# Ordinales menores que $\epsilon_0$

**Carlos Ivorra**

Un hilo de
Rincón Matemático
redactado por Eparoh

# Índice

# Prefacio

Este texto consiste en la redacción en formato PDF del hilo Ordinales menores que $\epsilon_0$ escrito por Carlos Ivorra.

Por las diferencias entre el formato web y el formato PDF existen pequeños cambios en el texto, pero esencialmente es idéntico al hilo enlazado anteriormente. Uno de estos cambios es utilizar recuadros de color amarillo para representar el texto indicado como "spoiler" en el hilo original.

Cada sección del texto (salvo la última) se corresponde con cada una de las respuestas de dicho hilo y al final de las mismas se encuentra un enlace al post original. La última sección recoge las respuestas más interesantes publicadas en el hilo de comentarios y respuestas anexo al hilo principal:

**(C1)** Si $\alpha = \langle \beta_1, \cdots, \beta_n \rangle$, entonces $\beta_1 \prec \alpha$, luego cada $\beta_i \prec \alpha$.

**(C2)** ¿Cómo se pueden definir (formalmente) conjuntos obtenidos de manera recursiva, como es el caso de $E$, en AP? Es decir, ¿cómo se puede formalizar la fórmula $n \in E$?

**(C3)** Discusión sobre la validez del primer argumento de Gentzen.

**(C4)** Respuesta de Eparoh al Acertijo metamatemático.

**(C5)** ¿Es posible formalizar en ZFC el segundo argumento de Gentzen?

**(C6)** Discusión sobre la validez del argumento de Takeuti.

**(C7)** Demostración de argentinator la buena ordenación de $\epsilon_0$.

**(C8)** No es posible demostrar en AP que Hércules siempre gana.

Por último, adjunto aquí dos archivos de Maple que contienen todos los programas (y algunos más) desarrollados en este texto.

# 1. Introducción

Un tema recurrente en este foro a lo largo de los años es si existe o no una matemática intuitiva —en el sentido de matemática no concebida como un mero deducir lógicamente sentencias de unos axiomas prefijados sin tener en cuenta su significado— rigurosa, fiable e incluso necesaria.

Las contradicciones que se encontraron los matemáticos a principios del siglo XX hicieron que se extendiera en la comunidad matemática un formalismo radical que, naturalmente, sólo afectó a quienes no se enfrentaron realmente al problema, es decir, a los expertos y no expertos en otras áreas de la matemática distintas de la lógica en general y de la teoría de la demostración en particular. Éstos se convencieron de que todo lo que no sea fijar unos axiomas y deducir a partir de ellos no es matemática seria, sin ser conscientes de que con esa concepción es imposible estudiar la corrección y adecuación de unos axiomas y reglas de razonamiento para decidir si son admisibles o no, o si unos son preferibles a otros en uno u otro sentido, etc.

Y, al margen de que razonar intuitivamente (con todo rigor) pueda ser imprescindible en ciertos contextos, el hecho es que es posible, tanto si es necesario como si no (y así, uno podría estudiar con todo rigor la aritmética elemental, buena parte de la teoría de grupos finitos, grafos, etc. sin necesidad alguna de ZFC o equivalentes). Sin embargo, parece que filosofar sobre este tema no sirve de nada a la hora de que un formalista radical deje de serlo, sino que la única forma en la que parece posible que alguien abandone sus prejuicios formalistas consiste en que se enfrente a la necesidad de razonar intuitivamente (por ejemplo, a la hora de fundamentar la matemática formal) y sólo entonces uno empieza a darse cuenta por sí mismo del dilema "intuición o estamos perdidos" y que la primera opción no tiene realmente nada de malo (pero he dicho "empieza a", no "termina por").

En este foro se han expuesto opiniones que se extienden por todo el espectro del formalismo radical, que, enunciadas familiarmente, podríamos expresar como que "eso de las matemáticas intuitivas son paparruchas" o "la matemática intuitiva no es más que matemática formal disfrazada", o incluso que los autores de libros de lógica y teoría de la demostración ocultan (o debería decir ocultamos) al mundo que todo eso que dicen (decimos) es un engaño.

Quiero dejar claro que no insinúo ni por asomo que los formalistas radicales sean algo así como terraplanistas o chalados de los que demuestran el Último Teorema de Fermat en diez líneas y dicen que los matemáticos tratan de ocultar que hay pruebas sencillas, etc. Al contrario, entiendo que el problema de la fundamentación de la matemática es delicado y que no se le puede pedir a nadie que diga: "acepto que existe una matemática intuitiva rigurosa aunque no entiendo cómo es esto posible", y que parece difícil que alguien, pese a su mejor voluntad, pueda llegar a entender esto "filosofando en el aire" sin meterse a fondo en harina y preocuparse de ver cómo se puede fundamentar satisfactoriamente la matemática formal, pero eso es algo que lleva mucho tiempo. De hecho, si yo tengo claras estas ideas, no es por ninguna genialidad por mi parte, sino porque dediqué muchos años hace tiempo en estudiar a fondo la fundamentación de la matemática, y este tiempo no es algo de lo que cualquiera pueda disponer en cualquier momento.

**Anécdota sobre la genialidad**

En cierta ocasión un crítico calificó de genio al violinista Pablo Sarasate, y él respondió: ¡Un genio! He practicado catorce horas diarias durante treinta y siete años, y ahora me llaman genio.

Igualmente estoy convencido de que entender lo que es la matemática intuitiva no es cuestión de ninguna genialidad, sino de haber dedicado tiempo suficiente a tratar de entender otras cosas más concretas que, para que tengan sentido, requiren, quieras o no, razonar intuitivamente.

Por ello, el propósito de este hilo es suministrar un "material didáctico" adicional, unas ideas que tal vez puedan contribuir a quien reflexione sobre ellas a formarse una idea más adecuada del problema (no trivial) que supone razonar de forma rigurosa y fiable en términos intuitivos, es decir, atendiendo a que lo que se diga sea verdad y no una mera consecuencia formal de unos axiomas.

La popularización de los teoremas de incompletitud de Gödel ha contribuido notablemente a que muchos matemáticos empiecen a entender que la matemática informal (pero rigurosa, porque el formalismo radical llega a identificar "informal", "intuitivo" con "no riguroso" o "poco serio", y no tiene nada que ver lo uno con lo otro) es viable, e incluso necesaria para entender plenamente algunos resultados. En este hilo me propongo exponer unas ideas que son relativamente sencillas pero que, a diferencia de los teoremas de incompletitud, no se han popularizado y, como están relacionadas con otras ideas mucho más técnicas, permanecen profundamente enterradas en los libros de teoría de la demostración en los que pocos se adentran.

He pensado en ello a raíz de un comentario que hice de pasada en este hilo, en el que mencioné lo que quiero exponer aquí como ejemplo extremo de lo que supone razonar intuitivamente.

Por si lee esto alguien que ya conoce estas ideas, las resumo aquí en pocas palabras para no tenerlo en ascuas:

**No leer, peligro de susto**

Voy a plantear el problema de si podemos dar por intuitivamente cierto (ojo, no como evidentemente cierto, sino como algo demostrable en términos intuitivos) que el ordinal $\epsilon_0$ está bien ordenado, cuando éste se define convenientemente a partir de los números naturales a través del hecho de que todo ordinal menor que $\epsilon_0$ está determinado por un número finito de ordinales menores por su forma normal de Cantor.

Pero si algún infractor del aviso no ha entendido nada de lo anterior, no debe preocuparse por ello. No voy a hablar ni de teoría de conjuntos, ni de "forma normal de Cantor", ni siquiera de lógica matemática. Sólo de la aritmética de los números naturales, y no voy a necesitar nada más que las propiedades elementales de la suma, el producto, etc. de números naturales.

Sin tecnicismos, lo que voy a hacer es definir una afirmación sobre números naturales (lo cual requiere introducir algunos conceptos y demostrar algunos hechos previos) y plantear la pregunta: ¿podemos afirmar que esto es verdad?

Superficialmente, la afirmación en cuestión se parece a la conjetura de Collatz. La recuerdo por si alguien no la conoce:

**La conjetura de Collatz**

Partimos de un número natural arbitrario $x_0$ y definimos una sucesión recurrentemente mediante:

$$x_{n+1} = \begin{cases} x_n/2 & \text{si} \quad n \text{ es par,} \\ 3x_n + 1 & \text{si} \quad n \text{ es impar.} \end{cases}$$

La conjetura de Collatz afirma que toda sucesión construida de este modo llega al 1 tras un número finito de pasos, pero nadie ha conseguido demostrarlo hasta ahora.

Concretamente, vamos a definir una clase de sucesiones de números naturales que, de momento, podemos llamar "de tipo S", y la afirmación en cuestión, que podemos llamar BO, es que todas las sucesiones de tipo S acaban llegando al 0.

Por ejemplo, ésta es una sucesión de tipo S:

$$29, 37, 4, 7, 17, 31, 8, 2, 6, 3, 1, 0.$$

Pero hay una diferencia sustancial entre la conjetura de Collatz y la afirmación BO, y es que, mientras no se conoce ninguna demostración de la primera, es relativamente fácil probar BO en la teoría de conjuntos ZF (la prueba requiere algunos resultados sobre ordinales, en especial el teorema de la forma normal de Cantor, pero aquí no vamos a hablar de nada de eso). Sin embargo, hay una razón por la cual el hecho de que BO sea demostrable en ZF no hace que deje de tener interés la pregunta de si BO es o no verdadera. Normalmente, la diferencia entre "X es verdad" y "X es demostrable en ZF" es despreciable para un formalista, no sin parte de razón, pero en este caso no es así. Veamos por qué:

Una de las consecuencias de los teoremas de incompletitud de Gödel es que, si una teoría de conjuntos como ZF es consistente, es imposible demostrar que lo es. Esto es algo que los formalistas saben y tienen asumido: pueden decir "para mí la matemática seria no es más que demostrar teoremas en ZFC" o, un poco más en general: "si me demuestras algo, dime cuáles son tus axiomas y yo comprobaré que lo que dices se deduce lógicamente de ellos y, si es así, te diré que está bien, sin cuestionarte tus axiomas, y sin cuestionarme si son consistentes o no (porque sé que es inútil intentarlo)".

Pero, sabiendo que no es posible probar la consistencia de ZF, un formalista debería admitir que es natural plantearse si es posible demostrar la consistencia de otras teorías axiomáticas más débiles, y un buen candidato a conejillo de indias es la aritmética de Peano (AP).

La aritmética de Peano

Aunque en este hilo no vamos a hablar para nada de axiomas ni de tecnicismos lógicos, recuerdo lo que es AP como parte de estos comentarios marginales para entender el valor de la afirmación BO:

La aritmética de Peano es la teoría axiomática que consta de estos axiomas:

*(i)* $\forall x\ x' \neq 0$ (El 0 no es el siguiente de ningún número natural.)

*(ii)* $\forall xy(x' = y' \to x = y)$ (Si dos números naturales tienen el mismo siguiente, son iguales).

*(iii)* $\forall x\ x + 0 = x$

*(iv)* $\forall xy(x + y' = (x + y)')$ (Definición recurrente de la suma)

*(v)* $\forall x\ x \cdot 0 = 0$

*(vi)* $\forall xy(x \cdot y' = x \cdot y + x)$ (Definición recurrente del producto)

*(vii)* $P(0) \wedge \forall x(P(x) \to P(x')) \to \forall x\ P(x)$ (Principio de inducción)

En ellos hay que entender que todas las variables hacen referencia exclusivamente a números naturales.

Pues bien, alguien para quien no suponga ningún trauma reconocer que los números naturales son "algo concreto" de lo que podemos hablar intuitivamente sabiendo lo que decimos, dirá que AP es obviamente consistente, porque los axiomas de Peano son verdaderos cuando se interpretan como afirmaciones sobre los números naturales, y las leyes de la lógica están diseñadas para que, cuando partimos de premisas verdaderas, llegamos necesariamente a conclusiones verdaderas, luego todos los teoremas que podemos deducir de los axiomas de Peano tienen que ser afirmaciones verdaderas sobre los números naturales, y por consiguiente es imposible demostrar cosas como que $0 \neq 0$ a partir de los axiomas de Peano, porque eso es falso, y si AP fuera contradictorio, se podría demostrar cualquier cosa a partir de sus axiomas, incluso $0 \neq 0$.

Un formalista radical, que considere que son los axiomas de Peano los que definen los números naturales y no los números naturales los que nos llevan a elegir los axiomas de Peano de forma que sean verdaderos, dirá que ese razonamiento es circular o, pasando al contraataque, dirá que si yo puedo decir que AP es consistente porque los números naturales satisfacen sus axiomas, él puede decir que ZF es consistente porque los conjuntos satisfacen sus axiomas, y entonces acabamos en la clásica palestra sobre si los números naturales tienen un sentido intuitivo objetivo mientras que los "conjuntos" no lo tienen, y de ahí no se sale filosofando.

Pues bien, en 1936, Gehrard Gentzen presentó una prueba de la consistencia de AP que era "casi" absolutamente finitista, en el sentido siguiente: Gentzen probó que es posible programar un ordenador de forma que si le damos como input la prueba de una contradicción en AP, el ordenador nos genera una sucesión de tipo S que, por más que se prolongue, nunca llegará a 0.

Obviamente, Gentzen no hablaba de ordenadores, pero lo he expresado así para enfatizar que es totalmente constructiva: igual que analizando un programa podemos concluir que genera la sucesión de los números primos, analizando el programa que Gentzen podría haber programado podemos concluir que genera una sucesión de tipo S que no llega nunca a 0, siempre y cuando le hayamos proporcionado una prueba de una contradicción en AP.

Por lo tanto, si podemos asegurar BO, es decir, que es imposible que una sucesión de tipo S se prolongue indefinidamente sin llegar al 0, podemos asegurar que AP es consistente.

La prueba de Gentzen es muy técnica, requiere saber bastante teoría de la demostración y, personalmente (después de haberla estudiado con detalle), me atrevería a decir que es bastante aburrida, pues obliga a distinguir casos y más casos. Pero no vamos a hablar de ella aquí. Lo que nos interesa es su hipótesis BO.

No creo descabellado afirmar que esta prueba de Gentzen no convence a nadie, pero no porque no sea concluyente, sino porque cualquiera que esté dispuesto a reconocer que es concluyente también reconocerá de antemano que AP es consistente (porque sus axiomas los cumplen los números naturales), por lo que la prueba de Gentzen demuestra (rigurosamente) lo que uno ya sabe. No obstante, tiene el interés técnico de que es "casi" finitista (el "casi" es porque requiere convencerse de que BO es cierta) y además puede ser interesante para un formalista que —quiero pensar— no objetará nada a la parte finitista de la prueba —la posibilidad de programar un ordenador como he dicho— y así puede concentrarse en algo mucho más concreto como si realmente podemos afirmar BO.

Con esto ya podemos entender la peculiaridad sobre lo que podemos exigir a una demostración de BO. Si nuestro propósito es convencernos de que AP es consistente probando BO, el hecho de que BO es demostrable en ZF no nos aporta nada.

En general, si demostramos que $2 + 2 = 4$ en ZF, no hemos probado realmente que $2 + 2 = 4$. Sólo hemos demostrado que si ZF es consistente entonces $2 + 2 = 4$, porque si ZF fuera contradictorio podríamos demostrar también que $2 + 2 = 372$, luego una prueba en ZF no nos garantizaría nada. Normalmente un formalista radical no le presta atención a este detalle y, dado que está dispuesto a trabajar en ZF y a suponer que es consistente para que tenga sentido su trabajo, y dado que necesita ZFC para probar cosas como el teorema de Alaoglu-Bourbaki (por decir algo), pues, de perdidos al río, lo aceptamos para todo, incluso para probar que $2 + 2 = 4$. Bien, se podría objetar alguna cosa, pero eso nos llevaría a las eternas discusiones filosóficas. Pero el caso es que en el caso concreto de BO ese planteamiento es inadmisible:

Si un formalista concede que, dado que no es posible probar la consistencia de ZF, es razonable investigar si podemos probar la consistencia de AP (y que ésta se reduce a probar BO), tiene que reconocer que es ridículo afirmar que AP es consistente por el hecho de que BO es demostrable en ZF, porque con ello sólo está probando que si ZF es consistente, también lo es AP, ¡pero eso es trivial! Como en ZF se pueden demostrar los axiomas de Peano, si se pudiera probar alguna contradicción a partir de ellos, también podríamos probar esa misma contradicción en ZF: primero probamos los axiomas de Peano en ZF, y prolongamos la demostración hasta llegar a la contradicción que se deduce de estos.

Así pues, lo que tiene interés no es la trivialidad de que AP es consistente si lo es ZF, sino llegar a convencernos de que AP es consistente sin apoyarnos en la consistencia

indemostrable de ZF. Gentzen dio un argumento absolutamente hipermegafinitista que ningún formalista debería objetar en virtud del cual todo se reduce a probar BO, pero si acabamos probando BO en ZF ¡estamos haciendo el tonto!

Por ello tiene sentido plantearse: vale, de los axiomas de ZF se deduce BO, pero, si no nos fiamos de los axiomas de ZF (no por vicio, sino porque aspiramos a probar la consistencia de AP y sería absurdo apoyarnos en algo más fuerte que lo que queremos probar) ¿podemos asegurar que BO es verdad? ¿Podemos asegurar que es inconcebible que exista un criterio que permita construir una sucesión de tipo S que nunca llegue al 0?

No se trata de dar un argumento para que venga un formalista y diga: a ver, en tu prueba estás suponiendo tales y tales axiomas. Suponiendo eso, la conclusión es correcta. Se trata de probar que no hay sucesiones de tipo S que no llegan al 0 si se prolongan lo suficiente sin fiar la conclusión a que tales o cuales axiomas sean ciertos o no. Se trata de demostrarlo a partir de hechos cuya certeza sea indudable. Se trata de convencerse de que es así, que no puede ser que exista una sucesión de tipo S que no llega al 0 igual que no puede ser que dos números naturales den una suma distinta según en qué orden se sumen.

Y si el formalista llega y dice: "pues tu prueba de BO se parece a una prueba en ZF como se parecen dos gotas de agua", en este contexto podemos decirle claramente que el parecido es irrelevante. Sí, la prueba tal cual se podrá formalizar en ZF, pero eso es ridículo, porque para demostrar así BO en ZF hay argumentos mucho más simples y directos (usando ordinales y la forma normal de Cantor). Independientemente de que la prueba se pueda formalizar en ZF, su interés reside en que pueda darse por válida sin interpretarla como una prueba en ZF, no porque sus afirmaciones se deducen lógicamente de teoremas de ZF, sino porque cada cosa que se dice es verdad, se pruebe o no en ZF. En este caso la diferencia es crucial. No importa si la prueba tiene una hermana gemela en ZF, importa que puede respirar fuera de ZF.

**Nota:** Tiene cierta importancia "filosófica" observar que la prueba de Gentzen no sólo afirma que si AP fuera contradictoria habría una sucesión de tipo S que nunca llegaría al 0, sino que dicha sucesión sería recursiva, es decir, calculable explícitamente por un ordenador.

Gentzen no dijo mucho sobre cómo justificar BO (entre otras cosas porque los nazis lo mataron a los 35 años), pero, al discutir su prueba de consistencia, analizando BO vino a decir que era claro que tenía que ser cierta por una serie de observaciones que, en esencia, contenían un "y así sucesivamente" un tanto cuestionable.

De hecho, Gödel lo cuestionó abiertamente y afirmó que, al margen de que podemos dar por hecho que BO es cierta igual que lo damos por hecho de cualquier teorema de ZF, prescindiendo de ello, no veía como algo intuitivamente justificado que BO tuviera que ser cierta, que la afirmación era demasiado compleja para que se pudiera dar por cierta a la ligera.

Más adelante, un matemático japonés, Gaisi Takeuti (que había estudiado con Gödel) presentó una prueba que ha dado mucho que hablar sobre si es intuitivamente aceptable o no (él mismo debatió mucho con Gödel acerca de su demostración). Nuevamente, la prueba de Takeuti no hace sino razonar sobre números naturales (no tiene nada que ver con la lógica ni con la teoría de conjuntos), eso sí, definiendo unos conceptos "sospechosamente abstractos". Según decía un profesor mío, es una de esas pruebas que les gustan a los lógicos que un día te levantas y la ves concluyente y otro día te parece que no vale.

En principio mi intención en este hilo es exponer lo necesario para definir BO y el argumento de Takeuti sin hacer referencia a nada que no sea aritmética pura y básica, por una parte para desenterrarlos de los libros de Teoría de la demostración y que estén accesibles para quien quiera interesarse por esto sin necesidad de digerir libros un tanto técnicos y, también, naturalmente, por si algún usuario del foro quiere seguir el desarrollo y plantear cualquier clase de duda u observación.

**Link al post original:** Ordinales menores que $\epsilon_0$

## 2. Pares de números naturales

Es bien conocido que $\mathbb{N}\times\mathbb{N}$ es biyectable con $\mathbb{N}$, y que una biyección explícita viene dada por una de las dos cosas distintas que se llaman "método diagonal de Cantor" (la otra es la que prueba la no numerabilidad de $\mathbb{R}$):

$$\begin{array}{llllll}
\vdots & & & & & \\
(0,4)\to 10 & & & & & \\
(0,3)\to 6 & (1,3)\to 11 & & & & \\
(0,2)\to 3 & (1,2)\to 7 & (2,2)\to 12 & & & \\
(0,1)\to 1 & (1,1)\to 4 & (2,1)\to 8 & (3,1)\to 13 & & \\
(0,0)\to 0 & (1,0)\to 2 & (2,0)\to 5 & (3,0)\to 9 & (4,0)\to 14\ldots &
\end{array}$$

Lo que no es tan conocido es que esta biyección $\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N}$ se puede expresar con fórmulas aritméticas. Por ejemplo, para calcular el número que corresponde al par $(3,1)$ vemos que, para llegar hasta él contando como muestra la figura, primero hemos de recorrer la diagonal formada por los números que cumplen $x+y=0$, que sólo tiene 1 par (el $(0,0)$), luego la diagonal formada por los números que cumplen $x+y=1$, que tiene 2 pares, luego la diagonal de los números que cumplen $x+y=2$, que tiene 3 pares, y así, tenemos que contar en total

$$1+2+3+4=10$$

pares antes de entrar en la diagonal $x+y=4$, que es la que contiene a nuestro par $(x,y)=(3,1)$. En general, antes de llegar a la diagonal de los pares que suman $x+y$ hemos de recorrer $x+y$ diagonales, con lo que habremos contado hasta

$$1+2+3+\cdots+(x+y)=\frac{(x+y)(x+y+1)}{2}$$

Volviendo a nuestro ejemplo concreto, como empezamos a contar en el 0, para contar 10 pares empleamos los números del 0 al 9, por lo que el par número 10 es el primero de la diagonal $x+y=4$. En general, el par $(x+y)(x+y+1)/2$ es el primero de la diagonal de los pares cuyas coordenadas suman $x+y$, es decir, ese número corresponde al par $(0,x+y)$. Para llegar al par $(x,y)$ tenemos que avanzar $x$ posiciones más, luego el par $(x,y)$ recibe el número

$$\langle x,y\rangle_2=\frac{(x+y)(x+y+1)}{2}+x. \tag{1}$$

Por ejemplo, $\langle 3,1\rangle_2 = \dfrac{4\cdot 5}{2} + 3 = 13$, como muestra la figura.

Así pues, la correspondencia

$$(x,y) \mapsto \langle x,y\rangle_2 = \frac{(x+y)(x+y+1)}{2} + x$$

determina una biyección entre los pares de números naturales y los números naturales. Llamaremos $p_2(z) = (x,y)$ a la biyección inversa.

Para calcular explícitamente $p_2$ observamos que si $z = \langle x,y\rangle_2$, entonces

$$\frac{(x+y)(x+y+1)}{2} \leq z < \frac{(x+y+1)(x+y+2)}{2},$$

pues el término de la derecha es el número que corresponde al primer par de la diagonal siguiente, la de los pares cuyas coordenadas suman $x+y+1$, luego

$$(x+y)^2 \leq (x+y)(x+y+1) \leq 2z < (x+y+1)(x+y+2) \leq (x+y+2)^2,$$

luego

$$x+y \leq \sqrt{2z} < x+y+2.$$

Esto nos deja sólo dos posibilidades para $x+y$, que tiene que ser $n = E[\sqrt{2z}]$ o bien $n = E[\sqrt{2z}] - 1$. Sólo hay que ver cuál de estos dos números cumple

$$\frac{n(n+1)}{2} \leq z < \frac{(n+1)(n+2)}{2}$$

y entonces

$$\begin{aligned} x &= z - \frac{n(n+1)}{2} \\ y &= n - x. \end{aligned} \tag{2}$$

Conviene observar que $x+y = n \leq 1+2+\cdots+n = n(n+1)/2 \leq \langle x,y\rangle_2$. Así pues, se cumple

$$x, y \leq \langle x,y\rangle_2 \tag{3}$$

Si el lector está familiarizado con algún lenguaje de programación o con alguna aplicación de cálculo simbólico, sería interesante que programara estas funciones para jugar con los conceptos que vamos a ir definiendo (todos ellos computables). Por ejemplo, yo he programado así estas funciones en Python:

```
def isqrt(n):
    #Parte entera de la raíz cuadrada de un entero
    x = n
    y = (x + 1) // 2
    while y < x:
        x = y
        y = (x + n // x) // 2
```

```
    return x

def par(x,y):
    #Par ordenado de dos números naturales
    u = (x+y) * (x+y+1) // 2 + x
    return u

def p2(z):
    #Coordenadas de z visto como par ordenado
    zz = 2*z
    n = isqrt(zz)
    while n * (n+1) > zz:
        n -= 1
    u= z - n * (n+1) // 2
    v = n-u
    return (u,v)
```

La primera función me la he copiado de internet, y sirve para calcular la parte entera de la raíz cuadrada de un número entero. La segunda es obvia. La tercera calcula $n = E(\sqrt{2z})$ y va restando 1 a $n$ hasta que $n(n+1) \leq 2z$. Entonces $n = x + y$ y podemos aplicar (2) para calcular $x, y$.

**Nota:** Disto mucho de ser un experto en Phyton, así que cualquier mejora a los programas que ponga será bien recibida.

De este modo tenemos un criterio explícito para asociar biunívocamente a cada número natural $z$ un par de números naturales $(x, y)$ y viceversa. Desde un punto de vista psicológico conviene pensar más bien que cada número natural $z$ tiene dos coordenadas asociadas $z_1, z_2$, es decir, que, por ejemplo, el número natural 230 054 **es** o **se descompone en** el par $(551, 126)$, exactamente igual que decimos que se descompone en el producto de primos $230\,054 = 2 \cdot 11 \cdot 10\,457$.

**Link al post original:** Pares de números naturales

# 3. Sucesiones finitas de números naturales

En el mensaje anterior hemos visto que cada número natural $n$ está determinado por dos coordenadas, de modo que dos números son iguales si y sólo si lo son sus coordenadas, y todo par de números son las coordenadas de un (único) número. Ahora bien, también podemos descomponer cada número en ternas de coordenadas si definimos

$$\langle x, y, z\rangle_3 = \langle \langle x, y\rangle_2 , z\rangle_2$$

La aplicación $(x, y, z) \mapsto \langle x, y, z\rangle_3$ biyecta las ternas ordenadas de números naturales con los números naturales.

Por ejemplo: $\langle 3, 5, 0\rangle_3 = \langle \langle 3, 5\rangle_2 , 0\rangle_2 = \langle 39, 0\rangle_2 = 819$.

Recíprocamente, si partimos de 819, podemos calcular $p_2(819) = (39, 0)$ y, a su vez, $p_2(39) = (3, 5)$, con lo que obtenemos la descomposición $819 = \langle 3, 5, 0\rangle_3$.

La tabla siguiente contiene la descomposición en ternas de los primeros números naturales:

$$\begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ (0,0,0) & (0,0,1) & (0,1,0) & (0,0,2) & (0,1,1) \\ \\ 5 & 6 & 7 & 8 & 9 \\ (1,0,0) & (0,0,3) & (0,1,2) & (1,0,1) & (0,2,0) \end{array}$$

Más en general, si definimos $\langle x\rangle_1 = x$ y $\langle x, y\rangle_2$ la aplicación que hemos estudiado en el mensaje anterior, podemos definir $n$-tuplas de cualquier longitud:

$$\langle x_1, x_2, x_3\rangle_3 = \langle\langle x_1, x_2\rangle_2, x_3\rangle_2,\ \langle x_1, x_2, x_3, x_4\rangle_4 = \langle\langle x_1, x_2, x_3\rangle_3, x_4\rangle_2,$$
$$\langle x_1, x_2, x_3, x_4, x_5\rangle_5 = \langle\langle x_1, x_2, x_3, x_4\rangle_4, x_5\rangle_2, \text{ etc.}$$

y de este modo podemos determinar cada número natural por una única coordenada (él mismo) o por dos coordenadas, o por tres, etc. Más precisamente, tenemos biyecciones que a cada $n$-tupla de números naturales le asignan un número natural, y podemos considerar sus inversas: $p_n : \mathbb{N} \longrightarrow \mathbb{N}^n$.

He aquí una implementación en Python:

```
def tupla(*l):
    #Tupla de una sucesión
    long = len(l)
    if long == 1:
        u = l[0]
    else:
        u = par(tupla(*l[:long-1]),l[long-1])
    return u

def pn(n,z):
    #Coordenadas de z visto como n-tupla
    u=[]
    for i in range(0,n-1):
        p = p2(z)
        u.append(p[1])
        z = p[0]
    u.append(z)
    u.reverse()
    u = tuple(u)
    return u
```

La primera función calcula recursivamente $\text{tupla}(x_1, \ldots, x_l) = \text{par}(\text{tupla}(x_1, \ldots, x_{l-1}), x_l)$, mientras que la segunda parte de un número $z$ y va descomponiendo: $z = \langle z', x\rangle$, va añadiendo los valores $x$ en una lista $u$ y pasa a hacer lo mismo con $z'$, así $n-1$ veces, hasta que finalmente añade a la lista $u$ el último valor $z$ obtenido, con lo que $u$ es la $n$-tupla asociada a $z$ salvo que está ordenada al revés, así que hay que darle la vuelta antes de devolver el resultado. (Insisto en que cualquier idea para hacer los algoritmos más eficientes será bienvenida.)

Así, un mismo número natural puede descomponerse —de forma única— en un par, en una terna, en una cuádrupla, etc. Por ejemplo, las descomposiciones del número 123 456 789 son:

$$(123456789),\ (15461, 251),\ (61, 114, 251),\ (6, 4, 114, 251),\ (0, 3, 4, 114, 251),$$
$$(0, 0, 3, 4, 114, 251),\ (0, 0, 0, 3, 4, 114, 251),\ (0, 0, 0, 0, 3, 4, 114, 251)\ldots$$

Pero necesitamos refinar estas técnicas para que cada número natural se identifique con una única descomposición de una longitud determinada, es decir, no queremos que el par $(15461, 251)$ y la terna $(61, 114, 251)$ se tengan que identificar con un mismo número natural. Más precisamente, vamos a definir una biyección $s \mapsto \langle s\rangle_\infty$ que a cada sucesión finita de números naturales (de cualquier longitud) le asigne un único número natural. La definición es sencilla, pero hay un tecnicismo en ella para hacerle un hueco a la sucesión vacía de longitud 0, para la que será $\langle\ \rangle_\infty = 0$.

La definición es:

$$\langle x_1, \ldots, x_n\rangle_\infty = \begin{cases} 0 & \text{si} \quad n = 0, \\ \\ \langle n-1, \langle x_1, \ldots, x_n\rangle_n\rangle_2 + 1 & \text{si} \quad n > 0. \end{cases} \tag{4}$$

De este modo, a la única sucesión vacía (de longitud $n = 0$) le asignamos el número 0, mientras que a una sucesión no vacía, como $(3, 0, 4, 4)$, de longitud 4 le asignamos el par:

$$\langle 3, 0, 4, 4\rangle_\infty = \langle 3, \langle 3, 0, 4, 4\rangle_4\rangle_2 + 1 = \langle 3, 5\,560\rangle_2 + 1 = 15\,476\,269 + 1 = 15\,476\,270.$$

Así, cada número natural se descompone de forma única en una sucesión finita de números naturales. Por ejemplo, si nos dan el 15 476 270, como no es 0 ya sabemos que se corresponde con una sucesión no vacía, le restamos 1 y descomponemos:

$$15\,476\,270 - 1 = \langle 3, 5\,560\rangle_2\,,$$

y la primera coordenada nos dice que la sucesión que buscamos tiene longitud $3 + 1 = 4$. Entonces reinterpretamos la segunda coordenada como $5\,560 = \langle 3, 0, 4, 4\rangle_4$ y ya tenemos la sucesión buscada. He aquí dos funciones en Python para calcular esta función y su inversa, así como la longitud de la sucesión codificada por un número:

```
def s(*l):
    #Número correspondiente a una sucesión dada
    if l == ():
        u = 0
    else:
        u = par(len(l) - 1,tupla(*l)) + 1
    return(u)

def long(s):
    #Longitud de una sucesión
    if s == 0:
        u = 0
```

```
    else:
        u = p2(s-1)[0]+1
    return(u)

def term(s):
    #Términos de un número
    if s == 0:
        u = ()
    else:
        z = p2(s-1)
        u = pn(z[0] + 1,z[1])
    return u
```

La función s implementa de forma obvia la función $\langle s\rangle_\infty$, la función long(s) distingue si $s = 0$, en cuyo caso codifica la sucesión vacía de longitud 0, o si $s > 0$, en cuyo caso la longitud de la sucesión que codifica se obtiene sumando 1 a la primera coordenada de $s-1$ visto como par. Finalmente, la función term, tras distinguir el caso $s = 0$, descompone $s - 1 = \langle z_0, z_1\rangle_2$ y luego descompone $z_1$ en sucesión de longitud $z_0 + 1$.

Con esto hemos conseguido nuestro primer objetivo: probar que cada número natural puede descomponerse de forma única en una sucesión finita de números naturales. Por ejemplo, $\langle 0, 1, 2, 3, 4, 5\rangle_\infty = 3\,374\,956\,582\,776$. La tabla siguiente muestra las primeras descomposiciones:

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| () | (0) | (1) | (0, 0) | (2) |
| 5 | 6 | 7 | 8 | 9 |
| (0, 1) | (0, 0, 0) | (3) | (1, 0) | (0, 0, 1) |
| 10 | 11 | 12 | 13 | 14 |
| (0, 0, 0, 0) | (4) | (0, 2) | (0, 1, 0) | (0, 0, 0, 1) |
| 15 | 16 | 17 | 18 | 19 |
| (0, 0, 0, 0, 0) | (5) | (1, 1) | (0, 0, 2) | (0, 0, 1, 0) |
| 20 | 21 | 22 | 23 | 24 |
| (0, 0, 0, 0, 1) | (0, 0, 0, 0, 0, 0) | (6) | (2, 0) | (0, 1, 1) |
| 25 | 26 | 27 | 28 | 29 |
| (0, 0, 0, 2) | (0, 0, 0, 1, 0) | (0, 0, 0, 0, 0, 1) | (0, 0, 0, 0, 0, 0, 0) | (7) |

En lo sucesivo usaremos únicamente las funciones $\langle x, y\rangle_2$, $\langle x_1, \ldots, x_n\rangle_\infty$ y sus inversas.

En (3) hemos probado que $x, y \leq \langle x, y\rangle_2$, de donde se sigue fácilmente que $x_i \leq \langle x_1, \ldots, x_n\rangle_n$, de donde a su vez,

$$x_i \leq \langle n - 1, \langle x_1, \ldots, x_n\rangle_n\rangle_2 < \langle x_1, \ldots, x_n\rangle_\infty . \tag{5}$$

El lector debería asimilar todo esto hasta que vea natural que digamos, por ejemplo, que 28 tiene longitud 7, mientras que 29 tiene longitud 1. Así, esta sucesión, que en otro contexto parecería bastante vulgar y caprichosa

$$0,\quad 1,\quad 3,\quad 6,\quad 10,\quad 15,\quad 21,\quad 28,\quad 36,\quad 45,\quad 55\ldots$$

aquí resulta bastante natural.

Si algún lector está dispuesto a seguir este hilo programando, se puede plantear cómo determinar si un número natural extiende a otro (en el sentido de que la sucesión que determina extiende a la del otro), como 24, que extiende a 5, y, en caso negativo, cómo determinar el primer término en el que ambos difieren.

**Link al post original:** Sucesiones finitas de números naturales

# 4. Ordinales

Ya podemos entrar en el meollo de este hilo. Vamos a definir una relación $\preceq$ en un subconjunto $E$ de $\mathbb{N}$ que, como el nombre sugiere, será una relación de orden, pero eso lo probaremos más tarde. La definiremos recurrentemente, definiendo conjuntos finitos $R_n$, de modo que $R_n$ será el conjunto de todos los números naturales $z$ que, vistos como pares $z = \langle x, y\rangle_2$ con $x, y \leq n$, cumplen $x \preceq y$.

La relación en $E$ será reflexiva, de modo que un número natural $n$ estará en $E$ si y sólo si el par $\langle n, n\rangle_2$ está en $R_n$ (es decir, si y sólo si $n \preceq n$).

Partimos de $R_0 = \{0\}$. Como $0 = \langle 0, 0\rangle_2$, con esto estamos diciendo que $0 \in E$ y que $0 \preceq 0$.

Supongamos ahora que ya tenemos definido $R_n$, es decir, que para todo número $x \leq n$ ya está decidido si $x$ está o no en $E$ (según si se cumple $x \preceq x$ o, equivalentemente si $\langle x, x\rangle_2 \in R_n$ o no) y para todo par de números $x, y \leq n$ ya está decidido si cumplen o no $x \preceq y$.

Para definir $R_{n+1}$ en primer lugar tenemos que decidir si $n+1 \in E$. En caso negativo será $R_{n+1} = R_n$.

Para ello expresamos $n + 1 = \langle s_1, \ldots, s_l\rangle_\infty$ como sucesión de números naturales. Por (5) $s_i \leq n$ para todo $i$, y la condición para incluir $n + 1 \in E$ es que se cumpla que todos los $s_i$ estén en $E$ (es decir, que $\langle s_i, s_i\rangle_2 \in R_n$) y que además la sucesión sea decreciente: $s_1 \succeq s_2 \succeq \cdots \succeq s_l$.

Si esto es así establecemos, por definición, que $\langle n + 1, n + 1\rangle_2 \in R_{n+1}$ y ahora tenemos que decidir, para cada $x \leq n$, si añadimos a $R_{n+1}$ el par $\langle x, n + 1\rangle_2$ o el par $\langle n + 1, x\rangle_2$.

Si no se cumple que $\langle x, x\rangle_2 \in R_n$ (es decir, si no hemos metido a $x$ en $E$), no incluimos ninguno de los dos pares, mientras que si $\langle x, x\rangle_2 \in R_n$, expresamos

$$\begin{aligned} n + 1 &= \langle s_1, \ldots, s_l\rangle_\infty, \\ x &= \langle t_1, \ldots, t_r\rangle_\infty \end{aligned}$$

y consideramos las posibilidades siguientes:

a) Si la sucesión de $n + 1$ se prolonga hasta la de $x$, es decir, si se cumple que $x = \langle s_1, \ldots, s_l, t_{l+1}, \ldots, t_r\rangle_\infty$, entonces metemos $\langle n + 1, x\rangle_2$ en $R_{n+1}$.

b) Si la sucesión de $x$ se prolonga hasta la de $n + 1$, entonces metemos $\langle x, n + 1\rangle_2$ en $R_{n+1}$.

c) Si ninguna sucesión extiende a la otra, podemos fijar el mínimo número natural en el que difieren, es decir, el mínimo $i$ tal que $s_j = t_j$ para $j < i$, pero $s_i \neq t_i$ (notemos que las sucesiones no pueden ser iguales, porque $x < n+1$).

   En tal caso, si $s_i \preceq t_i$ metemos $\langle n+1, x\rangle_2$ en $R_{n+1}$, y si $t_i \preceq s_i$ metemos el par opuesto $\langle x, n+1\rangle_2$.

Esto completa la definición recurrente de los conjuntos $R_n$, con lo que tenemos definido el conjunto $E$ de todos los números naturales $n$ que cumplen que $\langle n, n\rangle_2$ esta en $R_n$ y, para números en $E$, la relación $x \preceq y$ dada por $\langle x, y\rangle_2 \in R_n$, donde $n = \max\{x, y\}$.

Copio aquí (desde el hilo de comentarios) dos exposiciones alternativas de esta misma construcción que Eparoh y argentinator han considerado preferibles para sí mismos, por si a alguien más le resultan esclarecedoras:

Versión de Eparoh

1) Definimos $R_0 = \{0\}$.

2) De forma recursiva se define $R_{n+1}$ siguiendo estos pasos:

   i) Expresamos $n+1 = \langle s_1, \cdots, s_l\rangle_\infty$ (donde cada $s_i \leq n$ por (5)) y comprobamos si se cumplen:
      - $\langle s_i, s_i\rangle_2 \in R_n$ para cada $i = 1, \cdots, l$.
      - $\langle s_{i+1}, s_i\rangle_2 \in R_n$ para cada $i = 1, \cdots, l-1$.

   ii) Si no se cumplen los dos puntos anteriores, entonces $R_{n+1} = R_n$.

   iii) En caso contrario, definimos $R_{n+1}$ como el conjunto de naturales que resulta de añadir a $R_n$ los siguientes números:
      - $\langle n+1, n+1\rangle_2$
      - Para cada $x \leq n$:
        - Si $\langle x, x\rangle_2 \notin R_n$, entonces no añadimos ni $\langle n+1, x\rangle_2$ ni $\langle x, n+1\rangle_2$.
        - En caso contrario expresamos $x = \langle t_1, \cdots, t_r\rangle_\infty$ (donde cada $t_i < x \leq n$ por (5)) y comprobamos:
          - Si $x$ extiende a $n+1$, añadimos $\langle n+1, x\rangle_2$.
          - Si $n+1$ extiende a $x$, añadimos $\langle x, n+1\rangle_2$.
          - Si no se da ninguno de los casos anteriores y es $i$ el menor índice para el cual es $s_i \neq t_i$, entonces:
            - Si $\langle s_i, t_i\rangle_2 \in R_n$, añadimos $\langle n+1, x\rangle_2$.
            - Si $\langle t_i, s_i\rangle_2 \in R_n$, añadimos $\langle x, n+1\rangle_2$.

Tras esta gran recursión, dados dos naturales $x, y$ definimos la relación

$$x \preceq y \longleftrightarrow \langle x, y\rangle_2 \in R_{\max\{x,y\}}$$

y el conjunto $E$ formado por todos los naturales $n$ que cumplen que $\langle n, n\rangle_2 \in R_n$.

Versión de argentinator

Dado que para cada $n \in \mathbb{N}$ se establece si $x \preceq y$ cuando $x, y \leq n$, podría definirse una relación $\preceq_n$ con dominio el segmento inicial $[0, n] = \{0, 1, 2, ..., n\}$.

Luego se haría:

$$\preceq \quad := \quad \bigcup_{n=0}^{\infty} \mathbb{N}^n.$$

Yo dejaría la definición de los conjuntos $R_n$ para el final, enfocándome en definir $\preceq_n$.

Las condiciones para establecer $x \preceq y$ en $[0, n]$ me parecen escritas de una forma extensa. Intentaré ser más sintético, separando con más claridad los casos posibles:

Supogamos definida $\preceq_n \subset [0, n] \times [0, n]$.

Dados $a, b \in [0, n]$, si $a \preceq_n b$, entonces establecemos:

$$a \preceq_{n+1} b.$$

Por lo tanto, $\preceq_{n+1}$ extiende $\preceq_n$.

Denotamos $n + 1 = \langle s_1, \ldots, s_l \rangle_\infty$.

Si para todo $j, k$ con $1 \leq j \leq k \leq l$ vale que $s_j \succeq_n s_k$, se establece que:

$$n + 1 \ \preceq_{n+1} \ n + 1.$$

A continuación, si eso ocurre, continuamos agregando más elementos:

Sea $x \leq n$. Si no cumple que $x \preceq_n x$, no hacemos nada con $x$.

En cambio, si $x \preceq_n x$, avanzamos un poco más, y denotamos

$$x = \langle t_1, ..., t_r \rangle_\infty.$$

Sea $q$ el mínimo número natural tal que $s_j = t_j$ para $j < q$ con $j \leq l, j \leq r$.

Si $q = l + 1 \leq r$, ó bien $q \leq l, r$ y $s_q \preceq_n t_q$, establecemos:

$$n + 1 \preceq_{n+1} x.$$

En caso contrario, vale que $q = r + 1 \leq l$, ó bien $q \leq l, r$ y $t_q \preceq_n s_q$, en cuyo caso establecemos:

$$x \preceq_{n+1} n + 1.$$

La manera en que se define $\preceq_{n+1}$ indica que es un subconjunto de $[0, n + 1]^2$.

Luego, se definiría:

$$\preceq_\infty = \bigcup_{n=0}^{\infty} \preceq_n .$$

Ahora recién definiría los conjuntos $R_n$ y $E$:

$$\begin{aligned} R_n =& \{\langle a, b\rangle_2 : a \preceq_n b\}, \\ R_\infty =& \bigcup_{n=0}^{\infty} R_n, \\ E =& \{x \in R_\infty : x \preceq_\infty x\}. \end{aligned}$$

Y finalmente defino $\preceq$ como la restricción de $\preceq_\infty$ a $E$.

De esta construcción se siguen algunas consecuencias sencillas. Dejo los detalles como ejercicio para el lector, porque demostrarlas es una buena forma de familiarizarse con la definición:

**(O1)** $n \in E$ si y sólo si $n \preceq n$ (por definición de $E$).

**(O2)** Si $x \preceq y$, entonces $x, y \in E$.

Por inducción sobre $n = \max\{x, y\}$. Para $n = 0$ es trivial y, si vale para $n$, la construcción muestra que vale para $n + 1$.

**(O3)** $n \in E$ si y sólo si es una sucesión decreciente de elementos de $E$.

En efecto, esto vale trivialmente para 0 (que es la sucesión vacía, luego sus términos inexistentes están todos en $E$) y, si vale para números $x \leq n$, también vale para $n+1$ por la construcción.

**(O4)** Si $x, y \in E$, o bien $x \preceq y$, o bien $y \preceq x$.

Por inducción sobre $n = \max\{x, y\}$, pues para $n = 0$ es trivial y, si vale para $n$, no perdemos generalidad si suponemos que $y = n + 1$, y entonces, por construcción, si una sucesión prolonga a la otra, se cumple $x \preceq n + 1$ o bien $n + 1 \preceq x$, y en caso contrario ambas tienen que diferir en un primer término $i$. Por hipótesis de inducción se cumple $s_i \preceq t_i$ o bien $t_i \preceq s_i$ y, por construcción, esto implica que $x \preceq n + 1$ o bien $n + 1 \preceq x$.

**(O5)** Si $x \preceq y, y \preceq x$, entonces $x = y$.

Similar al caso anterior.

**(O6)** Si $x \preceq y \preceq z$, entonces $x \preceq z$.

Ésta la dejo entera como ejercicio.

Acabamos de definir una joya de la metamatemática. A los elementos de $E$ los llamaremos *ordinales* (deberíamos decir "ordinales menores que $\epsilon_0$", pero resulta un poco largo), y lo que hemos probado es que los ordinales son un conjunto de números naturales en los que tenemos definida una relación de orden total $\preceq$, que no hay que confundir con el orden usual $\leq$ definido sobre todos los números naturales. Además:

- *Un número natural es un ordinal si y sólo si es una sucesión decreciente de ordinales.*
- *Dos ordinales cumplen $x \preceq y$ si y sólo si, vistos como sucesiones de ordinales,*

$$x = \langle s_1, \ldots, s_l \rangle_\infty$$

$$y = \langle t_1, \ldots, t_r \rangle_\infty$$

*se cumple que $x$ se extiende hasta $y$, es decir, $y = \langle s_1, \ldots, s_l, t_{l+1}, \ldots, t_r \rangle_\infty$, o bien ambas sucesiones difieren en un mínimo índice $i$ tal que $s_i \preceq t_i$.*

Estas dos últimas afirmaciones parecen circulares, pero toda la construcción técnica precedente sirve para justificar que no hay circularidad, sino recurrencia.

En este punto, lo más saludable que puede hacer un lector que quiera seguir el hilo es programarse estas definiciones y jugar con los ordinales a ver si conjetura algunas cosas básicas sobre su ordenación. En los mensajes siguientes la estudiaremos con detalle. Pongo aquí mis programas en Python:

Para que no haga falta repetir una y otra vez los mismos cálculos recurrentes, he creado unas variables globales que guarden el máximo $n$ para el que hemos calculado $R_n$ así como el conjunto $R_n$ y el conjunto de los ordinales menores o iguales que $n$.

```
pares ={0} #Tupla de pares de ordinales crecientes calculados
ordinales = [0] #Lista de ordinales calculados
puntero = 0 #Máximo número natural que hemos visto si es un ordinal

def calcula(n):
    #Calcula la relación de orden entre ordinales hasta los pares de
    #coordenadas menores o iguales que n
    global puntero, ordinales, pares
    while puntero < n:
        puntero += 1
        s = term(puntero)
        ls = len(s)
        i = 0
        while i < ls-1 and par(s[i+1],s[i]) in pares:
                i += 1
#Aquí hemos comprobado que la sucesión s es decreciente hasta i.
#Si i = sl-1, es que es toda decreciente, pero comprobamos que su último
#término s[ls-1] sea tambien un ordinal por si la longitud es 1 y no se
#ha comparado ningún par.
        if i == ls-1 and s[i] in ordinales:
            pares.add(par(puntero,puntero))
            ordinales.append(puntero)
#Ahora comparamos puntero con todos los ordinales menores
            for x in range(0,puntero):
                if x in ordinales:
                    t = term(x)
                    lt = len(t)
                    m = min(ls,lt)
```

```
                    j = 0
                    while(j < m and s[j] == t[j]):
                        j += 1
#Aquí j es el menor ordinal en el que s y t difieren, salvo si j = m.
                    if j == m:
                        if ls <= lt:
                            pares.add(par(puntero,x))
#En este caso s se prolonga hasta t.
                        else:
                            pares.add(par(x, puntero))
#En este caso t se prolonga hasta s.
                    else:
                        if par(s[j],t[j]) in pares:
                            pares.add(par(puntero,x))
                        else:
                            pares.add(par(x, puntero))
#Añadimos un par u otro según si el primer término en el que difieren es
   menor en uno o en otro.

def ord(a):
    #Determina si a es un ordinal
    calcula(a)
    return (a in ordinales)

def comp(a, b):
    #Determina si a <= b como ordinales
    calcula(max(a,b))
    return (par(a, b) in pares)
```

Por ejemplo, si ejecutamos el código:

```
ord(100)
print(len(ordinales))
print(ordinales)
```

Veremos que hay 30 ordinales menores que 100, que son el 0 y

$$1, 2, 3, 4, 6, 7, 8, 10, 11, 15, 17, 21, 22, 23, 28, 29, 31, 36, 37, 45, 47, 55, 56, 57, 66, 67, 78, 91, 93.$$

Para entender por qué estos números son ordinales y otros no, conviene ordenarlos respecto de orden $\preceq$, para lo cual he usado un algoritmo copiado de internet (adaptado ligeramente para que use la función "comp" para comparar):

```
def ordena(array):
    n = len(array)
    for i in range(n):
        # Create a flag that will allow the function to
        # terminate early if there's nothing left to sort
        already_sorted = True
```

```
        # Start looking at each item of the list one by one,
        # comparing it with its adjacent value. With each
        # iteration, the portion of the array that you look at
        # shrinks because the remaining items have already been
        # sorted.
        for j in range(n - i - 1):
            #if array[j] > array[j + 1]:
            if (par(array[j + 1], array[j]) in pares) and array[j] !=
    array[j+1]:
                # If the item you're looking at is greater than its
                # adjacent value, then swap them
                array[j], array[j + 1] = array[j + 1], array[j]
                # Since you had to swap two elements,
                # set the 'already_sorted' flag to 'False' so the
                # algorithm doesn't finish prematurely
                already_sorted = False
        # If there were no swaps during the last iteration,
        # the array is already sorted, and you can terminate
        if already_sorted:
            break
     return array
```

Si ahora ejecutamos:

```
ord(100)
ordena(ordinales)
print(len(ordinales))
for a in ordinales:
    print(a, term(a))
```

obtenemos que los primeros 30 ordinales (ordenados según $\preceq$) son:

| | | | | | |
|---|---|---|---|---|---|
| 0 | $()$ | 55 | $(0,0,0,0,0,0,0,0,0,0)$ | 22 | $(6)$ |
| 1 | $(0)$ | 66 | $(0,0,0,0,0,0,0,0,0,0,0)$ | 56 | $(10)$ |
| 3 | $(0,0)$ | 78 | $(0,0,0,0,0,0,0,0,0,0,0,0)$ | 4 | $(2)$ |
| 6 | $(0,0,0)$ | 91 | $(0,0,0,0,0,0,0,0,0,0,0,0,0)$ | 23 | $(2,0)$ |
| 10 | $(0,0,0,0)$ | 2 | $(1)$ | 47 | $(2,1)$ |
| 15 | $(0,0,0,0,0)$ | 8 | $(1,0)$ | 93 | $(2,2)$ |
| 21 | $(0,0,0,0,0,0)$ | 31 | $(1,0,0)$ | 37 | $(8)$ |
| 28 | $(0,0,0,0,0,0,0)$ | 17 | $(1,1)$ | 29 | $(7)$ |
| 36 | $(0,0,0,0,0,0,0,0)$ | 7 | $(3)$ | 11 | $(4)$ |
| 45 | $(0,0,0,0,0,0,0,0,0)$ | 57 | $(3,0)$ | 67 | $(11)$ |

Por ejemplo:

- 0 es un ordinal porque, al ser la sucesión vacía, es trivialmente una sucesión decreciente de ordinales.
- $1 = \langle 0 \rangle_\infty$ es un ordinal porque es una sucesión de ordinales, trivialmente decreciente,

ya que tiene longitud 1. Además $0 \preceq 1$ porque la sucesión vacía se extiende a cualquier otra sucesión.

- $2 = \langle 1\rangle_\infty$ es un ordinal por el mismo motivo que 1 y además $1 = (0) \preceq (1) = 2$ porque ambas sucesiones tienen longitud 1, luego difieren en su primer término y $0 \prec 1$.
- $23 = \langle 2, 0\rangle_\infty$ y $47 = \langle 2, 1\rangle_\infty$ son ordinales porque son sucesiones decrecientes de ordinales (por los puntos precedentes) y $23 \preceq 47$ porque difieren en su segundo término y $0 \prec 1$.
- $5 = \langle 0, 1\rangle_\infty$ no es un ordinal porque, aunque es una sucesión de ordinales, no es decreciente.
- $16 = \langle 5\rangle_\infty$ no es un ordinal porque no es una sucesión de ordinales.

Conviene señalar que los 30 ordinales anteriores son los 30 primeros ordinales respecto del orden usual de los números naturales, pero no son los 30 primeros ordinales respecto de $\preceq$. Si calculamos más ordinales, muchos ordinales nuevos tendrán que intercalarse en la sucesión anterior.

Como decíamos, en los mensajes siguientes estudiaremos los ordinales y su relación de orden, pero de momento ya podemos explicar a qué llamábamos sucesiones de tipo S en el primer mensaje y qué dice la afirmación BO. Las sucesiones de tipo S son simplemente las sucesiones decrecientes de ordinales, y BO afirma, pues, que toda sucesión decreciente de ordinales, si se prolonga lo suficiente, llega al 0.

Dejo aquí algunas cuestiones que el lector puede plantearse como ejercicios y que trataré con detalle en el mensaje siguiente:

1. Probar que el 0 es el mínimo ordinal.
2. Probar que todo ordinal $\alpha$ tiene un siguiente $\alpha'$, es decir, que $\alpha \prec \alpha'$ y que $\alpha' \preceq \beta$, para todo ordinal $\beta \succ \alpha$. Concretamente, si $\alpha = \langle s_1, \dots, s_l\rangle_\infty$, probar que $\alpha' = \langle s_1, \dots, s_l, 0\rangle_\infty$ es un ordinal y cumple lo requerido.

   De este modo, los menores ordinales son

   $$0 = \langle\rangle_\infty = 0, \quad 0' = \langle 0\rangle_\infty = 1, \quad 0'' = \langle 0, 0\rangle_\infty = 3, \quad 0''' = \langle 0, 0, 0\rangle_\infty = 6, \quad \dots$$

   Estos ordinales se llaman *ordinales finitos*, porque son los que se obtienen del 0 en un número finito de pasos. Los demás son los *ordinales infinitos*.
3. Probar que $\omega = \langle 1\rangle_\infty = 2$ es el menor ordinal infinito, es decir, que es mayor que todo ordinal finito y menor o igual que todo ordinal infinito.

   Por lo tanto, los menores ordinales son:

   $$0 = \langle\rangle_\infty = 0, \quad 0' = \langle 0\rangle_\infty = 1, \quad 0'' = \langle 0, 0\rangle_\infty = 3, \quad \dots$$
   $$\omega = \langle 1\rangle_\infty = 2, \quad \omega' = \langle 1, 0\rangle_\infty = 8, \quad \omega'' = \langle 1, 0, 0\rangle_\infty = 31, \quad \dots$$
4. Probar que existe un mínimo ordinal mayor que $\omega, \omega', \omega'', \dots$ ¿qué número natural es? (Está en la tabla anterior).

**Link al post original:** Ordinales

# 5. La forma normal de Cantor

En este mensaje veremos cómo expresar los ordinales de forma natural, de modo que a simple vista se vea cuándo un ordinal es mayor o menor que otro (si no son muy complicados). Recordemos lo básico (a partir de aquí omitiré el subíndice $\infty$ en las expresiones como sucesiones):

- Un ordinal es un número natural $\alpha = \langle \delta_1, \ldots, \delta_m \rangle$ que (como sucesión) es una sucesión decreciente de ordinales: $\delta_1 \succeq \ldots \succeq \delta_m$.
- Dados dos ordinales $\alpha = \langle \delta_1, \ldots, \delta_m \rangle$, $\beta = \langle \epsilon_1, \ldots, \epsilon_n \rangle$, se cumple $\alpha \preceq \beta$ si y sólo si $\alpha$ se puede prolongar hasta $\beta$ o si el mínimo índice tal que $\delta_i \neq \epsilon_i$ cumple, de hecho, que $\delta_i \preceq \epsilon_i$.

Toda la construcción del mensaje precedente sólo tiene dos finalidades:

1) Justificar que esta definición no es circular.
2) Poner en evidencia que los ordinales no son "unas cosas raras que a saber si existen", sino que son simplemente números naturales, de modo que un ordenador siempre puede decidir si un número natural es o no un ordinal y si un ordinal es o no menor que otro.

Pero, si aceptamos que la definición anterior es correcta, de ella se deducen todas las propiedades de los ordinales. Por ejemplo:

**(O7)** 0 es el mínimo ordinal.

Esto se debe a que $0 = \langle\rangle$ es la sucesión vacía, luego trivialmente es un ordinal y se extiende a cualquier otro, luego $0 \preceq \alpha$ para todo ordinal $\alpha$.

**(O8)** Todo ordinal $\alpha = \langle \beta_1, \ldots, \beta_m \rangle$ tiene un siguiente, en concreto $\alpha' = \langle \beta_1, \ldots, \beta_m, 0 \rangle$, de modo que $\alpha \prec \alpha'$ y si $\alpha \prec \gamma$, entonces $\alpha' \preceq \gamma$.

En efecto, como 0 es el mínimo ordinal, se cumple que $\beta_m \succeq 0$, luego $\alpha'$ es una sucesión decreciente de ordinales y es, por lo tanto, un ordinal. Obviamente $\alpha \prec \alpha'$ y, si $\alpha \prec \gamma = \langle \delta_1, \ldots, \delta_n \rangle$, hay dos posibilidades:

1) Si $\gamma = \langle \beta_1, \ldots, \beta_m, \delta_{m+1}, \ldots, \delta_n \rangle$ extiende a $\alpha$, o bien $\delta_{m+1} = 0$ y entonces también extiende a $\alpha'$, o bien $0 \prec \delta_{m+1}$, en cuyo caso $\alpha'$ y $\gamma$ difieren precisamente en el término $m+1$, de modo que $\alpha' \prec \gamma$.
2) Si $\alpha$ y $\gamma$ difieren por primera vez en $\delta_i \prec \gamma_i$, entonces $\alpha'$ y $\gamma$ difieren en el mismo término, luego $\alpha' \prec \gamma$.

Con esto ya podemos asegurar que los primeros ordinales son

$$0 = \langle\,\rangle\,, \quad 0' = \langle 0 \rangle\,, \quad 0'' = \langle 0, 0 \rangle\,, \quad 0''' = \langle 0, 0, 0 \rangle\,, \quad 0'''' = \langle 0, 0, 0, 0 \rangle\,, \quad \ldots$$

A estos ordinales los llamaremos *ordinales finitos*, pues son los que se obtienen de 0 aplicando un número finito de veces la operación "siguiente". Los demás ordinales son los *ordinales infinitos*.

A partir de aquí usaremos la notación:

$$1 = 0', \quad 2 = 0'', \quad 3 = 0''', \quad \dots$$

Esto entra en conflicto con la notación usual para los números naturales y, para evitarlo, a partir de ahora llamaré

$$\bar{0}, \quad \bar{1}, \quad \bar{2}, \quad \bar{3}, \quad \dots$$

a los números naturales. Así podemos afirmar que

$$0 = \bar{0}, \quad 1 = 0' = \bar{1}, \quad 2 = 1' = \bar{3}, \quad 3 = 2' = \bar{6}, \quad 4 = 3' = \overline{10}, \quad \cdots$$

pero en realidad el número natural que es cada ordinal será irrelevante en la práctica.

**(O9)** $\omega = \langle 1 \rangle = \bar{2}$ es el menor ordinal infinito.

En efecto, como 1 es un ordinal, tenemos que $\omega$ es una sucesión decreciente de ordinales, luego es un ordinal, ciertamente infinito (pues no consta de ceros) y si $\alpha = \langle \beta_1, \dots, \beta_n \rangle$ es un ordinal infinito, alguno de sus términos tiene que ser no nulo, pero como la sucesión tiene que ser decreciente, necesariamente $\beta_1 \neq 0$, luego $1 \preceq \beta_1$, luego $\omega \preceq \alpha$.

Por lo tanto, los primeros ordinales son:

$$0 \prec 1 \prec 2 \prec \cdots \omega \prec \omega' \prec \omega'' \prec \cdots$$

En particular, $\omega$ es el menor ordinal límite, donde un *ordinal límite* se define como un ordinal no nulo que no sea el sucesor de otro ordinal (lo que, visto como sucesión decreciente de ordinales, equivale a que no sea la sucesión vacía y que su último término no sea un 0).

Si $\alpha = \langle \beta_1, \dots, \beta_n \rangle$ es un ordinal no nulo (de modo que $n \geq 1$), en lo sucesivo lo representaremos así:

$$\alpha = \omega^{\beta_1} + \cdots + \omega^{\beta_n}.$$

**OJO:** Más adelante definiremos una suma de ordinales, de modo que esta expresión podrá verse como la suma de los ordinales $\omega^{\beta_1} = \langle \beta_1 \rangle, \dots, \omega^{\beta_n} = \langle \beta_n \rangle$, pero aquí debemos destacar que NO tenemos definida una suma de ordinales y que esta expresión hay que verla como una mera notación que sustituye a $\langle \beta_1, \dots, \beta_n \rangle$. En particular, para que tenga sentido (de momento) la sucesión de exponentes tiene que ser decreciente.

Por ejemplo, tenemos definido

$$\omega^3 + \omega^3 + \omega^2 + \omega^1 + \omega^1 + \omega^0 + \omega^0 + \omega^0 = \langle 3, 3, 2, 1, 1, 0, 0, 0 \rangle$$

pero no tenemos definido $\omega^2 + \omega^5$, ya que $\langle 2, 5 \rangle$ no es un ordinal.

Adoptaremos también los convenios siguientes:

- Como $\omega^0 = \langle 0 \rangle = 1$, en lugar de $\omega^0$ escribiremos 1 y, en lugar de $1+1+1$ escribiremos 3.
- Además, $\omega^1 = \langle 1 \rangle = \omega$, por lo que en lugar de $\omega^1$ escribiremos simplemente $\omega$.
- Cuando se repitan "sumandos", como en $\omega^3 + \omega^3$, escribiremos $\omega^3 \cdot 2$.

Con estos convenios:

$$\langle 3, 3, 2, 1, 1, 0, 0, 0 \rangle = \omega^3 \cdot 2 + \omega^2 + \omega \cdot 2 + 3.$$

Por ejemplo:

$$\omega' = \langle 1, 0 \rangle = \omega + 1, \quad \omega'' = \langle 1, 0, 0 \rangle = \omega + 2, \quad \omega''' = \langle 1, 0, 0, 0 \rangle = \omega + 3, \quad \ldots$$

En estos términos, los primeros ordinales son:

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots \quad \omega, \quad \omega + 1, \quad \omega + 2, \quad \ldots$$

Ahora es fácil ver que el menor ordinal mayor que todos éstos es $\langle 1, 1 \rangle = \omega + \omega = \omega \cdot 2$, luego los primeros ordinales son:

$$0, \quad 1, \quad 2, \quad \ldots, \quad \omega, \quad \omega + 1, \quad \omega + 2, \quad \ldots, \quad \omega \cdot 2, \quad \omega \cdot 2 + 1, \quad \ldots$$

Esta forma de expresar los ordinales (como sumas de potencias de $\omega$ con exponentes decrecientes) se llama *forma normal de Cantor*. Pongo aquí dos funciones en Python que calculan la forma normal de Cantor de un ordinal (dado como número natural) en forma de cadena imprimible por Python y en LaTeX:

```
def fnc(n):
    #Expresa el ordinal n en forma normal de Cantor
    if n == 0:
        u = "(0)"  #u contendrá la fnc de n
    else:
        u = ""
        s = term(n)
        l = len(s)
        i=0
        while i<l:
            j = i   #Fijamos un término y contamos todos los siguientes
   iguales.
            t = s[i]
            while j< l and s[j] == t:
                j += 1
            if t == 0:
                #Si el término repetido es 0, suma k = j-i.
                u = u + str(j-i) + " + "
```

```
            else:
                if j-i == 1:
                    c = ""   #Si el término repetido es 1, no se pone el
    coeficiente.
                else:
                    #En otro caso el coeficiente es k = j-i
                    c = "\u00b7" + str(j-i)
                exp = fnc(t)    #fnc del exponente de omega.
                if exp == "(1)":
                    exp = ""    #Si el exponente es 1, no se pone.
                else:
                    exp = "^" + exp  #En caso contrario, elevamos al
    exponente.
                u = u + "\u03c9" + exp + c + " + "
            i = j
        u = "(" + u[:-3] + ")"   #Quita el último + y añade paréntesis.
    return u

def latex(n):
    #Expresa el ordinal n en forma normal de Cantor en LaTeX
    if n == 0:
        u = "0" #u contendrá la expresión en LaTeX
    else:
        u = ""
        s = term(n)
        l = len(s)
        i=0
        while i<l:
            j = i     #Fijamos un término y contamos todos los siguientes
    iguales.
            t = s[i]
            while j< l and s[j] == t:
                j += 1
            if t == 0:
                #Si el término repetido es 0, suma k = j-i.
                u = u + str(j-i) + " + "
            else:
                if j-i == 1:
                    c = ""  #Si el término repetido es 1, no se pone el
    coeficiente.
                else:
                    #En otro caso el coeficiente es k = j-i
                    c = "\cdot" + str(j-i)
                exp = latex(t)  #Expresión en LaTeX del exponente de
    omega.
                if exp == "1":
                    exp = ""    #Si el exponente es 1, no se pone.
```

```
                else:
                    exp = "^{" + exp + "}"  #En caso contrario, elevamos
al exponente.
                #Añadimos a u omega elevado al exponente por el
coeficiente.
                u = u+ "\omega" + exp + c + " + "
            i = j
        u = u[:-3]  #Quita el último +
    return u
```

Con la función latex he calculado la tabla siguiente, que contiene todos los ordinales menores que 200 (he omitido las sucesiones de ceros correspondientes a los ordinales finitos, que ocupan mucho espacio para nada):

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $\overline{0}$ | $()$ | 0 | $\overline{105}$ | – | 14 | $\overline{22}$ | $(\overline{6})$ | $\omega^3$ |
| $\overline{1}$ | $(\overline{0})$ | 1 | $\overline{120}$ | – | 15 | $\overline{56}$ | $(\overline{10})$ | $\omega^4$ |
| $\overline{3}$ | $(\overline{0},\overline{0})$ | 2 | $\overline{136}$ | – | 16 | $\overline{121}$ | $(\overline{15})$ | $\omega^5$ |
| $\overline{6}$ | $(\overline{0},\overline{0},\overline{0})$ | 3 | $\overline{153}$ | – | 17 | $\overline{4}$ | $(\overline{2})$ | $\omega^\omega$ |
| $\overline{10}$ | – | 4 | $\overline{171}$ | – | 18 | $\overline{23}$ | $(\overline{2},\overline{0})$ | $\omega^\omega+1$ |
| $\overline{15}$ | – | 5 | $\overline{190}$ | – | 19 | $\overline{47}$ | $(\overline{2},\overline{1})$ | $\omega^\omega+\omega$ |
| $\overline{21}$ | – | 6 | $\overline{2}$ | $(\overline{1})$ | $\omega$ | $\overline{173}$ | $(\overline{2},\overline{3})$ | $\omega^\omega+\omega^2$ |
| $\overline{28}$ | – | 7 | $\overline{8}$ | $(\overline{1},\overline{0})$ | $\omega+1$ | $\overline{93}$ | $(\overline{2},\overline{2})$ | $\omega^\omega\cdot 2$ |
| $\overline{36}$ | – | 8 | $\overline{31}$ | $(\overline{1},\overline{0},\overline{0})$ | $\omega+2$ | $\overline{37}$ | $(\overline{8})$ | $\omega^{\omega+1}$ |
| $\overline{45}$ | – | 9 | $\overline{17}$ | $(\overline{1},\overline{1})$ | $\omega\cdot 2$ | $\overline{154}$ | $(\overline{17})$ | $\omega^{\omega\cdot 2}$ |
| $\overline{55}$ | – | 10 | $\overline{139}$ | $(\overline{1},\overline{1},\overline{0})$ | $\omega\cdot 2+1$ | $\overline{29}$ | $(\overline{7})$ | $\omega^{\omega^2}$ |
| $\overline{66}$ | – | 11 | $\overline{7}$ | $(\overline{3})$ | $\omega^2$ | $\overline{11}$ | $(\overline{4})$ | $\omega^{\omega^\omega}$ |
| $\overline{78}$ | – | 12 | $\overline{57}$ | $(\overline{3},\overline{0})$ | $\omega^2+1$ | $\overline{122}$ | $(\overline{4},\overline{0})$ | $\omega^{\omega^\omega}+1$ |
| $\overline{91}$ | – | 13 | $\overline{107}$ | $(\overline{3},\overline{1})$ | $\omega^2+\omega$ | $\overline{67}$ | $(\overline{11})$ | $\omega^{\omega^{\omega^\omega}}$ |

Ahora es fácil comparar dos ordinales a simple vista: Hay que comparar el término $\omega^\beta\cdot k$ en el que difieren situado más hacia la izquierda. Será menor el ordinal que tenga menor exponente $\beta$ y, en caso de igualdad, el que tenga el menor coeficiente $k$.

Por ejemplo, si queremos comparar los ordinales

$$\alpha = \omega^{\omega^{4\cdot 3}}\cdot 5+\omega^{\omega^{3\cdot 5+\omega^2\cdot 7+\omega+3}}\cdot 7+\omega^{\omega+2}+\omega^5\cdot 8+\omega\cdot 3+10$$
$$\beta = \omega^{\omega^{4\cdot 3}}\cdot 5+\omega^{\omega^{3\cdot 5+\omega^2+\omega\cdot 8+9}}\cdot 3+\omega^{\omega+2}+\omega^5\cdot 8+\omega\cdot 3+10$$

vemos que difieren en su segundo término, por lo que tenemos que comparar sus exponentes, que son

$$\omega^3\cdot 5+\omega^2\cdot 7+\omega+3$$
$$\omega^3\cdot 5+\omega^2+\omega\cdot 8+9$$

También difieren en su segundo término, y ahora los exponentes son ambos iguales a 2, por lo que comparamos los coeficientes, que son $7\succ 1$, luego $\alpha\succ\beta$.

**Relación con los ordinales de la teoría de conjuntos**

En ZF se pueden definir los ordinales de una forma muy distinta a como los hemos definido aquí (y, de hecho, obtenemos muchos más ordinales que los que nosotros hemos definido). Con la construcción conjuntista, cada ordinal es el conjunto de todos los ordinales menores que él. Por ejemplo:

$$0 = \varnothing, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad \ldots$$
$$\omega = \{0, 1, 2, \ldots\}, \quad \omega + 1 = \{0, 1, 2, \ldots, \omega\}, \quad \ldots$$

También se define de forma natural una suma, un producto y una exponenciación de ordinales, que nosotros introduciremos en el mensaje siguiente. Cantor demostró que todo ordinal $\alpha \neq 0$ se expresa de forma única en lo que ahora se llama forma normal de Cantor:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n,$$

con $\alpha \geq \beta_1 \geq \cdots \geq \beta_n$ y $k_1, \ldots, k_n < \omega$.

El ordinal $\epsilon_0$ se define como el supremo de los ordinales:

$$\omega < \omega^\omega < \omega^{\omega^\omega} < \omega^{\omega^{\omega^\omega}} < \cdots < \epsilon_0$$

y es el menor ordinal con la propiedad de que $\omega^{\epsilon_0} = \epsilon_0$ (los números con esta propiedad se llaman *números* $\epsilon$). Esto hace que su forma normal de Cantor sea simplemente $\epsilon_0 = \omega^{\epsilon_0}$. Sin embargo, los números $\alpha < \epsilon_0$ tienen todos forma normal con $\alpha > \beta_1 > \cdots > \beta_n$, por lo que, a través de su forma normal de Cantor, cada ordinal menor que $\epsilon_0$ está determinado por una sucesión decreciente de ordinales menores.

Esto hace que si en ZF construimos el conjunto $E$ de los números naturales a los que hemos llamado "ordinales", la aplicación $E \longrightarrow \epsilon_0$ que a cada ordinal de los nuestros le hace corresponder el ordinal usual con la misma forma normal es biyectiva y conserva el orden, por lo que los ordinales que hemos construido forman un conjunto ordenado isomorfo a $\epsilon_0$.

En el mensaje siguiente definiremos la suma y el producto de ordinales (menores que $\epsilon_0$) de modo que este isomorfismo de conjuntos ordenados conserve también la suma y el producto.

Podemos definir:

$$\omega^{(0)} = 1, \quad \omega^{(1)} = \omega, \quad \omega^{(2)} = \omega^\omega,$$

y, en general,

$$\omega^{(n+1)} = \omega^{\omega^{(n)}} = \left\langle \omega^{(n)} \right\rangle.$$

Por ejemplo, la tabla anterior muestra que

$$\omega^{(0)} = \bar{1}, \quad \omega^{(1)} = \bar{2}, \quad \omega^{(2)} = \bar{4}, \quad \omega^{(3)} = \overline{11}, \quad \omega^{(4)} = \overline{67}, \quad \ldots$$

Terminamos este mensaje con la observación siguiente:

**(O10)** Para todo ordinal $\alpha$ existe un $n \prec \omega$ tal que $\alpha \prec \omega^{(n)}$. En otras palabras, la sucesión $\{\omega^{(n)}\}_{n=0}^{\infty}$ no está acotada.

Vamos a probarlo por inducción sobre $\alpha$ (por la inducción usual en los números naturales, es decir, vamos a ver que si todos los números naturales $\beta < \alpha$ que son ordinales cumplen la afirmación, lo mismo le sucede a $\alpha$).

Si $\alpha = 0$ es trivial. Pongamos que $\alpha = \langle \beta_1, \ldots, \beta_m \rangle$, y hemos visto en (5) que $\beta_1 < \alpha$ (en el orden de los números naturales), luego por hipótesis de inducción existe un $n$ tal que $\beta_1 \prec \omega^{(n)}$, y entonces

$$\alpha = \omega^{\beta_1} + \cdots + \omega^{\beta_m} \prec \omega^{\omega^{(n)}} = \omega^{(n+1)}.$$

Un ejercicio interesante es programar una función que a cada ordinal $\alpha$ le calcule un $n$ que cumpla el teorema.

**Link al post original:** La forma normal de Cantor

# 6. La aritmética ordinal

Para terminar la presentación de los ordinales voy a definir la suma y el producto de ordinales. Las definiciones pueden parecer caprichosas, pero son las necesarias para que las operaciones se correspondan con las que se definen en teoría de conjuntos de forma natural.

En el mensaje anterior hemos visto que todo ordinal no nulo se puede expresar de forma única como

$$\alpha = \omega^{\delta_1} + \cdots + \omega^{\delta_n},$$

donde $\delta_1 \succeq \cdots \succeq \delta_n$, o bien de la forma

$$\alpha = \omega^{\delta_1} \cdot k_1 + \cdots + \omega^{\delta_n} \cdot k_n,$$

donde $\delta_1 \succ \cdots \succ \delta_n$ (la $n$ no es la misma en los dos casos, sino que la segunda expresión es más corta, porque resulta de agrupar todos los términos consecutivos iguales).

## 6.1. Suma de ordinales

Definimos $\alpha + 0 = \alpha$, $0 + \beta = \beta$ y, para ordinales no nulos

$$\alpha = \omega^{\delta_1} + \cdots + \omega^{\delta_m}, \quad \beta = \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n}$$

definimos la suma como

$$\alpha + \beta = \omega^{\delta_1} + \cdots + \omega^{\delta_r} + \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n},$$

donde hemos suprimido todos los términos $\omega^{\delta_i}$ con $\delta_i \prec \epsilon_1$ (en particular, si $\delta_1 \prec \epsilon_1$ es $\alpha + \beta = \beta$).

Por ejemplo:

$$(\omega^{\omega^3}+\omega^{\omega^2+\omega}+\omega^4+\omega^2+5)+(\omega^4+\omega^3+\omega^2+3)=\omega^{\omega^3}+\omega^{\omega^2+\omega}+\omega^4+\omega^4+\omega^3+\omega^2+3.$$

La suma de ordinales es una de las pocas operaciones que los matemáticos consienten en llamar "suma" a pesar de que no es conmutativa. Por ejemplo:

$$(\omega^5+\omega^2+7)+(\omega^5+\omega+2)=\omega^5\cdot 2+\omega+2$$
$$(\omega^5+\omega+2)+(\omega^5+\omega^2+7)=\omega^5\cdot 2+\omega^2+7.$$

En cambio, no es difícil probar que la suma es asociativa. Observemos que las expresiones en forma normal que hasta ahora eran una mera notación ahora pueden verse como sumas de sus términos, es decir, un ordinal como $\omega^{\omega^2}+\omega^{\omega+3}+\omega^5+8$ es la suma de sus cuatro términos en el sentido que acabamos de definir.

En particular, $\alpha+1$ se obtiene añadiendo un sumando $1=\omega^0$ a la expresión de $\alpha$, que nunca cancela a ningún otro sumando, y ya sabemos que el ordinal que resulta de añadir un exponente 0 a otro $\alpha$ es el ordinal siguiente (el menor ordinal mayor que $\alpha$).

Veamos ahora algunas propiedades de la suma de ordinales.

**(S1)** La suma de ordinales finitos coincide con la suma usual de números naturales.

Por ejemplo:

$$2+3=(\omega^0+\omega^0)+(\omega^0+\omega^0+\omega^0)=5$$

**(S2)** Si $\lambda$ es un ordinal límite, entonces $\alpha+\lambda$ es el supremo de los ordinales $\alpha+\beta$ con $\beta\prec\lambda$.

En efecto, pongamos que $\alpha=\omega^{\delta_1}+\cdots+\omega^{\delta_m}$ y $\lambda=\omega^{\epsilon_1}+\cdots+\omega^{\epsilon_n}$, donde $\epsilon_n\succ 0$, ya que $\lambda$ es un ordinal límite. Entonces

$$\alpha+\lambda=\omega^{\delta_1}+\cdots+\omega^{\delta_k}+\omega^{\epsilon_1}+\cdots+\omega^{\epsilon_n},$$

donde $k$ es el mayor índice que cumple $\delta_k\succeq\epsilon_1$ (con la posibilidad de que $k=0$ y no esté la primera parte). Es fácil ver que si $\beta\prec\lambda$, entonces $\alpha+\beta\prec\alpha+\lambda$. Por otra parte, tomemos $\eta\prec\alpha+\lambda$ y vamos a ver que existe un $\beta\prec\lambda$ tal que $\eta\prec\alpha+\beta$. Distingamos varios casos:

1) Puede ser que la expresión de $\eta$ se prolongue hasta la de $\alpha+\lambda$, en cuyo caso hay dos posibilidades:

   *a*) Si $\eta=\omega^{\delta_1}+\cdots+\omega^{\delta_j}$, con $j\leq k$, entonces $\eta\preceq\alpha=\alpha+0$, con $0\prec\lambda$, y se cumple lo que queremos probar.

   *b*) Si $\eta=\omega^{\delta_1}+\cdots+\omega^{\delta_k}+\omega^{\epsilon_1}+\cdots+\omega^{\epsilon_j}$, con $j<n$, entonces tomamos $\beta=\omega^{\epsilon_1}+\cdots+\omega^{\epsilon_j}\prec\lambda$ y se cumple que $\eta\prec\alpha+\beta$.

2) La alternativa es que un (mínimo) exponente de $\eta$ sea menor que el correspondiente de $\alpha+\lambda$, y también hay dos casos:

*a*) Si $\eta = \omega^{\delta_1} + \cdots + \omega^{\delta_j} + \omega^{\delta'_{j+1}} + \cdots$, con $\delta'_{j+1} \prec \delta_{j+1}$, entonces $\eta \prec \alpha = \alpha + 0$, como antes.

*b*) Si $\eta = \omega^{\delta_1} + \cdots + \omega^{\delta_k} + \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_j} + \omega^{\epsilon'_{j+1}} + \cdots$, con $\epsilon'_{j+1} \prec \epsilon_{j+1}$, entonces:

- Si $j+1 < n$ tomamos $\beta = \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_j} + \omega^{\epsilon_{j+1}} \prec \lambda$ y $\eta \prec \alpha + \beta$.
- Si $j+1 = n$ tomamos $\beta = \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_{n-1}} + \omega^{\epsilon'_n} + 1 \prec \lambda$ y $\eta \prec \alpha + \beta$.

En particular, si partimos de un ordinal, $\alpha$, podemos construir la sucesión creciente

$$\alpha \prec \alpha + 1 \prec \alpha + 2 \prec \alpha + 3 \prec \cdots \prec \alpha + \omega$$

y tenemos que $\alpha + \omega$ es precisamente el supremo de esta sucesión. En otras palabras, $\alpha + \omega$ es el menor ordinal límite mayor que $\alpha$.

**(S3)** Si $\alpha \preceq \beta$, existe un único ordinal $\gamma$ tal que $\alpha + \gamma = \beta$.

En efecto, podemos suponer que ambos ordinales son no nulos, digamos

$$\alpha = \omega^{\delta_1} + \cdots + \omega^{\delta_m}, \quad \beta = \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n}.$$

Puesto que $\alpha \preceq \beta$, hay dos posibilidades:

1) Si $\beta$ extiende a $\alpha$, entonces $\gamma$ es necesariamente la suma de los términos que le faltan a $\alpha$ para llegar a $\beta$.

2) Si existe un mínimo $i$ tal que $\delta_i \prec \epsilon_i$, entonces tiene que ser $\gamma = \omega^{\epsilon_i} + \cdots + \omega^{\epsilon_n}$.

**(S4)** $\alpha \preceq \alpha + \beta$ y la desigualdad es estricta si $\beta \neq 0$.

En efecto, podemos suponer que $\beta \neq 0$. Pongamos que

$$\alpha = \omega^{\delta_1} + \cdots + \omega^{\delta_m}, \quad \beta = \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n}.$$

Si $\delta_m \succeq \epsilon_1$ entonces

$$\alpha + \beta = \omega^{\delta_1} + \cdots + \omega^{\delta_m} + \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n},$$

que claramente es mayor que $\alpha$. En caso contrario, si $i$ es el mínimo índice tal que $\delta_i \prec \epsilon_1$, tenemos que

$$\alpha + \beta = \omega^{\delta_1} + \cdots + \omega^{\delta_{i-1}} + \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n},$$

y para comparar la suma con $\alpha$ tenemos que comparar los exponentes $\delta_i \prec \epsilon_1$, luego la suma es mayor.

**(S5)** $\beta \prec \gamma$ si y sólo si $\alpha + \beta \prec \alpha + \gamma$.

En efecto, hemos visto en **(S3)** que $\gamma = \beta + \delta$, para cierto $\delta \succ 0$, luego, por **(S4)**, $\alpha + \beta \prec \alpha + \beta + \delta = \alpha + \gamma$.

Recíprocamente, si $\alpha + \beta \prec \alpha + \gamma$ tiene que ser $\beta \prec \gamma$, porque en caso contrario sería $\gamma \preceq \beta$ y, por la parte ya probada, $\alpha + \gamma \preceq \alpha + \beta$, contradicción.

Para finalizar con la suma ordinal, concluimos con el siguiente programa de Python que permite calcularla:

```
def suma(m,n):
    #Calcula la suma de dos ordinales.
    ss = term(m)
    tt = term(n)
    if n == 0:
        u = m
    else:
        i = len(ss)-1
        while i >= 0 and comp(ss[i],tt[0]) and ss[i] != tt[0]:
            i -= 1
        ss = list(ss)[0:i+1]
        ss.extend(tt)
        u = s(*ss)
    return u
```

## 6.2. Producto de ordinales

La definición del producto de dos ordinales parece más caprichosa aún.

Ante todo, definimos $\alpha \cdot 0 = 0 \cdot \alpha = 0$ y $\alpha \cdot 1 = \alpha$.

En segundo lugar, si $\alpha = \omega^{\delta_1} + \cdots + \omega^{\delta_m}$ y $\beta = \omega^{\epsilon}$, con $\epsilon > 0$, definimos $\alpha \cdot \omega^{\epsilon} = \omega^{\delta_1 + \epsilon}$, de modo que el producto sólo depende del primer término de $\alpha$.

Por último, si $\beta = \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n}$, definimos $\alpha \cdot \beta = \alpha \cdot \omega^{\epsilon_1} + \cdots + \alpha \cdot \omega^{\epsilon_n}$, donde los productos del miembro derecho están en uno de los dos casos anteriores, según si $\epsilon_i$ es nulo o no.

Por ejemplo:

$$(\omega^5+\omega^5+\omega^2+\omega)(\omega^2+1+1) = \omega^7+(\omega^5+\omega^5+\omega^2+\omega)+(\omega^5+\omega^5+\omega^2+\omega) = \omega^7+\omega^5\cdot 4+\omega^2+\omega.$$

El producto de ordinales tampoco es conmutativo. Por ejemplo:

$$3 \cdot \omega = (\omega^0 + \omega^0 + \omega^0) \cdot \omega^1 = \omega^1 = \omega$$

mientras que $\omega \cdot 3 = \omega + \omega + \omega$.

Veamos ahora algunas propiedades del producto de ordiales.

En general, los productos —hasta ahora formales— $\omega^{\delta} \cdot n$ que aparecen en las expresiones en forma normal son productos en el sentido que acabamos de definir:

**(P1)** Si $n$ es un ordinal finito no nulo

$$\alpha \cdot n = \alpha \cdot (1 + \cdots + 1) = \alpha + \cdots + \alpha.$$

En particular, esto implica que el producto de ordinales finitos se corresponde con el producto usual de números naturales.

Por ejemplo, si $\alpha = \omega^\omega \cdot 3 + \omega^4 \cdot 5 + \omega + 3$, entonces

$$\begin{aligned}\alpha \cdot 4 = (\omega^\omega \cdot 3 + \omega^4 \cdot 5 + \omega + 3) + (\omega^\omega \cdot 3 + \omega^4 \cdot 5 + \omega + 3) + (\omega^\omega \cdot 3 + \omega^4 \cdot 5 + \omega + 3) + \\ + (\omega^\omega \cdot 3 + \omega^4 \cdot 5 + \omega + 3) = \omega^\omega \cdot 12 + \omega^4 \cdot 5 + \omega + 3,\end{aligned}$$

pues $\omega^\omega$ cancela los términos intermedios.

**(P2)** $\alpha \cdot \omega$ es el supremo de la sucesión

$$\alpha \prec \alpha \cdot 2 \prec \alpha \cdot 3 \prec \alpha \cdot 4 \prec \cdots$$

En el ejemplo que hemos puesto, por definición, $\alpha \cdot \omega = \omega^{\omega+1} = \langle \omega + 1 \rangle$, mientras que

$$\begin{aligned}\alpha = \omega^\omega \cdot 3 + \omega^4 \cdot 5 + \omega + 3 \prec \omega^\omega \cdot 6 \preceq \\ \preceq \alpha \cdot 2 = \omega^\omega \cdot 6 + \omega^4 \cdot 5 + \omega + 3 \prec \omega^\omega \cdot 9 \preceq \\ \preceq \alpha \cdot 3 = \omega^\omega \cdot 9 + \omega^4 \cdot 5 + \omega + 3 \prec \omega^\omega \cdot 12 \preceq \\ \preceq \alpha \cdot 4 = \omega^\omega \cdot 12 + \omega^4 \cdot 5 + \omega + 3 \prec \cdots\end{aligned}$$

Es decir

$$\alpha \prec \omega^\omega \cdot 6 \preceq \alpha \cdot 2 \prec \omega^\omega \cdot 9 \preceq \alpha \cdot 3 \prec \omega^\omega \cdot 12 \preceq \alpha \cdot 4 \prec \cdots,$$

luego el supremo de la sucesión $\alpha \cdot n$ coincide con el de la sucesión $\omega^\omega \cdot n$, es decir, el supremo de la sucesión $\langle \omega, \ldots, \omega \rangle$ ($n$ veces), y dicho supremo (teniendo en cuenta que el orden es el lexicográfico) es precisamente $\langle \omega + 1 \rangle = \omega^{\omega+1} = \alpha \cdot \omega$.

En el caso general, si $\alpha = \omega^{\delta_1} \cdot k_1 + \cdots + \omega^{\delta_l} \cdot k_l$, tenemos que $\alpha \cdot n = \omega^{\delta_1} \cdot k_1 \cdot n + \cdots + \omega^{\delta_l} \cdot k_l$ y que el supremo de esta sucesión coincide con el de $\omega^{\delta_1} \cdot k_1 \cdot n$, o también con el de la sucesión $\omega^{\delta_1} \cdot n = \langle \delta_1, \ldots, \delta_1 \rangle$ ($n$ veces), que, como el orden es el lexicográfico, es $\langle \delta_1 + 1 \rangle = \omega^{\delta_1 + 1} = \alpha \cdot \omega$.

Concluimos con la siguiente función que calcula el producto de ordinales:

```
def prod(m,n):
    #Calcula el producto de dos ordinales.
    if m == 0 or n == 0:
        u = 0
    else:
        ss = term(m)
        tt = term(n)
        i = len(tt)
        while i>0 and tt[i-1] == 0:
            i -=1
        u = list(tt[:i])
```

```
        for j in range(0, len(u)):
            u[j] = suma(ss[0], u[j])
        u = s(*u)
        for j in range(i, len(tt)):
            u = suma(u, m)
    return u
```

### 6.3. Exponenciación de ordinales

No vamos a definir en general la exponenciación de ordinales, pero lo cierto es que tenemos definidas las potencias $\omega^\delta$, para todo ordinal $\delta$, y la definición de producto hace ahora que $\omega^\delta \cdot \omega^\epsilon = \omega^{\delta+\epsilon}$. Esto implica a su vez que si $k$ es finito, entonces $(\omega^\delta)^k = \omega^{\delta \cdot k}$.

Observemos que se cumple lo siguiente:

**(E1)** Si $\lambda$ es un ordinal límite, entonces $\omega^\lambda$ es el supremo de los ordinales $\omega^\alpha$, con $\alpha \prec \lambda$.

En efecto, es inmediato que $\omega^\alpha \prec \omega^\lambda$ y, si $0 \prec \beta \prec \omega^\lambda$, entonces $\beta = \omega^{\epsilon_1} + \cdots + \omega^{\epsilon_n}$, donde necesariamente $\epsilon_1 \prec \lambda$, y así $\beta \prec \omega^{\epsilon_1+1}$, con $\alpha = \epsilon_1 + 1 \prec \lambda$.

En particular, si

$$\alpha_0 \prec \alpha_1 \prec \alpha_2 \prec \cdots \prec \alpha$$

es una sucesión estrictamente creciente de ordinales con supremo $\alpha$, se cumple que $\omega^\alpha$ es el supremo de la sucesión

$$\omega^{\alpha_0} \prec \omega^{\alpha_1} \prec \omega^{\alpha_2} \prec \cdots$$

Con esto ya estamos en condiciones de "filosofar" sobre los ordinales y su buena ordenación, pero eso será en la entrega siguiente.

**Link al post original:** La aritmética ordinal

## 7. Paréntesis computacional

Los programas en Python que he puesto en los mensajes anteriores estaban pensados para reproducir las definiciones y mostrar que todas ellas son computables en la práctica, pero codificar los ordinales finitos como números naturales no es nada eficiente.

Por ejemplo, un ordinal con el que se puede operar fácilmente a mano como

$$\omega^{\omega \cdot 3+1} + \omega^2 + \omega \cdot 4 + 1$$

resulta ser el número natural

$$
\begin{aligned}
&11530666991150342448994626388921885518005911255934894140474732961791791083660712912722754207710772336335609569692792059293609963027611102766335087874358734282151769355786319873274935895672655107149176330281486816261329149834437391545780225820896059804283356024041148576074143102992496912172463989461163632816961210172990102909421936122483920718403337089269807884614217217604963460544524700882832518963416772805594543681582089563819264722096297437202698199136694274793031169345781320859986909138000097445119292557097880078
\end{aligned}
$$

Y a poco que aumentemos la complejidad del ordinal los números naturales se vuelven astronómicos y Python no puede con ellos. Esto se resuelve codificando los ordinales de otra forma. Adjunto aquí un módulo Python que he programado para ello.

Se carga con

```
from ordinales import *
```

y para ver su contenido basta teclear

```
help(ordinales)
```

Permite operar con ordinales de forma natural, identificando los números naturales con los ordinales finitos. He aquí un ejemplo de código:

```
u = []
for i in range(0, 100):
    a =OdC(i)
    if a != -1:
        u.append(a)
ordena(u)

for i in range(0, len(u)):
    print(int(u[i]), " ", term(int(u[i])), " ", u[i])
```

Este programa recorre los números del 0 al 99, determina cuáles de ellos corresponden a ordinales, los ordena según el orden $\preceq$ y luego los muestra como sucesiones de números naturales y en forma normal. Si ponemos LaTeX(u[i]) los escribe en LaTeX.

Otro ejemplo:

```
a = w**3 * 4 + w**2 * 5 + w + 7
b = w**2 + w + 3

print("({}) \u00b7 ({}) = {}".format(a, b, a*b))
```

produce el resultado

$$(\omega^3 \cdot 4 + \omega^2 \cdot 5 + \omega + 7) \cdot (\omega^2 + \omega + 3) = \omega^5 + \omega^4 + \omega^3 \cdot 12 + \omega^2 \cdot 5 + \omega + 7,$$

mientras que con el código de los mensajes precedentes Python se me congela porque el producto es un número natural astronómico.

**Link al post original:** Paréntesis computacional

# 8. ¿Están los ordinales bien ordenados?

Llegados a este punto, ya podemos empezar a "filosofar".

El problema principal que plantea la construcción que he dado de los ordinales es el siguiente:

*¿Existe una sucesión infinita decreciente de ordinales?*

Así:

$$\alpha_0 \succ \alpha_1 \succ \alpha_2 \succ \alpha_3 \succ \cdots$$

O equivalentemente:

*Si vamos construyendo una sucesión decreciente de ordinales como la anterior, ¿llegaremos necesariamente a 0 tras un número finito de pasos?*

Porque, mientras no lleguemos a 0, la sucesión se puede prolongar. Si tratamos esta pregunta como los matemáticos tratan habitualmente cualquier pregunta de naturaleza matemática, la respuesta es muy simple: NO. Y la razón es que en ZF se puede demostrar que no.

**Ordinales en ZF**

Aunque no vamos a entrar en ello aquí, lo que sucede es que en ZF los ordinales (los que hemos definido aquí y muchos más) se pueden definir de un modo completamente distinto que hace relativamente fácil probar que están bien ordenados, es decir, que todo conjunto no vacío de ordinales tiene un mínimo elemento, y esto equivale a que no existen sucesiones decrecientes infinitas de ordinales.

Además, los ordinales que hemos definido aquí se corresponden biunívocamente con los ordinales conjuntistas menores que uno de ellos, $\epsilon_0$, de modo que la biyección conserva el orden, por lo que si existiera una sucesión decreciente de (nuestros) ordinales también la habría de ordinales conjuntistas, y en ZF se prueba que esto es imposible.

Normalmente, el hecho de que algo pueda probarse en ZF (o en ZFC) hace que un matemático dé por zanjado el problema, pero esta afirmación que nos ocupa es un caso peculiar en el que "el protocolo habitual" no es razonable.

La razón es la que expliqué en el primer mensaje: Gentzen demostró que si la aritmética de Peano AP es contradictoria, entonces existe una sucesión estrictamente decreciente de ordinales. Más aún, que se puede programar a un ordenador para que vaya generando una sucesión decreciente de ordinales con la garantía de que nunca terminará.

Más precisamente, Gentzen mostró cómo asociar un ordinal (es decir, un número natural que, de hecho, es un ordinal) a cualquier demostración en AP, y probó que a partir de una demostración de una contradicción es posible construir siempre otra demostración de una contradicción con ordinal menor. La construcción es completamente finitista, de modo que es posible programar a un ordenador para que si le damos una demostración de una contradicción en AP él vaya construyendo sucesivamente nuevas demostraciones, cada una con un ordinal asociado menor que la anterior.

Por lo tanto, si podemos asegurar que no existen tales sucesiones decrecientes, podemos asegurar que AP es consistente. Otra cosa es que muchos pensemos que AP es obviamente consistente, pero ese "obviamente" no satisfará a un formalista radical que no acepte que hablemos informalmente de números naturales o, por lo menos, que "abusemos" de ello.

Pero muy, muy radical tendría que ser un formalista para cuestionar que un programa de ordenador hace lo que un análisis detallado de su programa muestra que puede hacer, y por ello aquí no voy a cuestionar la corrección del resultado de Gentzen (no creo que nadie se haya planteado nunca hacerlo). Es un hecho innegable que podemos programar un ordenador con un criterio para construir una sucesión decreciente de ordinales, con la única "pega" de que dicho criterio necesita partir de una demostración formal de una contradicción en AP.

El interés de todo esto es obtener una prueba "absoluta" de la consistencia de AP que no dependa de la consistencia de ZF, porque es trivial que si ZF es consistente también lo es AP. Y es por esto que —justo en este caso— no podemos aceptar el criterio usual de los matemáticos por el que si algo es demostrable en ZF, pues ya está demostrado y punto.

Un matemático "se fía" de ZF, porque sabe (o debería saber) que no es posible demostrar que ZF es consistente, pero, precisamente por eso, porque es imposible demostrarlo, no debe extrañarnos que no tengamos ninguna prueba de ello, sin que eso sea motivo para sospechar que ZF es contradictorio. Pero si confiar en ZF es razonable habitualmente, no es razonable fiarse de ZF justamente cuando lo que queremos es ver si podemos probar para AP lo que no podemos probar para ZF: su consistencia.

Por eso no vale la actitud del formalista que dice: tú déjame claro cuáles son tus axiomas y con eso yo ya doy tus afirmaciones por buenas (supuesto que sean lógicamente correctas). Si dejamos claro que "los axiomas" son los de ZF, la prueba de que no hay sucesiones decrecientes de ordinales no aporta nada. La pregunta realmente interesante es:

*¿Podemos asegurar que es imposible que un ordenador genere una sucesión decreciente de ordinales?*

No se trata de si se puede demostrar en ZF, sino de si es verdad. También se puede probar en ZF que $2+2=4$, pero si ZF resultara ser contradictorio, eso no sería motivo para sospechar que, a lo mejor, resulta que dos y dos no son cuatro. Tenemos argumentos sobrados para estar convencidos de que $2+2=4$ tanto si ZF es consistente como si no. Por eso probar que $2+2=4$ en ZF no nos aporta nada que no sepamos ya. Nos podemos fiar más de la conclusión que de sus premisas. Eso vale para $2+2=4$ y para muchas afirmaciones más, pero la cuestión es si también vale para la que nos ocupa:

*¿Podemos asegurar que es imposible que un ordenador genere una sucesión decreciente de ordinales de modo que, aunque ZF resultara ser contradictorio, no tendríamos motivos para poner esto en duda, como no dudaríamos de que dos y dos seguirían siendo cuatro?*

Para no llegar a una prueba ridículamente trivial de la consistencia de AP (una prueba que se limite al hecho obvio de que si ZF es consistente también lo es AP), no nos vale que "a partir de tales o cuales axiomas" se pueda demostrar lo que queremos, sino que necesitamos un argumento que nos convenza de que eso es verdad pase lo que pase con los axiomas de ZF y su consistencia.

Insisto en que no es que no sea paranoico plantearse que ZF podría ser contradictorio, sino que no podemos dar por hecho que es consistente cuando se trata de probar la consistencia de una teoría más modesta como AP sin caer con ello en el ridículo.

Muchos formalistas radicales tienden a recelar de cosas intuitivamente obvias (las que dan trabajo en ZF) y, en cambio, aceptan alegre e irreflexivamente otras cosas nada obvias (las que en ZF no dan ningún problema), como es el uso indiscriminado de palabras como "para todo" o "existe" (que la lógica de ZF permite usar sin preocupación alguna). Así, yo diría que "existe una sucesión" es un concepto muy difuso, porque yo no sé lo que significa "la totalidad de las sucesiones" como para poder darle un significado preciso a una afirmación sobre la totalidad de las sucesiones (o sobre si existe una entre ellas que cumpla algo), por lo que no podría decir tranquilamente que una afirmación con tal generalidad tiene que ser objetivamente verdadera u objetivamente falsa. En ZF se prueba que la totalidad de las sucesiones de números naturales es un conjunto no numerable, y —yo al menos— no sé lo que significan las afirmaciones que involucran una cantidad no numerable de cosas.

Afortunadamente, en nuestro caso no tenemos que preocuparnos por este problema, porque la cuestión no es si existe una sucesión decreciente de ordinales, sino de si existe una que pueda calcular un ordenador, y la familia de todas las sucesiones calculables por un ordenador (los conjuntos recursivamente numerables) es algo perfectamente definido y sobre lo que se puede hablar objetivamente. No estamos hablando de si existe una entelequia, sino de si existe un programa de ordenador que tendría que hacer algo muy concreto. Gentzen probó que ese programa existe si AP es contradictoria. Si no, el programa "está cojo", tenemos un algoritmo, pero le falta un *input* para que pueda funcionar.

Uno podría plantearse si no sucederá como con $2+2=4$, que el argumento que lo prueba en ZF es válido intuitivamente, con lo que se puede "extirpar" de la axiomática para dar lugar a un argumento convincente que no dependa de los axiomas en concreto de ZF, sino de hechos intuitivamente justificables.

No parece un buen camino. La prueba en ZF se basa en las propiedades de los ordinales conjuntistas, y los ordinales conjuntistas son precisamente la fuente de una de las paradojas a las que tuvieron que enfrentarse los matemáticos de principios del siglo XX que creían que podían hablar de cosas tan abstractas sin el marco y las limitaciones que impone una teoría axiomática formal. En cualquier caso, no voy a discutir esa vía porque nos llevaría a los tecnicismos de la construcción de los ordinales en ZF y de su relación con los axiomas. Una muestra de que no es algo trivial es que en la teoría Z de Zermelo (que sólo tiene un axioma menos, el axioma del reemplazo, y que basta para fundamentar casi toda la matemática clásica) no se puede construir siquiera el ordinal $\omega \cdot 2$. Así que, construir los ordinales en una teoría de conjuntos, incluso $\epsilon_0$, es "droga dura".

Dedicaré el mensaje siguiente a empezar a exponer los argumentos en favor de la buena ordenación de $\epsilon_0$ (de los ordinales que hemos definido aquí), pero antes merece la pena observar nuestro problema desde un ángulo distinto:

*¿Es válida la inducción hasta $\epsilon_0$? Es decir, si, bajo la hipótesis de que todos los ordinales $\beta \prec \alpha$ cumplen una propiedad $P(\beta)$, demostramos $P(\alpha)$, ¿podemos asegurar que todos los ordinales cumplen dicha propiedad?*

Esto es equivalente a la no existencia de sucesiones decrecientes de ordinales.

Efectivamente, si tienes una sucesión decreciente de ordinales, no se cumple la inducción respecto de la propiedad $P(\alpha) \equiv$ "$\alpha$ no aparece en la sucesión", pues si todos los ordinales menores que $\alpha$ no aparecen en la sucesión, seguro que $\alpha$ tampoco aparece, y no por ello podemos concluir que ningún ordinal aparece en la sucesión.

Recíprocamente, si no hay sucesiones decrecientes de ordinales, se cumple el principio de inducción, pues si supones que si todo ordinal menor que $\alpha$ cumple $P$, también $\alpha$ cumple $P$, es necesario que todos los ordinales cumplan $P$, ya que si hubiera un $\alpha_0$ que no cumpliera $P$, por la hipótesis tendría que haber otro $\alpha_1 \prec \alpha_0$ que tampoco cumpliera $P$, y así podríamos continuar construyendo una sucesión de ordinales que no cumplen $P$.

El resultado de Gentzen se puede formular equivalentemente en términos de inducción hasta $\epsilon_0$. Para ello consideramos, concretamente, la propiedad

$$P(\alpha) \equiv \alpha \text{ no es el ordinal asociado a la prueba de una contradicción en AP.}$$

Gentzen demostró que si un ordinal no cumple $P(\alpha)$, es decir, si se trata del ordinal asociado a una prueba de una contradicción en AP, entonces existe otro ordinal $\beta \prec \alpha$ que tampoco cumple $P(\beta)$ (hay una prueba de una contradicción con ordinal menor). Dicho al revés: si todos los ordinales $\beta \prec \alpha$ cumplen $P(\beta)$, podemos asegurar $P(\alpha)$.

Si es válido el principio de inducción que acabo de enunciar, de aquí se puede deducir que todos los ordinales cumplen $P(\alpha)$, es decir, que ninguno está asociado a la prueba de una contradicción en AP, luego no existe tal prueba (toda prueba tiene un ordinal asociado) y AP es consistente.

La ventaja de este enfoque es que este principio de inducción puede formalizarse en AP. Todas las definiciones que hemos dado en este hilo son puramente aritméticas y son formalizables en AP. Igual que podemos definir aritméticamente la propiedad "n es un número primo", también podemos definir $n \in E$, y del mismo modo que podemos definir "m divide a n", podemos definir $\alpha \prec \beta$. Por lo tanto, para cada propiedad expresable aritméticamente $\phi(x)$, podemos formular este principio de inducción:

$$\phi - \mathrm{IND}(\epsilon_0) \equiv \forall \alpha \in E\ (\forall \beta \in E(\beta \prec \alpha \rightarrow \phi(\beta)) \rightarrow \phi(\alpha)) \rightarrow \forall \alpha \in E\, \phi(\alpha). \qquad (6)$$

Ahí afirmamos lo que habíamos planteado antes en azul:

Si bajo el supuesto de que todo $\beta \prec \alpha$ cumple $\phi(\beta)$ podemos probar $\phi(\alpha)$, esto garantiza que todo ordinal cumple $\phi(\alpha)$.

Este principio puede *enunciarse*, pero no *demostrarse* en AP, y la razón es que todo el argumento de Gentzen es formalizable en AP. En AP se puede demostrar que la sentencia $\phi - \mathrm{IND}(\epsilon_0)$ (para una fórmula concreta $\phi(\alpha)$, la que afirma que $\alpha$ no es el ordinal asociado a una prueba de una contradicción en AP) implica que AP es consistente, y los teoremas de Gödel implican que no es posible demostrar la consistencia de AP en AP.

Por lo tanto, tenemos dos enunciados equivalentes:

(BO) No existen sucesiones estrictamente decrecientes de ordinales.

y

IND($\epsilon_0$) La inducción hasta $\epsilon_0$ es válida, es decir, que si, bajo la hipótesis de que todo ordinal menor que $\alpha$ cumple una propiedad, podemos probar que $\alpha$ también la cumple, podemos estar seguros de que todos los ordinales la cumplen.

No necesitamos considerar propiedades arbitrarias (con toda la vaguedad que ello conlleva), sino que a efectos de lo que nos ocupa basta considerar una propiedad en concreto:

La de no ser el ordinal de la prueba de una contradicción en AP, que se corresponde con la no existencia de sucesiones decrecientes de ordinales de pruebas de contradicciones en AP (y estas afirmaciones son formalizables en AP, e incluso en teorías mucho más débiles, porque estamos hablando de conceptos recursivos, calculables por ordenadores, y no de afirmaciones aritméticas arbitrarias).

La finalidad principal de los mensajes anteriores es que estas propiedades no son abstracciones matemáticas como si la hipótesis del continuo es verdadera o falsa, o incluso si es verdad que existen conjuntos no medibles Lebesgue. Estos ordinales que hemos definido son algo muy concreto que "cabe" en un ordenador, y cabe preguntarse si un ordenador podría o no generar una sucesión decreciente de ordinales. O existe tal sucesión o no existe, pero ¿podemos razonar que no existe sin que nuestro razonamiento se apoye en el postulado de que los axiomas de ZF son consistentes?

Ante todos estos razonamientos con ordinales, Hermann Weyl señaló que Gentzen había demostrado la consistencia de la inducción hasta $\omega$ suponiendo la inducción hasta $\epsilon_0$.

Empezaremos a abordar este problema en el mensaje siguiente, pero, por si alguien quiere ir meditando sobre ello, planteo los casos más simples:

Si empezamos a construir una sucesión decreciente de ordinales y el primero $\alpha_0$ es un número natural, seguro que la sucesión llegará a 0 en un número finito de pasos. Si empiezo en $\alpha_0 = 4$, lo más que puedo retrasar lo inevitable es haciendo $4 \succ 3 \succ 2 \succ 1 \succ 0$. Puedo llegar a 0 en menos de cuatro pasos, pero no en más.

Supongamos ahora que empezamos en un ordinal infinito $\alpha_0 \prec \omega \cdot 2$. Hemos visto (en **(S2)**) que $\alpha_0$ es, a lo sumo, de la forma $\alpha_0 = \omega + n$, donde $n$ es un ordinal finito. Si, por ejemplo, $\alpha_0 = \omega + 4$, aunque descendamos a paso de pulga, lo más lento que podemos hacer es

$$\omega + 4 \succ \omega + 3 \succ \omega + 2 \succ \omega + 1 \succ \omega$$

y en cuanto (inevitablemente) hemos llegado a $\omega$, yendo a pasitos pequeños, el paso siguiente es necesariamente un paso de gigante, y hemos de pasar a un ordinal finito. Podemos elegir el 4, o el 4 000 o $10^{1000}$, pero en cuanto hayamos dado ese paso, estaremos a un número finito de pasos del 0, y llegaremos a 0 en un número finito de pasos.

Por lo tanto, si empezamos en $\omega + 4$ (o en cualquier $\omega + n$), es seguro que en un número finito de pasos llegaremos a $\omega$ y, en cuanto demos el paso siguiente, "tendremos los pasos contados" para llegar a 0.

Hemos probado que no puede haber sucesiones decrecientes de ordinales que empiecen en un ordinal $\alpha_0 \prec \omega \cdot 2$, y eso no depende de ningún axioma de ZF. Cualquiera que entienda lo que son los ordinales (que hemos definido aquí) entiende que es absolutamente imposible —caiga la consistencia de la teoría que caiga— construir una sucesión decreciente de ordinales que empiece en $\alpha_0 \prec \omega \cdot 2$ y que no llegue a 0 en un número finito de pasos. Dicho número no puede ser acotado a priori, porque todo dependerá de dónde aterricemos cuando pasemos $\omega$, pero será necesariamente finito.

Seguro que el lector se convence de que lo mismo vale si partimos de $\alpha_0 \prec \omega \cdot 3$. La cuestión es: ¿hasta que altura podemos razonar que si empezamos desde ahí llegaremos a 0? ¿podemos ir ascendiendo hasta asegurar que no importa lo alto que empecemos siempre caeremos hasta 0 o llega un punto en el que ya no está claro que pasa? Lo analizaremos en el mensaje siguiente.

**Link al post original:** ¿Están los ordinales bien ordenados?

# 9. Ordinales accesibles

Entramos ya en el problema de convencernos (si es posible) de que no existen sucesiones decrecientes de ordinales.

Aun a riesgo de resultar repetitivo, quiero insistir en que se trata de un problema bien planteado, en el mismo sentido que lo está un problema de ajedrez del tipo: juegan blancas y ganan. O bien es cierto y las blancas tienen una estrategia que les permite ganar hagan lo que hagan las negras, o no es así, pero no vale decir "si suponemos estos axiomas ganan las blancas, y si no, no lo sé". Una vez fijadas las reglas del ajedrez, o las blancas tienen una estrategia ganadora o no la tienen, pero no hay medias tintas.

Igualmente, una vez hemos definido lo que son los ordinales y su relación de orden, o es posible programar un ordenador para que genere una sucesión decreciente de ordinales (que no acabe nunca) o es imposible. No vale decir "suponiendo estos axiomas sí, y si no, no sé". Si uno se plantea si existen conjuntos no medibles Lebesgue, la respuesta sí que depende de si adoptamos unos axiomas u otros, pero aquí estamos hablando de si un ordenador puede o no puede hacer algo, y ahí no caben respuestas relativas a axiomas.

Conviene introducir la definición siguiente:

Un ordinal $\alpha$ es accesible si no existen sucesiones estrictamente decrecientes de ordinales menores que $\alpha$.

En estos términos, queremos probar que todo ordinal es accesible, pero esta definición nos permite ascender poco a poco, tratando de probar que ordinales cada vez mayores son accesibles.

Observemos que, trivialmente, si un ordinal es accesible, lo son todos los menores que él.

Recordemos ahora que hemos probado que la sucesión

$$\omega^{(1)} = \omega \prec \omega^{(2)} = \omega^\omega \prec \omega^{(3)} = \omega^{\omega^\omega} \prec \cdots$$

no está acotada, sino que todo ordinal es menor que uno de éstos, luego basta probar que todos los ordinales $\omega^{(n)}$ son accesibles.

Obviamente, $\omega$ es accesible. Si un ordenador empieza a enumerar ordinales hacia abajo empezando en un ordinal finito $\alpha_0 \prec \omega$, es seguro que llegará a 0 en un número finito de pasos. Concretamente, si empieza con $\alpha_0 = 10$, llegará a 0 a lo sumo en 10 pasos, y si empieza en $10^{1000}$, a lo sumo en $10^{1000}$ pasos, pero es inconcebible que un ordenador imprima un número natural y siga hacia abajo y no llegue nunca a 0.

Más aún, en el mensaje anterior probamos que $\omega \cdot 2$ es accesible, porque si empezamos en un ordinal de la forma $\omega + k$, tras un número finito de pasos tendremos que llegar (o rebasar) $\omega$ y luego, tras otro número finito de pasos, llegaremos a 0.

Más en general, podemos probar lo siguiente:

**(A1)** Si $\alpha$ y $\beta$ son ordinales accesibles, también lo es $\alpha+\beta$.

En efecto, supongamos que existiera una sucesión decreciente:

$$\alpha+\beta \succ \alpha_0 \succ \alpha_1 \succ \alpha_2 \succ \alpha_3 \succ \cdots$$

No podría ser $\alpha_0 \prec \alpha$, porque eso contradiría que $\alpha$ es accesible. Así pues, tendría que ser $\alpha \preceq \alpha_0 \prec \alpha+\beta$.

¿Podría ocurrir que todos los términos de la sucesión cumplieran $\alpha \preceq \alpha_n \prec \alpha+\beta$?

Vamos a ver que esto es imposible. Para ello usamos que, por **(S3)**, cada $\alpha_n$ podría expresarse entonces como $\alpha_n = \alpha+\beta_n \prec \alpha+\beta$. Tenemos, pues, que

$$\alpha+\beta \succ \alpha+\beta_0 \succ \alpha+\beta_1 \succ \alpha+\beta_2 \succ \cdots$$

y, por **(S5)**, esto implica que

$$\beta \succ \beta_0 \succ \beta_1 \succ \cdots,$$

lo que contradice la accesibilidad de $\beta$.

Por consiguiente, tiene que haber un $n$ tal que $\alpha_n \prec \alpha$, y entonces la sucesión

$$\alpha \succ \alpha_n \succ \alpha_{n+1} \succ \alpha_{n+2} \succ \cdots$$

contradice la accesibilidad de $\alpha$.

En resumen: una sucesión decreciente que empiece en un ordinal menor que $\alpha+\beta$ tiene que rebasar $\alpha$ tras un número finito de pasos (por la accesibilidad de $\beta$) y luego tiene que llegar a 0 en otro número finito de pasos (por la accesibilidad de $\alpha$).

Por consiguiente, el hecho de que $\omega$ sea accesible implica inmediatamente la accesibilidad de

$$\omega+\omega = \omega\cdot 2 \prec \omega\cdot 2+\omega = \omega\cdot 3 \prec \omega\cdot 3\cdot\omega+\omega = \omega\cdot 4 \prec \cdots$$

Más precisamente, lo que hemos visto es que una sucesión decreciente que empiece en un ordinal, digamos, menor que $\omega\cdot 5$, tiene que rebasar $\omega\cdot 4$ en un número finito de pasos, y luego rebasará $\omega\cdot 3$ en un número finito de pasos, y así hasta rebasar $\omega$ y finalmente llegar a 0.

Ahora conviene probar otro principio general:

**(A2)** Si $\lambda$ es el supremo de una sucesión creciente

$$\delta_0 \prec \delta_1 \prec \delta_2 \prec \cdots \prec \lambda$$

de ordinales accesibles, entonces $\lambda$ también es accesible.

Esto es trivial: si una sucesión decreciente empieza en un $\alpha_0 \prec \lambda$, por definición de supremo existirá un $n$ tal que $\alpha_0 \prec \delta_n$, luego en realidad sería

$$\delta_n \succ \alpha_0 \succ \alpha_1 \succ \alpha_2 \succ \cdots,$$

lo cual contradiría la accesibilidad de $\delta_n$.

Por ejemplo, hemos visto que $\omega^2$ es el supremo de la sucesión

$$\omega \prec \omega \cdot 2 \prec \omega \cdot 3 \prec \omega \cdot 4 \prec \cdots \prec \omega^2,$$

y como hemos razonado que todos los ordinales $\omega \cdot n$ son accesibles, podemos concluir que $\omega^2$ también lo es. Explítitamente, una sucesión decreciente que empezara en un ordinal $\alpha_0 \prec \omega^2$, cumpliría de hecho que $\alpha_0 \prec \omega \cdot n$, para cierto $n$, y ya hemos razonado que eso es imposible.

Más en general, ahora podemos probar:

**(A3)** Si $\alpha$ es accesible, también lo es $\alpha \cdot \omega$.

En efecto, según hemos razonado, serán accesibles los ordinales

$$\alpha \prec \alpha + \alpha = \alpha \cdot 2 \prec \alpha \cdot 2 + \alpha = \alpha \cdot 3 \prec \cdots \prec \alpha \cdot \omega,$$

Los primeros por la accesibilidad de la suma de ordinales y el último por ser supremo de ordinales accesibles (es supremo por **(P2)**).

Por lo tanto, podemos asegurar la accesibilidad de la sucesión

$$\omega \prec \omega^2 \prec \omega^3 \prec \omega^4 \prec \cdots$$

y la de su supremo, $\omega^\omega = \omega^{(2)}$ (lo es por **(E1)**).

Si vamos multiplicando $\omega^\omega$ por $\omega$ muchas veces, obtenemos la sucesión de ordinales accesibles

$$\omega^\omega \prec \omega^{\omega+1} \prec \omega^{\omega+2} \prec \omega^{\omega+3} \prec \cdots$$

y el supremo de esta sucesión es $\omega^{\omega\cdot 2}$ (de nuevo, por **(E1)**).

Si ahora vamos multiplicando este ordinal por $\omega$ vamos obteniendo la accesibilidad de

$$\omega^{\omega\cdot 2} \prec \omega^{\omega\cdot 2+1} \prec \omega^{\omega\cdot 2+2} \prec \omega^{\omega\cdot 2+3} \prec \cdots \prec \omega^{\omega\cdot 3}$$

y es claro entonces que, de este modo, podemos ir probando la accesibilidad de todos los ordinales

$$\omega^\omega \prec \omega^{\omega\cdot 2} \prec \omega^{\omega\cdot 3} \prec \omega^{\omega\cdot 4} \prec \omega^{\omega\cdot 5} \prec \cdots \prec \omega^{\omega^2},$$

donde $\omega^{\omega^2}$ es el supremo de la sucesión por **(P2)** y **(E1)**.

Si no desfallecemos y seguimos multiplicando por $\omega$, obtenemos la accesibilidad de

$$\omega^{\omega^2} \prec \omega^{\omega^2+1} \prec \omega^{\omega^2+2} \prec \omega^{\omega^2+3} \prec \cdots \prec \omega^{\omega^2+\omega}.$$

Todo esto es prometedor, pues cada vez estamos más arriba, pero así no vamos a acabar nunca, a menos que encontremos un patrón general en los argumentos que estamos dando.

Para empezar, podemos razonar que, del mismo modo que hemos pasado de la accesibilidad de $\omega^\omega$ a la de $\omega^{\omega^2}$ a base de multiplicar por $\omega$ (sumando 1 al exponente) y tomar supremos, exactamente el mismo argumento nos permite pasar de la accesibilidad de $\omega^{\omega^2}$

a la de $\omega^{\omega^2+\omega^2} = \omega^{\omega^2\cdot 2}$, y no es necesario que repitamos todo el proceso de nuevo. El mismo bloque de razonamientos nos permite ir probando la accesibilidad de

$$\omega^{\omega^2} \prec \omega^{\omega^2\cdot 2} \prec \omega^{\omega^2\cdot 3} \prec \omega^{\omega^2\cdot 4} \prec \cdots \prec \omega^{\omega^2\cdot\omega} = \omega^{\omega^3}.$$

Pero el mismo bloque de pasos que nos ha permitido pasar de la accesibilidad de $\omega$ a la de $\omega^{\omega^3}$, aplicado ahora a $\omega^{\omega^3}$, nos permite pasar a la de $\omega^{\omega^3\cdot 2}$, y aplicando sistemáticamente dicho bloque de pasos llegamos a la accesibilidad de

$$\omega^{\omega^3} \prec \omega^{\omega^3\cdot 2} \prec \omega^{\omega^3\cdot 3} \prec \omega^{\omega^3\cdot 4} \prec \cdots \prec \omega^{\omega^4}.$$

Si admitimos que sabemos razonar la accesibilidad de todos los ordinales de la forma

$$\omega^{\omega} \prec \omega^{\omega^2} \prec \omega^{\omega^3} \prec \omega^{\omega^4} \prec \cdots$$

entonces, por ser $\omega^{\omega^\omega} = \omega^{(3)}$ el supremo de dicha sucesión (una vez más, por **(P2)** y **(E1)**), obtendríamos la accesibilidad de $\omega^{(3)}$.

Y en este punto uno se plantea si sería legítimo concluir con un "y así sucesivamente".

Gentzen consideraba que sí:

**Cita de Gentzen**

Podemos, por ejemplo, visualizar los casos iniciales con características 1, 2, 3 con detalle. A medida que la característica crece, no se añade nada básicamente nuevo, el método de progresión es siempre el mismo. Desde luego, hay que admitir que la complejidad de los infinitos múltiplemente anidados que hay que recorrer crece considerablemente; este recorrido debe considerarse siempre como potencial [...] La dificultad reside en que, aunque el sentido finitista preciso de "recorrer" los ordinales es razonablemente claro en los casos iniciales, se vuelve de tal complejidad en el caso general que apenas es remotamente visualizable.

Pero Gödel no estuvo de acuerdo:

**Cita de Gödel**

La situación, a grandes rasgos, puede ser descrita como sigue:

La inducción transfinita hasta $\epsilon_0$ podría probarse finitistamente si y sólo si la consistencia de la teoría de números pudiera probarse finitistamente. Por otra parte, la validez de esta inducción no puede hacerse inmediatamente evidente, como sucede, por ejemplo, en el caso de $\omega^2$. Es decir, uno no puede captar de un vistazo las diversas posibilidades estructurales que existen para las sucesiones decrecientes y no existe, por lo tanto, un conocimiento concreto inmediato de la terminación de cada una de dichas sucesiones. Pero, más aún, tal conocimiento concreto (en el sentido de Hilbert) no puede alcanzarse a través de una transición gradual de ordinales menores a otros mayores, porque los pasos concretamente evidentes, como $\alpha \mapsto \alpha^2$ son tan pequeños que tendrían que repetirse $\epsilon_0$ veces para llegar hasta $\epsilon_0$.

La cuestión sobre la que el lector debería meditar es si lo dicho le convence de que no hay sucesiones decrecientes de ordinales, o si no, en caso de que esto no le parezca concluyente, se le ocurre un razonamiento alternativo que lo sea.

**Link al post original:** Ordinales accesibles

# 10. Un acertijo metamatemático

En este mensaje "demostraré" que la aritmética de Peano es contradictoria.

Obviamente, la prueba tiene trampa. Me basaré en un argumento de Gentzen.

Probaremos que todo ordinal es accesible demostrando el principio de inducción hasta $\epsilon_0$:

Si, suponiendo que todo ordinal $\beta \prec \alpha$ cumple una propiedad $P(\beta)$ podemos razonar que también se cumple $P(\alpha)$, entonces podemos concluir que todo ordinal cumple $P(\alpha)$.

Si admitimos esto, tomando $P(\alpha) \equiv$ "$\alpha$ es accesible", podemos concluir que todo ordinal es accesible, pues es inmediato que si todos ordinales menores que $\alpha$ son accesibles, entonces $\alpha$ también lo es.

Notemos que, si la propiedad $P(\alpha)$ puede definirse aritméticamente (recordemos que los ordinales no son más que números naturales, luego $P(\alpha)$ podría ser cualquier propiedad del estilo "$\alpha$ es múltiplo de 5" etc.) este principio de inducción puede formalizarse en el lenguaje de la aritmética mediante la fórmula dada en (6):

$$P - \mathrm{IND}(\epsilon_0) \equiv \forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P(\beta)) \to P(\alpha)) \to \forall \alpha \in E\, P(\alpha).$$

Para probar esto definimos dos propiedades a partir de $P(\alpha)$:

- $P^*(\alpha)$ significará que todos los ordinales $\beta \preceq \alpha$ tienen la propiedad $P(\beta)$.
  Formalmente:
  $$P^*(\alpha) \equiv \forall \beta \in E(\beta \preceq \alpha \to P(\beta)).$$
- A su vez, $P'(\eta)$ significará que si un ordinal $\alpha$ cumple $P^*(\alpha)$, entonces también se cumple $P^*(\alpha + \omega^\eta)$.
  Formalmente:
  $$P'(\eta) \equiv \forall \alpha \in E(P^*(\alpha) \to P^*(\alpha + \omega^\eta)).$$

En primer lugar vamos a demostrar:

$$\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P(\beta)) \to P(\alpha)) \to \forall \eta \in E(\forall \delta \in E(\delta \prec \eta \to P'(\delta)) \to P'(\eta)). \tag{7}$$

Informalmente: Vamos a ver que si, bajo el supuesto de que todos los ordinales menores que $\alpha$ cumplen $P$, podemos probar que también $\alpha$ cumple $P$, entonces también podemos asegurar que si todos los ordinales menores que $\alpha$ cumplen $P'$, necesariamente $\alpha$ cumple $P'$.

Suponemos, pues, que se cumple

$$\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P(\beta)) \to P(\alpha)) \tag{8}$$

y vamos a probar en primer lugar que esto implica

$$\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P^*(\beta)) \to P^*(\alpha)). \tag{9}$$

Para ello fijamos $\alpha \in E$ y suponemos que $\forall \beta \in E(\beta \prec \alpha \to P^*(\beta))$.

De la propia definición de $P^*$ se sigue que $P^*(\beta) \to P(\beta)$, luego tenemos

$$\forall \beta \in E(\beta \prec \alpha \to P(\beta)). \tag{10}$$

Ahora, aplicando (8) concluimos $P(\alpha)$, y uniendo esto a (10) llegamos a que $\forall \beta \in E(\beta \preceq \alpha \to P(\beta))$, que es $P^*(\alpha)$, por definición. Con esto tenemos probado (9).

Nuestro objetivo es probar

$$\forall \eta \in E(\forall \delta \in E(\delta \prec \eta \to P'(\delta)) \to P'(\eta)). \tag{11}$$

Así que fijamos $\eta \in E$ tal que

$$\forall \delta \in E(\delta \prec \eta \to P'(\delta)), \tag{12}$$

y tenemos que probar $P'(\eta)$. Para ello fijamos un ordinal $\alpha$, suponemos $P^*(\alpha)$ y tenemos que probar $P^*(\alpha + \omega^\eta)$.

Distinguimos tres casos, según si $\eta = 0$, $\eta$ es un ordinal sucesor o bien es un ordinal límite.

1) Si $\eta = 0$ tenemos que probar $P^*(\alpha + 1)$, pero la hipótesis $P^*(\alpha)$ equivale a que $\forall \beta \in E(\beta \prec \alpha + 1 \to P(\beta))$, y entonces podemos aplicar (8) para obtener $P(\alpha + 1)$, que junto a $P^*(\alpha)$ nos da $P^*(\alpha + 1)$, como queríamos.

2) Supongamos ahora que $\eta = \delta + 1$ para algún ordinal $\delta$, y entonces tenemos que probar $P^*(\alpha + \omega^{\delta+1})$ y, por (9), basta probar a su vez

$$\forall \beta \in E(\beta \prec \alpha + \omega^\delta \cdot \omega \to P^*(\beta)). \tag{13}$$

Ahora bien, por **(S2)**, $\alpha + \omega^\delta \cdot \omega$ es el supremo de los ordinales $\alpha + \gamma$ con $\gamma \prec \omega^\delta \cdot \omega$, luego si $\beta \prec \alpha + \omega^\delta \cdot \omega$, entonces existe un $\gamma < \omega^\delta \cdot \omega$ tal que $\beta \prec \alpha + \gamma$. Usando ahora **(P2)**, existe un $k \prec \omega$ tal que $\gamma \prec \omega^\delta \cdot k$, luego en total (usando **(S5)**) $\beta \prec \alpha + \omega^\delta \cdot k$.

Esto hace que baste con demostrar:

$$\forall k \in E(k \prec \omega \to P^*(\alpha + \omega^\delta \cdot k)). \tag{14}$$

En efecto, admitiendo (14), para probar (13) basta observar que si $\beta \prec \alpha + \omega^\delta \cdot \omega$ existe un $k$ tal que $\beta \prec \alpha + \omega^\delta \cdot k$, luego por (14) se cumple $P^*(\alpha + \omega^\delta \cdot k)$, luego también $P^*(\beta)$, por la definición de $P^*$, y así tenemos (13).

Demostramos (14) por inducción sobre $k$.

Para $k = 0$ hay que probar $P^*(\alpha)$, que se cumple por hipótesis.

Suponemos $P^*(\alpha + \omega^\delta \cdot k)$ y, como $\delta \prec \eta$, por (12) tenemos $P'(\delta)$ que, por definición de $P'$, implica

$$P^*(\alpha + \omega^\delta \cdot k) \to P^*(\alpha + \omega^\delta \cdot k + \omega^\delta)$$

y lo segundo es precisamente $P^*(\alpha + \omega^\delta \cdot (k+1))$, lo que completa la inducción, la prueba de (14) y, por lo tanto, la de (13).

3) Falta el caso en que $\eta$ es un ordinal límite.

   Para probar $P^*(\alpha+\omega^\eta)$ tomamos $\beta \prec \alpha+\omega^\eta$, con lo que existe (por **(S2)**) un $\gamma \prec \omega^\eta$ tal que $\beta \prec \alpha+\gamma$ y a su vez (por **(E1)**) existe un $\delta \prec \eta$ tal que $\gamma \prec \omega^\delta$ y, por **(S5)**, $\beta \prec \alpha+\omega^\delta$.

   Por (12) tenemos $P'(\delta)$, y por definición de $P'$ tenemos que $P^*(\alpha) \to P^*(\alpha+\omega^\delta)$, pero estamos suponiendo $P^*(\alpha)$, luego tenemos $P^*(\alpha+\omega^\delta)$ y, por definición de $P^*$, también $P^*(\beta)$.

   Esto prueba que

$$\forall \beta \in E(\beta \prec \alpha+\omega^\eta \to P^*(\beta)),$$

   y por (9) concluimos $P^*(\alpha+\omega^\eta)$.

Esto termina la prueba de (7).

Recordemos que

$$\omega^{(0)} = 1, \omega^{(1)} = \omega, \omega^{(2)} = \omega^\omega, \omega^{(3)} = \omega^{\omega^\omega}, \ldots$$

Con esto es fácil probar que, si se cumple $P(0)$, entonces se cumple

$$\forall \alpha \in E(\alpha \preceq \omega^{(n)} \to P'(\alpha)) \to \forall \alpha \in E(\alpha \preceq \omega^{(n+1)} \to P(\alpha)) \tag{15}$$

Informalmente: Si todos los ordinales menores o iguales que $\omega^{(n)}$ cumplen $P'$, entonces los ordinales hasta $\omega^{(n+1)}$ cumplen $P$.

En efecto, suponemos que $\forall \alpha \in E(\alpha \preceq \omega^{(n)} \to P'(\alpha))$, con lo que en particular tenemos $P'(\omega^{(n)})$, es decir

$$\forall \alpha \in E(P^*(\alpha) \to P^*(\alpha+\omega^{(n+1)})).$$

Luego tomando $\alpha = 0$ (puesto que $P^*(0)$ es lo mismo que $P(0)$) llegamos a $P^*(\omega^{(n+1)})$, que es, precisamente, $\forall \alpha \in E(\alpha \preceq \omega^{(n+1)} \to P(\alpha))$.

Con esto ya podemos probar fácilmente el principio de inducción. Para ello observemos que hemos razonado con una propiedad arbitraria $P$, pero todo lo que hemos hecho con $P$ vale en particular para la propiedad $P'$, es decir, que tiene sentido considerar la propiedad $P''$, e igualmente podemos considerar $P'''$, $P''''$, etc.

Supongamos

$$\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P(\beta)) \to P(\alpha))$$

y tenemos que probar que todo ordinal cumple $P(\alpha)$.

Para ello, dado un ordinal $\alpha$, sabemos que existe un $n$ tal que $\alpha \prec \omega^{(n)}$, luego basta probar que todo ordinal menor que $\omega^{(n)}$ cumple $P(\alpha)$. Por ejemplo, si $\alpha \prec \omega^{(4)}$, podemos razonar así:

Aplicando repetidamente (7), tenemos:

$$\begin{aligned}
&\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P(\beta)) \to P(\alpha))\\
&\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P'(\beta)) \to P'(\alpha))\\
&\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P''(\beta)) \to P''(\alpha))\\
&\forall \alpha \in E(\forall \beta \in E(\beta \prec \alpha \to P'''(\beta)) \to P'''(\alpha))
\end{aligned}$$

En particular, tenemos $P(0), P'(0), P''(0), P'''(0)$ (pues los antecedentes de las implicaciones anteriores para $\alpha = 0$ se cumplen trivialmente). Más aún, la última implicación nos permite probar por inducción que $\forall\beta \in E(\beta \prec \omega \to P'''(\beta))$, de donde, a su vez, esa misma implicación nos lleva a $P'''(\omega)$, luego en total tenemos que

$$\forall\alpha \in E(\alpha \preceq \omega^{(1)} \to P'''(\alpha)).$$

Ahora podemos aplicar repetidamente (15) (ya que contamos con $P''(0), P'(0), P(0)$), lo que nos da

$$\forall\alpha \in E(\alpha \preceq \omega^{(2)} \to P''(\alpha))$$
$$\forall\alpha \in E(\alpha \preceq \omega^{(3)} \to P'(\alpha))$$
$$\forall\alpha \in E(\alpha \preceq \omega^{(4)} \to P(\alpha)).$$

Así hemos probado que todo ordinal $\alpha \preceq \omega^{(4)}$ cumple $P(\alpha)$. Hemos supuesto $n = 4$, pero es claro que el argumento vale igualmente para cualquier $n$, sin más que aplicar las veces que haga falta (7) y luego (15). Por lo tanto, hemos probado que $\forall\alpha \in E\, P(\alpha)$.

Esto demuestra el principio de inducción hasta $\epsilon_0$ con un argumento que cualquier finitista radical denunciará que "en realidad" es pura lógica formal, es decir, que no hemos hecho ni más ni menos que lo que hace cualquier matemático cuando razona en ZF.

De hecho, podemos decir más. Supongamos que partimos de una propiedad aritmética $P$, es decir, una propiedad de los números naturales definible a partir de la aritmética elemental y, por lo tanto, definible en la aritmética de Peano. Las propiedades $P', P'', P'''$, etc., son entonces propiedades aritméticas (porque se definen a partir de $P$ y de la aritmética ordinal, pero toda la aritmética ordinal se define a partir de la aritmética elemental de los números naturales, según hemos visto en los mensajes anteriores), y en todo el argumento no hemos usado ninguna propiedad "extraña" de los números naturales que no sea demostrable en AP. Entonces, ¿hemos demostrado el principio de inducción $P - \mathrm{IND}(\epsilon_0)$ en AP (para propiedades aritméticas)?

Si es así, tenemos un problema, porque Gentzen demostró que, para cierta propiedad aritmética P (la que expresa que $\alpha$ no es el ordinal asociado a la prueba de una contradicción en AP), el principio $P - \mathrm{IND}(\epsilon_0)$ implica la consistencia de AP, luego si hemos demostrado $P - \mathrm{IND}(\epsilon_0)$ en AP resulta que la consistencia de AP es demostrable en AP, y el segundo teorema de incompletitud de Gödel implica entonces que la aritmética de Peano es contradictoria.

Que en AP se puede demostrar que $P - \mathrm{IND}(\epsilon_0)$ implica la consistencia de AP es un hecho muy técnico que aquí no podemos discutir pero que aceptan unánimemente cuantos entienden el asunto. Doy mi palabra de honor de que ahí no hay trampa (conocida por la comunidad matemática). Y lo mismo vale para el teorema de incompletitud de Gödel.

La cuestión es si la demostración que acabamos de ver del principio de inducción es formalizable en AP o no, es decir, si hemos usado en algún momento algo que no pueda demostrarse a partir de los axiomas de Peano. Y la respuesta no es nada técnico, no hay que ir a los mensajes anteriores a ver si hay algo que hayamos probado usando algo sospechoso, sino que el fallo está aquí mismo, bien a la vista, y no es sino un ejemplo más del eterno problema de la matemática formal.

**Link al post original:** Un acertijo metamatemático

# 11. Una demostración infinitamente larga

Bien, Eparoh ha resuelto el enigma en el hilo de comentarios.

Todo el argumento anterior es formalizable en la aritmética de Peano excepto la última parte. Más precisamente, del mismo modo que los matemáticos demuestran teoremas "en ZFC" sin mencionar ZFC, e incluso en muchas ocasiones sin saber siquiera qué es ZFC, todo lo anterior puede verse como una demostración en AP de las afirmaciones (supuesto que $P$ sea una propiedad aritmética):

$$P-\mathrm{IND}(\omega^{(1)}):\forall\alpha\in E(\forall\beta\in E(\beta\prec\alpha\to P(\beta))\to P(\alpha))\to\forall\alpha\in E(\alpha\prec\omega^{(1)}\to P(\alpha))$$
$$P-\mathrm{IND}(\omega^{(2)}):\forall\alpha\in E(\forall\beta\in E(\beta\prec\alpha\to P(\beta))\to P(\alpha))\to\forall\alpha\in E(\alpha\prec\omega^{(2)}\to P(\alpha))$$
$$P-\mathrm{IND}(\omega^{(3)}):\forall\alpha\in E(\forall\beta\in E(\beta\prec\alpha\to P(\beta))\to P(\alpha))\to\forall\alpha\in E(\alpha\prec\omega^{(3)}\to P(\alpha))$$
$$P-\mathrm{IND}(\omega^{(4)}):\forall\alpha\in E(\forall\beta\in E(\beta\prec\alpha\to P(\beta))\to P(\alpha))\to\forall\alpha\in E(\alpha\prec\omega^{(4)}\to P(\alpha))$$
$$\vdots$$

En otras palabras, hemos demostrado (y en AP podemos demostrar) que la inducción hasta $\omega^{(1)}$ es válida, que la inducción hasta $\omega^{(2)}$ es válida, que la inducción hasta $\omega^{(3)}$ es válida, etc., pero NO es posible demostrar en AP (admitiendo que es consistente) que la inducción hasta $\epsilon_0$ es válida.

Si pudiéramos demostrar en AP que la inducción hasta $\epsilon_0$ es válida, podríamos probar en AP que AP es consistente, y Gödel nos daría automáticamente la demostración de una contradicción en AP.

Con más detalle. El argumento anterior nos da una demostración de $P-\mathrm{IND}(\omega^{(2)})$ en la que se usa la propiedad $P$ y la propiedad $P'$ definida a partir de ella, y en la que se usan una vez las afirmaciones (7) y (15).

Por otra parte, el argumento del mensaje anterior nos da también una demostración de $P-\mathrm{IND}(\omega^{(3)})$ que es más compleja, porque usa las propiedades $P, P', P''$ y más larga, porque requiere usar dos veces las propiedades (7) y (15).

Y el mismo argumento nos da una demostración de $P-\mathrm{IND}(\omega^{(4)})$ más compleja (usa $P, P', P'', P'''$) y más larga (usa las propiedades (7) y (15) tres veces).

Y así sucesivamente. Desde un punto de vista formal, el argumento anterior no es el esbozo de una demostración (en el mismo sentido en que las demostraciones que vienen en todos los libros de matemáticas son esbozos de demostraciones formales en ZFC), sino que es un esquema que nos asegura que podemos construir una demostración de

$$P-\mathrm{IND}(\omega^{(n)}):\forall\alpha\in E(\forall\beta\in E(\beta\prec\alpha\to P(\beta))\to P(\alpha))\to\forall\alpha\in E(\alpha\prec\omega^{(n)}\to P(\alpha)),$$

para $n=0,1,2,3\ldots$

Si nos dan $n=1\,000$ sabemos cómo demostrar que la inducción transfinita vale hasta $\omega^{(1000)}$, pero globalmente no tenemos una única demostración, sino que sabemos construir una demostración para cada $n$, una demostración que será más larga y compleja cuanto mayor sea $n$, pero que sigue un sencillo patrón general.

Sin embargo, desde un punto de vista metamatemático (intuitivo), no falta nada por demostrar. Esas infinitas demostraciones prueban que la inducción transfinita es válida

para todo ordinal. Sabemos probar que es válida hasta $\omega^{(1)}$, y hasta $\omega^{(2)}$, y hasta $\omega^{(3)}$, etc. y, como todo ordinal es menor que uno de éstos, sabemos que la inducción transfinita es válida para todos los ordinales (menores que $\epsilon_0$).

El formalista que crea que las demostraciones metamatemáticas son meras demostraciones formales "disfrazadas", aquí tiene un ejemplo sobre el que reflexionar: tenemos un argumento intutivamente convincente que no es formalizable porque usa el ingrediente intuitivo por excelencia, que los números naturales son sólo el 0, el 1, el 2, el 3, etc.

Intuitivamente, si estamos seguros de que algo se puede demostrar para $\omega^{(1)}$, y para $\omega^{(2)}$, y para $\omega^{(3)}$, etc., podemos asegurar que eso se cumple para todos los $\omega^{(n)}$ y, en este caso, eso significa que eso se cumple para todos los ordinales. Sin embargo, formalmente, NO tenemos una prueba para todos los ordinales, es decir, una prueba de

$$\forall n \; P - \mathrm{IND}(\omega^{(n)}),$$

sino un esquema que nos garantiza cómo construir infinitas pruebas, una para cada número natural. Formalmente no es lo mismo, intuitivamente sí.

Decía en el primer mensaje que demostrar la inducción transfinita en ZF es hacer el ridículo (si lo que pretendemos es probar la consistencia de AP), porque la consistencia de AP es trivial como teorema de ZF, y lo que interesa es una prueba que no dependa de ZF. La prueba que hemos dado en el mensaje anterior es, ciertamente, independiente de ZF, en el sentido de que no dejaría de ser concluyente aunque ZF resultara ser contradictorio. Pero, de cara a probar la consistencia de AP, no deja de ser un tanto ridícula:

Aunque el final de la prueba trasciende a AP, lo cierto es que el argumento principal no es más que un razonamiento en AP. Quiero decir que cualquiera que lo acepte como válido, tácitamente está aceptando que razonar en AP es fiable (y en particular, consistente), luego en esencia estamos demostrando la consistencia de AP fiándonos de AP.

Claro que es difícil precisar qué significaría demostrar la consistencia de AP sin fiarse de AP. Una de las razones por las que la teoría de Gentzen suscita perplejidad es porque es difícil conceder que demuestre realmente algo, ya que uno tiende a acabar convencido de que le están demostrando lo que ya sabe que es cierto, con lo que es difícil juzgar si el argumento es concluyente.

Esto no quita para que la relación entre la consistencia, los ordinales y la inducción sea muy interesante, pero, si realmente queremos un argumento para la consistencia de AP que sea "más concreto", "más finitista", "más a prueba de escépticos de la intuición", más qué sé yo... No parece que con este argumento hayamos descendido nada en evidencia o conclusividad que el mero argumento basado en que existen los números naturales y cumplen los axiomas de AP, por lo que éstos no pueden probar mentiras sobre números naturales.

Quizá un argumento como el de la sección anterior sería más aceptable en esa línea, pero con el dado allí tal cual se plantea la duda de si realmente se está concluyendo algo o si es un mero "repugna a la naturaleza de una recta".

En el mensaje siguiente daré la demostración de Takeuti que había prometido.

**Link al post original:** Una demostración infinitamente larga

# 12. El argumento de Takeuti

Expongo ahora el argumento de Takeuti sobre la buena ordenación de los ordinales (menores que $\epsilon_0$). Se basa en esta definición:

Diremos que un ordinal es 1-accesible si es accesible. De forma recursiva, supuesto definido lo que es un ordinal $n$-accesible, diremos que un ordinal $\alpha$ es $n+1$-accesible si cuando $\beta$ es $n$-accesible, también lo es $\beta\cdot\omega^\alpha$.

Ahora generalizamos dos hechos que hemos probado para ordinales accesibles.

**(A4)** Si $\delta_0 \prec \delta_1 \prec \cdots$ es una sucesión estrictamente creciente de ordinales $n$-accesibles que tiene a $\lambda$ por supremo, entonces $\lambda$ también es $n$-accesible.

En **(A2)** probamos el caso para $n=1$, luego supongamos que es cierta para $n$ y veamos que también vale para $n+1$.

Para ello partimos de una sucesión creciente de ordinales $n+1$-accesibles y sea $\beta$ otro ordinal $n$-accesible (que podemos suponer no nulo). Entonces, por definición de la $n+1$-accesibilidad, cada ordinal $\beta\cdot\omega^{\delta_i}$ es $n$-accesible. Ahora bien, es fácil ver (se deja como ejercicio) que la sucesión

$$\beta\cdot\omega^{\delta_0} \prec \beta\cdot\omega^{\delta_1} \prec \cdots$$

tiene supremo $\beta\cdot\omega^\lambda$, luego por hipótesis de inducción es $n$-accesible, y esto prueba la $n+1$-accesibilidad de $\lambda$.

**(A5)** Si $\alpha$ es $n$-accesible, también lo es $\alpha\cdot\omega$.

El caso para $n=1$ está probado en **(A3)**.

Supuesta cierta para $n$, tomamos un ordinal $n+1$-accesible $\alpha$ y otro $n$-accesible $\beta$. Tenemos que probar que $\beta\cdot\omega^{\alpha\cdot\omega}$ es $n$-accesible. Pero este ordinal es el supremo de la sucesión

$$\beta\cdot\omega^{\alpha} \prec \beta\cdot\omega^{\alpha\cdot 2} \prec \beta\cdot\omega^{\alpha\cdot 3} \prec \cdots$$

luego, por **(A4)**, basta probar que cada $\beta\cdot\omega^{\alpha\cdot k}$ es $n$-accesible, pero $\beta\cdot\omega^{\alpha\cdot k} = \beta\cdot\omega^\alpha\cdots\omega^\alpha$, y basta usar $k$ veces la accesibilidad de $\alpha$.

Como consecuencia inmediata:

**(A6)** El ordinal 1 es $n$-accesible para todo número natural $n\geq 1$.

En efecto, sabemos que (trivialmente) 1 es 1-accesible y, si $\beta$ es un ordinal $n$-accesible, entonces $\beta\cdot\omega^1$ es $n$-accesible por **(A5)**, y esto significa, por definición, que 1 es $n+1$-accesible.

Con esto ya es fácil probar que todos los ordinales $\omega^{(n)}$ son accesibles. Por ejemplo, para $n=5$ razonamos así:

1. Según acabamos de probar, 1 es 6-accesible.
2. Como 1 también es 5-accesible, por definición $\omega = 1\cdot\omega^1$ es 5-accesible.

3. Como 1 es 4-accesible, por definición $\omega^{(2)} = 1 \cdot \omega^{\omega}$ e 4-accesible.

4. Como 1 es 3-accesible, por definición $\omega^{(3)} = 1 \cdot \omega^{\omega^{(2)}}$ es 3-accesible.

5. Como 1 es 2-accesible, por definición $\omega^{(4)} = 1 \cdot \omega^{\omega^{(3)}}$ es 2-accesible.

6. Como 1 es 1-accesible, por definición $\omega^{(5)} = 1 \cdot \omega^{\omega^{(4)}}$ es 1-accesible.

La pregunta filosófica es:

¿Es esto una demostración finitista? ¿Sirve este argumento (junto con la prueba de Gentzen) para que alguien se convenza de que la aritmética de Peano es consistente?

**Link al post original:** El argumento de Takeuti

# 13. Ordinales menores que $\epsilon_0$

No cabe duda de que el argumento de Gentzen tiene interés por varios motivos.

Por una parte, nos proporciona un ejemplo sencillo de afirnación sencilla sobre los números naturales (la buena ordenación de los ordinales o, equivalentemente, el principio de inducción hasta $\epsilon_0$) que, aunque cualquiera debería aceptar que es cierto, no es demostrable a partir de los axiomas de Peano, lo que pone en evidencia que sabemos más cosas sobre los números naturales que lo que afirman estos axiomas.

Esto ya podría dar que pensar a algunos formalistas radicales, pero lo más importante —o, al menos, la razón por la que me propuse escribir este hilo— es que la prueba de la validez de la inducción hasta $\epsilon_0$, por mucho que se parezca a una demostración formal típica (expuesta con el nivel de informalidad propio de todos los textos matemáticos) y por mucho que —por supuesto— se pueda considerar como una demostración formal típica en ZF, el caso es que considerarla como tal la desvirtúa por completo, en cuanto a que, si aporta algo, es precisamente como argumento informal, independiente de cualquier teoría axiomática, pues es la hipótesis de una prueba de la consistencia de AP que sólo tiene valor en la medida en que no dependa de la consistencia de ZF, pues es trivial que la consistencia de ZF implica la de AP.

Por ello un formalista radical debería plantearse que el hecho de que todo argumento metamatemático "convincente" sea formalizable en ZF y que, por lo tanto, todo argumento metamatemático convincente pueda presentarse bajo el aspecto de una demostración formal típica no es razón para concluir que los razonamientos metamatemáticos son razonamientos formales disfrazados, o algo así.

Por otro lado, quienes consideran dudosa la evidencia de la buena ordenación de los números naturales, o del principio de inducción usual, pueden hacerse una idea del grado de sofisticación que puede necesitar un argumento metamatemático intuitivo, y cómo en un momento dado es inevitable tener que recurrir a que los números naturales son 0, 1, 2, 3 ... y ninguno más, por lo que todo intento de evitar enfrentarse a este hecho no es más que un intento de posponer lo inevitable.

Para terminar de destacar aspectos de interés de la teoría de Gentzen cabe señalar que la prueba de que la inducción hasta $\epsilon_0$ implica la consistencia de AP no sólo es formalizable en AP, sino en una teoría formal mucho más restrictiva, conocida como Aritmética Recursiva

Primitiva, que puede decirse que formaliza el finitismo más estricto posible (sin entrar en el ultrafinitismo, que niega la existencia de los números muy grandes). La teoría ARP sólo permite demostrar teoremas que se prueben explícitamente sin hacer referencia más que a una cantidad finita de números naturales. Una evidencia de su limitación es que en ARP no se puede demostrar siquiera la inducción hasta $\omega \cdot 2$.

Así pues, Gentzen separó toda la parte estrictamente finitista de la prueba de la consistencia de AP de un único ingrediente no finitista: la inducción hasta $\epsilon_0$.

Como acabo de señalar (o más bien, recordar, pues ya lo he dicho muchas veces), demostrar la inducción hasta $\epsilon_0$ en ZF es pervertirla, convertirla en una trivialidad, pero el debate filosófico que suscitan las demostraciones informales es justo el contrario: si al demostrar informalmente la validez de la inducción hasta $\epsilon_0$ no estamos suponiendo ya la consistencia de AP que en principio podríamos demostrar a partir de ella.

Por ejemplo, uno puede demostrar que existen rectas perpendiculares a partir de unos axiomas razonables para la geometría euclídea, pero sin duda tal teorema será tan evidente o incluso más que algunos de los axiomas. Nadie necesitará una demostración a partir de unos axiomas evidentes para convencerse de que es verdad que existen rectas perpendiculares (otra cosa es que la axiomatización de la geometría sirva para lo que sirve, pero no para convencer a alguien de algo obvio a partir de otras obviedades o incluso de cosas menos obvias). Aquí pasa (o podría pasar) lo mismo: ¿existirá alguien que diga "yo no estaba convencido de que AP era consistente hasta que no vi la prueba de Gentzen"?

Es poco probable, pero no porque el argumento de Gentzen no sea convincente, sino porque es difícil encontrar a alguien que no esté convencido de antemano. Sobre eso se ha escrito mucho. A poco que busquéis en Google encontraréis artículos al respecto.

Se trata de comparar el argumento de Gentzen con el obvio: AP tiene que ser consistente porque sus axiomas son afirmaciones verdaderas sobre números naturales, luego sus teoremas también, luego nunca se podrá demostrar a partir de ellos ninguna falsedad.

La cuestión es si este uso de los números naturales como garantes de que en AP siempre se dicen cosas verdaderas (no como en ZFC, que no podemos hacer referencia a ninguna realidad clara que "esté ahí" y que nos permita decir que los axiomas de ZFC dicen cosas verdaderas sobre esos objetos) es distinto del uso que estamos haciendo de los números naturales al hablar de ordinales y probar su buena ordenación.

Por ejemplo, un posible argumento en favor de Gentzen sería que el argumento "directo" por el que uno se convence de la consistencia de AP exige admitir que cualquier afirmación sobre números naturales, sea la que sea, tiene que ser verdadera o falsa en un cierto sentido intuitivo, aunque en muchos casos sea imposible saber cuál es el caso. En cambio, el argumento de Gentzen sólo requiere una parte estrictamente finitista que se formaliza con afirmaciones muy limitadas en su significado, y de la prueba de la validez de la inducción hasta $\epsilon_0$ que sólo requiere reconocer que unas afirmaciones muy concretas sobre números naturales (no cualquier afirmación en general) son verdaderas.

Aunque cabe señalar que digo "muy concretas" en el sentido de "unas afirmaciones determinadas", pero éstas son, en otro sentido de la palabra, bastante abstractas. Me refiero a lo que, en términos de la prueba de Takeuti, se expresa como ordinales $n$-accesibles.

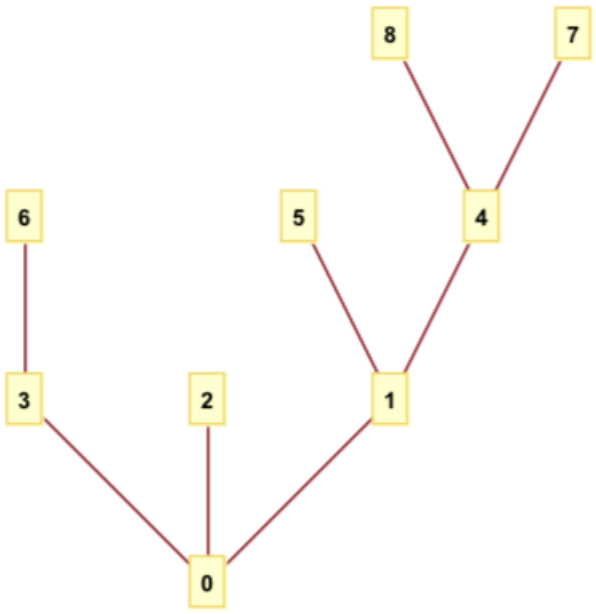
En principio con esto termina lo que quería contar en este hilo, pero voy a prolongarlo un poco más relacionando lo que hemos visto con un problema famoso interesante.

**Link al post original:** Ordinales menores que $\epsilon_0$

# 14. Hércules y la Hidra

Como sabe todo el mundo que tiene Wikipedia a mano, Hércules mató a su esposa y a sus hijos en un arrebato de locura que le provocó la diosa Hera (que no llevaba bien que su marido Zeus hubiera engendrado a Hércules con otra mujer). Angustiado por su crimen, Hércules consultó el oráculo de Delfos, que le dijo que para expiar su culpa tenía que ponerse al servicio del rey Euristeo de Micenas, que le encomendó doce trabajos. El segundo de ellos fue matar a la Hidra de Lerna, un monstruo con muchas cabezas (hasta 10.000, según las fuentes) que podía regenerar dos cabezas por cada una que le cortaban. Pese a ello, Hércules se las arregló para matar a la Hidra.

No obstante, aquí vamos a enfrentarlo a una Hidra mucho más peligrosa. No sabemos cómo es exactamente ni cuántas cabezas tiene, pero podría ser tal que así:

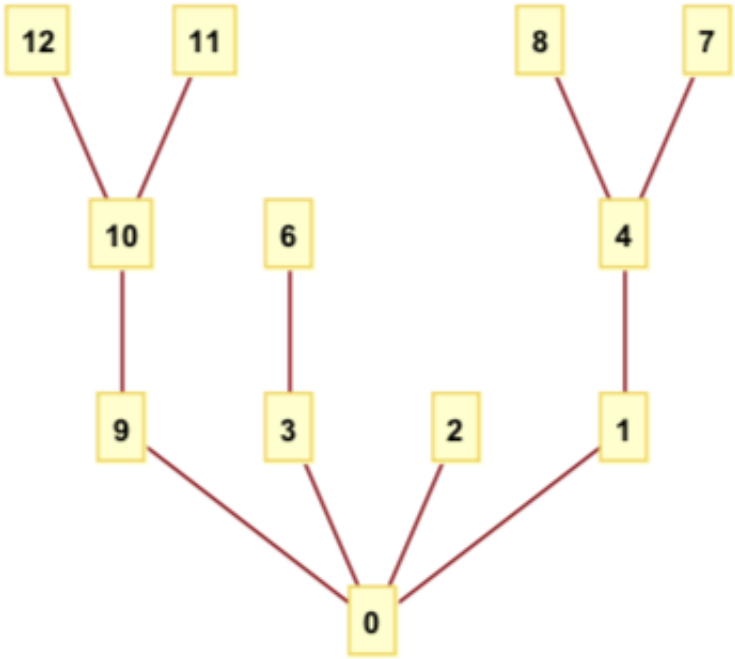



Para un matemático, que ve las cosas más esquemáticamente, una hidra es un árbol con una única raíz, que en la figura hemos numerado como 0, de la que puede salir un número finito de nodos (en la figura tres, numerados como 1, 2, 3), de los cuales a su vez pueden salir más nodos, etc., pero sólo puede haber un número finito de nodos en total. Los nodos de los que no salen más nodos son las cabezas de la hidra. La hidra de la figura tiene 5 cabezas.

No parece tan peligrosa como la Hidra de 10.000 cabezas a la que tuvo que enfrentarse Hércules, pero su peligro se debe a que su capacidad de regenerar cabezas es muy superior.

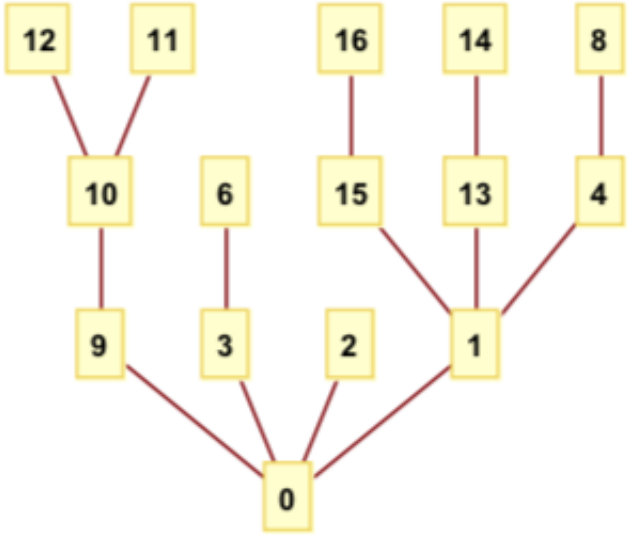
Supongamos que Hércules decide atacar a la Hidra cortándole la cabeza numerada como 5 (con su "cuello" correspondiente, es decir, que quitamos la rama que une el nodo 1 con

el 5). Nos fijamos entonces en la rama de la que salía el cuello amputado, es decir, la que une la raíz 0 con el nodo 1. Dicha rama se duplica con todo lo que tiene sobre ella, con lo que la Hidra pasa a tener este aspecto:

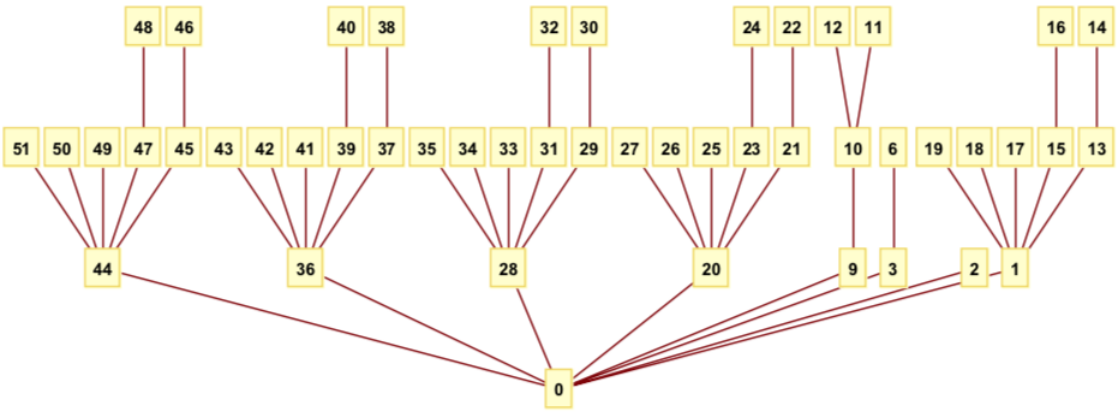



La copia de la rama 0-1 es la rama 0-9. Ahora la Hidra tiene 6 cabezas.

Pongamos que, en un segundo asalto, Hércules decide cortar la cabeza número 7. Nos fijamos ahora en la rama 1-4 de la que salía dicha cabeza. Esta vez la Hidra no regenera una copia de dicha arista y todo lo que hay sobre ella, sino DOS copias, y el resultado es:




Las copias de la rama 1-4 son las ramas 1-13 y 1-15, con lo que ahora la Hidra tiene 7 cabezas. Si en el tercer asalto Hércules le amputa la cabeza 8, la Hidra genera TRES copias de la arista 1-4 y, si en el cuarto asalto Hércules corta la cabeza número 4, la Hidra regenera CUATRO copias de la arista 0-1, y el resultado es




Ahora la Hidra tiene 29 cabezas.

Es crucial señalar que si Hércules corta una cabeza que sale directamente de la raíz de la Hidra, entonces no se produce regeneración alguna. Por ejemplo, si en el quinto asalto Hércules corta la cabeza número 2, la Hidra no sufrirá más cambio que la amputación de dicha cabeza (pero el contador de asaltos sigue avanzando y en el sexto asalto, si se corta una cabeza que no salga de la raíz, la Hidra generará SEIS copias de la rama de la que salía).

El problema que se plantea es si Hércules podrá matar a la Hidra en un número finito de pasos, es decir, reducirla a su raíz, sin cabeza alguna. Naturalmente, esto puede depender de la hidra inicial concreta a la que se enfrente o de la estrategia que siga para elegir qué cabeza corta en cada momento.

Si yo fuera malévolo y despiadado, podría haber planteado este problema en la sección de "propuestos por todos" a ver quién se anima a ayudar a Hércules derrotar a la Hidra (si es que se puede). Pero lo he planteado en este hilo.

Es un sano ejercicio jugar un poco con las hidras, para lo cual conviene programarlas. Es importante codificar las hidras de forma práctica que permita subir y bajar por ellas con facilidad. A continuación pongo cómo lo he hecho yo con Python, por si le sirve a alguien de guía para adaptarlo a su lenguaje favorito.

Salvo que alguien encuentre una forma más práctica, yo diría que lo mejor es codificar una hidra como una sucesión de nodos. El nodo $i$-ésimo contiene dos datos: el índice del nodo "padre" del cual sale y el conjunto de índices de los nodos "hijos" que salen de él. Así, si estamos en un nodo lo tenemos fácil para bajar o para subir a los nodos siguientes.

Me ha parecido que sería más eficiente computacionalmente llevar la cuenta redundante del conjunto de índices correspondientes a cabezas, para no tener que calcularlas cada vez que queremos elegir una para cortarla.

Por comodidad he definido una clase "nodo" que simplemente contiene la información del nodo padre y del conjunto de nodos hijos, y la Hidra la he definido como un diccionario que a cada índice le asigna un nodo:

```
class nodo:
    def __init__(self, pdr, hjs = None):
        if hjs == None:
            hjs = set()
        self.padre = pdr
```

```
        self.hijos = hjs
    def __str__(self):
        return("{}->{}".format(self.padre,self.hijos))
    def __repr__(self):
        return("nodo({},{})".format(self.padre,self.hijos))

Hidra = ({0:nodo(None)})
Cabezas = set() #Conjunto de índices de las cabezas
Puntero = 0 #Último índice usado[/code]
```

Este código define la "Hidra muerta":

```
{0: nodo(None,set())}
```

Consta de un único nodo 0 sin padre y con un conjunto vacío de hijos.

Para dotarla de cabezas uso las funciones siguientes:

```
def indice():
    #Nuevo índice
    global Puntero
    Puntero += 1
    return Puntero

def añade(i,r = None):
    #Añade una cabeza que sale del nodo i con índice r
    global Hidra
    if r == None:
        r = indice()
    Hidra[r]=nodo(i) #Añadimos una cabeza de índice r.
    Hidra[i].hijos.add(r) #La incluimos entre los hijos de i.
    Cabezas.add(r) #La incluimos en la lista de cabezas
    if i in Cabezas: #Si i era una cabeza, deja de serlo.
        Cabezas.discard(i)
```

La función indice() simplemente va generando números no usados para tomarlos como índices de los nuevos nodos, mientras que la función añade() le añade a la Hidra una nueva cabeza que sale del nodo i con índice r.

Por ejemplo, si hacemos:

```
Hidra.clear()
Hidra = ({0:nodo(None)})
Puntero = 0
Asalto = 0
añade(0)
añade(0)
añade(0)
añade(1)
añade(1)
añade(3)
añade(4)
```

```
añade(4)
```

Generamos la Hidra de la primera imagen. Primero hemos añadido tres cabezas sobre el nodo 0 (que son los nodos 1, 2, 3), luego hemos añadido nodos 4 y 5 sobre el nodo 1, luego un nodo 6 sobre el nodo 3 y luego los nodos 7 y 8 sobre el nodo 4.

El resultado se ve así:

```
{0: nodo(None,{1, 2, 3}), 1: nodo(0,{4, 5}), 2: nodo(0,set()), 3: nodo
   (0,{6}), 4: nodo(1,{8, 7}), 5: nodo(1,set()), 6: nodo(3,set()), 7:
   nodo(4,set()), 8: nodo(4,set())}
```

Por ejemplo, el nodo 1 tiene por padre al nodo 0 y por hijos a los nodos 4 y 5.

Los gráficos los he hecho con Mathematica, porque tiene una instrucción a la que le das un árbol y ella se encarga de dibujarlo de la forma más clara posible, y queda muy bien. En Python he programado algo más rudimentario, simplemente para ver qué vamos teniendo entre manos:

```
def arb(i):
    u = []
    h = sorted(Hidra[i].hijos)
    n = len(h)
    if n == 0:
        u = [str(i)]
    else:
        l = 0
        for j in h:
            s = arb(j)
            ll = len(s)
            if l == 0:
                s[0] = ("{}___".format(i))+s[0]
            else:
                s[0] = "|___"+s[0]
            u.append(s[0])
            for k in range(1, ll):
                s[k] == "    "+s[k]
                if l+1 < n:
                    s[k] = "|   "+s[k]
                else:
                    s[k] = "    "+s[k]
                u.append(s[k])
            l += 1
            if l < n:
                u.append("|")
    return u

def arbol():
    #Representa la Hidra en forma de árbol.
    s = arb(0)
    t =""
```

```
    for i in s:
        t = t + "\n" + i
    return(t)
```

El resultado es:

```
0___1___4___7
|   |       |
|   |       |___8
|   |
|   |___5
|
|___2
|
|___3___6
```

Para cortar cabezas a la Hidra se puede usar este código:

```
def traslada(i, j):
    #Traslada todo lo que hay sobre el nodo i al nodo j
    global Hidra
    for k in Hidra[i].hijos:
        r = indice()
        añade(j,r) #Añadimos una cabeza (provisional) en r.
        traslada(k,r) #Trasladamos sobre r todo lo que hay sobre k.

def corta(i,n):
    #Corta la cabeza i y regenera n veces
    global Hidra, Cabezas
    if not i in Cabezas:
        raise Exception("El nodo {} no es una cabeza.".format(i))
    cuello = Hidra[i].padre
    del(Hidra[i]) #Borramos la cabeza i
    Cabezas.discard(i) #La borramos tambien de la lista de cabezas
    Hidra[cuello].hijos.remove(i) #La borramos del conjunto de hijos.
    if cuello != 0:
        pecho = Hidra[cuello].padre
        if Hidra[cuello].hijos == set():
            Cabezas.add(cuello) #Si el cuello no tenía más hijos, ahora
   es cabeza.
        for s in range(0,n): #Regeneramos n veces la Hidra.
            r = indice()
            añade(pecho, r) #Creamos un nuevo nodo sobre el pecho.
            traslada(cuello, r) #Y trasladamos todo lo que hay sobre el
   cuello.
```

```
def ataca(n):
    #Le corta a la Hidra la cabeza n-sima y calcula la regeneración
   correspondiente.
    global Asalto
    Asalto += 1
    if n != None:
        corta(n, Asalto)
```

Por ejemplo, así se generan las Hidras de las imágenes de este mensaje:

```
print(arbol())
ataca(5)
print(arbol())
ataca(7)
print(arbol())
ataca(8)
print(arbol())
ataca(4)
print(arbol())
```

El código siguiente muestra la evolución del combate si Hércules juega con más fuerza que maña, cortando en cada asalto la primera cabeza que se le ocurre:

```
import random

while Asalto < 100:
    n = random.randrange(0,len(Cabezas))
    c = list(Cabezas)[n]
    ataca(c)
    print("Asalto {}: Cortamos la cabeza {} -> quedan {} cabezas"
          .format(Asalto, c, len(Cabezas)))
```

Si el lector juega con estos programas (o los que él se programe) podrá hacerse una idea sobre si Hércules necesitaría o no algo de asesoramiento sobre qué estrategia usar para derrotar a la Hidra. Se puede empezar con la que he puesto de ejemplo o con alguna otra más sencilla, para familiarizarse con el problema.

**Link al post original:** Hércules y la Hidra

# 15. Hércules siempre gana

Es interesante programar un combate entre Hércules y la Hidra, por ejemplo en el que en cada asalto se corte una cabeza elegida al azar. Acabo de organizar uno partiendo de la Hidra del mensaje anterior, y el número de cabezas ha ido evolucionando así:

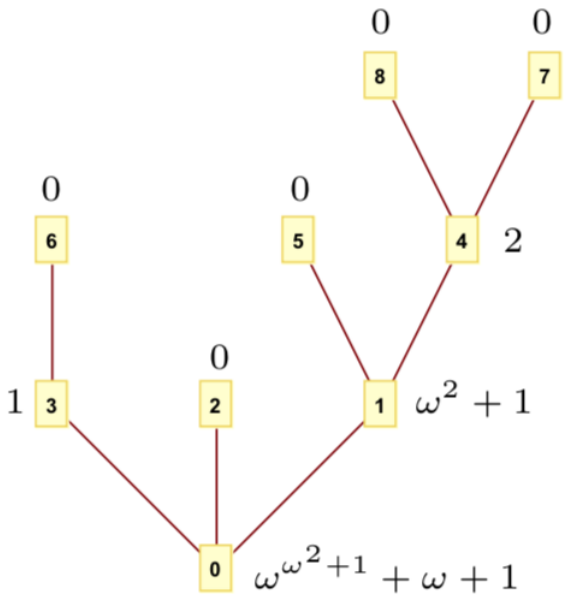
| Asalto | Cabezas | Asalto | Cabezas |
|---|---|---|---|
| 0 | 5 | 30 | 5 535 |
| 1 | 8 | 40 | 10 319 |
| 2 | 13 | 50 | 19 488 |
| 3 | 21 | 60 | 29 675 |
| 4 | 24 | 70 | 39 043 |
| 5 | 33 | 80 | 55 710 |
| 6 | 38 | 90 | 79 635 |
| 7 | 44 | 100 | 107 377 |
| 8 | 52 | 200 | 449 556 |
| 9 | 60 | 300 | 1 325 027 |
| 10 | 69 | 400 | 2 972 177 |
| 20 | 1 956 | 500 | 5 839 070 |

Todo apunta a que Hércules perderá el combate y que, si tiene alguna opción de ganar, tendrá que ser con alguna ingeniosa estrategia, porque lo de cortar cabezas al azar no funciona.

Sin embargo, no es así. Sucede que Hércules siempre gana a la Hidra sea cual sea el criterio que use para elegir la cabeza que corta en cada asalto.

La prueba es muy sencilla teniendo en cuenta lo que hemos visto en este hilo.

Se basa en que a cada Hidra le podemos asignar un ordinal con el criterio siguiente (la figura muestra el caso del ejemplo de la sección anterior):



Primero asignamos un ordinal a cada nodo de la Hidra:

- A cada cabeza le asignamos el ordinal 0
- Para calcular el ordinal de un nodo, consideramos los ordinales de sus "hijos", digamos que son $\delta_1, \ldots, \delta_n$, los ordenamos de mayor a menor, y le asignamos al nodo el ordinal $\omega^{\delta_1} + \cdots + \omega^{\delta_n}$
- El ordinal de la Hidra es el de su raíz.

Así, en el ejemplo, las cinco cabezas tienen ordinal 0, el nodo 4 tiene ordinal $\omega^0 + \omega^0 = 2$, el nodo 1 tiene ordinal $\omega^2 + \omega^0 = \omega^2 + 1$, el nodo 3 tiene ordinal $\omega^0 = 1$ y el nodo 0 tiene ordinal $\omega^{\omega^2+1} + \omega^1 + \omega^0 = \omega^{\omega^2+1} + \omega + 1$.

Recíprocamente, a partir del ordinal podemos reconstruir la Hidra. Si nos dan el ordinal $\omega^{\omega^2+1} + \omega + 1$, vemos que se trata de una Hidra de cuya raíz salen tres ramas, correspondientes a los tres sumandos. La correspondiente al sumando $1 = \omega^0$ termina en una cabeza, la correspondiente al sumando $\omega^1$ llega a un nodo de ordinal $1 = \omega^0$, luego de él sale una única cabeza, y la correspondiente al sumando $\omega^{\omega^2+1}$ llega a un nodo de ordinal $\omega^2 + 1$, luego de él salen dos ramas, la correspondiente a $1 = \omega^0$ llega a una cabeza y la correspondiente a $\omega^2$ llega a un nodo del que salen dos cabezas.

En particular, la única Hidra de ordinal 0 es la Hidra muerta.

Ahora sólo tenemos que observar que, cuando Hércules le corta una cabeza a la Hidra, tras la regeneración correspondiente, la Hidra resultante tiene ordinal menor que la anterior.

En efecto, supongamos que le cortamos a la Hidra una cabeza que no sale de la raíz, sino de un nodo que tiene por debajo otro nodo de ordinal $\alpha$. Este $\alpha$ será de la forma

$$\alpha = \omega^{\eta_0} \cdot k_0 + \cdots + \omega^{\eta_n} \cdot k_n,$$

con $\eta_0 \succ \eta_1 \succ \cdots \succ \eta_n$. Pongamos que la cabeza cortada está en una de las ramas de ordinal $\eta_i$. Entonces $\eta_i = \eta' + 1$, donde el 1 corresponde a la cabeza cortada. Por lo tanto, tras la decapitación, tenemos que cambiar uno de los sumandos $\omega^{\eta_i}$, con lo que nos queda $\omega^{\eta_i}(k_i - 1)$, y por otra parte tenemos que añadir $m + 1$ sumandos $\omega^{\eta'}$, donde $m$ es el número de asalto en curso. En total, hemos de cambiar:

$$\omega^{\eta_i} \cdot k_i \mapsto \omega^{\eta_i}(k_i - 1) + \omega^{\eta'} \cdot (m + 1).$$

En suma, quitamos un término $\omega^{\eta_i}$ y añadimos $m+1$ términos $\omega^{\eta'} \prec \omega^{\eta_i}$. Claramente, esto hace que $\alpha$ cambie a un ordinal $\alpha' \prec \alpha$, y es claro que entonces el ordinal de la raíz también pasa de un ordinal $\beta$ a otro $\beta' \prec \beta$, pues para compararlos nos encontraremos todos los términos iguales hasta llegar al correspondiente a la rama donde estaba la cabeza, para comparar estos términos comparamos los exponentes, y serán todos iguales excepto los correspondientes a la rama donde estaba la cabeza, y así vamos subiendo hasta llegar a los exponentes $\alpha' \prec \alpha$. Si la cabeza cortada sale de la raíz, el ordinal de la Hidra pasa de un cierto $\alpha + 1$ hasta $\alpha$, luego también disminuye estrictamente.

Por lo tanto, cada combate entre Hércules y la Hidra va generando una sucesión decreciente de ordinales, luego tiene que llegar a 0 en un número finito de pasos, y cuando eso suceda la Hidra habrá muerto. No importa el criterio que use Hércules para cortar las cabezas.

En el mensaje siguiente analizaré la evolución del combate para una estrategia concreta.

De momento, concluyo observando que las Hidras nos proporcionan una representación gráfica de los ordinales menores que $\epsilon_0$, pues cada ordinal se corresponde con una Hidra posible.

**Link al post original:** Hércules siempre gana

# 16. Una estrategia para Hércules

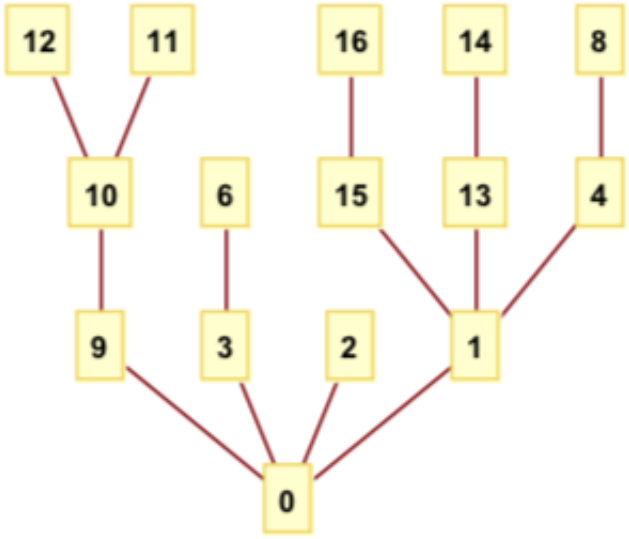
Hemos visto que Hércules siempre gana a la Hidra, sea cual sea el criterio que elija para cortar cabezas. No obstante, vamos a ver una estrategia posible que podemos probar que es ganadora sin necesidad de hablar de ordinales.

Para ello definimos la *altura* de un nodo de la Hidra como el número de nodos que tiene por debajo. Diremos que dos cabezas son *hermanas* si ambas salen del mismo nodo.

La estrategia que le proponemos a Hércules es la siguiente:

*En cada asalto, Hércules corta una cabeza de altura máxima que tenga el mayor número posible de hermanas.*

Por ejemplo, esta Hidra




tiene 5 cabezas de altura 3, pero la estrategia exige cortar la 11 o la 12, que forman una familia de dos hermanas, mientras que las otras tres no tienen hermanas.

En general, a cada hidra le podemos asociar tres números $(h, m, s)$, donde $h$ es la máxima altura de sus cabezas, $m$ es el máximo número de cabezas hermanas de altura $h$ y $s$ es el número de familias con $m$ cabezas hermanas de altura $h$.

En la hidra anterior es $(h, m, s) = (3, 2, 1)$.

Si a una hidra con valores $(h, m, s)$ le cortamos en el asalto $n$-simo una cabeza de altura $h$ según la estrategia, su familia de $m$ cabezas ha perdido una, y pasa a tener $m-1$ cabezas. Por otra parte, la hidra genera $n$ familias de $m-1$ cabezas hermanas. Esto no influye en que los números de la nueva hidra son $(h, m, s-1)$.

Tras un número finito de asaltos, llegaremos a una hidra de tipo $(h, m, 1)$, es decir, con una única familia de $m$ cabezas hermanas. Al cortar una de estas cabezas ya no habrá familias de cabezas de altura $h$ con $m$ hermanas, y la nueva hidra será de tipo $(h, m-1, s)$, para cierto valor de $s$, que volverá a disminuir una unidad en cada asalto y, al llegar a 0, se descuenta un valor a $m$. Por lo tanto, tras un número finito de asaltos, llegaremos a una hidra $(h, 1, 1)$, que tiene una única cabeza de altura $h$.

Al cortar esta última cabeza, pasamos a una hidra de tipo $(h-1, m, s)$, para ciertos valores de $m$ y $s$.

En resumen, la terna $(h, m, s)$ se comporta como un cronómetro en cuenta atrás. Cuando los segundos llegan a 0, se reduce un minuto y $s$ aumenta, no hasta 59, sino hasta un número arbitrario de segundos que continúan la cuenta atrás. Así, al cabo de $m$ minutos (cada uno con un número distinto de segundos), llegamos a $m = 0$, y entonces se reduce una hora, mientras que los minutos y los segundos aumentan a valores arbitrarios, pero lo cierto es que al cabo de $h$ horas de distinta duración, la hidra llega a tener una única cabeza de altura $h = 0$, lo que significa que está muerta.

En términos de ordinales, esta estrategia funciona así.

Consideremos la Hidra de 5 cabezas que habíamos puesto como ejemplo al plantear el juego de Hércules, la que tiene ordinal

$$\omega^{\omega^2+1} + \omega + 1.$$

El exponente 2 corresponde a un único grupo de 2 cabezas hermanas de altura 3.

Por lo tanto su "esperanza de vida" (si Hércules sigue la estrategia que estamos considerando) es $(h, m, s) = (3, 2, 1)$. Al cortarle una de las dos cabezas posibles pasamos a la Hidra de 5 cabezas

$$\omega^{\omega\cdot 2+1} + \omega + 1,$$

cuya esperanza de vida es $(3, 1, 2)$ (tiene dos cabezas sin hermanas de altura 3). En el asalto siguiente pasamos a la hidra de 7 cabezas

$$\omega^{\omega+4} + \omega + 1,$$

con $(h, m, s) = (3, 1, 1)$ y ahora, al cortar la última cabeza de altura 3, obtenemos la hidra de 10 cabezas

$$\omega^8 + \omega + 1,$$

con $(h, m, s) = (2, 8, 1)$.

A partir de aquí podemos razonar en general. Supongamos que, tras el $n$-simo asalto, la Hidra tiene ordinal

$$\omega^a \cdot b + \omega^{a-1} \cdot c + \cdots$$

En nuestro ejemplo, tras el asalto $n = 3$, tenemos $(a, b, c) = (8, 1, 0)$.

En general, la Hidra tiene $b$ familias de $a$ cabezas hermanas de altura 2 y $c$ familias de $a - 1$ cabezas hermanas de altura 2.

Tras el asalto $n+1$, una de las $b$ familias pierde un miembro, con lo que sólo quedan $b-1$ familias de $a$ cabezas hermanas, pero el número $c$ de familias de $a - 1$ cabezas hermanas

aumenta en 1 (por el grupo de $a$ cabezas que ha perdido un miembro) y en $n+1$ por la regeneración, luego el resultado es

$$\omega^a \cdot (b-1) + \omega^{a-1} \cdot (c+n+2) + \cdots$$

Tras $b$ asaltos, es decir, tras el asalto $n+b$, el ordinal será:

$$\omega^{a-1} \cdot (c + (n+2) + (n+3) + \cdots + (n+b+1))) + \cdots = \omega^{a-1} \cdot \left(c + \frac{(2n+b+3)b}{2}\right) + \cdots$$

En otras palabras, si partimos de

$$\omega^a \cdot b + \omega^{a-1} \cdot c + \cdots$$

tras el asalto $n$, entonces, tras el asalto $n+b$, el exponente $a$ se ha convertido en $a-1$ y $b$ se ha convertido en $c + (2n+b+3)b/2$.

Aplicando esta fórmula podemos construir la tabla siguiente para la hidra de nuestro ejemplo:

| $n$ | ordinal |
|---:|---|
| 3 | $\omega^8 + \omega + 1$ |
| 4 | $\omega^7 \cdot 5 + \omega + 1$ |
| 9 | $\omega^6 \cdot 40 + \omega + 1$ |
| 49 | $\omega^5 \cdot 1\,220 + \omega + 1$ |
| 1 269 | $\omega^4 \cdot 805\,810 + \omega + 1$ |
| 807 079 | $\omega^3 \cdot 325\,688\,659\,655 + \omega + 1$ |
| 325 689 466 734 | $\omega^2 \cdot 53\,036\,814\,370\,901\,491\,046\,740 + \omega + 1$ |

En este punto, el $\omega$ que estaba suelto (la cabeza de altura 1) hace que por primera vez sea $c = 1$, luego al aplicar la fórmula una vez más resulta que, tras el asalto

$$n = 53\,036\,814\,371\,227\,180\,513\,474$$

el ordinal es

$$\omega \cdot 1\,406\,451\,839\,324\,004\,993\,542\,381\,326\,234\,890\,768\,738\,031\,071 + 1$$

y una última aplicación de la fórmula (también con $c = 1$) nos da que, tras el asalto

$$n = 1\,406\,451\,839\,324\,004\,993\,542\,434\,363\,049\,261\,995\,918\,544\,545,$$

la Hidra tiene ordinal finito:

$$989\,053\,388\,168\,938\,379\,565\,429\,552\,367\,644\,648\,402\,300\,580$$
$$972\,977\,512\,412\,313\,364\,046\,356\,366\,229\,560\,313\,533\,900\,782,$$

lo que significa que tiene ese número de cabezas hermanas que salen de su raíz. Según las reglas del juego, cada vez que Hércules corta una de ellas, no se produce ninguna

regeneración, por lo que la Hidra muere al cabo de ese número de asaltos, es decir, que muere tras el asalto

$$989\,053\,388\,168\,938\,379\,565\,429\,552\,367\,644\,648\,402\,300\,582$$
$$379\,429\,351\,736\,318\,357\,588\,790\,729\,278\,822\,309\,452\,445\,327.$$

Si Hércules pudiera cortar 100 cabezas por segundo, tardaría aproximadamente $3{,}12 \cdot 10^{80}$ años en matar a la Hidra. La edad del Universo se estima en $1{,}37 \cdot 10^{10}$ años.

**Link al post original:** Una estrategia para Hércules

# 17. Comentarios

**(C1)** Si $\alpha = \langle \beta_1, \cdots, \beta_n \rangle$, entonces $\beta_1 \prec \alpha$, luego cada $\beta_i \prec \alpha$.

Veamoslo por inducción sobre $\alpha$.

Si $\alpha = 0$ es claro y, si $\alpha = 1 = \langle 0 \rangle$ es también cierto, con lo que supongamos que es cierto para cada ordinal $\beta < \alpha = \langle \beta_1, \cdots, \beta_n \rangle$, y veamos que también lo es para $\alpha$.

Por (5) sabemos que $\beta_1 < \alpha$, luego si es $\beta_1 = \langle \gamma_1, \cdots, \gamma_m \rangle$, por hipótesis de inducción tenemos que $\gamma_1 \prec \beta_1$. Así pues, se tiene que $\alpha$ y $\beta_1$ difieren en su primer elemento, siendo además $\gamma_1 \prec \beta_1$, con lo que efectivamente $\beta_1 \prec \alpha$.

**(C2)** ¿Cómo se pueden definir (formalmente) conjuntos obtenidos de manera recursiva, como es el caso de $E$, en AP? Es decir, ¿cómo se puede formalizar la fórmula $n \in E$?

Como norma general (para hacerte una idea de qué se puede probar en AP y qué no), conviene que tengas en cuenta que en AP se puede definir y demostrar exactamente lo mismo que en ZFC sin el axioma de infinitud más el axioma que afirma que todo conjunto es finito. Eso te permite hablar también de conjuntos infinitos (definibles explícitamente por fórmulas) en el mismo sentido en que en ZFC se habla de clases propias, es decir, que en AP "conjuntos" como $E$ son clases propias.

Hay varias formas de hacer estas cosas en AP, unas más elegantes y largas, y otras más directas. La idea de fondo es usar de un modo u otro lo que se conoce como función $\beta$ de Gödel, que permite codificar de forma un tanto rudimentaria cualquier sucesión finita de números naturales en términos de una expresión aritmética con dos parámetros.

Más concretamente, para cada sucesión finita $s_1, \ldots, s_n$ de números naturales existen números $c, d$ tales que $\beta(c, d, i) = s_i$ para $i = 1, \ldots, n$.

No es que puedas demostrar esto en AP, literalmente, porque para ello tendrías que tener ya formalizado el concepto de sucesión finita, sino que, cuando necesitas una sucesión finita, en lugar de decir "existen $s_1, \ldots, s_n$", puedes decir "existen $c, d$ tales que..." y luego, donde dirías $s_i$, dices $\beta(c, d, i)$, y puedes contar con que eso va a funcionar bien.

Una vez puedes asociar a cada dos números naturales una sucesión finita de números naturales, puedes depurar eso de varias formas. Si quieres ir directo al grano, puedes usar la función $\beta$ para dar definiciones recurrentes. Por ejemplo, si quieres definir la sucesión de Fibonacci, puedes hacerlo así:

$\mathrm{Fib}(n) = x$ si y sólo si existen $c, d$ tales que $\beta(c, d, 0) = 1$ y $\beta(c, d, 1) = 1$ y para todo $1 < i < i + 1 < n$ se cumple que $\beta(c, d, i + 2) = \beta(c, d, i) + \beta(c, d, i + 1)$ y $\beta(c, d, n) = x$.

Y ahí tienes una definición recurrente expresada en términos aritméticos.

Pero todo se puede hacer más fino si estás dispuesto a gastar tiempo. Por ejemplo, se puede usar $\beta$ para definir la codificación de sucesiones que hemos introducido en este hilo, de modo que acabamos teniendo definidas aritméticamente las funciones $\mathrm{long}(s)$ y $p(i, s) = s_i$ que determinan la longitud de un número natural visto como sucesión y sus componentes, para $i < \mathrm{long}(s)$, y a partir de ese momento trabajar con esta condificación más fina.

Pero, más aún, puedes definir, $m \in n$ como "el dígito $m$-simo de la expresión de $n$ en base 2 es igual a 1", y con eso tienes una relación de pertenencia que cumple los axiomas de ZFC menos el axioma de infinitud, y a partir de ahí puedes trabajar en AP como en ZFC sin infinitud (y con el axioma que afirma que todo conjunto es finito).

Una forma concreta de hacerlo la tienes en la sección 5.5 de mi libro de lógica, que diría así a ojo que no depende de nada anterior si pasas por alto algunos comentarios sobre la jerarquía de Kleene y donde leas $\mathrm{I}\Sigma_1$ piensas simplemente en AP.

**(C3)** Discusión sobre la validez del primer argumento de Gentzen.

EPAROH: A mi me ha convencido en el sentido siguiente:

> Si tu me das cualquier ordinal $\alpha$ (de los definidos en el post claro), tengo hecho un pequeño programa que calcula el menor natural $n$ para el cual se cumple $\alpha \prec \omega^{(n)}$. Una vez tienes esto con dicho $n$ ya fijo, se puede seguir el argumento que se da en la Sección 9 que, aunque implique usar un "y así sucesivamente" unas pocas veces, creo que está claro que cada afirmación que se hace es perfectamente válida. Así pruebas que $w^{(n)}$ es accesible y con ello lo era el $\alpha$ de partida.

CARLOS IVORRA: Yo creo que no hay duda de que en esa sección se demuestra que $\omega^{(3)}$ es accesible (o se puede extender la prueba hasta que no quede ningún paso en el aire), pero, ¿cuál sería el argumento que prueba que si $\omega^{(n)}$ es accesible también lo es $\omega^{(n+1)}$? Lo único que hemos visto es que "razonando, razonando", se puede pasar de $\omega^{(1)}$ a $\omega^{(2)}$ y de $\omega^{(2)}$ a $\omega^{(3)}$, y nada parece indicar que haya nada de especial en el 3 que no permita pasar al 4, etc., pero los razonamientos necesarios necesitan cada vez más pasos y más casos, y no tenemos una descripción general del argumento que es necesario para pasar de $n$ a $n + 1$, sino un mero "si te pones a razonar (a trepar por los ordinales), seguro que vas a poder llegar a $\omega^{(n+1)}$, ¿por qué no ibas a poder?"

> Y una cosa es que los razonamientos que hemos dado sean sin duda razonamientos convincentes, y otra distinta que el "¿por qué no iba a poder continuar de esta misma manera?" cuele como "razonamiento", si no está claro qué queremos decir exactamente por "de esta misma manera".

EPAROH: Toda la razón sí. Por eso digo que me convence como argumento, pero no me deja todo el buen sabor de boca que me gustaría, por no tener precisamente un argumento general (como si lo teníamos para pasar, por ejemplo, de $\omega^n$ a $\omega^{n+1}$) para pasar de la accesibilidad de $\omega^{(n)}$ a $\omega^{(n+1)}$.

ARGENTINATOR: Este argumento, así como se muestra ahí, no me parece válido. Lo cual es una cosa distinta a si ayuda a "convencer" de la accesibilidad de $\epsilon_0$.

Da la sensación de que hay una estructura en los ordinales que permite afirmar que son todos accesibles, pero que el "argumentador" no es capaz de poner de manifiesto cuál es esa estructura de una forma creíble.

La "lógica" que aparece allí me parece insuficiente.

**(C4)** Respuesta de Eparoh al Acertijo metamatemático.

Diría que la parte que no puede formalizarse en AP empieza aquí:

Aplicando repetidamente (7), tenemos:

Porque una demostración formal es una sucesión finita de fórmulas, pero con este "aplicamos repetidamente (7)", el número de fórmulas en la "demostración" dependerá del $n$ para el cual se cumpla que $\alpha \prec w^{(n)}$. Es decir, creo que para cualquier $n$ fijo es posible demostrar en AP la inducción hasta cualquier $\omega^{(n)}$ siguiendo el argumento que has dado, pero no es posible demostrarla hasta $\epsilon_0$ pues precisaríamos de una infinitud de demostraciones concatenadas y eso no es una demostración formal pues, por definición, deben tener una longitud finita. Vamos, que el problema creo que está siempre en el "repetimos una cantidad arbitraria de veces" que es válido intuitivamente (pues queda perfectamente especificado como deberíamos repetir el proceso independientemente del $n$, no como en lo discutido sobre la Sección 9), pero no es posible formalizarlo en una teoría axiomática débil como es AP que no permite con sus axiomas hablar de conjuntos infinitos.

**(C5)** ¿Es posible formalizar en ZFC el segundo argumento de Gentzen?

EPAROH: Leída la Sección 11 veo claro que si era lo que pensaba, pero ahora me surge una duda: ¿En ZFC es posible formalizar el argumento anterior?

No me refiero a si es posible probar la inducción hasta el ordinal $\epsilon_0$ (que eso se que en ZF es casi trivial por las propiedades de los ordinales), sino si el argumento dado en la Sección 10 podría formalizarse en ZFC. A simple vista, me parece que se tiene el mismo problema aunque trabajemos en una teoría axiomática más potente: conocer pruebas individuales de la inducción hasta $w^{(n)}$ para cada natural $n$ no te da inmediatamente una prueba de $\forall n\ P-\mathrm{IND}(\omega^{(n)})$ por el requerimiento de finitud de las demostraciones formales. Ahora bien, igual me equivoco y alguno de los axiomas de ZFC si permite dar dicho paso. ¿Cuál es el caso?

CARLOS IVORRA: Pues... según lo mires. En cierto sentido, tienes razón cuando dices que en ZF tendrías igualmente una sucesión de infinitas demostraciones que no hacen una demostración, pero eso tiene remedio sin que podamos decir que estamos cambiando de argumento.

La idea básica es que en ZFC se puede formalizar todo (bueno, todo no, eso es esencialmente cierto pero tiene algo de "letra pequeña" que comento un poco más abajo).

En ZF (y de hecho en AP) se puede demostrar que, para cada número natural $n$, existe una demostración de que $\omega^{(n)}$ es accesible.

Observa que, si identificamos con números naturales los signos de un lenguaje formal, una fórmula no es más que una sucesión de números naturales, que en AP puede verse como un único número natural, y a su vez una demostración es una sucesión de fórmulas, que también puede verse como un número natural. Igual que puede definirse en AP cuándo un número natural es un ordinal, se puede definir cuándo es una demostración de tal o cual fórmula. Así, podemos construir una fórmula aritmética $\phi(n)$ que signifique "$\omega^{(n)}$ es accesible", y también otra que diga que, "para cada $n$ existe una demostración de la fórmula $\phi(n)$".

Todo esto es lo que Gödel hizo codificando fórmulas y demostraciones con "números de Gödel", y probó que, en efecto, todo los conceptos lógicos "fórmula, demostración, etc." son definibles a partir de los axiomas de Peano.

Por supuesto, en ZF todo esto se puede hacer de forma mucho más fácil. En resumen, tanto en ZF como en AP podemos demostrar la fórmula que dice:

"Para cada número natural $n$ existe una demostración en AP de que el ordinal $\omega^{(n)}$ es accesible."

La diferencia es que en AP no podemos ir más lejos, mientras que en ZF podemos probar que si existe una demostración de la fórmula $\omega^{(n)}$ es accesible, dicha fórmula será verdadera en el modelo natural definido por los números naturales, y el hecho de que la fórmula "$\omega^{(n)}$ es accesible" sea verdadera en el modelo natural implica que $\omega^{(n)}$ es accesible. Por lo tanto, en ZF podemos demostrar que todos los $\omega^{(n)}$ son accesibles y, por consiguiente, que todo ordinal (menor que $\epsilon_0$) es accesible.

En cambio, en AP no podemos pasar de "se puede demostrar que $\omega^{(n)}$ es accesible" a "$\omega^{(n)}$ es accesible". Para ello habría que definir una función que a cada número natural que codifique una fórmula le asigne un valor 0 o 1 según que la fórmula correspondiente sea verdadera o falsa en los números naturales, para luego probar que los axiomas de Peano son verdaderos y todas sus consecuencias también, por lo que si una fórmula es demostrable, entonces es verdadera.

Esto se puede hacer sin problemas en ZF, pero en AP falla justo lo primero: no es posible definir en AP si un número natural que codifica una fórmula, codifica una fórmula verdadera o falsa (con su interpretación natural), pues eso es precisamente lo que afirma el teorema de Tarski sobre indefinibilidad de la verdad. En una teoría aritmética se puede definir el concepto de fórmula de dicha teoría aritmética, incluso el concepto de fórmula demostrable, pero no el concepto de fórmula verdadera, en el sentido de que si un número $n$ codifica una sentencia $\alpha$, se cumpla

$$n \text{ es verdadera} \leftrightarrow \alpha$$

En ZF se puede definir una fórmula que diga si un número que codifica una fórmula aritmética codifica una fórmula aritmética verdadera en el modelo $\mathbb{N}$ y eso nos permite terminar de formalizar el argumento de Gentzen. Lo que

prohíbe el teorema de Tarski para ZF es definir qué significa que una fórmula del lenguaje de ZF sea verdadera de modo que si $n$ codifica una sentencia $\alpha$ (del lenguaje de ZF, no del lenguaje de la aritmética) se cumpla

$$n \text{ es verdadera} \leftrightarrow \alpha$$

Vamos, que una teoría aritmética no puede definir qué significa que una fórmula de su propio lenguaje (no de otro más pequeño) sea verdadera.

Esto es un ejemplo de que en ZF no se puede formalizar "todo, todo". Uno podría esbozar una demostración de "fórmula verdadera" que "debería" funcionar en ZF, pero que no funciona porque involucra clases propias de una forma que ZF no es capaz de gestionar. Hay resultados que en ZF sólo se pueden probar para conjuntos, pero no para clases propias.

Pero las clases propias de ZF están a años luz de distancia de los conceptos intuitivamente bien definidos, por lo que estas limitaciones de ZF no impiden formalizar ningún argumento que sea intuitivamente convincente.

EPAROH: Creo que entiendo la idea, ¿pero podrías explicar esto un poco más en detalle?

> **Cita de Carlos Ivorra**
>
> La diferencia es que en AP no podemos ir más lejos, mientras que en ZF podemos probar que si existe una demostración de la fórmula $\omega^{(n)}$ es accesible, dicha fórmula será verdadera en el modelo natural definido por los números naturales, y el hecho de que la fórmula "$\omega^{(n)}$ es accesible" sea verdadera en el modelo natural implica que $\omega^{(n)}$ es accesible. Por lo tanto, en ZF podemos demostrar que todos los $\omega^{(n)}$ son accesibles y, por consiguiente, que todo ordinal (menor que $\epsilon_0$) es accesible.

No veo del todo claro como se está pasando de infinitas fórmulas a una demostración finita, pues parece que lo que se hace es traducir el problema de demostrar que $\omega^{(n)}$ es accesible a demostrar que la fórmula "$\omega^{(n)}$ es accesible" es cierta en el modelo natural. Pero, ¿si esto se ve para cada $n$ por separado no volvemos a estar en las mismas?

También, ¿por qué que la fórmula "$\omega^{(n)}$ es accesible" sea cierta en el modelo natural implica que es demostrable en ZF?

CARLOS IVORRA: En ZF (o en AP) tú puedes demostrar la fórmula:

$$\forall n \in \mathbb{N}\, \exists d(d \text{ es una demostración de "}\omega^{(n)} \text{ es accesible"}) \tag{16}$$

Esto no es una sucesión de demostraciones, esto es la demostración (única) de que existe una sucesión infinita $\{d_n\}_{n=1}^{\infty}$ tal que cada $d_n$ es una demostración de la fórmula "$\omega^{(n)}$ es accesible".

Para ello se construye $d_n$ estableciendo que en la prueba se usa $n-1$ veces la implicación (7) y otras tantas la implicación (15) del mensaje en el que doy la prueba de Gentzen (Sección 10). Todo ese argumento puede verse como una prueba en ZF de la afirmación anterior, literalmente igual que cualquier texto

en un libro de matemáticas usual puede verse como una demostración en ZF descrita superficialmente.

En particular, no se hace para cada $n$ por separado, sino que se prueba que, dado un $n$ arbitrario, puedes construir una demostración (una sucesión de números naturales, si quieres) usando $n-1$ veces tal ingrediente y tal otro, y te sale una demostración de la accesibilidad de $\omega^{(n)}$ para el $n$ arbitrario considerado. Pero es esencial que con esto no demuestras que $\omega^{(n)}$ es accesible, sino sólo que la fórmula que afirma esto es demostrable. En AP esto es una barrera insuperable, en ZF no.

Con eso tienes una única demostración [metamatemática] de que existe una sucesión de demostraciones en AP (formalizadas en ZF) de la fórmula en cuestión.

Si lo quieres hacer en AP (aunque no aprovecha de mucho, porque al final nos quedamos estancados), en lugar de construir una sucesión infinita (en AP no hay objetos infinitos), tienes que definir explícitamente la fórmula $\phi(n,d)$ que significa "$d$ es la demostración que se construye de tal y tal forma" y demostrar que para todo $n$ existe una única $d$ que cumple $\phi(n,d)$ y que es una demostración de $\omega^{(n)}$ es accesible.

En AP no podemos ir más alla, pero en ZF tienes un teorema general que dice:

Si $\alpha$ es una sentencia de la aritmética de Peano y tiene una demostración en AP, entonces $\mathbb{N} \vDash \alpha$.

Uniendo esto a (16) obtienes el teorema siguiente:

$$\forall n \in \mathbb{N}\ \mathbb{N} \vDash \text{“}\omega^{(n)} \text{ es accesible”}$$

donde ahí hay que entender que "$\omega^{(n)}$ es accesible" no es la fórmula metamatemática que afirma tal cosa, sino el número natural (o la sucesión de sucesiones de números naturales) que codifica dicha fórmula en ZF.

Por último, podemos usar que $\vDash$ se define de modo que se puede probar que, para toda sentencia aritmética (metamatemática) $\alpha$ formalizada en ZF como la sucesión de números naturales "$\alpha$", se cumple

$$(\mathbb{N} \vDash \text{“}\alpha\text{”}) \leftrightarrow \alpha$$

es decir, que la formalización de $\alpha$ satisface la formalización de "ser verdadera en $\mathbb{N}$" si y sólo si se cumple $\alpha$. En particular,

$$\mathbb{N} \vDash \text{“}\omega^{(n)} \text{ es accesible”} \leftrightarrow \omega^{(n)} \text{ es accesible}$$

y con esto llegamos a que

$$\forall n \in \mathbb{N}\ \omega^{(n)} \text{ es accesible,}$$

que es un único teorema que implica la accesibilidad de todos los ordinales.

> **Cita de Eparoh**
>
> También, ¿por qué que la fórmula "$\omega^{(n)}$ es accesible" sea cierta en el modelo natural implica que es demostrable en ZF?

No, yo no he dicho eso. De hecho, es falso. No sé si lo dices por la equivalencia:

$$(\mathbb{N} \vDash \text{“}\alpha\text{”}) \leftrightarrow \alpha$$

Pero ahí no dice lo que dices. Ahí dice que los dos miembros significan lo mismo. Así que, si hemos demostrado que "$\alpha$" es cierta en $\mathbb{N}$, podemos dar por demostrado $\alpha$.

De otro modo. Es lo mismo demostrar $\alpha$ que demostrar que "$\alpha$" es verdadera en $\mathbb{N}$, pero eso no significa que si "$\alpha$" es verdadera tenga que ser demostrable. Sólo que si ("$\alpha$" es verdadera) es demostrable, entonces $\alpha$ es demostrable.

EPAROH: Ahora está todo mucho más claro, aunque hay una pequeña cosa que no me termina de encajar del todo:

> **Cita de Carlos Ivorra**
>
> En AP no podemos ir más alla, pero en ZF tienes un teorema general que dice:
>
> Si $\alpha$ es una sentencia de la aritmética de Peano y tiene una demostración en AP, entonces $\mathbb{N} \vDash \alpha$

Aquí, ¿lo que he marcado en azul es correcto o debería poner ZF?

Si es correcto, no termino de entender el matiz porque si una sentencia $\alpha$ en la aritmética de Peano tiene una demostración en AP, entonces por el teorema de corrección ¿no se cumple directamente que $\mathbb{N} \vDash \alpha$? ¿Por qué es esto un teorema de ZF?

CARLOS IVORRA: Lo que has marcado en azul es correcto. En ZF puedes definir el concepto de "demostración en AP". Una fórmula es un teorema de AP si es la última fórmula de una sucesión de fórmulas tales que cada una de ellas sea un axioma de Peano, un axioma lógico o una consecuencia lógica de fórmulas precedentes.

> **Cita de Eparoh**
>
> Si es correcto, no termino de entender el matiz porque si una sentencia $\alpha$ en la aritmética de Peano tiene una demostración en AP, entonces por el teorema de corrección ¿no se cumple directamente que $\mathbb{N} \vDash \alpha$? ¿Por qué es esto un teorema de ZF?

Es que el teorema del que estoy hablando no es sino la formalización en ZF del teorema de corrección. Me preguntabas cómo formalizar en ZF el razonamiento de Gentzen, y lo que te digo es que en la formalización tienes que usar la formalización del teorema de corrección.

**(C6)** Discusión sobre la validez del argumento de Takeuti.

EPAROH: Respecto al argumento de Takeuti, me parece "matemáticamente" convincente en el sentido de que el argumento dado lo veo muy similar a una demostración matemática usual. Sin embargo, yo creo que (pura opinión) no lo llamaría finitista.

En el argumento de Gentzen, el problema lo teníamos con el "y así sucesivamente", pues aunque parece claro que el mismo proceso dado se puede extender para probar la accesibilidad de cualquier $\omega^{(n)}$, como ya comentó Carlos, no existe un argumento general que te permita pasar de $n$ a $n+1$ pues lo casos se multiplican y multiplican.

Este problema creo que lo soluciona Takeuti, porque su argumento te permite probar con exactamente $n+1$ pasos que $\omega^{(n)}$ es accesible. Por tanto, desde un punto de vista metamatemático, no cabe duda de que todo $\omega^{(n)}$ será accesible pues, tu puedes darme cualquiera de ellos, por muy grande que sea el $n$ y yo, en tan solo $n+1$ pasos te demuestro que es accesible. Ahora bien, a mi parecer lo hace a costa de introducir una definición inicial que sobrepasa los límites del finitismo. Si no me equivoco (corregidme si es así, pues realmente me gustaría saber si hay algún argumento que muestre que efectivamente la definición no es constructiva) la definición de ordinal accesible ya no es finitista, no es constructiva pues (creo que) no es posible programar un ordenador para que, dado un ordinal cualquiera, de como salida si es o no accesible. No digo que no esté perfectamente bien definida tal y como explica Carlos al comienzo de la Sección 9, sino que no parece que podamos construir de forma recursiva todos los ordinales accesibles (no al menos en base a la propia definición). Por tanto, si ya dicha definición no es constructiva, la de ordinal $n$-accesible será "$n$ ordenes de magnitud" menos constructiva, pues requiere de comprobar si toda una familia infinita de ordinales son $(n-1)$-accesibles, para lo cual se requiere a su vez comprobar si una familia infinita de ordinales es $(n-2)$-accesible, etc.

Ahora bien, aunque la definición no sea finitista, si creo que es metamatemáticamente aceptable pues, como la definición de accesibilidad está bien definida, la de $n$-accesibilidad, que es únicamente una recursión de ésta, también lo estará. Quiero decir que, dado un ordinal $\alpha$, o bien existe un ordinal accesible $\beta$ tal que $\beta \cdot \omega^{\alpha}$ no es accesible, y por tanto $\alpha$ no es 2-accesible, o bien esto no ocurre nunca y $\alpha$ si es 2-accesible. No sabemos cual será el caso, pero solo existen estas dos posibilidades. Por tanto, la 2-accesibilidad está bien definida y a partir de ella podemos ver que la 3-accesibilidad estará bien definida, etc.

Bueno, a ver si no he dicho ninguna tontería entre todo lo anterior.

Por cierto, el argumento de Takeuti es también perfectamente formalizable en AP y nos permite (de forma aparentemente más directa que la de la Sección 10) obtener un esquema que nos asegura que es posible construir una demostración en AP de "$\omega^{(n)}$ es accesible" para cada $n = 0, 1, 2, \cdots$ ¿Verdad?

CARLOS IVORRA: Estoy de acuerdo con lo siguiente:

> **Cita de Eparoh**
>
> Este problema creo que lo soluciona Takeuti, porque su argumento te permite probar con exactamente $n+1$ pasos que $\omega^{(n)}$ es accesible. Por tanto, desde un punto de vista metamatemático, no cabe duda de que todo $\omega^{(n)}$ será accesible pues, tu puedes darme cualquiera de ellos, por muy grande que sea el $n$ y yo, en tan solo $n+1$ pasos te demuestro que es accesible.

Ahora bien, tengo algunos matices sobre lo siguiente:

> **Cita de Eparoh**
>
> Ahora bien, a mi parecer lo hace a costa de introducir una definición inicial que sobrepasa los límites del finitismo. Si no me equivoco (corregidme si es así, pues realmente me gustaría saber si hay algún argumento que muestre que efectivamente la definición no es constructiva) la definición de ordinal accesible ya no es finitista, no es constructiva pues (creo que) no es posible programar un ordenador para que, dado un ordinal cualquiera, de como salida si es o no accesible.

Dicho así, tu planteamiento admite una respuesta "tramposa", pero con una trampa que no se puede descartar trivialmente. Uno podría decir que ese programa de ordenador sí que existe y es muy sencillo: tú le das un ordinal y el te responde que sí que es accesible. ¿Puedes cuestionar que el programa cumple lo requerido?

Eso está relacionado con una pequeña cuasiparadoja sobre las funciones recursivas. Se puede decir que una función es recursiva si la puede calcular un ordenador, pero, según eso, uno podría decir que la función dada por

$$f(n) = \begin{cases} 1 & \text{si} \quad \text{ZFC es consistente,} \\ \\ 0 & \text{si} \quad \text{ZFC no es consistente.} \end{cases}$$

no es recursiva, porque ningún ordenador nos puede decir si ZFC es consistente o no lo es. Sin embargo, esa función sí que es recursiva, porque es una función constante y todas las funciones constantes son recursivas. Un ordenador puede calcularla, ya sea dando como resultado siempre 0 o siempre 1.

> **Cita de Eparoh**
>
> No digo que no esté perfectamente bien definida tal y como explica Carlos al comienzo de la Sección 9, sino que no parece que podamos construir de forma recursiva todos los ordinales accesibles (no al menos en base a la propia definición).

Ahí estás matizando en la dirección correcta, pero si todos los ordinales son accesibles, sí que podemos construir de forma recursiva todos los ordinales

accesibles (es decir, todos los ordinales). La razón por lo que estas salidas por la tangente que estoy haciendo no son triviales es porque, cuando diseñas un algoritmo, tienes que justificar que cumple lo que se pretende, y no tienes limitaciones a priori sobre qué argumentos puedes dar para justificarlo con tal de que sean concluyentes. Por lo que si tú razonas —de cualquier forma que consideres concluyente— que todo ordinal es accesible, estás probando que el "algoritmo" que dice que sí cuando le das cualquier ordinal está cumpliendo lo requerido.

Pero lo cierto (tratando de eludir la salida por la tangente) es que si no sabemos si un ordinal (infinito) es accesible y queremos que un ordenador nos saque de la duda, no podemos, por lo menos tratando de aplicar la mera definición de accesibilidad. Y el punto está en que la accesibilidad de un ordinal equivale a que todos los ordinales menores que él cumplan una determinada propiedad. Más aún, la 2-accesibilidad de un ordinal equivale a que todos los ordinales (mayores o menores que él) cumplan una determinada propiedad. Esto es lo que tú mismo dices aquí:

**Cita de Eparoh**

Por tanto, si ya dicha definición no es constructiva, la de ordinal $n$-accesible será "$n$ ordenes de magnitud" menos constructiva, pues requiere de comprobar si toda una familia infinita de ordinales son $(n-1)$-accesibles, para lo cual se requiere a su vez comprobar si una familia infinita de ordinales es $(n-2)$-accesible, etc.

También coincido con esto:

**Cita de Eparoh**

Ahora bien, aunque la definición no sea finitista, si creo que es metamatemáticamente aceptable pues, como la definición de accesibilidad está bien definida, la de $n$-accesibilidad, que es únicamente una recursión de ésta, también lo estará. Quiero decir que, dado un ordinal $\alpha$, o bien existe un ordinal accesible $\beta$ tal que $\beta \cdot \omega^\alpha$ no es accesible, y por tanto $\alpha$ no es 2-accesible, o bien esto no ocurre nunca y $\alpha$ si es 2-accesible. No sabemos cual será el caso, pero solo existen estas dos posibilidades. Por tanto, la 2-accesibilidad está bien definida y a partir de ella podemos ver que la 3-accesibilidad estará bien definida, etc.

Pero aquí apuntaría algo que me parece relevante. Dices "no sabemos cuál es el caso", pero ¿realmente no lo sabemos? Una cosa es que la definición no nos lo diga, ni nos de una forma obvia de averiguarlo, pero, si estamos de acuerdo en que el concepto está bien definido y podemos razonar que todo ordinal cumple la definición, entonces sí que sabemos cuál es el caso.

**Cita de Eparoh**

Por cierto, el argumento de Takeuti es también perfectamente formalizable en AP y nos permite (de forma aparentemente más directa que la de la Sección 10) obtener un esquema que nos asegura que es posible construir una demostración en AP de "$\omega^{(n)}$ es accesible" para cada $n = 0, 1, 2, \cdots$ ¿Verdad?

Sí.

Lo más curioso que encuentro yo en la demostración de Takeuti es que, normalmente, una prueba general se puede particularizar a un ejemplo concreto que nos permita ver mejor la idea del argumento, pero en este caso no es así. Si tratamos de particularizarla a la prueba de que $\omega^{(5)}$ es accesible, no obtenemos nada en particular. La prueba requiere en primer lugar que 1 es 6-accesible, lo cual es una mera reformulación del hecho de que $\alpha$ $n$-accesible implica $\alpha \cdot \omega$ $n$-accesible, y a partir de ahí se razona que $\omega$ es 5-accesible antes de que sepamos nada sobre qué ordinales son 4-accesiles.

Aunque la 5-accesibilidad se define en términos de la 4-accesibilidad, podemos probar que $\omega$ es 5-accesible sin saber nada sobre qué ordinales son 4-accesibles, y a su vez es la 5-accesibilidad de $\omega$ la que nos da la 4-accesibilidad de $\omega^\omega$ antes de saber nada sobre qué ordinales son 3-accesibles, etc.

Así, tenemos que trabajar con unas definiciones que no podemos comprobar en principio, pero podemos decir que "cada ordinal la cumplirá o no", para luego razonar que todos los ordinales tienen que cumplirlas, pero empezando por la propiedad más complicada y descendiendo hacia las más simples.

Yo diría que la prueba de Takeuti está cerca del límite de lo que supone "hablar sin saber de qué está uno hablando". Es lo que sucede si uno se pone a hablar de ordinales en el sentido general de Cantor dando por hecho que los ordinales son "algo concreto" de lo que se puede hablar sin necesidad de fijar una teoría axiomática. Entonces uno se encuentra con que el conjunto de todos los ordinales es mayor que todos los demás, pero que a la vez debe tener un siguiente y así cae uno en la cuenta de que no sabemos de qué hablamos cuando decimos "todos los ordinales", y por eso es necesario limitar las afirmaciones sobre conjuntos abstractas a las expresables en una teoría axiomática con visos de consistencia.

Si uno lo piensa fríamente, se convence (creo yo) de que el concepto de ordinal $n$-accesible está bien definido en el sentido que tú mismo decías: que está claro que cada ordinal tiene que ser $n$-accesible o no serlo, en un sentido objetivo independiente de que no sepamos a priori si un ordinal lo es o no.

Sin embargo, esa forma de razonar que permite extraer consecuencias de la 5-accesibilidad antes de saber nada de la 4-accesibilidad, etc. "suena" a que el razonamiento sólo son palabras de las que vete a saber si puedes fiarte, pero en realidad no es eso, sino más bien que el razonamiento parte de conceptos que tenemos que usar a sabiendas de que son afirmaciones con sentido no verificables directamente y, admitiendo (temporalmente) que realmente son afirmaciones con un significado objetivo, podemos razonar de arriba hacia abajo

justificando que ese sentido exige que todos los ordinales sean $n$-accesibles para todo $n$, y a partir de ahí el concepto de $n$-accesibilidad se vuelve trivialmente "concreto" (hasta, en un sentido tramposo, se podría decir que "finitista") por aquello de que es fácil programar a un ordenador para que determine si un ordinal dado es accesible o no: sólo tiene que decir que sí, sin más.

**(C7)** Demostración de argentinator la buena ordenación de $\epsilon_0$.

Para concluir, se expone a continuación una demostración no finitista (dada por argentinator y redactada por Carlos Ivorra) de la buena ordenación de $\epsilon_0$. Aunque no sea finitista, creo que hasta resultaría convincente a un finitista no muy radical pues, aunque no es constructiva, la reducción al absurdo si es en cierto modo constructiva y aunque haya que hacer infinitas comparaciones, son siempre fácilmente numerables y muy fáciles de tener "bajo control".

**Demostración:**

Suponemos que no existen sucesiones estrictamente decrecientes de ordinales $\prec \omega^{(n)}$ y vamos a ver que tampoco las hay de ordinales $\prec \omega^{(n+1)}$.

Para ello suponemos que existe una que denotamos por $\{\alpha_j\}_j$, donde $\alpha_j = \left\langle \alpha_{j,1}, \dots, \alpha_{j,m_j} \right\rangle$ (notemos que $m_j \geq 1$ o, de lo contrario, $\alpha_j = 0$).

Llamo a $\alpha_{1,1}$ el "primer exponente" de la sucesión. Necesariamente $\alpha_{1,1} \prec \omega^{(n)}$, pues si fuera $\omega^{(n)} \preceq \alpha_{1,1}$, entonces $\omega^{(n+1)} = \left\langle \omega^{(n)} \right\rangle \preceq \langle \alpha_{1,1} \rangle \preceq \alpha_1$.

De hecho, $\alpha_{j,k} \preceq \alpha_{j,1} \preceq \alpha_{1,1} \prec \omega^{(n)}$.

Afirmo que si existe una sucesión decreciente de ordinales $\prec \omega^{(n+1)}$ con primer exponente $\beta_0 \prec \omega^{(n)}$, existe otra con primer exponente $\beta_1 \prec \beta_0$. Esto nos da ya una contradicción, pues así podemos construir una sucesión $\omega^{(n)} \succ \beta_0 \succ \beta_1 \succ \beta_2 \succ \cdots$, en contra de lo supuesto.

Para ello partimos de nuestra sucesión $\{\alpha_j\}_j$ con $\beta_0 = \alpha_{1,1}$.

Si existe un $j$ tal que $\beta_1 = \alpha_{j,1} \prec \alpha_{1,1} = \beta_0$, entonces la sucesión $\alpha_j \succ \alpha_{j+1} \succ \alpha_{j+2} \succ \cdots$ es una sucesión decreciente de ordinales con primer exponente $\beta_1$.

En caso contrario tenemos que todos los $\alpha_{j,1}$ son iguales a $\beta_0$. Esto obliga a que existan todos los $\alpha_{j,2}$, o si no, sería $\alpha_j \preceq \alpha_{j+1}$.

Podría darse el caso de que todos los $\alpha_{j,2}$ fueran iguales. En tal caso tendrían que existir todos los $\alpha_{j,3}$, que podrían ser todos iguales, en cuyo caso tendrían que existir todos los $\alpha_{j,4}$, etc.

Por lo tanto, tiene que existir un mínimo $k \leq m_1$ tal que, para cada $1 \leq l < k$, se cumple que todos los $\alpha_{j,l}$ son iguales a un mismo $\gamma_l$, luego existen todos los $\alpha_{j,k}$, pero $k$ es el mínimo índice para el que no son todos iguales. En particular tiene que haber un mínimo $j_0$ tal que $\beta_1 = \alpha_{j_0,k} \prec \alpha_{1,k}$.

Esto significa que nuestra sucesión es de la forma

$$\begin{aligned}
\alpha_1 &= \langle \gamma_1, \ldots, \gamma_{k-1}, \alpha_{1,k}, \ldots, \alpha_{1,m_1} \rangle \\
\alpha_2 &= \langle \gamma_1, \ldots, \gamma_{k-1}, \alpha_{1,k}, \ldots, \alpha_{2,m_2} \rangle \\
&\vdots \\
\alpha_{j_0} &= \left\langle \gamma_1, \ldots, \gamma_{k-1}, \beta_1, \ldots, \alpha_{j_0,m_{j_0}} \right\rangle \\
\alpha_{j_0+1} &= \left\langle \gamma_1, \ldots, \gamma_{k-1}, \alpha_{j_0+1,k}, \ldots, \alpha_{j_0+1,m_{j_0+1}} \right\rangle \\
&\vdots
\end{aligned}$$

Pero entonces, la sucesión

$$\begin{aligned}
\alpha^*_{j_0} &= \left\langle \beta_1, \ldots, \alpha_{j_0,m_{j_0}} \right\rangle \\
\alpha^*_{j_0+1} &= \left\langle \alpha_{j_0+1,k}, \ldots, \alpha_{j_0+1,m_{j_0+1}} \right\rangle \\
&\vdots
\end{aligned}$$

que resulta de eliminar los términos comunes, es una sucesión decreciente de ordinales con primer exponente $\beta_1$, lo que termina la prueba.

**(C8)** No es posible demostrar en AP que Hércules siempre gana.

En el hilo hemos analizado la estrategia consistente en cortar en cada asalto la cabeza más alta y, de entre las de altura máxima, la que tenga mayor número de hermanas, y hemos visto que en AP podemos probar que Hércules siempre gana si usa esa estrategia.

La situación es distinta si consideramos la estrategia opuesta: cortar en cada asalto la cabeza de menor altura y, de entre las que altura mínima, la que tenga un menor número de hermanas.

Esta estrategia es definible en AP, pero se puede demostrar que no es posible demostrar en AP que es una estrategia ganadora, pero la única prueba que conozco usa cálculo secuencial (el el teorema 8.27 de mi libro de Cálculo secuencial).

Un poco más de detalle.

Podemos considerar la función $N(\alpha)$ que determina el número de asaltos necesarios para vencer a la Hidra de ordinal $\alpha$ siguiendo la estrategia indicada, y es trivialmente una función recursiva, pues un ordenador puede calcularla: sólo tiene que ir calculando el combate siguiendo la estrategia y dar como salida el número de asaltos que ha necesitado para acabar.

Que sea recursiva se traduce en que existe una fórmula aritmética $\psi(\alpha, n)$ (con una estructura especialmente simple, a saber, que consta de un único cuantificador existencial seguido de una fórmula con cuantificadores acotados) que la representa en AP, es decir, que si se cumple $N(\alpha) = n$, en AP se puede demostrar $\phi(\bar\alpha, \bar n)$ y si $N(\alpha) \neq n$, en AP se puede demostrar $\neg\phi(\bar\alpha, \bar n)$, donde $\bar\alpha$ y $\bar n$ son los numerales correspondientes a los números naturales $\alpha$ y $n$ (por ejemplo, si $\alpha = 3$ entonces $\bar\alpha = SSS0$).

Eso significa que toda función recursiva se puede calcular en AP. Sin embargo, eso no significa que sea *demostrablemente recursiva*. Eso quiere decir que en AP se pueda demostrar $\forall\alpha\exists!n\,\psi(\alpha, n)$, lo que supone demostrar que $\psi$ define una función sobre todos

los números naturales. (En realidad la clave es la existencia, pues la unicidad se puede garantizar siempre modificando la fórmula $\psi$.)

Pues bien, si en AP se pudiera probar que la estrategia que he descrito es ganadora, la función $N(\alpha)$ sería demostrablemente recursiva en AP, pues eso es lo que significa que la estrategia es ganadora, que, para todo $\alpha$ existe un número de asaltos $n$ tras el que la Hidra muere. Pero sucede que eso es falso, la función $N(\alpha)$ no es demostrablemente recursiva en AP, pero la prueba no es trivial.