\tau_n$ si y sólo si $\langle \mathcal{J}(\tau_1),\dots,$
$\dots \mathcal{J}(\tau_n)\rangle \in \mathcal{J}(\Pi^n)$
$\mathcal{J}$ sat $\bigwedge X^n\alpha$ si y sólo si para cada $R^n \in A_n$: $\mathcal{J}^{R^n}_{X^n}$ sat α
$\mathcal{J}$ sat $\bigvee X^n\alpha$ si y sólo si para algún $R^n \in A_n$: $\mathcal{J}^{R^n}_{X^n}$ sat α
$\mathcal{J}(\lambda x_1,\dots,x_n \alpha) = \{\langle a_1,\dots,a_n\rangle / \mathcal{J}^{a_1,\dots,a_n}_{x_1,\dots,x_n} \text{ sat } \alpha\}$.
donde $a_1,\dots,a_n \in A$.

Las definiciones de modelo y teoría para la lógica de 2º orden son idénticas a las ya dadas en 1º orden.

No obstante, al no poder disponer de un cálculo deductivo suficiente para la lógica de 2º orden, las relaciones de consecuencia lógica y de deducibilidad no son equivalentes. Ello significa que no podemos tener una formalización completa de una teoría de 2º orden; eso es, de un conjunto de axiomas a partir de los cuales y con la sola ayuda de un cálculo deductivo podamos encontrar todos los teoremas de la teoría. Consideraremos,pues, una teoría completa de 2º orden como el conjunto de todas las consecuencias lógicas de un conjunto dado de axiomas, aunque algunas de ellas sean inaccesibles a partir de ellos mediante un cálculo deductivo dado.

Veremos a continuación que la aritmética de 2º orden,la teoría de los números reales de 2º orden y la geometría euclídea de 2º orden son categóricas. Sin embargo, antes de probar que la aritmética y la teoría de los números reales de 2º orden son categóricas, probaremos que no lo son si formalizamos sus axiomas en el lenguaje L de 1º orden; eso es, veremos que en este caso existen modelos no isomorfos al modelo standard, los llamados modelos no-standard de la aritmética y de los números reales. Esto probará la insuficiencia de la lógica de 1º orden para caracterizar unívocamente dichas estructuras.

Estas tres teorías constituyen la base de la mayor parte de la matemática clásica; de ahí la importancia que tiene el que sean categóricas.

La Aritmética de Peano

La aritmética no es categórica en el lenguaje de la lógica de 1º orden. Vamos a ver a continuación que existen modelos no-standard, es decir, modelos no isomorfos al modelo standard, de esta teoría.
Más adelante veremos, en cambio, que la aritmética sí es categórica en el lenguaje lógico de 2º orden.

Los axiomas de aritmética de Peano son los siguientes, en 1º orden :

1- $\bigwedge x\ (0 \neq Sx)$
2- $\bigwedge xy\ (Sx = Sy \longrightarrow x = y)$
3- $\bigwedge x\ (x + 0 = x)$
4- $\bigwedge x\ (x + Sy = S(x + y))$
5- $\bigwedge x\ (x \,.\, 0 = 0)$
6- $\bigwedge x\ (x \,.\, Sy = (x \,.\, y) + x)$

Y para cada φ donde x no está ligada en φ , siendo φ una fórmula de la lógica de 1º orden y $(v_0, \ldots, v_n)$ las variables que aparecen en φ .

7- $\varphi(0, v_1, \ldots, v_n) \wedge \bigwedge x(\ \varphi(x, v_1, \ldots, v_n) \longrightarrow \varphi(Sx, v_1, \ldots, v_n)) \longrightarrow \bigwedge x\ \varphi(x, v_1, \ldots, v_n)$

El axioma 7 es pues en realidad un esquema axiomático, el llamado esquema axiomático de inducción aritmética.

El modelo standard de esta teoría es $\langle \mathbb{N}, +, .; S, 0 \rangle$ donde S es la función monaria "el sucesor de.." y $+$ y $.$ tienen su significado habitual, de suma y producto. Por este motivo en los axiomas hemos utilizado los signos $+$ y $.$ para indicar los dos functores binarios.

Todos los modelos de la teoría que no son isomorfos al modelo standard son llamados "modelos no-standard". Vamos a ver que existen modelos no-standard para esta teoría. Para ello necesitaremos el teorema siguiente:

Teorema : (Teorema de Compacidad) : Un conjunto Δ de sentencias de L tiene un modelo si y sólo si cada subconjunto finito de Δ tiene un modelo.

(Una prueba de este teorema puede verse en : "Lógica de primer orden", Jesús Mosterín . Pág. 134).

Teorema : (Aritmética no-standard) : Sea L un lenguaje de 1º orden con un functor 0-ario c, un functor monario f^1 y dos functores binarios f_1^2 , f_2^2 . Sea :

$\mathcal{N} = \langle \mathbb{N}, +, \cdot, S, 0 \rangle$ el sistema de los números naturales con el cero, la función monaria "el sucesor de", la suma y el producto.

Sea $\mathcal{T}(\mathcal{N}) = \{ \varphi / \varphi \in$ sentencias de L $\wedge$ $\mathcal{N}$ es modelo de $\varphi \}$.

Entonces existe una estructura $\mathcal{M}$ tal que $\mathcal{M}$ es modelo de $\mathcal{T}(\mathcal{N})$ y $\mathcal{M}$ no es isomórfico a $\mathcal{N}$.

Prueba: Sea L U $\{ k \}$ la extensión alfabética de L conseguida al añadir a L una constante individual k.

Sea $\Sigma = \mathcal{T}(\mathcal{N})$ U $\{ \varphi_n / n \in \omega \}$ donde para cada $n \in \omega$, $\varphi_n = k \neq \tau_n$ siendo $\tau_n = f_1^1, \ldots, f_n^1 0$. Eso es, $\tau_0 = 0$, $\tau_1 = f^1 0$, ..., $\tau_n = f^1, \ldots, f^1 0$, (n veces).

Vamos a probar que cada subconjunto finito de Σ tiene un modelo.

En efecto, sea $\Sigma_0 \subset \Sigma$, Σ_0 finito. Existirá un $\varphi_{n_0} \in \Sigma_0$ que sea el máximo de los que tienen

esta forma. Es decir, existirá un $n_0 + 1$ tal que para cada $m \geqslant n_0 + 1$: $\varphi_m \notin \Sigma_0$.
Luego $\langle \mathbb{N}, +, \cdot, S, n_0 + 1 \rangle$ es modelo de Σ_0, pues para todo φ_i tal que $\varphi_i \leqslant \varphi_{n_0}$, $\varphi_i \in \Sigma_0$ y $\varphi_i = \neg k$ y $\neg k = \tau_i$ para todo $i \leqslant n_0$.

Con esto hemos demostrado que cada subconjunto finito Σ_0 de Σ tiene un modelo. Utilizando ahora el teorema de compacidad, Σ tiene también un modelo, llamémosle $\mathcal{M}$.
Puesto que $\mathcal{T}(\mathcal{N}) \subset \Sigma$ y $\mathcal{M}$ es modelo de Σ, también $\mathcal{M}$ es modelo de $\mathcal{T}(\mathcal{N})$.
Sea $\mathcal{M}_0$ la reducción de $\mathcal{M}$ obtenida al adaptarlo al lenguaje de $\mathcal{T}(\mathcal{N})$ es decir, a L. Eso es, quitándole la función 0-aria f_k que servía de denotación a la constante individual k. Claramente $\mathcal{M}_0$ es modelo de $\mathcal{T}(\mathcal{N})$.
Vamos a demostrar que $\mathcal{M}_0$ no es isomorfo a $\mathcal{N}$. (1)
Supongamos que $\mathcal{M}_0 \cong \mathcal{N}$. Sea h el isomorfismo de $\mathcal{N}$ en $\mathcal{M}_0$. Puesto que $\mathcal{M}$ tenía el mismo universo que $\mathcal{M}_0$, $f_k \in M$, donde M es el universo de ambos sistemas. Y puesto que h es un isomorfismo, hay un $n \in \mathbb{N}$ tal que $h(n) = f_k$.
Entonces tendremos que :
$\mathcal{M}_0, \mathcal{F}_x^{f_k}$ sat $\neg x = \tau_n$ siendo $\mathcal{M}_0\mathcal{F}$ una interpretación sobre el sistema $\mathcal{M}_0$.
y también $\mathcal{N}, \mathcal{F}_x^n$ sat $x = \tau_n$
Esto constituye una contradicción, como veremos :

Sea $\mathcal{A} = \langle A, \langle f_i \rangle_{i \in I}, \langle R_j \rangle_{j \in J} \rangle$ y sea $x_1, \ldots, x_n \in \mathcal{A}$
Si τ es un término con a lo sumo $x_1, \ldots, x_n$ variables libres, escribiremos $\mathcal{A}[x_1, \ldots, x_n]$ (τ) en vez de $\mathcal{A}, \mathcal{F}_{x_1, \ldots, x_n}^{x_1, \ldots, x_n}(\tau)$
Si φ es una fórmula con a lo sumo $x_1, \ldots, x_n$ variables libres, escribiremos $\mathcal{A}[x_1, \ldots, x_n]$ sat φ en vez de $\mathcal{A}, \mathcal{F}_{x_1, \ldots, x_n}^{x_1, \ldots, x_n}$ sat φ.

(1) A partir de aquí, puede verse una prueba alternativa más sencilla en el Anexo 3 .

Teorema : Si $\mathcal{A}$ y $\mathcal{B}$ son dos sistemas y $\mathcal{A} \cong \mathcal{B}$ entonces para cada φ con a lo sumo $x_1, \ldots, x_n$ variables libres se cumple : para cada $x_1, \ldots, x_n \in \mathcal{A}$, $\mathcal{A}[x_1, \ldots, x_n]$ sat φ si y sólo si $\mathcal{B}[h(x_1), \ldots, h(x_n)]$ sat φ, siendo $h: A \longrightarrow B$ el isomorfismo entre $\mathcal{A}$ y $\mathcal{B}$.

Prueba : Para cada término τ con a lo sumo $x_1, \ldots, x_n$ variables libres se cumple :

$h(\mathcal{A}[x_1, \ldots, x_n](\tau)) = \mathcal{B}[h(x_1), \ldots, h(x_n)](\tau)$

En efecto :

$h(\mathcal{A}[x_1, \ldots, x_n](x_i)) = h(x_i) = \mathcal{B}[h(x_1), \ldots, h(x_n)](x_i)$.

$h(\mathcal{A}[x_1, \ldots, x_n](f_j \tau_1, \ldots, \tau_m)) = h(f_j(\mathcal{A}[x_1, \ldots, x_n](\tau_1), \ldots, \mathcal{A}[x_1, \ldots, x_n](\tau_m))) = g_j(h(\mathcal{A}[x_1, \ldots, x_n](\tau_1)), \ldots, h(\mathcal{A}[x_1, \ldots, x_n](\tau_m))) = g_j(\mathcal{B}[h(x_1), \ldots, h(x_n)](\tau_1), \ldots, \mathcal{B}[h(x_1), \ldots, h(x_n)](\tau_m)) = \mathcal{B}[h(x_1), \ldots, h(x_n)](f_j \tau_1, \ldots, \tau_m)$.

Demostraremos ahora que se cumple el teorema para fórmulas simples : $R^m \tau_1, \ldots, \tau_m$.

$\mathcal{A}[x_1, \ldots, x_n]$ sat $R^m_j \tau_1, \ldots, \tau_m$ si y sólo si $\langle \mathcal{A}[x_1, \ldots, x_n](\tau_1), \ldots, \mathcal{A}[x_1, \ldots, x_n](\tau_m) \rangle \in R^m_j$.

si y sólo si $\langle h(\mathcal{A}[x_1, \ldots, x_n](\tau_1)), \ldots, h(\mathcal{A}[x_1, \ldots, x_n](\tau_m)) \rangle \in S^m_j$.

si y sólo si $\langle \mathcal{B}[h(x_1), \ldots, h(x_n)](\tau_1), \ldots, \mathcal{B}[h(x_1), \ldots, h(x_n)](\tau_m) \rangle \in S^m_j$.

si y sólo si $\mathcal{B}[h(x_1), \ldots, h(x_n)]$ sat $R^m_j \tau_1, \ldots, \tau_n$

Si se cumple para φ, entonces se cumple para $\neg \varphi$.

$\mathcal{A}[x_1, \ldots, x_n]$ sat $\neg \varphi$ si y sólo si no $\mathcal{A}[x_1, \ldots, x_n]$ sat φ.

si y sólo si no $\mathcal{B}[h(x_1), \ldots, h(x_n)]$ sat φ

si y sólo si $\mathcal{B}[h(x_1), \ldots, h(x_n)]$ sat $\neg \varphi$.

Si se cumple para φ y ψ ,entonces se cumple para $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \longrightarrow \psi$, $\varphi \longleftrightarrow \psi$.

$\mathcal{A}[x_1,\ldots,x_n]$ sat $\varphi \wedge \psi$ si y sólo si $\mathcal{A}[x_1,\ldots,x_n]$ sat φ y $\mathcal{A}[x_1,\ldots,x_n]$ sat ψ .

si y sólo si $\mathcal{B}[h(x_1),\ldots,h(x_n)]$ sat φ y $\mathcal{B}[h(x_1),\ldots,h(x_n)]$ sat ψ .

si y sólosi $\mathcal{B}[h(x_1),\ldots,h(x_n)]$ sat $\varphi \wedge \psi$.

De manera similar para $\varphi \vee \psi$, $\varphi \longrightarrow \psi$, $\varphi \longleftrightarrow \psi$.

Si se cumple para φ , se cumple para $\bigwedge x\, \varphi$ y $\bigvee x_i\, \varphi$.

$\mathcal{A}[x_1,\ldots,x_n]$ sat $\bigwedge x\, \varphi$ si y sólo si para cada $x \in$ A: $\mathcal{A}[x_1,\ldots,x_n]$ sat φ .

si y sólo si para cada h(x) $\in \mathcal{B}$: $\mathcal{B}[h(x_1),\ldots,h(x_n)]$ sat φ .

si y sólo si $\mathcal{B}[x_1,\ldots,x_n]$ sat $\bigwedge x\, \varphi$.

Del mismo modo para $\bigvee x_i\, \varphi$.

Puesto que teníamos $\mathcal{M}_0, \mathcal{F}_x^{f_k}$ sat $\neg x = \tau_n$ y $\mathcal{N}, \mathcal{F}_x^{n}$ sat $x = \tau_n$
Entonces por el teorema anterior tendremos que n= τ_n y $\neg n = \tau_n$ lo cual es evidentemente contradictorio.
Por tanto $\mathcal{M}_0$ y $\mathcal{N}$ no son isomorfos. Lo que queríamos demostrar.

Hemos probado, pues, la existencia de modelos no-standard de la aritmética de 1º orden.

Si el axioma 7 lo escribimos en el lenguaje de la lógica de 2º orden, con lo cual ya no será un esquema axiomático sino un simple axioma, tendremos la aritmética de 2º orden, la cual sí es categórica.

7- $\bigwedge P \; (P0 \wedge \bigwedge x \; (Px \longrightarrow PSx) \longrightarrow \bigwedge x Px)$

Vamos a probar que la aritmética de 2º orden es categórica.

La teoría de los números naturales de 2º orden tiene como axiomas:

1- $\bigwedge x(Sx \neq 0)$
2- $\bigwedge xy \; (Sx = Sy \longrightarrow x = y)$
3- $\bigwedge P \; (P0 \wedge \bigwedge x \; (Px \longrightarrow PSx) \longrightarrow \bigwedge x Px)$

Si esta teoría es categórica, entonces también lo es la aritmética de 2º orden ya que la suma y el producto son definibles a partir de 0 y S (Véase la Nota 4). Vamos a probar, pues, que esta teoría es categórica.

Sean $\mathscr{A}$ y $\mathscr{B}$ dos modelos de la teoría. Vamos a probar que son isomorfos.

$$\mathscr{A} = \langle A , S , 0 \rangle , \quad \mathscr{B} = \langle B , S', 0' \rangle$$

Teorema: Existe una biyección $h: A \longrightarrow B$ tal que:
i- $h(0) = 0'$
ii- $h(S(x)) = S'(h(x))$ para todo $x \in A$

Esto se sigue del lema siguiente:

Lema: Existe una función $h: A \longrightarrow B$ tal que h cumple i- y ii- .

Como paso previo para la prueba del Lema1 consideraremos relaciones entre elementos de A y elementos de B.
Por ejemplo Rxy donde $x \in A$ y $y \in B$.
Una relación de este tipo será una <u>relación de Peano</u> si cumple las dos condiciones siguientes:
1- ROO'
2- Si Rxy entonces $RSxS'y$ para todo $x \in A$ y $y \in B$

Sea R_0 la intersección de todas las relaciones de Peano. Esto es : R_0xy si y sólo si Rxy para todas las relaciones de Peano.Se sigue que :
(*) si R_0xy y R es una relación de Peano entonces Rxy.

Vamos a ver que R_0 es una relación de Peano. Es la relació de Peano más pequeña. Para probar esto debemos comprobar que R cumple las condiciones 1 y 2.

1- Para cada relación de Peano R tenemos ROO'. Luego R_0OO' pues R_0 es la intersección de todas ellas.
2- Supongamos que R_0xy. Debemos probar que $R_0SxS'y$. Debemos probar, pues, que $RSxS'y$ para cualquier relación de Peano R.
   Sea R una relación de Peano cualquiera.
   Luego Rxy pues R_0xy y entonces $RSxS'y$ pues R es una relación de Peano.

Vamos a probar que R_0 representa una función, es decir, que para cada elemento $x \in A$ hay exactamente un elemento $y \in B$ tal que R_0xy.
Vamos a probar esto por inducción sobre los números naturales:
Debemos probar que : a) hay exactamente un $y \in B$ tal que R_0Oy. b) Si, para algún $x \in A$, hay exactamente un y tal que R_0xy, entonces hay exactamente un $z \in B$ tal que R_0Sxz.

a) Que existe uno es evidente, R_0OO' pues R_0 es una relación de Peano. Vamos a probar que es único :

Supongamos que $R_0 Ob$. Tenemos que mostrar que $b = O'$
Supongamos que $b \neq O'$
Definimos la relación R_0' de la manera siguiente, para cualesquiera x,y.
$R_0'xy$ si y sólo si R_0xy pero no $x = O$ y $y = b$.
Entonces claramente no $R_0'Ob$.
Vamos a probar que R_0' es una relación de Peano :
1- $R_0'OO'$, pues $R_0 OO'$ pero no $O = O$ y $O' = b$, pues $b \neq O'$
2- Sea $R_0'xy$. Debemos mostrar que $R_0'SxS'y$:
Tenemos que R_0xy, pues $R_0'xy$ y entonces $R_0SxS'y$, pues R_0 es una relación de Peano.
Para probar que $R_0'SxS'y$ hemos de mostrar que $Sx = O$ y $S'y \neq b$ no pueden ser ambos ciertos.
Pero $Sx \neq O$ por el axioma 1 : $\bigwedge x\ (Sx \neq O)$

Puesto que R_0' es una relación de Peano tenemos que $R_0'xy$ por (*) siempre que R_0xy.
Pero esto contradice nuestra suposición de que R_0Ob pero no $R_0'Ob$.

b) Supongamos que para un $x \in A$ hay exactamente un y tal que R_0xy.
Tenemos que probar que hay exactamente un z tal que R_0Sxz.
Que existe uno es evidente, pues ya que R_0 es una relación de Peano y tenemos que R_0xy , se sigue $R_0SxS'y$.
Vamos a probar que es único :
Supongamos que hay más de uno : Si $R_0SxS'y$ también R_0Sxz para un $z \neq S_0'y$.
Definimos la relación R_0' de la siguiente manera, para cualesquiera a,b.
$R_0'ab$ si y sólo si R_0ab pero no $Sx = a$ y $z = b$.
Entonces claramente no $R_0'Sxz$.
Vamos a probar que R_0' es una relación de Peano :
1- $R_0'OO'$ pues R_0OO' pero no $Sx = O$ y $z = O'$. Pues $Sx \neq O$ por el axioma 1 .
2- Sea $R_0'ab$. Debemos mostrar que $R_0'SaS'b$.
Tenemos que R_0ab pues $R_0'ab$ y entonces $R_0SaS'b$ pues R_0 es una relación de Peano.
Para probar que $R_0'SaS'b$ hemos de mostrar que $Sx = Sa$ y

y z = S'b no pueden ser ambos ciertos.
Si Sx = Sa entonces x = a por el axioma 2 .
Así tendremos que R_0xb.
Pero luego, por la suposición que hemos hecho al principi
de b) tenemos b = y .
Ahora, si también z = S'b tendríamos que z = S'y lo que contradice nuestra suposición inicial.

Puesto que R_0' es una relación de Peano tenemos que $R_0'Sxy$ siempre que R_0Sxy (por $*$) . Pero esto contradice nuestra suposición de que R_0Sxz pero no $R_0'Sxz$.

Hemos visto que la relación de Peano R_0 representa una función : para cada $x \in A$ hay exactamente un $y \in B$ tal que R_0xy . Así hay una función h definida para cada $x \in A$ la cual asigna a cada $x \in A$ el $y \in B$ tal que R_0xy.
Tenemos así la relación $R_0xh(x)$ $(**)$
Para probar el Lema 1 debemos probar i) y ii)

i) $R_0Oh(0)$ por $(**)$
   R_000' pues R_0 es una relación de Peano.
   Luego $h(0) = 0'$
ii) $R_0xh(x)$ por $(**)$
   $R_0SxS'h(x)$ pues R_0 es una relación de Peano.
   $R_0Sxh(Sx)$ por $(**)$
   Luego $h(Sx) = S'h(x)$

Sabemos ahora que existe una función $h:A \longrightarrow B$ tal que cumple i) y ii).
El mismo resultado podría obtenerse simétricamente para una función $h':B \longrightarrow A$ tal que cumpliera i)' y ii)' es decir

i)' $h'(0') = 0$
ii)' $h'(S'x) = Sh'(x)$ para todo $x \in B$

Vamos a probar ahora que $h'(h(x)) = x$ para todo $x \in A$:

Sea R un predicado monario cualquiera de $\mathscr{A}$. Sea $\mathscr{A}$

modelo del axioma 3. Entonces :
Si $\mathcal{A}$ Mod P0 y $\mathcal{A}$ Mod $\bigwedge x(Px \longrightarrow PSx)$ entonces $\mathcal{A}$ Mod $\bigwedge xPx$. Y luego :
R0 y si Rx entonces RSx para todo x, entonces Rx para todo $x \in A$.
Es decir, que si pudiéramos probar que R0 y (1)
si Rx entonces RSx para todo $x \in A$ (2)
obtendríamos que Rx para todo $x \in A$ (3)
Al paso de (1) y (2) a (3) lo llamamos "prueba por inducción sobre los números naturales". Este método sirve para demostrar que todos los elementos de A cumplen una determinada propiedad R.

Ahora escogemos como R la propiedad tal que se da para un elemento $x \in A$ si y sólo si $h'(h(x)) = x$:

1- $h'(h(0)) = h'(0')$ por i) $h'(0') = 0$

2- Sea $h'(h(x)) = x$ luego tenemos
$h'(h(Sx)) = h'(S'\,h(x))$ por ii) $h(Sx) = S'h(x)$
pero $h'(S'h(x)) = Sh'(h(x))$ por ii)' $h'(S'x) = Sh'(x)$
y entonces $Sh'(h(x)) = Sx$ por hipótesis.

Hemos probado pues que para todo $x \in A$, $h'(h(x)) = x$

Tenemos que si $a_1 = a_2$ entonces $h(a_1) = h(a_2)$ pues h es una función y si $h(a_1) = h(a_2)$ entonces $h'(h(a_1))=h'(h(a_2))$ pues h' es una función y entonces $a_1 = a_2$ pues para todo $x \in A$, $h'(h(x)) = x$.
Luego $a_1 = a_1$ si y sólo si $h(a_1) = h(a_1)$. Por tanto h será biyectiva. Además, para todo $x \in B$ existe un $y \in A$ tal que $h(y) = x$, dado que $x = h(h'(x))$.
Así, existe una función h biyectiva entre $\mathcal{A}$ y $\mathcal{B}$ tal que cumple las condiciones i) y ii) de isomorfía. Por tanto $\mathcal{A}$ y $\mathcal{B}$ serán isomorfos y la teoría de los números naturales de 2º orden será categórica.

Sea $\mathcal{L} = \{ +, \cdot, \leq, 0, 1 \}$ un lenguaje de 1º orden donde $+$, $\cdot$, son functores binarios, $\leq$ es un relator binario y 0 , 1 , son constantes individuales. Escribiremos, en lo que sigue, $x + y$, $x.y$, $x \leq y$, en lugar de $+xy$, $.xy$, $\leq xy$.

La teoría de los números reales tiene los axiomas siguientes :

1 - 11 : Los axiomas de la teoría de Cuerpos.
12- 15 : Los axiomas de la teoría de Orden Lineal.
16- : $\bigwedge xyz \; (x \leq y \longrightarrow x + z \leq y + z)$
17- : $\bigwedge xyz \; (x \leq y \wedge 0 \leq z \longrightarrow x.z \leq y.z)$

Hasta aquí tenemos los axiomas de la teoría de cuerpos ordenados. Sólo nos falta el axioma de Dedekind (18) para tener la teoría de cuerpos ordenados completos, oteoría de los números reales.

18- : $\bigwedge xy \; (\alpha(x) \wedge \beta(y) \longrightarrow x < y) \longrightarrow$
$\longrightarrow \bigvee z \bigwedge xy \; (\alpha(x) \wedge \beta(y) \wedge x \neq z \wedge$
$\wedge\, y \neq z \longrightarrow x < z \wedge z < y)$
donde escribimos $x < y$ en lugar de $x \leq y \wedge$
$\wedge\, x \neq y$. Y donde α y β son fórmulas de $\mathcal{L}$ en las cuales ocurre que : x no está ligada en α e y no está ligada en β.

Este axioma 18 es en realidad una lista infinita de axiomas .
(Véase la Nota 5)

El modelo standard de esta teoría es :

$$\langle \mathbb{R}, +, \cdot, \leq, 0, 1 \rangle$$

Todos los modelos de la teoría que no son isomorfos al modelo standard, son llamados "modelos no-standard". Veremos a continuación que existen modelos no-standard de esta teoría.

Teorema : Sea $\mathcal{L}$ un lenguaje de 1º orden con dos functores 0-arios c_1, c_2 ; dos functores binarios f_1, f_2, y un relator binario R . Sea $\mathcal{R} = \langle \mathbb{R}, +, \cdot, \leq, 0, 1 \rangle$ la estructura formada por los números feales con el 0 y el 1 como constantes, la suma y el producto, y la relación "menor o igual que" .
Sea $\mathcal{T}(\mathcal{R}) = \{ \varphi / \varphi \in$ sentencias de $\mathcal{L} \wedge \mathcal{R}$ es modelo de $\varphi \}$.
Entonces, hay una estructura $\mathcal{S}$ tal que $\mathcal{S}$ es modelo de $\mathcal{T}(\mathcal{R})$ y $\mathcal{S}$ no es isomorfo a $\mathcal{R}$.

Prueba : Sea c una constante individual distinta de 0 y 1 .
Sea $\mathcal{L} \cup \{c\}$ la extensión alfabética de $\mathcal{L}$ que resulta al añadirle la constante c.

Sea $\Sigma = \mathcal{T}(\mathcal{R}) \cup \{ \varphi_n / n \in \omega \}$ donde para cada $n \in \omega$, $\varphi_n = n.1 < c$ siendo $n.1 = 1 + 1 + , \ldots , + 1$, n veces .

Cda subconjunto finito Σ_0 de Σ tiene un modelo . Efectivamente, sea $\Sigma_0 \subset \Sigma$ y sea Σ_0 finito. Entonces existirá un $\varphi_{n_0} \in \Sigma_0$ que es el máximo. Eso es, existirá un $n_0 + 1$ tal que para todo $m \geq n_0 + 1$ ocurre que $\varphi_m \notin \Sigma_0$.
Luego, la estructura $\langle \mathbb{R}, +, \cdot, \leq, 0, 1, n_0 \rangle$ será un modelo de Σ_0. n_0 sirve de denotación a la constante c .

Así pues, cada subconjunto finito Σ_0 de Σ tiene un modelo. Luego, por el teorema de compacidad, Σ tiene también un modelo.Llamémosle $\mathcal{S}$. (1)

(1) A partir de aquí puede verse una prueba alternativa más sencilla en el Anexo 4.

Prueba : (continuación)

Puesto que $\mathcal{S}$ es modelo de Σ y $\mathcal{T}(\mathcal{R})$ es un subconjunto de Σ, $\mathcal{S}$ también será modelo de $\mathcal{T}(\mathcal{R})$.

Definimos a continuación la propiedad arquimediana de un cuerpo ordenado :

Definición : Un cuerpo ordenado $\mathcal{A}$ es arquimediano si y sólo si para todo par de elementos a, b positivos y pertenecientes al universo de $\mathcal{A}$, existe un elemento n tal que $n \in \mathbb{N}$ y tal que $n.a \geqslant b$.

Vamos a probar que $\mathcal{S}$ no es arquimediano:

Sea b la función 0-aria que sirve de denotación a la constante c en el modelo $\mathcal{S}$.
Tanto 1 como b son positivos, pues $c \geqslant n.1$.
Luego, si $\mathcal{S}$ fuese arquimediano, debería existir un n tal que $n.1 \geqslant b$.
Pero esto es imposible, pues $\mathcal{S}$ es modelo de Σ y por tanto, también es modelo de todas las sentencias $\{ \varphi_n / n \in \omega \}$ donde $\varphi_n = n.1 \leqq c$.
Luego, $\mathcal{S}$ es modelo de $\mathcal{T}(\mathcal{R})$ y $\mathcal{S}$ no es arquimediano.

Sea $\mathcal{S}_0$ la reducción de $\mathcal{S}$ al lenguaje de $\mathcal{T}(\mathcal{R})$. Eso es, quitándole la función 0-aria que servía de denotación a la constante c. Claramente, $\mathcal{S}_0$ no es tampoco arquimediano, pues tiene el mismo universo que $\mathcal{S}$.

Vamos a probar que $\mathcal{S}$ y $\mathcal{R}$ no son isomorfos.

Prueba : (continuación)

Supongamos que sí lo sean.

Sea h un isomorfismo entre $\mathcal{R}$ y $\mathcal{S}_0$.

Luego, hay un r $\in \mathbb{R}$ tal que h(r) = b , pues b pertenece también al universo de $\mathcal{S}_0$.

Puesto que $\mathcal{R} \cong \mathcal{S}_0$, debe ocurrir que :

$$n.1 \leq r \longleftrightarrow n.1 \leq h(r)$$

pues sabemos que si $\mathcal{R} \cong \mathcal{S}_0$ entonces, para cada φ con a lo sumo $x_1, \dots, x_n$ variables libres se cumple : para cada $x_1, \dots, x_n \in \mathcal{R}$

$$\mathcal{R} \left[x_1, \dots, x_n \right] \text{ sat } \varphi \longleftrightarrow \mathcal{S}_0 \left[h(x_1), \dots, \right.$$
$$\left. \dots, h(x_n) \right] \text{ sat } \varphi \text{ .}$$

siendo h el isomorfismo entre $\mathcal{R}$ y $\mathcal{S}_0$.

(Véase la demostración de este teorema en la prueba de la existencia de modelos no-standard de la aritmética de Peano).

Evidentemente se cumple que $n.1 \leq h(r)$, es decir, que $n.1 \leq b$ para todo n, pues $\mathcal{S}_0$ no es arquimediano.

En cambio, $n.1 \leq r$ no se cumple para todo n, pues $\mathcal{R}$ sí es arquimediano.

Así pues, hemos demostrado que $\mathcal{R} \not\cong \mathcal{S}_0$.

Por tanto, $\mathcal{S}_0$ es un modelo no-standard de la teoría de los números reales.

La teoría de los números reales de 2º orden tiene los mismos axiomas que la teoría de los números reales de 1º orden, con la diferencia de que el esquema axiomático nº18, se convierte en un simple axioma al ser expresado en el lenguaje lógico de 2º orden. El axioma 18 queda de la manera siguiente:

$$18-\ \bigwedge P \bigwedge Q \left[\bigwedge xy\ (Px \wedge Qy \longrightarrow x < y) \longrightarrow \right.$$
$$\longrightarrow \bigvee z \bigwedge xy\ (Px \wedge Qy \wedge x \neq z \wedge y \neq z \longrightarrow$$
$$\longrightarrow x < z \wedge z < y)$$

Donde P y Q son variables relacionales de 2º orden .

Vamos a probar que esta teoría es categórica. Puesto que el sistema $\mathcal{R} = \langle \mathbb{R}, +, ., \leq, 0, 1 \rangle$ es un modelo de la teoría, probaremos que cualquier otro modelo $\mathcal{A}$ de la teoría es isomorfo a $\mathcal{R}$.

Proposición: Si $\mathcal{A}$ es un modelo de la teoría de los números reales de 2º orden, entonces $\mathcal{A}$ es isomorfo a $\mathcal{R}$.

Prueba : Sea $\mathcal{A} = \langle A, +', .', \leq', 0', 1' \rangle$ un modelo de la teoría de los números reales de 2º orden.

Debemos mostrar que existe una biyección $h : \mathbb{R} \longrightarrow A$ tal que :

i) $h(x + y) = h(x) +' h(y)$

ii) $h(x.y) = h(x) .' h(y)$

iii) $x \leq y \longleftrightarrow x \leq' y$

Definiremos primero la función h para el subconjunto $\mathbb{Z}$ de $\mathbb{R}$.

Sea $h: \mathbb{Z} \longrightarrow A$ tal que :

$h(0) = 0'$

$h(n) = \underbrace{1' +', \ldots, +' 1'}_{n \text{ veces}}$ para $n > 0$

Prueba : (continuación)

$h(-n) = -'(1' +', \ldots, +' 1')$ para $n < 0$

Escribimos $-'a = x$ en lugar de $x +' a = 0'$

Claramente h es una función de $\mathbb{Z}$ en A , pues si n=m para cualesquiera $n,m \in \mathbb{Z}$, $h(n) = h(m)$.

Fácilmente se comprueba que $h: \mathbb{Z} \longrightarrow A$ cumple la condiciones i) ii) y iii) :

i) $h(x + y) = \underbrace{1' +', \ldots, +' 1'}_{x+y \text{ veces}} = \underbrace{(1' +', \ldots, +' 1')}_{x \text{ veces}} +'$

$+' \underbrace{(1' +', \ldots, +' 1')}_{y \text{ veces}} = h(x) +' h(y)$

Pues $+'$ es asociativa en $\mathcal{A}$.

ii) $h(x.y) = \underbrace{1' +', \ldots, +' 1'}_{x.y \text{ veces}} = \underbrace{\underbrace{(1' +', \ldots, +' 1')}_{x \text{ veces}} +', \ldots, +' (1' +', \ldots, +' 1')}_{y \text{ veces}} = \underbrace{h(x) +', \ldots, +' h(x)}_{y \text{ veces}} =$

$= h(x) \,.'\, \underbrace{(1' +', \ldots, +' 1')}_{y \text{ veces}} = h(x) \,.'\, h(y)$

Pues .' es distributiva en $\mathcal{A}$ respecto de $+'$. Y además, $h(x) = h(x) \,.'\, 1'$.

iii) Sea $0 \leqslant x \leqslant y$. Puesto que el sistema $\langle \mathbb{Z}, +, 0 \rangle$ es un grupo cíclico cuyo elemento generador es 1 para todo $x \in \mathbb{Z}$ tal que $x > 0$, tendremos que:

$$\underbrace{(1 +, \ldots, + 1)}_{x \text{ veces}} \leqslant \underbrace{(1 +, \ldots, + 1)}_{y \text{ veces}}$$

Prueba : (continuación)

Lo que quiere decir que :

$$\underbrace{(1 +,\ldots, + 1)}_{y \text{ veces}} + -\underbrace{(1 +,\ldots, + 1)}_{x \text{ veces}} = \underbrace{(1+,\ldots,+1)}_{z \text{ veces}}$$

donde $z \geqslant 0$.

Y luego, $h'(\underbrace{(1 +,\ldots, + 1)}_{y \text{ veces}} + -\underbrace{(1 +,\ldots, + 1)}_{x \text{ veces}})=$

$=h\underbrace{(1+,\ldots, +1)}_{z \text{ veces}}$

De donde, $h\underbrace{(1 +,\ldots, + 1)}_{y \text{ veces}} +' -'h\underbrace{(1+ ,\ldots, + 1)}_{x \text{ veces}}=$

$= h\underbrace{(1 + ,\ldots, + 1)}_{z \text{ veces}}$

Entonces, $h(y) +' -'h(x) = h(z)$. Donde $h(z) \geqslant 0'$.

Luego, $h(x) \leqslant h(y)$.

El mismo razonamiento vale en el caso de que $x \leqslant y \leqslant 0$.(Entonces el eleemento generador sería -1 en lugar de 1).

Vamos a extender el dominio de la función h al subconjunto $\mathbb{Q}$ de $\mathbb{R}$.

Escribiremos $m/n = x$ en lugar de $m = n.x$

$m,n \in \mathbb{Z}$.

Sea $h(m/n) = h(m)/'h(n)$

Prueba : (continuación)

h es una función , pues si $m/n = k/j$ entonces $m.j = k.n$ y luego, $h(m.j) = h(k.n)$ pues $m,n,k,j \in \mathbb{Z}$ y $h \upharpoonright \mathbb{Z}$ es una función. De aquí tendremos que $h(m) .' h(j) = h(n) .' h(k)$ pues $h \upharpoonright \mathbb{Z}$ cumple la condición ii) . De donde $h(m)/'h(n) = h(k)/'h(j)$.

Comprobemos ahora que para cualesquiera r_1 , $r_2 \in \mathbb{Q}$ se cumple que :

i) $h(r_1 + r_2) = h(r_1) +' h(r_2)$

ii) $h(r_1 . r_2) = h(r_1) .' h(r_2)$

iii) $r_1 \leq r_2 \longleftrightarrow h(r_1) \leq' h(r_2)$

Sean $r_1 = m/n$ y $r_2 = k/j$, donde $m,n,k,j \in \mathbb{Z}$

i) $h(r_1 + r_2) = h(m/n + k/j) = h((m.j) + (n.k)/n.j) = h((m.j) + (n.k))/'h(n.j) = h(m.j) +' h(n.k)/'h(n.j) = (h(m).'h(j)) +' (h(n).'h(k))/'h(n).'h(j) = (h(m)/'h(n)) +' (h(k)/'h(j)) = h(m/n) +' h(k/j) = h(r_1) +' h(r_2)$

ii) $h(r_1 . r_2) = h(m/n . k/j) = h(m.k / n.j) = h(m.k)/'h(n.j) = h(m).'h(k)/'h(n).'h(j) = (h(m)/'h(n)).'(h(k)/'h(j)) = h(m/n) .' h(k/j) = h(r_1) .'h(r_2)$

iii) Sea $r_1 \leq r_2$. Luego, $m/n \leq k/j$ y entonces, $m.j \leq n.k$, donde $m,n,k,j \in \mathbb{Z}$ y por tanto, $h(m.j) \leq h(n.k)$, pues h cumple iii) . Y luego, $h(m).'h(j) \leq h(n).'h(k)$, pues $h \upharpoonright \mathbb{Z}$ cumple ii) Y de aquí , $h(m)/'h(n) \leq h(k)/'h(j)$, de donde $h(m/n) \leq h(k/j)$. Por tanto, $h(r_1) \leq h(r_2)$. (Un razonamiento análogo puede hacerse en sentido inverso).

Prueba : (continuación)

Extenderemos ahora el dominio de la función h a $\mathbb{R}$.

Para un elemento cualquiera $x \in \mathbb{R}$, sea A_x el subconjunto de A que consiste en todos los $h(r)$ para todos los números racionales $r < x$.

Definición: decimos que un subconjunto $A' \subset A$ está acotado superiormente si y sólo si existe un elemento $a \in A$ tal que para todo $a' \in A'$ ocurre que $a' \leq a$. Si ocurre lo contrario, eso es, que para todo $a' \in A'$, $a' \geq a$, entonces decimos que A' está acotado inferiormente.

Por tanto, A_x no es vacío (pues $\mathbb{Q}$ no está acotado inferiormente) y está acotado superiormente . En efecto, si r_o es un número racional tal que $r_o > x$ (y tal número existe pues $\mathbb{Q}$ no está acotado superiormente) entonces $h(r_o) >' h(r)$ para todos los $h(r)$ de A_x , pues $h \restriction \mathbb{Q}$ cumple la condición iii).

Decimos que z es la"cota superior mínima", o abreviadamente, el "supremo" de A_x si y sólo si :

1- z es una cota superior de A_x .

2- si y es una cota superior de A_x , entonces $z \leq y$.

Nótese que el supremo de A_x , si existe, es único, pues A está linealmente ordenado.

A_x tiene un supremo. En efecto:

La prueba viene dada por el lema siguiente:

Prueba : (continuación)

Lema : Si F es un cuerpo ordenado completo, entonces todo subconjunto $S \subset F$ acotado superiormente tiene un supremo.

Prueba : Sea $S \subset F$ y sea S acotado superiormente.
Sea P el conjunto de todas las cotas superiores de S.
Para todo $x \in S$ y para todo $y \in P$ ocurre que: $x \leq y$
Si para algún $y \in P$ ocurre que $y = x$ para algún $x \in S$ entonces claramente y será el supremo de S . Si esto no ocurre , eso es, si para todo $x \in S$ y para todo $y \in P$ ocurre que $x < y$, entonces, por el Axioma 18, existirá un z de F tal que $x < z < y$ para todo $x \in S$ y para todo $y \in P$. Luego, $z \notin S$, pues es mayor que todo elemento de S , y $z \notin P$, pues es menor que todo elemento de P . Pero z es una cota superior de S y por tanto, $z \in P$, lo que es absurdo.
Así pues, existe un $x \in S$ y un $y \in P$ tales que $x = y$ y tal y es el supremo de S.

Definimos ahora la función h para un elemento cualquiera $x \in \mathbb{R}$ de la manera siguiente:
$h(x) = \sup A_x$ (léase $\sup A_x$: el supremo de A_x).

Tenemos pues $h(x)$ definido de dos maneras, una para $x \in \mathbb{Q}$ y otra para $x \in \mathbb{R}$.
Vamos a ver que dichas definiciones concuerdan cuando x es un número racional :

Mostraremos que si $x \in \mathbb{Q}$, entonces
$\sup A_x = h(x)$

Prueba : (continuación)

Sabemos que si $x,y \in \mathbb{Q}$ y $y < x$, entonces $h(y) <' h(x)$. Así, todo elemento de A_x es menor que $h(x)$. Por tanto,

$$\sup A_x \leqslant' h(x)$$

Supongamos que $\sup A_x <' h(x)$. Luego existirá un número racional r tal que :

$$\sup A_x <' h(r) <' h(x)$$

En efecto, pues si a y b son elementos de A tales que $a < b$, entonces existe siempre un número racional r tal que $a < h(r) < b$. Supongamos que no existiera tal número racional r , eso es, supongamos que para todo número racional $r = m/n$, ocurre que $h(m/n) \geqslant \varepsilon$ donde $\varepsilon = b -' a$. Entonces tendríamos que para todo $n \in \mathbb{Z}$, $h(n) \leqslant h(m)/\varepsilon$ lo que significa que $h(m)/\varepsilon$ es una cota superior del subconjunto $A' \subset A$ formado por todos los $h(n)$, donde $n \in \mathbb{Z}$. Pero A' no tiene cota superior, pues si tuviera una cota superior tendría un supremo. Supongamos que lo tenga y sea éste s. Para todo $n \in \mathbb{Z}$ ocurrirá que $s \geqslant h(n)$. De ahí se sigue que $s \geqslant h(n + 1)$ pues $n + 1 \in \mathbb{Z}$. Por tanto, $s \geqslant h(n) +' h(1)$. Luego, $s -' 1' \geqslant h(n)$ para todo $n \in \mathbb{Z}$ Lo que significa que $s -' 1'$ es también una cota superior de A' en contradicción con el hecho de que s es el supremo de A'. Por tanto, tal número racional existe.

Puesto que $h(r) <' h(x)$ tenemos que $r < x$ pues $r,x \in \mathbb{Q}$; lo que significa que $h(r) \in A_x$ y esto contradice el que $\sup A_x <' h(r)$. Por tanto, no puede ser que $\sup A_x <' h(x)$,con lo que tenemos :

$$\sup A_x = h(x)$$

Prueba : (continuación)

Así pues, las dos definiciones concuerdan cuando $x \in \mathbb{Q}$.

Vamos a demostrar ahora que h cumple las condiciones de isomorfía . Empezaremos por la condición iii):

iii) Sean $x,y \in \mathbb{R}$ tales que $x \leq y$.
Luego, claramente, $\sup A_x \leq \sup A_y$
y por tanto, $h(x) \leq h(y)$
(Del mismo modo a la inversa)

Probaremos ahora que $h: \mathbb{R} \longrightarrow A$ es biyectiva.
Para ello debemos comprobar que:
1- $x \neq y$ si y sólo si $h(x) \neq h(y)$
2- Si $a \in A$, entonces $a = h(z)$ para algún $z \in \mathbb{R}$.

1- Sea $x \neq y$. Luego, o bien $x < y$ o bien $y < x$. En el primer caso $h(x) < h(y)$ y en el segundo caso $h(y) < h(x)$ por iii). En cualquier caso $h(x) \neq h(y)$. (Del mismo modo a la inversa).

2- Sea $a \in A$ y sea B el conjunto de todos los números racionales r tales que $h(r) < a$.
B no es vacío y está acotado superiormente.
Luego, B tendrá un supremo. Sea $z = \sup B$.
Veamos que $a = h(z)$:
Supongamos que $a \neq h(z)$. Luego, o bien $a < h(z)$ o bien $a > h(z)$.
Si $a > h(z)$, entonces deberá existir un número racional r tal que $h(z) < h(r) < a$ lo que significa que $z < r$ y que r está en B. Y esto contradice el hecho de que $z = \sup B$.
Si $a < h(z)$ entonces deberá existir un número racional r tal que $a < h(r) < h(z)$

Prueba : (continuación)

De donde se sigue que $r < z$. Puesto que $z = \sup B$, tendremos que $r < s$ para algún $s \in B$. Por tanto, $h(r) < h(s) < a$ lo cual contradice que $a < h(r)$.
Así pues, $a = h(z)$ para algún $z \in \mathbb{R}$.

i) Sean $x, y \in \mathbb{R}$.
Supongamos que $h(x + y) \neq h(x) +' h(y)$.
Luego, o bien $h(x + y) < h(x) +' h(y)$ o bien $h(x + y) > h(x) +' h(y)$.
En el primer caso existirá un número racional r tal que : $h(x + y) < h(r) < h(x) +' h(y)$ de donde tenemos que $x + y < r$.
Luego, r podría escribirse como la suma de dos números racionales r_1 , r_2 : $r = r_1 + r_2$ donde $x < r_1$ y $y < r_2$. Por tanto, $h(r) = h(r_1 + r_2) = h(r_1) +' h(r_2) > h(x) +' h(y)$ lo que es una contradicción.
Luego, $h(x + y) = h(x) +' h(y)$. (Del mismo modo se prueba en el segundo caso).

ii) Sean $x, y \in \mathbb{R}$.
Supongamos que $h(x.y) \neq h(x) .' h(y)$
Procediendo del mismo modo que en el caso anterior, llegaremos a una contradicción.
Con lo cual queda probado que:
$h(x . y) = h(x) .' h(y)$

Así pues, h es un isomorfismo entre $\mathscr{R}$ y $\mathscr{A}$. Por tanto, la teoría de los números reales de segundo orden es categórica.

Dividiremos los axiomas de la geometría euclídea en cinco grupos:

1- axiomas de existencia.
2- axiomas de orden.
3- axiomas de congruencia.
4- axioma de las paralelas.
5- axiomas de continuidad.

El único axioma de 2º orden es el segundo axioma de continuidad. Los demás pueden formalizarse en la lógica de primer orden.

Para mayor comodidad en la lectura expondremos los axiomas de manera semiformalizada.

De hecho, sólo utilizando símbolos para puntos (letras mayúsculas latinas), un símbolo para la relación ternaria "estar entre" (E) entre puntos, y un símbolo para la relación binaria "congruente con" ($\simeq$) entre segmentos y entre ángulos, se pueden formalizar todos los axiomas de la geometría euclídea , además de los símbolos lógicos y de las variables, claro. Pero una tal formalización sería prácticamente ilegible, por lo que utilizaremos otros conceptos (que pueden ser sibolizados),además de los de "punto", "estar entre" y "congruente con", que definiremos a partir de éstos. Dichos conceptos, que iremos definiendo a medida que sean necesarios, son los de línea, plano, espacio, radio, segmento, ángulo,triángulo y tetraedro.

Hilbert, en sus "Fundamentos de la Geometría" toma como elementos básicos no definidos los de punto, línea y plano. Aquí, y para simplificar las pruebas posteriores utilizaremos como concepto primitivo sólo el de "punto" a partir del cual definiremos los demás.

En cuanto a las relaciones,Hilbert, además de las de "estar entre" y "congruente con" se vale de las relaciones "estar en" o "pertenecer a" para indicar que un punto (o un conjunto de puntos) forma parte de una línea o de un plano o que una línea (o un conjunto de líneas) está en un plano.Aquí no utilizaremos estas relaciones, pues son definibles a partir de la relación "estar entre", como podrá verse en las definiciones posteriores.

Así pues, a pesar de que en los axiomas aparezcan otros conceptos aparte de los de "punto", "estar entre" y "congruente con" debe tenerse presente que con sólo éstos sería suficiente.

1- axiomas de existencia :

Definición: Si A y B son dos puntos distintos, al conjunto de los puntos consistente en A, B y todos los puntos P tales que E APB o bien E PAB o bien E BAP lo llamaremos la <u>línea</u> AB.

1-1. Existen al menos tres puntos que no están en la misma línea.

Definición: El <u>segmento</u> $A \vdash\dashv B$ es el conjunto de todos los puntos P tales que E PAB y además A y B.

Definición: Si A,B y C no están en la misma línea, el <u>triángulo</u> ABC (o ΔABC) es el conjunto de todos los puntos de $A \vdash\dashv B$, $A \vdash\dashv C$ y $B \vdash\dashv C$.

Definición: Si A,B y C no están en la misma línea, el <u>plano</u> ABC es el conjunto de todos los puntos que están en las líneas que pasan por dos puntos de ΔABC.

1-2. Existen al menos cuatro puntos que no están en el mismo plano.

Definición: Si A,B,C y D son puntos distintos y no están en el mismo plano, el <u>tetraedro</u> ABCD (o ΔABCD) es el conjunto de todos los puntos que están dentro y en los triángulos ABC, ABD,ACD, y BCD. Un punto X está dentro de ΔABC si y sólo si hay puntos Z y W en caras distintas de ΔABC tales que E XZW. Las caras de ΔABC son los segmentos $A \vdash\dashv B$, $A \vdash\dashv C$ y $B \vdash\dashv C$.

Definición: El conjunto de todos los puntos de las líneas que pasan por dos puntos de ΔABCD es el <u>espacio</u> ABCD.

1-3. Todos los puntos están en el mismo espacio.

Este axioma 1-3 hace que la geometría euclídea quede restringida a tres dimensiones.

2- Axiomas de orden.

2-1. Si E BAC entonces A,B y C son distintos y E BCA.

2-2. Si A y C son distintos entonces hay un punto B tal que E BAC y hay un punto D tal que E CAD.

2-3. Si E BAC entonces no E CBA.

2-4. (Axioma de Pasch) Dados tres puntos A,B y C que no estén en la misma línea y dada una línea L en la que no esté ninguno de ellos, si un punto del segmento $A \vdash\!\dashv B$ está en dicha línea, entonces un punto de $A \vdash\!\dashv C$ o un punto de $B \vdash\!\dashv C$ también estará en dicha línea.

3- Axiomas de congruencia.

Definición: Si A,B y C son tres puntos distintos que están en una misma línea, el <u>radio</u> AB (o [AB) es el conjunto de puntos consistente en A , B y todos los puntos X tales que E XAB o E BAX . El radio CA] es el conjunto de puntos consistente en C,A y todos los puntos Y tales que E YCA o E CYA. En ambos casos A es el punto terminal.

3-1. Dado un segmento $A \vdash\!\dashv B$ y un punto A' en una línea L, en cada radio de L con punto terminal A hay un y sólo un punto B' tal que $A \vdash\!\dashv B \cong A' \vdash\!\dashv B'$.

3-2. Si $A \vdash\!\dashv B \cong A' \vdash\!\dashv B'$ entonces $A' \vdash\!\dashv B' \cong A \vdash\!\dashv B$.

3-3. Si $A \vdash\!\dashv B \simeq A' \vdash\!\dashv B'$ y $A' \vdash\!\dashv B' \simeq A'' \vdash\!\dashv B''$ entonces $A \vdash\!\dashv B \simeq A'' \vdash\!\dashv B''$.

3-4. Si $\text{E}\,BAC$ y $\text{E}\,B'A'C'$ y $A \vdash\!\dashv B \simeq A' \vdash\!\dashv B'$ y $B \vdash\!\dashv C \simeq B' \vdash\!\dashv C'$ entonces $A \vdash\!\dashv C \simeq A' \vdash\!\dashv C'$.

Definición: Si $h = [AB$ y $k = [AC$ son radios distintos con un punto terminal común, dicho par de radios constituyen el <u>ángulo</u> $\widehat{hk}$ o $\widehat{kh}$ (o bien el ángulo $\widehat{BAC}$ o $\widehat{CAB}$). (Los radios son las caras del ángulo y el punto terminal es el vértice del ángulo).

Definición: Sea una línea L en un plano α . Dos puntos X,Y de α estarán en el mismo lado de L en α si y sólo si $X \vdash\!\dashv Y$ y L no tienen ningún punto en común. <u>Un lado de L en α</u> estará formado por todos los puntos de α que están en el mismo lado de L en α y además L.

3-5. Sea un ángulo $\widehat{hk}$ en un plano α y una línea L en un plano α' así como un lado dado de L en α' . Sea h' un radio en L con punto terminal A . Existe entonces un único radio k' de punto terminal A en α' tal que $\widehat{hk} \simeq \widehat{h'k'}$ en el lado dado de L en α' .Todo ángulo es congruente a sí mismo.

3-6. Sean A,B,C tres puntos que no están en la misma línea y A',B',C' tres puntos que no están en la misma línea. Si tenemos que $A \vdash\!\dashv B \simeq A' \vdash\!\dashv B'$, $A \vdash\!\dashv C \simeq A' \vdash\!\dashv C'$ y $\widehat{BAC} \simeq \widehat{B'A'C'}$ entonces $\widehat{ABC} \simeq \widehat{A'B'C'}$ y $\widehat{ACB} \simeq \widehat{A'C'B'}$.

4- Axioma de las paralelas. (Axioma de Euclides)

4-1. Sea L una línea cualquiera y sea A un punto que no está en L. Sea α el plano determinado por L y A. Luego, hay una y sólo una línea L' en α que pasa por A y no tiene ningún punto en común con L.(no corta a L o es paralela a L).

5- Axiomas de continuidad.

5-1 (Axioma de Arquímedes). Sean $A \longmapsto B$ y $C \longmapsto D$ segmentos cualesquiera. Existe entonces en la línea AB un número finito de puntos $A_1, A_2, \ldots, A_n$ tales que el punto A_1 está situado entre A y A_2, el punto A_2 entre A_1 y A_3, etc. Los segmentos $A \longmapsto A_1$, $A_1 \longmapsto A_2, \ldots, A_{n-1} \longmapsto A_n$ son todos congruentes con el segmento $C \longmapsto D$ y el punto B está situado entre A y A_n.

5-2 (Axioma de Cantor). Sea un conjunto infinito de segmentos $A_1 \longmapsto B_1, A_2 \longmapsto B_2, \ldots$ en una línea cualquiera L tales que cada segmento esté situado en el interior del segmento precedente,(eso es,que para todo i, si X está en $A_i \longmapsto B_i$ entonces X está en $A_{i-1} \longmapsto B_{i-1}$) y para todo segmento $A_i \longmapsto B_i$ exista un índice $n \neq i$ tal que el segmento $A_n \longmapsto B_n$ es menor que tal segmento(eso es, que todo punto $X \in A_n \longmapsto B_n$ pertenece a tal segmento). Existe entonces en la línea L un punto Y tal que Y está en todos los segmentos $A_1 \longmapsto B_1, A_2 \longmapsto B_2, A_3 \longmapsto B_3, \ldots$ (Claramente este punto es único).

Escogiendo los símbolos primitivos adecuados, sólo los axiomas de continuidad precisan de la lógica de segundo orden para su formalización. No obstante, si utilizamos como símbolos primitivos sólo E y $\simeq$, además de las variables para puntos, entonces las definiciones dadas deben también formalizarse en segundo orden.

Antes de probar que la Geometría Euclídea de segundo orden es categórica, y para facilitar su lectura, damos a continuación un esquema de la prueba:

1- Se prueba primero que existe un isomorfismo h entre los números reales del intervalo $[0,1]$ y los puntos de un segmento $A \vdash\!\dashv B$ cualquiera. Ello se hace en dos pasos:

1-1 Se prueba que existe un isomorfismo h entre los números racionales de $[0,1]$ y el subconjunto de los puntos X del segmento $A \vdash\!\dashv B$ tales que $n(A \vdash\!\dashv X) \simeq m(A \vdash\!\dashv B)$ para algún $m/n \in [0,1]$.

1-2 Se extiende el isomorfismo a todo el intervalo $[0,1]$ y a todo el segmento $A \vdash\!\dashv B$.

2- Comprobamos a continuación que existe un isomorfismo g entre los números reales y la línea AB.

3- Se define la función "distancia" entre puntos de AB y se comprueba que la congruencia entre segmentos de AB y la relación E entre puntos de AB pueden expresarse en términos de dicha función. Este resultado va a ser imprescindible para la prueba final.

4- Probamos que existe un sistema de coordenadas cartesianas de origen A.

5- Se prueba que existe un isomorfismo entre los puntos del espacio euclídeo y $\mathbb{R}^3$. Para ello definimos una función f entre los puntos del espacio euclídeo y tríadas de puntos de los ejes de coordenadas y comprobamos que es biyectiva.

6- Se prueba que existe un isomorfismo entre dos espacios euclídeos cualesquiera. Se definen para ello las funciones d_0 y d_1 (distancias) entre puntos de dos espacios euclídeos P_0 y P_1 respectivamente a partir de la función d (distancia entre puntos de la línea AB).

================

Proposición : La Geometría Euclídea de segundo orden es categórica.

Prueba: Sea $\langle P , E , \simeq \rangle$ un modelo de la geometría euclídea.

Sean $A,B \in P$ distintos.
Consideremos el segmento $A \longmapsto B$.

Para todo X,Y de $A \longmapsto B$ tenemos que:

$X =' Y \longleftrightarrow A \longmapsto X \simeq A \longmapsto Y$

por el axioma 3-1.

Por otra parte definimos:

Prueba: (continuación)

$$X <' Y \longleftrightarrow E\,XAY$$

Vamos a probar que $\langle A \vdash\!\dashv B, =', <' \rangle$ es isomorfo a $\langle [0,1], =, < \rangle$ donde $[0,1]$ es el intervalo cerrado de los números reales comprendidos entre 0 y 1, $=$ es la relación de igualdad entre números reales y $<$ es la relación "menor que" entre números reales.

1-1 Prueba: Sea $E\,XAB$.
Simbolizaremos por $n(A \vdash\!\dashv X)$ el segmento que resulta de repetir n veces el segmento $A \vdash\!\dashv X$ sobre la línea AB a partir de A. O más exactamente, al segmento $A \vdash\!\dashv Y$ tal que $A \vdash\!\dashv Y$ es congruente con el segmento construido de la manera siguiente: tomamos $A \vdash\!\dashv X$. Luego tomamos el punto X' tal que $A \vdash\!\dashv X \simeq X \vdash\!\dashv X'$. Repetimos este proceso hasta que tenemos n segmentos $A \vdash\!\dashv X$, $X \vdash\!\dashv X'$, $X' \vdash\!\dashv X''$..... todos congruentes. Tomamos finalmente el segmento $A \vdash\!\dashv X''\ldots\ldots'$ (n-1 veces).

Vamos a probar ahora el lema siguiente:

Lema: Para cualquier entero positivo n y para cualquier segmento $C \vdash\!\dashv D$, existe un punto X de $C \vdash\!\dashv D$ tal que $n(C \vdash\!\dashv X) \simeq C \vdash\!\dashv D$.

Prueba: si n=1 tal punto X existe pues en este caso será el punto D.
Supongamos que existe para n=m y veamos que también existe para $n=m+1$.
Veamos que existe un $W \in C \vdash\!\dashv D$ tal que: $m(W \vdash\!\dashv D) \simeq C \vdash\!\dashv W$. Supongamos lo contrario, eso es, que para todo punto $W \in C \vdash\!\dashv D$, $m(W \vdash\!\dashv D) \not\simeq C \vdash\!\dashv W$
Luego, o bien $m(W \vdash\!\dashv D) < C \vdash\!\dashv W$ o bien

Prueba: (continuación)

o bien $m(W \vdash\!\dashv D) > C \vdash\!\dashv W$ (donde el signo $\angle$ indica que si $m(W' \vdash\!\dashv D) \simeq C \vdash\!\dashv W$ para algún W' y tal W' existe pues el lema vale para m, entonces $E\ W'CW$ y $>$ indica que $E\ WCW'$) para todo $W \in C \vdash\!\dashv D$.

Sea α el conjunto de los $W \in C \vdash\!\dashv D$ tales que $m(W \vdash\!\dashv D) \angle C \vdash\!\dashv W$

Sea β el conjunto de los $W \in C \vdash\!\dashv D$ tales que $m(W \vdash\!\dashv D) > C \vdash\!\dashv W$

Luego, para todo $W \in C \vdash\!\dashv D$,o bien $W \in \alpha$ o bien $W \in \beta$. Luego, para todo $X_0 \in \alpha$ y para todo $X_1 \in \beta$, existirá un Y tal que $E\ YX_0X_1$ ya que para todo $X_0 \in \alpha$ y para todo $X_1 \in \beta$ $E\ X_1CX_0$ (Véase el axioma 5-2).

$Y \notin \alpha$ pues $E\ YCX_0$ para todo $X_0 \in \alpha$.

$Y \notin \beta$ pues $E\ X_1CY$ para todo $X_1 \in \beta$.

lo que es una contradicción.

Así pues, $m(W \vdash\!\dashv D) \simeq C \vdash\!\dashv W$ para algún $W \in C \vdash\!\dashv D$.

Luego, $m + 1(W \vdash\!\dashv D) \simeq C \vdash\!\dashv D$.

Sea X tal que $W \vdash\!\dashv D \simeq C \vdash\!\dashv X$.

Tendremos que $m + 1(C \vdash\!\dashv X) \simeq C \vdash\!\dashv D$ lo que queríamos probar.

Sea $n(A \vdash\!\dashv Y) \simeq A \vdash\!\dashv B$ y sea $m(A \vdash\!\dashv Y) \simeq A \vdash\!\dashv X$ tal que $m \leq n$. Luego, $n(A \vdash\!\dashv X) \simeq m(A \vdash\!\dashv B)$.

Sea ahora la función $h: A \vdash\!\dashv B \longrightarrow [0,1]$ tal que:

$h(A) = 0$

$h(B) = 1$

$h(X) = m/n$ si y sólo si $n(A \vdash\!\dashv Y) \simeq m(A \vdash\!\dashv B)$

Vamos a probar que $h(X) \leq h(Y) \longleftrightarrow X \leq' Y$

Prueba: Sea $h(X) = m/n$ y sea $h(Y) = m'/n'$

Supongamos que $h(X) = h(Y)$. Luego, $m/n = m'/n'$ de donde $m = k.m'$ y $n = k.n'$ para un entero positivo k.

Prueba: (continuación)

Sea $n(A \mapsto X) \simeq m(A \mapsto B)$ y $n'(A \mapsto Y) \simeq m'(A \mapsto B)$
Luego, $n(A \mapsto X) \simeq m(A \mapsto B) \simeq k.m'(A \mapsto B) \simeq k.n'(A \mapsto Y) \simeq n(A \mapsto Y)$ de donde $X =' Y$.
Supongamos que $h(X) < h(Y)$. Luego, $m/n < m'/n'$ eso es, $m.n' < n.m'$. De donde:
$m.n'(A \mapsto B) <' n.m'(A \mapsto B)$ y de aquí :
$n'.n(A \mapsto X) <' n.n'(A \mapsto Y)$. Por tanto, $X <' Y$.

Supongamos que $X =' Y$. Tenemos que:
$A \mapsto X \simeq m/n(A \mapsto B)$ y $A \mapsto Y \simeq m'/n'(A \mapsto B)$
Por tanto, $m/n(A \mapsto B) \simeq m'/n'(A \mapsto B)$. De donde $m/n = m'/n'$.
Si $X <' Y$ entonces tendremos que:
$m/n(A \mapsto B) <' m'/n'(A \mapsto B)$. De donde $m/n < m'/n'$.
Lo que queríamos probar.

1-2 Pero la función h no tiene como dominio a todo el conjunto $A \mapsto B$. En efecto:

Sea P_0 el subconjunto de $A \mapsto B$ formado por todos los puntos X tales que $h(X) = m/n$ para algún $m/n \in [0,1]$.
Veamos que todo subconjunto P_1 de P_0 formado por todos los elementos $Y \in P_0$ tales que $Y <' Z$ para algún $Z \in P_0$ no tiene elemento máximo, eso es, no hay ningún elemento $W \in P_1$ tal que $W \geq' X$ para todo $X \in P_1$.
Efectivamente, supongamos lo contrario, eso es, que exista un elemento $W \in P_1$ tal que $W \geq' X$ para todo $X \in P_1$.
Puesto que $W \in P_1$, $W <' Z$. Luego, dado que W y Z pertenecen a P_0 , $h(W) = m/n$ y $h(Z) = m'/n'$ para algún m/n y m'/n' de $[0,1]$. De donde $m/n < m'/n'$ pues $W <' Z$ y por tanto, $m.n' < m'.n$. Luego, $m.n' + k = m'.n$ para algún entero positivo k. De donde $m.n' < m.n' + k/2 < n.m'$. De lo cual se sigue que $m/n < (2.m.n' + k)/2.n.n' < m'/n'$.

Prueba: (continuación)

Luego, existirá un punto W' tal que $h(W') = (2.m.n' + k)/2.n.n')$. De donde $W <' W' <' Z$ y $W' \in P_1$ lo que contradice lo supuesto. Así pues, P_1 no tiene elemento máximo.

Pero P_0 debe ser distinto de $A \mapsto B$, pues de lo contrario, $A \mapsto B$ no satisfacería el axioma de Arquímedes, el cual debe ser satisfecho pues $A \mapsto B \in \mathcal{P}$.

En efecto, supongamos que en $A \mapsto B$ sólo existan los elementos de P_0. Luego, existirá un punto X de $A \mapsto B$ tal que para ningún n, $n(A \mapsto X) >' A \mapsto B$ lo cual es precisamente la negación de la propiedad arquimediana.

Prueba: es evidente, pues para todo n existe un punto X de $A \mapsto B$ tal que $n(A \mapsto X) \simeq A \mapsto B$ (Por el lema probado anteriormente). Nótese que para todo $m < n$, $m(A \mapsto X) <' A \mapsto B$.

Luego, existirá un punto X de $A \mapsto B$ tal que para todo n, $n(A \mapsto X) \leq' A \mapsto B$. Lo que queríamos probar.

Esto es una consecuencia del hecho de que todo subconjunto P_0 formado por todos los $Y \in P_0$ tales que $Y <' Z$ para algún $Z \in P_0$ no tiene elemento máximo.

En efecto, sea $n(A \mapsto X) \simeq m(A \mapsto B)$ y sea P_1 el subconjunto de P_0 formado por todos los Y de P_0 tales que $Y <' X$. Si P_1 tuviera elemento máximo, eso es, un elemento W tal que $W \geq' Y$ para todo $Y \in P_1$ entonces existiría un n' tal que : $n'(A \mapsto W) \simeq m(A \mapsto B)$. Luego, $m/n > m/n'$. De donde $n < n'$.

Así pues, para todo punto X de $A \mapsto B$ tal que $n(A \mapsto X) \simeq m(A \mapsto B)$ para algún n, existe un n' tal que $n'(A \mapsto X) >' m(A \mapsto B)$. Eso es, se cumple la propiedad arquimediana.

Por tanto, puesto que $A \mapsto B$ debe satisfacer el axioma de Arquímedes, debemos admitir que todo

Prueba: (continuación)

subconjunto P_1 de P_0 formado por todos los $Y \in P_0$ tales que $Y <' Z$ para algún Z de P_0 tiene elemento máximo.

Para todo $X \in A \mapsto B$ y para todo $Y <' X$ de $A \mapsto B$, sea r_X el subconjunto de $[0,1]$ formado por todos los h(Y) de la forma m/n.
r_X no es vacío, pues $0 \in r_X$, y está acotado superiormente, 1 es una cota superior . Luego, r_X tiene un supremo.
Definimos de nuevo la función h del modo siguiente : $h(X) = \sup r_X$.

Veamos que esta definición concuerda con la anterior cuando h(X) es de la forma m/n.
Todo elemento de r_X tiene que ser menor o igual que h(X) pues $X \leq' Y \longleftrightarrow h(X) \leq h(Y)$
Por tanto, $\sup r_X \leq h(X)$.
Supongamos que $\sup r_X < h(X)$. Luego, existirá un $h(Y) = m/n$ tal que $\sup r_X < h(Y) < h(X)$ (Véase la Pág. 99). Con lo que $h(Y) > \sup r_X$ y $h(Y) \in r_X$ lo que es una contradicción. Luego, $\sup r_X = h(X)$.

Veamos ahora que $h: A \mapsto B \longrightarrow [0,1]$ es biyectiva. Para ello debemos probar que :
i- $X =' Y \longleftrightarrow h(X) = h(Y)$ donde $X,Y \in A \mapsto B$
ii- Para todo $r \in [0,1]$ existe un W de $A \mapsto B$ tal que $h(W) = r$.

Prueba: i- Sea $X =' Y$. Luego, $r_X = r_Y$ y por tanto, $\sup r_X = \sup r_Y$ de donde $h(X) = h(Y)$. Análogamente a la inversa.
ii- Sea $r \in [0,1]$. r es el supremo del conjunto de todos los $r_0 \in [0,1]$ tales que r_0 pertenece a $\mathbb{Q}$ y $r_0 < r$.
Veamos que todo punto X de $A \mapsto B$ es el supremo

Prueba: (continuación)

de A_X donde A_X es el subconjunto de todos los puntos Y de $A \longmapsto B$ tales que $Y <' X$ y $h(Y) = r_0$ donde $r_0 \in \mathbb{Q}$.
A_X tiene supremo, pues A_X tiene elemento máximo, eso es, un elemento W tal que para todo $Y \in A_X$, $W \geqslant' X$.
Si $W >' X$ entonces existiría un punto Z de $A \longmapsto B$ tal que $W >' Z >' X$ y tal que $h(Z) = s$ donde $s \in \mathbb{Q}$. En efecto, supongamos lo contrario. Ello significa que para todo número racional s de $[0,1]$ distinto de 0, $s \geqslant h(W')$ donde $A \longmapsto W' \simeq W \longmapsto X$. Consideremos los s de la forma $1/n$. Luego, para todo entero positivo n , $n(A \longmapsto W') \leqslant' A \longmapsto B$ lo que contradice el axioma de arquímedes. Por tanto, $W =' X$.
Así pues, para todo r de $[0,1]$ existe un X de $A \longmapsto B$ tal que $h(X) = r$. Tal X será el supremo de A_X .

Para probar que h es un isomorfismo, bastará comprobar que : $X \leqslant' Y \longleftrightarrow h(X) \leqslant h(Y)$ para todo X,Y de $A \longmapsto B$.
Que $X =' Y \longleftrightarrow h(X) = h(Y)$ ya lo hemos probado más arriba.
Por otra parte,que $X <' Y \longleftrightarrow h(X) < h(Y)$ es evidente, pues si $X <' Y$, $\sup A_X <' \sup A_Y$ de donde $h(X) < h(Y)$. Análogamente a la inversa.

Así pues, h es un isomorfismo entre
$\langle A \longmapsto B , =' , <' \rangle$ y $\langle [0,1] , = , < \rangle$.

2- De aquí se sigue que existirá un isomorfismo f_n entre $\langle n(A \longmapsto B), =' , <' \rangle$ y $\langle [0,n] , = , < \rangle$ para cada n entero positivo.
Simbolizamos por $-n(A \longmapsto B)$ el segmento que resulta de la siguiente construcción: tomamos el punto

Prueba: (continuación)

X de la línea AB tal que $E\ AXB$ y tal que $X \vdash\!\dashv A \simeq A \vdash\!\dashv B$. Luego tomamos el punto X' de la misma línea tal que $E\ XX'A$ y tal que $X' \vdash\!\dashv X \simeq X \vdash\!\dashv A$ y así sucesivamente. Tomamos finalmente $A \vdash\!\dashv X^{''\cdots\cdots'\ (n-1 \text{ veces})}$.

Por tanto, también xistirá un isomorfismo f'_n entre $\langle -n(A \vdash\!\dashv B), =', <' \rangle$ y $\langle [-n,0] , =, < \rangle$ para cada n entero positivo.

Dado que tanto la geometría euclídea como la teoría de los números reales incluyen como teorema la propiedad arquimediana, tenemos que cualquier punto de AB estará en algún $n(A \vdash\!\dashv B)$ donde $n \in \mathbb{Z}$ y cualquier número real estará en algún $[0,n]$ donde $n \in \mathbb{Z}$.
Luego, puesto que para todo n, $f_{n-1} \subset f_n$, se sigue que $f = \bigcup f_n$ es un isomorfismo entre $\langle [AB , =' , <' \rangle$ y $\langle \mathbb{R}^+, = , < \rangle$
y puesto que para todo $-n$, $f'_{n-1} \subset f'_n$ se sigue que $f' = \bigcup f'_n$ será un isomorfismo entre $\langle XA] , =' , < \rangle$ y $\langle \mathbb{R}^-, = , < \rangle$.
De todo lo que antecede se sigue que deberá existir un isomorfismo $g = f \cup f'$ entre $\langle AB , =' , <' \rangle$ y $\langle \mathbb{R}, = , < \rangle$.

3- Definimos ahora una función $d: AB \times AB \longrightarrow \mathbb{R}$ a la que llamaremos "distancia" de la manera siguiente: $d(XY) = \left| g(X) - g(Y) \right|$ donde X,Y pertenecen a AB y g es el isomorfismo entre AB y $\mathbb{R}$.
$g(X) = \sup r_X$ donde r_X está formado por todos los $r \in \mathbb{Q}$ tales que $r < g(X)$.
Pero $\sup r_X = \sup \{ m/n \ / \ n(A \vdash\!\dashv X) >' m(A \vdash\!\dashv B) \}$
pues $g(X) = m/n$ si y sólo si $n(A \vdash\!\dashv X) \simeq m(A \vdash\!\dashv B)$

Prueba: (continuación)

Lo mismo vale para $g(Y)$.

Si $X \vdash\!\dashv Y \simeq Z \vdash\!\dashv W$ entonces

$$\sup \{ m/n \ / \ n(X \vdash\!\dashv Y) >' m(A \vdash\!\dashv B) \} =$$

$$\sup \{ m/n \ / \ n(Z \vdash\!\dashv W) >' m(A \vdash\!\dashv B) \}$$

(donde $n(X \vdash\!\dashv Y)$ simboliza el segmento $X \vdash\!\dashv Y$ repetido n veces a partir de A. Igualmente con $n(Z \vdash\!\dashv W)$). Tendremos, pues, que:

$$\Big| \sup \{ m/n \ / \ n(A \vdash\!\dashv X) >' m(A \vdash\!\dashv B) \} -$$

$$\sup \{ m/n \ / \ n(A \vdash\!\dashv Y) >' m(A \vdash\!\dashv B) \} \Big| =$$

$$\Big| \sup \{ m/n \ / \ n(A \vdash\!\dashv Z) >' m(A \vdash\!\dashv B) \} -$$

$$\sup \{ m/n \ / \ n(A \vdash\!\dashv W) >' m(A \vdash\!\dashv B) \Big|$$

ya que si $X <' Y$, se sigue que

$$\{ m/n \ / \ n(A \vdash\!\dashv X) >' m(A \vdash\!\dashv B) \} \subset$$

$$\{ m/n \ / \ n(A \vdash\!\dashv Y) >' m(A \vdash\!\dashv B) \}$$

Por tanto, $\left| g(X) - g(Y) \right| = \left| g(Z) - g(W) \right|$

Análogamente a la inversa. Luego,

$X \vdash\!\dashv Y \simeq Z \vdash\!\dashv W \longleftrightarrow d(XY) = d(ZW)$.

Veamos ahora que $\mathrm{E}\,XYZ \longleftrightarrow d(YX) + d(XZ) = d(YZ)$

Sea $\mathrm{E}\,XYZ$. Luego, $Y <' X <' Z$ y por tanto $g(Y) < g(X) < g(Z)$.

si $g(X) < 0$, $(g(Y) - g(X)) < 0$ y $(g(X) - g(Z)) < 0$.

si $g(X) = 0$, $(g(Y) - g(X)) < 0$ y $(g(X) - g(Z)) < 0$.

si $g(X) > 0$, $(g(Y) - g(X)) < 0$ y $(g(X) - g(Z)) < 0$.

Luego, en cualquier caso,

$$d(YX) + d(XZ) = \left| g(Y) - g(X) \right| + \left| g(X) - g(Z) \right|$$

$$= \left| g(Y) - g(X) + g(X) - g(Z) \right| = \left| g(Y) - g(Z) \right|$$

$$= d(YZ)$$

Prueba: (continuación)

Sea $d(YX) + d(XZ) = d(YZ)$. Luego,

$$\left| g(Y) - g(X) \right| + \left| g(X) - g(Z) \right| =$$

$\left| g(Y) - g(Z) \right|$ lo que quiere decir que $(g(Y) - g(X))$ tiene el mismo signo que $(g(X) - g(Z))$. De donde se sigue que $g(Y) < g(X) < g(Z)$ y por tanto $Y <' X <' Z$ Luego, $\boldsymbol{E}\, XYZ$. Lo que queríamos probar.

4- Decimos que una línea L es perpendicular a otra línea L' si y sólo si tienen un punto en común A y existe un punto $B \in L$ y un punto $C \in L'$ tales que $\widehat{CAB}$ es un ángulo recto. Decimos que un ángulo $\widehat{CAB}$ es recto si y sólo si existe un punto Y tal que $\boldsymbol{E}\, ABY$ y tal que $\widehat{CAB} \simeq \widehat{CAY}$.

Veamos que existe una línea AC tal que AC es perpendicular a AB y cuyo punto común es A.
Que existe una línea AC que tiene en común con AB sólo el punto A es evidente, pues existe al menos un punto $C \notin AB$.
Debemos ver, pues, solamente, que existe una tal línea AC tal que $\widehat{CAB}$ es un ángulo recto.
Sea $X \notin AB$ y sea el ángulo $\widehat{XAB}$. Existirá entonces un punto $Y \notin AB$ tal que $\widehat{XAB} \simeq \widehat{YAB}$ y tal que X e Y están en lados distintos del plano determinado por AB y X, el cual queda dividido en dos partes por la línea AB. (Axioma 3-5)
Sean los puntos Z,W tales que $A \mapsto Z \simeq A \mapsto W$ donde $Z \in AX$ y $W \in AY$. Sea la línea ZW . Si $A \in ZW$ entonces $\widehat{ZAB} \simeq \widehat{WAB}$ y dichos ángulos son rectos.
Si ello no ocurre, de todos modos la línea ZW es perpendicular a AB. En efecto, pues ZW corta la línea AB. Sea V el punto de intersección.
Tenemos pues dos triángulos $\triangle AZV$ y $\triangle AVW$.
Puesto que $A \mapsto V \simeq A \mapsto V$, $A \mapsto Z \simeq A \mapsto W$ y

Prueba: (continuación)

$\widehat{ZAV} \simeq \widehat{WAV}$ se sigue que $\widehat{ZVA} \simeq \widehat{WVA}$ (Axioma 3-6)
Por tanto, $\widehat{ZVA}$ es recto y ZW es perpendicular a AB. El hecho de que ZW sea perpendicular a AB en el punto A es sólo una cuestión de construcción.
Luego, existe una línea AC tal que AC es perpendicular a AB en el punto A.
Sea α el plano en el que están A, B y C.
Luego, existirá una línea AD tal que AD es perpendicular a AB y perpendicular a AC. En efecto, todas las líneas perpendiculares a AB en el punto A están en el mismo plano. Sea éste β . Lo mismo ocurre con todas las perpendiculares a AC por el punto A . Sea este plano γ . β y γ tienen un punto en común, A. Luego, tienen una línea en común AD y ésta es perpendicular a AB y perpendicular a AC.
Por tanto, existen tres líneas AB, AC y AD perpendiculares entre sí por el punto A.

Hemos probado que para toda línea AB,
$\langle AB , =' , <' \rangle \cong \langle \mathbb{R} , = , < \rangle$
Por tanto tendremos que:
$\langle AC , =' , <' \rangle \cong \langle AD , =', <' \rangle \cong$
$\langle AB , =' , <' \rangle \cong \langle \mathbb{R} , = , < \rangle$
(Suponemos que $A \mapsto B \simeq A \mapsto C \simeq A \mapsto D$ y que los isomorfismos se han definido de forma análoga).

5- Sea ahora $\mathbb{P}$ el conjunto de los puntos del espacio euclídeo. Sea f una función tal que a cada punto X de $\mathbb{P}$ le asigna una tríada de puntos $(X_\alpha, X_\beta, X_\gamma)$ donde X_α es el punto de intersección entre la línea AB y la perpendicular a esta línea que pasa por el punto X ; X_β es el punto de intersección entre la línea AC y la perpendicular a ésta que pasa por X y X_γ es el punto de intersección entre la línea AD y la perpendicular a

Prueba: (continuación)

ésta que pasa por X.
Estas perpendiculares existen y son únicas.
En efecto, por X pasa una paralela y sólo una a AB (respectivamente a AC y AD). Sea ésta L.
Luego, existe una perpendicular a L en el punto X y puesto que L y AB son paralelas, dicha perpendicular lo es también a AB. Que es única es evidente, pues de haber dos tendrían que estar en planos distintos, pero AB y X están en el mismo plano.
f es inyectiva, pues dicha tríada es única y si $X \neq Y$ se sigue que $f(X) \neq f(Y)$.
f es exhaustiva, pues dados tres puntos $X_\alpha \in AB$, $X_\beta \in AC$, $X_\gamma \in AD$, siempre podemos tener tres líneas perpendiculares a AB,AC y AD en los puntos X_α ,X_β y X_γ respectivamente que coincidan en un punto X . En efecto, pues las perpendiculares a X_α están en el plano α , las perpendiculares a X_β en el plano β y las perpendiculares a X_γ en el plano γ . Tenemos, pues, tres planos que intersectan entre sí, pues son perpendiculares entre sí. Luego, la intersección de dos de ellos es una línea y la intersección de ésta con el tercero nos da un punto.
Así pues, f es biyectiva.

6- Sea ahora h : $P \longrightarrow \mathbb{R}^3$ tal que:
$h\ (X) = (\ g(X_\alpha), g(X_\beta), g(x_\gamma))$
donde g es el isomorfismo entre una lína y $\mathbb{R}$ anteriormente construido.
Puesto que f es biyectiva y g también, se sigue que h es biyectiva.

Sean $\langle P_0, E_0, \simeq_0 \rangle$ y $\langle P_1, E_1, \simeq_1 \rangle$ dos modelos de la geometría euclídea cualesquiera.

Prueba: (continuación)

Luego, existirán biyecciones:

$h_0 : \mathbb{P}_0 \longrightarrow \mathbb{R}^3$ y $h_1 : \mathbb{P}_1 \longrightarrow \mathbb{R}^3$

Sea $h: \mathbb{P}_0 \longrightarrow \mathbb{P}_1$ tal que:

$h(X) = h_1^{-1}(h_0(X))$

h es biyectiva, pues h_0 y h_1 lo son.

Sean $d_0 : \mathbb{P}_0^2 \longrightarrow \mathbb{R}$ y $d_1 : \mathbb{P}_1^2 \longrightarrow \mathbb{R}$

funciones a las que llamaremos "distancia" y que definimos de la siguiente manera:

$$d_0(XY) = \sqrt{d(X_\alpha Y_\alpha)^2 + d(X_\beta Y_\beta)^2 + d(X_\gamma Y_\gamma)^2}$$

por el teorema de Pitágoras. Donde d es la distancia definida anteriormente. Nótese que d_0 coincide con d si restringimos su dominio a los puntos de AB. Del mismo modo definimos d_1 .

La función h preserva la distancia:

En efecto, sean $h_0(X) = (r_\alpha, r_\beta, r_\gamma)$ y $h_0(Y) = (s_\alpha, s_\beta, s_\gamma)$. Tendremos que:

$h_1(h(X)) = h_1(h_1^{-1}(h_0(X))) = h_0(X)$ y

$h_1(h(X)) = h_1(h_1^{-1}(h_0(Y))) = h_0(Y)$

Por tanto,

$$d_0(XY) = \sqrt{(r_\alpha - s_\alpha)^2 + (r_\beta - s_\beta)^2 + (r_\gamma - s_\gamma)^2} =$$

$d_1(h(X)h(Y))$

Veamos que h es un isomorfismo:

i- $E_0 XYZ \longleftrightarrow E_1 h(X)h(Y)h(Z)$

Si E_0 XYZ entonces X, Y y Z están alineados y por tanto, $d_0(YX) + d_0(XZ) = d_0(YZ)$.

Si $d_0(YX) + d_0(XZ) = d_0(YZ)$, entonces X, Y y Z deben estar alineados. En efecto, supongamos que no lo estén. Sea el triángulo ΔXYZ . Si ΔXYZ es rectángulo, se sigue que $d_0(YX) + d_0(XZ) >$ d (YZ) pues $d_0(YZ) = \sqrt{d_0(YX)^2 \quad d_0(XZ)^2}$.

Prueba: (continuación)

Sea $\triangle XYZ$ no rectángulo. Sea la perpendicular a $Y \longmapsto Z$ que pasa por X . Sea W el punto de intersección. Luego, $d_0(YZ) = d_0(YW) + d_0(WZ)$. Pero $d_0(YW) = \sqrt{d_0(XY)^2 - d_0(XW)^2}$ y $d_0(WZ) = \sqrt{d_0(XZ)^2 - d_0(XW)^2}$ de donde $d_0(XY) > d_0(YW)$ y $d_0(XZ) > d\ (WZ)$. Por tanto, $d_0(YX) + d\ (XZ) > d_0(YZ)$ contra lo supuesto.

Así pues, X,Y y Z están alineados y por lo tanto, $E_0 XYZ$.

Análogamente tendremos que $E_1 h(X)h(Y)h(Z)$ si y sólo si $d_1(h(Y)h(X)) + d_1(h(X)h(Z)) = d_1(h(Y)h(Z))$

De todo lo que antecede tenemos que si $E_0 XYZ$ entonces $d_0(YZ) = d_0(XY) + d_0(XZ)$ y de ahí $d_1(h(Y)h(Z)) = d_1(h(X)h(Y)) + d_1(h(X)h(Z))$ ya que h preserva la distancia. De donde,

$E_1 h(X)h(Y)h(Z)$

Análogamente a la inversa.

ii- $X \longmapsto Y \simeq_0 Z \longmapsto W \longleftrightarrow h(X) \longmapsto h(Y) \simeq_1 h(Z) \longmapsto h(W)$

Si $X \longmapsto Y \simeq_0 Z \longmapsto W$ entonces, $d_0(XY) = d_0(ZW)$ ya que $X \longmapsto Y$ y $Z \longmapsto W$ pueden ser considerados como las hipotenusas de dos triángulos rectángulos. Y por tanto, $d_0(XY) = \sqrt{d(X_\alpha Y_\alpha)^2 + d(X_\beta Y_\beta)^2 + d(X_\gamma Y_\gamma)^2} = \sqrt{d(Z_\alpha W_\alpha)^2 + d(Z_\beta W_\beta)^2 + d(Z_\gamma W_\gamma)^2} = d_0(ZW)$

De donde, $d_1(h(X)h(Y)) = d_1(h(Z)h(W))$ pues h preserva la distancia. Por tanto,

$h(X) \longmapsto h(Y) \simeq_1 h(Z) \longmapsto h(W)$

Análogamente a la inversa.

iii- $\widehat{ABC} \simeq_0 \widehat{DEF} \longleftrightarrow \widehat{h(A)h(B)h(C)} \simeq_1 \widehat{h(D)h(E)h(F)}$

Sea $\widehat{ABC} \simeq_0 \widehat{DEF}$. Puesto que podemos escoger A,C, D y F tales que $A \longmapsto B \simeq_0 D \longmapsto E$ y $B \longmapsto C \simeq_0 E \longmapsto F$ tendremos,por el axioma 3-6 que $\widehat{ACB} \simeq_0 \widehat{DFE}$ y que

Prueba: (continuación)

$\widehat{BAC} \simeq_0 \widehat{FDE}$. De donde se sigue que $A \mapsto C \simeq_0 D \mapsto F$. En efecto, pues si $A \mapsto C \not\simeq_0 D \mapsto F$ entonces existiría un punto W del radio $[DF$ tal que $A \mapsto C \simeq_0 D \mapsto W$ donde $F \neq W$. Aplicando el axioma 3-6 tenemos que $\widehat{DEW} \simeq_0 \widehat{ABC}$ pues $\widehat{DFE} \simeq_0 \widehat{BAC}$ y $A \mapsto C \simeq_0 D \mapsto W$ y $B \mapsto A \simeq_0 D \mapsto E$. Pero esto contradice el que $\widehat{ABC} \simeq_0 \widehat{DEF}$.

Así pues, $A \mapsto C \simeq_0 D \mapsto F$.

Tendremos, por tanto, que $A \mapsto B \simeq_0 D \mapsto E$, $B \mapsto C \simeq_0 E \mapsto F$ y $A \mapsto C \simeq_0 D \mapsto F$. De donde, $h(A) \mapsto h(B) \simeq_1 h(D) \mapsto h(E)$, $h(B) \mapsto h(C) \simeq_1 h(E) \mapsto h(F)$ y $h(A) \mapsto h(C) \simeq_1 h(D) \mapsto h(F)$.

Es un conocido teorema de la geometría euclídea el que establece: " Si en triángulos ABC y A'B'C' ocurre que $A \mapsto B \simeq A' \mapsto B'$, $A \mapsto C \simeq A' \mapsto C'$ y $B \mapsto C \simeq B' \mapsto C'$ entonces $\widehat{ABC} \simeq \widehat{A'B'C'}$, $\widehat{BAC} \simeq \widehat{B'A'C'}$ y $\widehat{ACB} \simeq \widehat{A'C'B'}$ ". (Véase por ejemplo : Fishback,"Projective and Euclidean Geometry" Pág. 20 , 2ª Edición)

Por tanto, $\widehat{h(A)h(B)h(C)} \simeq_1 \widehat{h(D)h(E)h(F)}$

Análogamente a la inversa.

Así pues, h es un isomorfismo entre $\langle P_0, E_0, \simeq_0 \rangle$ y $\langle P_1, E_1, \simeq_1 \rangle$. Puesto que estos modelos son modelos cualesquiera de la geometría euclídea, se sigue que la geometría euclídea de segundo orden es categórica.

A N E X O S

Anexo 1

Teorema: La relación de isomorfía entre estructuras es una relación de equivalencia.

Prueba: Sean $\mathcal{A}$, $\mathcal{B}$ y $\mathcal{C}$ tres estructuras del mismo tipo.

Propiedad reflexiva: $\mathcal{A} \cong \mathcal{B}$.

i) claramente existe una función $h: A \longrightarrow A$ biyectiva.

~~xxi)~~ La función que asigna a cada elemento él mismo.

ii) para cada $i \in I$, $x_1, \ldots, x_{\mu(i)} \in A$:

$$h(f_i(x_1, \ldots, x_{\mu(i)})) = f_i(x_1, \ldots, x_{\mu(i)}) = f_i(h(x_1), \ldots, h(x_{\mu(i)}))$$

iii) para cada $j \in J$, $x_1, \ldots, x_{\delta(j)} \in A$:

$$\langle x_1, \ldots, x_{\delta(j)} \rangle \in R_j \longleftrightarrow \langle h(x_1), \ldots, H(x_{\delta(j)}) \rangle \in R_j$$

Propiedad simétrica: si $\mathcal{A} \cong \mathcal{B}$ entonces $\mathcal{B} \cong \mathcal{A}$

Supongamos que $\mathcal{A} \cong \mathcal{B}$.

i) Sea h' la función inversa de h. Entonces, si h es biyectiva, también lo será h'. Pero h lo es puesto que $\mathcal{A} \cong \mathcal{B}$.

ii) para cada $i \in I$, $x_1, \ldots, x_{\mu(i)} \in B$:

$$h'(g_i(x_1, \ldots, x_{\mu(i)})) = h'(h(f_i(h'(x_1), \ldots, h'(x_{\mu(i)}))))$$

pues $h(f_i(x_1, \ldots, x_{\mu(i)})) = g_i(h(x_1), \ldots, h(x_{\mu(i)}))$ ya que $\mathcal{A} \cong \mathcal{B}$.

Pero como h' es la función inversa de h:

$$h'(h(f_i(h'(x_1), \ldots, h'(x_{\mu(i)})))) = f_i(h'(x_1), \ldots, h'(x_{\mu(i)}))$$

iii) para cada $j \in J$, $x_1, \ldots, x_{\delta(j)} \in B$:

$$\langle x_1, \ldots, x_{\delta(j)} \rangle \in S_j \longleftrightarrow \langle h'(x_1), \ldots, h'(x_{\delta(j)}) \rangle \in R_j$$

pero $\langle h'(x_1), \ldots, h'(x_{\delta(j)}) \rangle \in R_j \longleftrightarrow$

$\longleftrightarrow \langle h(h'(x_1)), \ldots, h(h'(x_{\delta(j)})) \rangle \in R_j$ ya que

$$\langle x_1, \ldots, x_{\delta(j)} \rangle \in R_j \longleftrightarrow \langle h(x_1), \ldots, h(x_{\delta(j)}) \rangle \in S_j$$

pues $\mathcal{A} \cong \mathcal{B}$.

Pero como h' es ls función inversa de h:

$\langle h(h'(x_1)), \ldots, H(h'(x_{\delta(j)})) \rangle \in R_j \longleftrightarrow$

$\longleftrightarrow \langle x_1, \ldots, x_{\delta(j)} \rangle \in R_j$.

Propiedad transitiva: si $\mathcal{A} \cong \mathcal{B}$ y $\mathcal{B} \cong \mathcal{C}$ entonces $\mathcal{A} \cong \mathcal{B}$.

i) Sea h la biyección entre A y B, y sea h′ la biyección entre B y C. Entonces existirá una función h′′ biyectiva entre A y C: $h'' = h \circ h'$.

ii) para cada $i \in I$, $x_1, \ldots, x_{\mu(i)} \in A$:

$h(f_i(x_1, \ldots, x_{\mu(i)})) = g_i(h(x_1), \ldots, h(x_{\mu(i)}))$ pues $\mathcal{A} \cong \mathcal{B}$

y $h'(g_i(h(x_1), \ldots, h(x_{\mu(i)})) = k_i(h'(h(x_1)), \ldots, h'(h(x_{\mu(i)})))$ pues $\mathcal{B} \cong \mathcal{C}$.

pero como $h'' = h \circ h'$:

$k_i(h'(h(x_1)), \ldots, h'(h(x_{\mu(i)}))) = k_i(h''(x_1), \ldots, h''(x_{\mu(i)})$

iii) para cada $j \in J$, $x_1, \ldots, x_{\delta(j)} \in A$:

$\langle x_1, \ldots, x_{\delta(j)} \rangle \in R_j \leftrightarrow \langle h(x_1), \ldots, h(x_{\delta(j)}) \rangle \in S_j$ pues $\mathcal{A} \cong \mathcal{B}$.

$\langle h(x_1), \ldots, h(x_{\delta(j)}) \rangle \in S_j \leftrightarrow \langle h'(h(x_1) .. h'(h(x_{\delta(j)})) \rangle \in T_j$. Pues $\mathcal{B} \cong \mathcal{C}$.

Pero como $h'' = h \circ h'$:

$\langle x_1, \ldots, x_{\delta(j)} \rangle \in R_j \longleftrightarrow \langle h''(x_1) .. h''(x_{\delta(j)}) \rangle \in T_j$

Anexo 2

Teorema: Si $\mathcal{A} \cong \mathcal{B}$ (son isomorfos) luego $\mathcal{A} \equiv \mathcal{B}$ (son elementalmente equivalentes). Lo contrario sólo se cumple en el caso de que $\mathcal{A}$ sea finito.

Prueba: Sea $\mathcal{A} \cong \mathcal{B}$

Sea φ una fórmula tal que $\mathcal{A}$ Mod φ

Sea $\mathcal{J}: V \longrightarrow A$ una interpretación del conjunto de variables de φ en el universo A, tal que $\mathcal{J}$ sat φ. $\mathcal{J}$ también interpreta los relatores y functores de φ.

Sea h el isomorfismo entre $\mathcal{A}$ y $\mathcal{B}$.

Entonces habrá una interpretación $\mathcal{J}': V \longrightarrow B$ tal

(*) que: $H(\mathcal{J}(x_1, \ldots, x_m)) = \mathcal{J}'(x_1, \ldots x_m)$

donde $\langle x_1, \ldots, x_m \rangle = V$

Sea $\varphi = R_m x_1, \ldots x_m$

(**) $\mathcal{J}$ sat $R_m x_1, \ldots, x_m \longleftrightarrow \langle \mathcal{J}(x_1), \ldots, \mathcal{J}(x_m) \rangle \in \mathcal{J}(R_m)$

puesto que h es un isomorfismo entre $\mathcal{A}$ y $\mathcal{B}$ ocurre que:

para $\mathcal{J}(x_1), \ldots, \mathcal{J}(x_m) \in A$, se cumple que :

$\langle \mathcal{J}(x_1), \ldots, \mathcal{J}(x_m) \rangle \in \mathcal{J}(R_m) \longleftrightarrow$

$\langle h(\mathcal{J}(x_1)), \ldots, h(\mathcal{J}(x_m)) \rangle \in h(\mathcal{J}(R_m))$

pero según (*)

$\langle h(\mathcal{J}(x_1)), \ldots, h(\mathcal{J}(x_m)) \rangle \in h(\mathcal{J}(R_m)) =$

$\langle \mathcal{J}'(x_1), \ldots, \mathcal{J}'(x_m) \rangle \in \mathcal{J}'(R_m)$

y según (**)

$\langle \mathcal{J}'(x_1), \ldots, \mathcal{J}'(x_m) \rangle \in \mathcal{J}'(R_m) \longleftrightarrow \mathcal{J}'$ sat $R_m(x_1, \ldots x_m)$

por tanto $\mathcal{B}$ es modelo de φ.

Lo mismo sucede en los demás casos: $\varphi = \neg\alpha, \alpha \wedge \beta, \alpha \vee \beta, \alpha \longrightarrow \beta, \alpha \longleftrightarrow \beta, \bigwedge_x \alpha, \bigvee_x \alpha$.

Para cada φ, si $\mathcal{A}$ Mod φ entonces $\mathcal{B}$ Mod φ

Luego, si $\mathcal{A} \cong \mathcal{B}$ entonces $\mathcal{A} \equiv \mathcal{B}$.

Sea $\mathscr{A}$ finito. Luego, si $\mathscr{A} \equiv \mathscr{B}$, entonces $\mathscr{A} \cong \mathscr{B}$. Efectivamente:

Puesto que $\mathscr{A} \equiv \mathscr{B}$, para toda fórmula φ se cumple que $\mathscr{A}$ Mod $\varphi \longleftrightarrow \mathscr{B}$ Mod φ .
Supongamos que $\mathscr{A}$ y $\mathscr{B}$ no sean biyectables. Luego, $|\mathscr{A}| \neq |\mathscr{B}|$. Pero tenemos que $|\mathscr{A}| = n$ donde $n < \omega$, pues $\mathscr{A}$ es finito.

Entonces, la sentencia que afirma la existencia de exactamente n elementos es verdadera (o satisfecha) en $\mathscr{A}$ y no lo es en $\mathscr{B}$. Por tanto, si $\mathscr{A}$ es finito y si $\mathscr{A} \equiv \mathscr{B}$, se sigue que $\mathscr{A}$ y $\mathscr{B}$ son biyectables.

Veamos ahora que debe existir alguna biyección h de $\mathscr{A}$ en $\mathscr{B}$ tal que cumpla las condiciones ii) y iii) de isomorfía :

ii) Para cada $i \in I$, $x_1, \ldots, x_{\mu(i)} \in A$:
$$h(f_i(x_1, \ldots, x_{\mu(i)})) = g_i(h(x_1), \ldots, h(x_{\mu(i)}))$$

iii) Para cada $j \in J$, $x_1, \ldots, x_{\delta(j)} \in A$:
$\langle x_1, \ldots, x_{\delta(j)} \rangle \in Rj$ si y sólo si $\langle h(x_1), \ldots, h(x_{\delta(j)})) \rangle \in Sj$

En efecto, puesto que $\mathscr{A} \equiv \mathscr{B}$ y $\mathscr{A}$ y $\mathscr{B}$ son biyectables, debe existir una biyección $h: \mathscr{A} \longrightarrow \mathscr{B}$ tal que para cada $i \in I$, $x_1, \ldots, x_{\mu(i)} \in A$,

$$h(f_i(x_1, \ldots, x_{\mu(i)})) = g_i(h(x_1), \ldots, h(x_{\mu(i)}))$$

para cada función i-aria de $\mathscr{A}$ y cada función i-aria de $\mathscr{B}$. Pues de lo contrario, habría un término τ_i tal que para alguna interpretación $\mathscr{F}$ de τ_i sobre $\mathscr{A}$,

$\mathcal{F}(\tau_i) = f_i(x_1,\ldots,x_{\mu(i)})$ y no existiría ninguna interpretación $\mathcal{F}'$ sobre $\mathcal{B}$ de τ_i tal que $\mathcal{F}(\tau_i)$ denotara algún elemento de $\mathcal{B}$. Con lo cual, si φ fuera una fórmula en la que apareciese τ_i, φ podría ser interpretada y posiblemente satisfecha en $\mathcal{A}$ y en cambio no podría ser interpretada y por supuesto no satisfecha en $\mathcal{B}$. Por tanto, no necesariamente $\mathcal{A} \equiv \mathcal{B}$.

Puesto que $\mathcal{A} \equiv \mathcal{B}$ y $\mathcal{A}$ y $\mathcal{B}$ son biyectables, debe existir una biyección $h: \mathcal{A} \longrightarrow \mathcal{B}$ tal que para cada $j \in J$, $x_1,\ldots,x_{\delta(j)} \in A$:

$$\langle x_1,\ldots,x_{\delta(j)} \rangle \in Rj \longleftrightarrow \langle h(x_1),\ldots,h(x_{\delta(j)}) \rangle \in Sj$$

para cada relación j-aria de $\mathcal{A}$ y cada relación j-aria de $\mathcal{B}$. Pues de lo contrario podría ocurrir que para alguna interpretación $\mathcal{F}$ de φ sobre $\mathcal{A}$ siendo φ una fórmula del tipo $P^n\tau_1\ldots\tau_n$, $\mathcal{F}$ satisfaciera φ y no hubiera ninguna interpretación $\mathcal{F}'$ de φ sobre $\mathcal{B}$, con lo que φ no podría ser interpretada y por tanto no satisfecha en $\mathcal{B}$. Luego, no necesariamente $\mathcal{A} \equiv \mathcal{B}$.

Así pues, si $\mathcal{A} \equiv \mathcal{B}$ y $\mathcal{A}$ es finito, se sigue que $\mathcal{A} \cong \mathcal{B}$.

Si $\mathcal{A}$ es infinito y $\mathcal{A} \equiv \mathcal{B}$, entonces no necesariamente $\mathcal{A} \cong \mathcal{B}$. Véanse los ejemplos de la aritmética de Peano y de la teoría de los números reales, cuyos modelos son infinitos y existen modelos elementalmente equivalentes que no son isomorfos, los modelos no-standard.

Anexo 3

Sea $\mathcal{M}_o = \langle M , +', \cdot', S', 0' \rangle$.

Sea $\mathcal{M}_o' = \{ \tau_n / n \in \omega \}$ donde

$\tau_n = S' , \ldots\ldots , S' 0'$

Claramente, $\mathcal{M}_o' \subseteq \mathcal{M}_o$

Supongamos que h: $\mathcal{N} \cong \mathcal{M}_o$

Luego, debe existir un $n_o \in \mathbb{N}$ tal que n_o es el más pequeño de los n $\in \mathbb{N}$ tales que $h(n) \in \mathcal{M}_o - \mathcal{M}_o'$. Entonces, $n_o \neq 0$, pues $h(0) = 0'$ y $0' \in \mathcal{M}_o'$.

Por tanto, $n_o = Sm$ para algún m $\in \mathbb{N}$.

Pero luego, $h(n_o) = h(Sm) = S'h(m)$ con lo que $h(m) \in \mathcal{M}_o'$ pues $m < n_o$. Y entonces, $h(n_o) \in \mathcal{M}_o'$ pues $n_o = Sm = S , \ldots\ldots , S0$ lo que contradice que $h(n_o) \in \mathcal{M}_o - \mathcal{M}_o'$.

Luego, $n_o \neq 0$ y $n_o \neq Sm$ para todo m $\in \mathbb{N}$.

Así pues, tal n_o no existe y por tanto,se sigue que $\mathcal{N} \not\cong \mathcal{M}_o$.

Anexo 4

Sea $\mathcal{S} = \langle S , +' , \cdot' , \leq , 0' , 1', k \rangle$

Sea $\mathcal{S}_0$ la reducción de $\mathcal{S}$ al quitarle la función 0-aria k que sirve de denotación a la constante individual c . (Claramente $\mathcal{S}_0$ es modelo de $\sum$ y k $\in \mathcal{S}_0$).

Veamos que $\mathcal{S}_0$ y $\mathcal{R}$ no son isomorfos.

Supongamos que sí lo sean. Sea h: $\mathcal{R} \cong \mathcal{S}_0$

Luego, $h(n) = n'$ para todo $n \in \mathbb{N}$. Donde
$n = 1 + ,\ldots, + 1$ n veces y donde
$n' = 1' +' ,\ldots, +' 1'$ n veces.

Pero entonces, si $k > n'$ para todo n' , tenemos que :

$x < n \longrightarrow h(x) < h(n) = n'$, pues h es un isomorfismo. Con lo que $h(x) < k$ para todo $x \in \mathcal{R}$.

Luego, no existe ningún $x \in \mathcal{R}$ tal que $h(x) = k$ y por tanto, $\mathcal{R} \not\cong \mathcal{S}_0$.

N O T A S

Nota 1

Definición: $\mathcal{A}' \sqsubseteq \mathcal{A}$ ($\mathcal{A}'$ es una subestructura de $\mathcal{A}$) si y sólo si:

i) $A' \subseteq A$

ii) Cada función m-aria f' de $\mathcal{A}'$ es la restricción a A' de la correspondiente función f en $\mathcal{A}$:
$f' = f \restriction (A')^m$.

iii) Cada relación n-aria R' de $\mathcal{A}'$ es la restricción a A' de la correspondiente relación R de $\mathcal{A}$:
$R' = R \cap (A')^n$.

Nota 2

El esquema axiomático 14 expresa la condición de que todo polinomio de grado n tiene una raíz.

Nota 3

<u>Algebra de Lindenbaum</u>

Sea P un conjunto infinito de variables proposicionales.

Sea Φ el conjunto de todas las fórmulas del lenguaje proposicional con variables en P.

Sea $\sim$ la relación de equivalencia lógica en Φ. Para todo φ, ψ de Φ, $\varphi \sim \psi$ si y sólo si $\varphi \leftrightarrow \psi$ es una tautología.

Para cada $\varphi \in \Phi$, sea $[\varphi] = \{ \psi : \varphi \sim \psi \}$

Tomemos $B = \{ [\varphi] : \varphi \in \Phi \}$

Definimos:

$$0 = [p \wedge \neg p]$$
$$1 = [p \vee \neg p]$$
$$-[\varphi] = [\neg \varphi]$$
$$[\varphi] \wedge [\psi] = [(\varphi \wedge \psi)]$$
$$[\varphi] \vee [\psi] = [(\varphi \vee \psi)]$$

Con estas operaciones, $\langle B, \wedge, \vee, -, 0, 1 \rangle$ es un álgebra de Boole, el Algebra de Lindenbaum.

Es numerable, pues P lo es , y no posee átomos. En efecto : $[\varphi] \leq [\psi]$ si y sólo si $\varphi \models \psi$

Sea ahora $[\varphi] \in B$, $[\varphi] \neq 0$. Sea p una variable proposicional que no aparece en φ . Tomemos $\alpha = (\varphi \wedge p)$ Entonces, $0 < [\alpha] < [\varphi]$ con lo que $[\varphi]$ no es un átomo.

Nota 4

La suma y el producto son definibles en segundo orden a partir de 0 y S. En efecto:

i) $\bigvee f(\bigwedge xy(fx0 \doteq x \wedge fxSy \doteq Sfxy))$

ii) $\bigvee g(\bigwedge xy(gx0 \doteq 0 \wedge gxSy \doteq f(gxy)x))$

Nota 5

La teoría de los números reales de primer orden a diferencia de la teoría de los números naturales de primer orden es completa.

B I B L I O G R A F I A

G. BIRKHOFF - S. MACLANE : "Algebra Moderna" .
Ed. Vicens-Vives.Barcelona1970

C.C.CHANG - H. JEROME KEISLER : "Model Theory".
Horth-Holland P.C. 1973

N. EFIMOV : "Géométrie Supérieure". Editions Mir.
Moscou,1981

W.T. FISHBACK : "Projective and Euclidean Geometry".
John Wiley & Sons Inc. 1969

H.G.FORDER : "The Foundations of Euclidean Geometry".
New-York Dover Publications Inc. 1958

PAUL R. HALMOS : "Lectures on Boolean Algebras".
Springer-Verlag,1974

H. HERMES : "Introduction to Mathematical Logic".
Springer-Verlag,1973

D. HILBERT : "Grundlagen der Geometrie". 7ª Ed. 1930.
Teubner.Leipzig-Berlin.

M.I.KARGAPOLOV-JU. I. MERZLJAKOV : "Fundamentals of the theory of Groups"
Springer-Verlag.1979

LANG : "Algebra" . Ed. Aguilar. Madrid 1971.

EDWIN E. MOISE : "Elementary geometry from an advanced standpoint".Addison-Wesley P.B. Inc.1963

J. MOSTERIN : "Lógica de primer orden".Ed.Barcelona 1970.

"Teoría axiomática de Conjuntos".Ed.Ariel
Barcelona 1971

"Un cálculo deductivo para la lógica de segundo orden". Cuadernos Teorema. Valencia,1979.

ABRAHAM ROBINSON : "Complete Theories". North-Holland P.C. 1956.

J.J.ROTMAN : "The Theory of Groups".2ªEd. Allyn and Bacon,Inc. Boston,1973.

ROBERT R. STOLL : "Set theory and Logic". W.H.Freeman and Co. 1961-1963.