Apuntes de
Teoría de Conjuntos

por Enrique Arrondo(*)

Versión del 20 de Marzo de 2012

Estas notas están basadas en el libro "Introduction to Set Theory", de Karel Hrbacek y Thomas Jech, donde el lector puede profundizar en los detalles (se recomienda vivamente la tercera edición, que mejora y completa sustancialmente la segunda). Agradezco a los distintos alumnos de los distintos cursos todas las sugerencias y erratas que me han indicado para mejorar la presentación de estas notas. Quiero agradecer muy especialmente a Lucía Martín Reyes y Ricardo Laorga Suárez por pasarme listas sistemáticas de erratas y sugerencias.

(*) Departamento de Álgebra, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, 28040 Madrid, arrondo@mat.ucm.es

1. Primeros axiomas y propiedades

En la Matemática actual, cualquier teoría se basa fuertemente en el uso de los conjuntos. Sin embargo, no está claro cómo definir un conjunto. Un conjunto debería ser una colección de objetos (llamados *elementos*) caracterizados por una propiedad común. En concreto, fijemos primero la siguiente:

Notación. Dada una colección de elementos X, si x es un elemento de X escribiremos $x \in X$, mientrar que si no lo es escribiremos $x \notin X$. Si P es una propiedad, indicaremos por $P(x)$ el hecho de que P sea cierta para el elemento x.

Con esta notación, un conjunto debería ser una colección de elementos X tales que exista un propiedad P de modo que $x \in X$ si y sólo si $P(x)$. Sin embargo ¿puede darse cualquier propiedad para caracterizar un conjunto? El siguiente ejemplo muestra que no se puede hacer de cualquier modo:

Ejemplo 1.1 (Paradoja de Russell[(*)])**.** Sea X el conjunto de todos los conjuntos que no se contienen a sí mismos como elementos. Al ser X un conjunto, podemos preguntarnos si se contiene a sí mismo como elemento. Si X se contiene como elemento, entonces por la definición de X se puede decir que X no es un elemento de X, lo que es una contradicción. Si, por el contrario, X no se contiene como elemento, entonces la definición de X nos dice que X está en X, lo que de nuevo es una contradicción.

La paradoja de Russell indica que no cualquier propiedad sirve para definir un conjunto, o más bien que no podemos llamar conjunto a cualquier cosa. Lo que vamos a hacer es ir dando a lo largo del curso una serie de axiomas (los llamados *Axiomas de Zermelo-Frenkel*) que debe satisfacer lo que queramos llamar conjunto (de hecho, este curso debería ser paralelo a uno de Lógica que demostrara que el sistema de axiomas que vamos a imponer es coherente). Iremos introduciendo los axiomas a medida que los necesitemos. De hecho, no es que al final de curso podamos dar una definición precisa de conjunto (incluso mencionaremos ciertas hipótesis que tanto su afirmación como su negación son compatibles con nuestros axiomas), pero al menos habremos reconstruido a través de nuestros axiomas los conjuntos básicos en Matemáticas (empezando por los naturales, racionales, reales,...).

Empezamos por un par de axiomas, el primero afirmando la existencia de conjuntos vacíos.

Axioma de Existencia. *Existe un conjunto sin elementos.*

El segundo axioma equivale a la típica demostración de la igualdad de dos conjuntos mediante el "doble contenido":

(*) La paradoja original era sobre el barbero de un pueblo que afeitaba a todos los del pueblo que no se afeitaban a sí mismos: ¿Se afeita entonces el barbero a sí mismo?

Axioma de Extensionalidad. *Si cada elemento de X es un elemento de Y y cada elemento de Y es un elemento de X, entonces $X = Y$.*

Este axioma nos permite demostrar la unicidad de muchos conjuntos definidos de alguna forma concreta. Haremos un ejemplo, dejando el resto de casos de unicidad como ejercicio, explícito o implícito:

Corolario 1.2. *Existe un único conjunto sin elementos.*

Demostración: Supongamos que X, Y sean dos conjuntos sin elementos. Entonces, es automático que cualquier elemento de X es un elemento de Y (ya que de hecho no hay elementos en X para los que hacer la comprobación). Análogamente cada elemento de Y es un elemento de X, por lo que el Axioma de Extensionalidad implica $X = Y$. □

Definición. Llamaremos *conjunto vacío* al único conjunto sin elementos, y lo denotaremos por $\emptyset$.

El siguiente axioma es el que permite definir un conjunto a partir de una propiedad, pero partiendo ya de un conjunto dado (en particular, no puede existir el conjunto de todos los conjuntos, porque entonces existiría el conjunto X de la paradoja de Russell).

Axioma de Separación. *Dada una propiedad P y un conjunto X, existe un conjunto Z tal que $x \in Z$ si y sólo si $x \in X$ y $P(x)$.*

El conjunto anterior Z es único (demuéstrese) y lo denotaremos como

$$Z = \{x \in X \mid P(x)\}.$$

Ejemplo 1.3. Si P es la propiedad $x = x$, entonces $Z = X$, mientras que si P es la propiedad $x \neq x$ entonces $Z = \emptyset$. En particular, el Axioma de Existencia se puede sustituir por otro más débil: que exista algún conjunto.

Corolario 1.4. *Dados dos conjuntos, X, Y, existe un (único) conjunto Z tal que $x \in Z$ si y sólo si $x \in X$ y $x \in Y$.*

Demostración: Definimos la propiedad P que sea pertenecer a Y. Entonces, por el Axioma de Separación, $Z = \{x \in X \mid P(x)\}$ es un conjunto, que es el conjunto buscado. La unicidad de Z se deja como ejercicio a partir del Axioma de Extensionalidad. □

Definición. El conjunto Z cuya existencia acabamos de demostrar se llama *intersección* de X e Y, y se denota $Z = X \cap Y$.

Ejercicio 1.5. Demostrar que, dados dos conjuntos X, Y, existe un (único) conjunto Z tal que $x \in Z$ si y sólo si $x \in X$ y $x \notin Y$. Dicho conjunto Z se llama *diferencia de los conjuntos X e Y*.

En realidad, los axiomas que tenemos hasta ahora sólo garantizan la existencia del conjunto vacío, y la existencia de conjuntos más pequeños a partir de conjuntos ya conocidos. Los siguientes axiomas nos van a permitir ya construir conjuntos más grandes. El primero de ellos nos permitirá construir conjuntos de dos elementos.

Axioma del Par. *Dados X, Y, existe un conjunto Z tal que $x \in Z$ si y sólo si $x = X$ o $x = Y$ (escribiremos $Z = \{X, Y\}$, o bien $Z = \{X\}$ si $X = Y$).*

Ejemplo 1.6. Tomando $X = Y = \emptyset$, llegamos a la conclusión de que $\{\emptyset\}$ es un conjunto no vacío, ya que contiene un elemento. Tomando ahora $X = \emptyset$, $Y = \{\emptyset\}$, llegaremos ahora a que $\{\emptyset, \{\emptyset\}\}$ es un conjunto de dos elementos.

Ya el siguiente axioma nos permite construir uniones arbitrarias de conjuntos (siempre que los conjuntos que queramos unir formen un conjunto: recordemos que no existe el conjunto de todos los conjuntos):

Axioma de la Unión. *Para todo conjunto S, existe un conjunto, que denotaremos $U = \bigcup S$, tal que $x \in \bigcup S$ si y sólo si $x \in X$ para algún $X \in S$.*

Ejemplo 1.7. Si $S = \{X, Y\}$, entonces obtenemos la unión de X e Y, que denotamos $X \cup Y$. Además, tomando $S = \{X \cup Y, Z\}$, podemos definir $X \cup Y \cup Z$ y, en general, la unión de un número finito de conjuntos (la forma rigurosa de hacer este tipo de cosas por recurrencia la veremos en la sección 2).

Definición. Dados dos conjuntos X, Y, se llama *diferencia simétrica* de X e Y al conjunto $X \Delta Y := (X - Y) \cup (Y - X)$.

Ejercicio 1.8. Demostrar que la unión, intersección, diferencia y diferencia simétrica satisfacen las siguientes propiedades:

(i) Conmutatividad:

$$X \cap Y = Y \cap X.$$
$$X \cup Y = Y \cup X.$$
$$X \Delta Y = Y \Delta X.$$

(ii) Asociatividad:

$$(X \cap Y) \cap Z = X \cap (Y \cap Z).$$
$$(X \cup Y) \cup Z = X \cup (Y \cup Z).$$

$$(X \Delta Y) \Delta Z = X \Delta (Y \Delta Z).$$

(iii) Distributividad:

$$(X \cap Y) \cup Z = (X \cap Z) \cup (Y \cap Z).$$
$$(X \cup Y) \cap Z = (X \cup Z) \cap (Y \cup Z).$$

(iv) Leyes de De Morgan:

$$X - (Y \cap Z) = (X - Y) \cup (X - Z).$$
$$X - (Y \cup Z) = (X - Y) \cap (X - Z).$$

Definición. Se llama *subconjunto* de un conjunto X a un conjunto Y tal que todo elemento de Y es un elemento de X. Escribiremos $X \subseteq Y$ (o $Y \supseteq X$), dejando la notación $X \subset Y$ (o $Y \supset X$) sólo cuando $Y \neq X$.

Axioma del Conjunto Potencia. *Dado cualquier conjunto X, existe un conjunto, que denotaremos $\mathcal{P}(X)$ tal que $x \in \mathcal{P}(X)$ si y sólo si x es un subconjunto de X.*

Ejercicio 1.9. Demostrar que $\mathcal{P}(X)$ es único.

Ejemplo 1.10. Dado un subconjunto S de $\mathcal{P}(X)$ (es decir, una colección de subconjuntos de X que formen un conjunto), se puede entonces definir $\bigcup S$ (que será la unión de dicha colección de subconjuntos).

Ejercicio 1.11. Comprobar las siguientes propiedades de la inclusión:

(i) $X \subseteq X$.

(ii) Si $X \subseteq Y$ e $Y \subseteq X$, entonces $X = Y$.

(iii) Si $X \subseteq Y$ e $Y \subseteq Z$, entonces $X \subseteq Z$.

El siguiente paso ahora será el de definir producto cartesiano, para lo cual necesitamos definir lo que es un par:

Definición. Llamaremos *par ordenado* a un elemento de la forma $(x, y) := \{\{x\}, \{x, y\}\}$.

La justificación de la definición viene del siguiente resultado:

Teorema 1.12. *$(x, y) = (x', y')$ si y sólo si $x = x'$ e $y = y'$.*

Demostración: Es evidente que $x = x'$ e $y = y'$ implican $(x, y) = (x', y')$, así que sólo hay que demostrar la otra implicación. Supongamos pues $(x, y) = (x', y')$ y distingamos dos casos:

–Si $x \neq y$, entonces $\{x\}$ y $\{x, y\}$ tienen respectivamente uno y dos elementos, luego son conjuntos distintos. Por tanto $\{\{x'\}, \{x', y'\}\}$ tiene que consistir también necesariamente

en dos conjuntos distintos, uno con un elemento y otro con dos. El único conjunto que puede tener dos elementos es $\{x', y'\}$, por lo que $\{x\} = \{x'\}$ y $\{x, y\} = \{x', y'\}$. La primera igualdad implica inmediatamente $x = x'$, lo que hace que de la segunda se deduzca también $y = y'$.

–Si $x = y$, entonces $\{x, y\} = \{x\}$, lo que implica $(x, y) = \{\{x\}\}$. Por tanto, $\{\{x'\}, \{x', y'\}\}$ también debe tener un único elemento, es decir, $\{x'\} = \{x', y'\}$, luego $x' = y'$ y $(x', y') = \{\{x'\}\}$. Como $\{\{x\}\} = \{\{x'\}\}$, se deduce entonces $\{x\} = \{x'\}$, y de aquí $x = x'$ (y por tanto también $y = y'$). □

Definición. Un conjunto R es una *relación binaria* si todos sus elementos son pares ordenados. Si $(x, y) \in R$, escribiremos xRy.

Observación 1.13. La ventaja de haber definido un par ordenado de una forma tan "extraña" es que los "elementos" de una relación binaria R forman un conjunto. En efecto, el conjunto $\bigcup R$ consistirá en los elementos de la forma $\{x, y\}$ donde (x, y) es un par de R, con lo que el conjunto $\bigcup(\bigcup R)$ consistirá en los elementos de la forma x o y.

Definición. Se llama *campo de una relación binaria* R al conjunto $\text{Campo}(R) := \bigcup(\bigcup R)$. Si $\text{Campo}(R)$ está contenido en un conjunto X diremos que R es una *relación en el conjunto* X. Se llama *dominio de una relación binaria* R al conjunto definido por

$$\text{dom}(R) := \{x \in \text{Campo}(R) \mid \text{ existe } y \text{ tal que } xRy\}.$$

Análogamente, se llama *recorrido de una relación binaria* R al conjunto definido por

$$\text{rec}(R) := \{y \in \text{Campo}(R) \mid \text{ existe } x \text{ tal que } xRy\}.$$

Claramente, $\text{Campo}(R) = \text{dom}(R) \cup \text{rec}(R)$.

Recíprocamente a la Observación 1.13, podemos partir ahora de dos conjuntos X, Y, y entonces $\mathcal{P}(\mathcal{P}(X \cup Y))$ consiste en los subconjuntos de $\mathcal{P}(X \cup Y)$, es decir, sus elementos son a su vez subconjuntos de $X \cup Y$, luego en particular estarán los pares (x, y) donde $x, y \in X \cup Y$. Podemos por tanto definir:

Definición. Se llama *producto cartesiano* de dos conjuntos X, Y al conjunto

$$X \times Y := \{z \in \mathcal{P}(\mathcal{P}(X \cup Y)) \mid z = (x, y) \text{ con } x \in X,\ y \in Y\}.$$

Como cualquier relación binaria está contenida en $\text{dom}(R) \times \text{rec}(R)$, a partir de ahora consideraremos las relaciones como subconjuntos de un un producto cartesiano.

Definición. Se llama *imagen de un conjunto X por una relación R* al conjunto

$$R[X] = \{y \in \text{rec}(R) \mid \text{existe } x \in X \text{ tal que } xRy\}$$

y se llama *imagen inversa de un conjunto Y por una relación R* al conjunto

$$R^{-1}[Y] = \{x \in \text{dom}(R) \mid \text{existe } y \in Y \text{ tal que } xRy\}.$$

Definición. Se llama *inversa de una relación $R \subseteq X \times Y$* al conjunto

$$R^{-1} := \{(y, x) \in Y \times X \mid xRy\}.$$

Obsérvese que entonces $yR^{-1}x$ si y sólo si xRy.

Nótese que en principio hemos creado una ambigüedad de notación. En efecto, dada una relación binaria R y un conjunto Y, la expresión $R^{-1}[Y]$ puede querer decir ahora la imagen inversa de Y por R o la imagen de Y por R^{-1}. El siguiente resultado nos indica que ambos conjuntos coinciden.

Lema 1.14. *Sean R una relación binaria e Y un conjunto. Entonces la imagen inversa de Y por R es igual a la imagen de Y por R^{-1}.*

Demostración: Un elemento x está en la imagen inversa de Y por R si y sólo si existe $y \in Y$ tal que xRy (nótese que la condición $x \in \text{dom}(X)$ es automática, y está puesta en la definición sólo para demostrar que la imagen inversa es un conjunto, usando el Axioma de Separación). Por tanto, la condición es equivalente a decir que existe $y \in Y$ tal que $yR^{-1}x$, es decir, que x está en la imagen de Y por R^{-1} (de nuevo la condición $x \in \text{rec}(R^{-1})$ de la definición de imagen es automática). □

Definición. Se llama *composición de relaciones binarias R, S* a la relación

$$S \circ R := \{(x, z) \in \text{dom}(R) \times \text{rec}(S) \mid \text{ existe } y \text{ tal que } xRy \text{ e } ySz\}.$$

Vamos a terminar esta sección estudiando los tres tipos de relaciones binarias más importantes: las funciones, las relaciones de equivalencia y las relaciones de orden.

Definición. Una relación binaria F se llama *función* si xFy_1 y xFy_2 implica $y_1 = y_2$. Este único valor y tal que xFy se llama *valor de la función* en x y se escribirá $y = F(x)$. Si $X = \text{dom}(F)$ y $\text{rec}(F) \subseteq Y$, se suele escribir $F : X \to Y$.

Observación 1.15. Teniendo en cuenta que las funciones son relaciones binarias, es decir, conjuntos de pares ordenados, que dos funciones F y G coincidan tiene un significado preciso como conjuntos. Evidentemente, una condición necesaria es que deben tener

el mismo dominio y el mismo valor para cada elemento del dominio. Recíprocamente, supongamos que $\mathrm{dom}(F) = \mathrm{dom}(G)$ y $F(x) = G(x)$ para cada $x \in \mathrm{dom}(F)$. Entonces, para cada $(x, y) \in F$ se tiene que $x \in \mathrm{dom}(F)$ y $F(x) = y$. Por nuestra hipótesis, entonces $x \in \mathrm{dom}(G)$ y además $G(x) = y$. Por tanto, $(x, y) \in G$. Esto implica $F \subseteq G$. De modo simétrico se demuestra $G \subseteq F$, lo que implica (usando el Axioma de Extensionalidad) $F = G$. Nótese que entonces no tiene mucho sentido hablar de función suprayectiva, ya que no existe de forma única el "conjunto de llegada" Y. Sí tiene sentido sin embargo:

Definición. Una función se dice *inyectiva* si $F(x) = F(y)$ implica $x = y$. Una *biyección entre dos conjuntos* X, Y es una función inyectiva $F : X \to Y$ tal que $\mathrm{rec}(F) = Y$.

Ejemplo 1.16. Nótese que la Observación 1.15 nos dice que para definir una función basta dar su dominio y los valores para cada punto del dominio. Pero cuidado, la forma de dar valores tiene que ser de forma "conjuntista", es decir, de forma que garantice que F forme un conjunto en nuestro sentido. De hecho, el no poder definir funciones "alegremente" es la base del Axioma de Elección que discutiremos en la sección 7. Por poner un ejemplo de cómo definir bien una función, hagámoslo con la *función identidad* sobre un conjunto X. En efecto, por el Axioma de Separación, existe el conjunto $\{(x, y) \in X \times X \mid x = y\}$ que define la función id_X de dominio X y tal que $id_X(x) = x$ para todo $x \in X$.

Ejercicio 1.17. . Sea f una función. Entonces f es inyectiva si y sólo si f^{-1} es una función. Además, en tal caso, $\mathrm{dom}(f^{-1}) = \mathrm{rec(f)}$, $\mathrm{rec}(f^{-1}) = \mathrm{dom(f)}$, $f \circ f^{-1} = id_{\mathrm{rec}(f)}$, $f^{-1} \circ f = id_{\mathrm{dom}(f)}$.

Observación 1.18. Vamos a aprovechar las funciones para simplificar la notación de la unión de conjuntos. Supongamos que tenemos una función $F : X \to S$ donde S es un conjunto de conjuntos. Por la observación anterior, F es la misma función si cambiamos S por $\mathrm{rec}(F)$, por lo que podemos supondremos S=$\mathrm{rec}(F)$ (es decir, que podemos ver F como un modo de parametrizar los conjuntos de S). Usaremos entonces la notación F_x para $F(x)$, y el recorrido de F lo escribiremos como $S = \{F_x\}_{x \in X}$ y lo llamaremos *sistema de conjuntos*. De esta forma, $\bigcup S$ lo escribiremos con el aspecto más habitual de $\bigcup_{x \in X} F_x$. Obviamente, toda esta construcción la podemos hacer si partimos simplemente de un conjunto de conjuntos S: basta tomar $F : S \to S$ como la función identidad.

Teorema 1.19. *Si F, G son funciones, entonces $G \circ F$ es también una función. Además,*

$$\mathrm{dom}(G \circ F) = \mathrm{dom}(F) \cap F^{-1}[\mathrm{dom}(G)]$$

y, para todo $x \in \mathrm{dom}(G \circ F)$,

$$(G \circ F)(x) = G(F(x)).$$

Demostración: Veamos primero que $G \circ F$ es una función. Para ello supongamos que tenemos $(x, z_1), (x, z_2) \in G \circ F$. Eso quiere decir que existen y_1, y_2 tales que

$$(x, y_1) \in F,\ (y_1, z_1) \in G$$

$$(x, y_2) \in F,\ (y_2, z_2) \in G.$$

Como F es una función de $(x, y_1), (x, y_2) \in F$ se sigue $y_1 = y_2$. Por tanto, tenemos $(y_1, z_1), (y_1, z_2) \in G$, y por ser G una función se tendrá $z_1 = z_2$. Esto demuestra que $G \circ F$ es una función.

Sea ahora $x \in \mathrm{dom}(G \circ F)$. Esto quiere decir que existe z tal que $(x, z) \in G \circ F$ (es decir, $z = (G \circ F)(x)$). Equivalentemente, existe y tal que $(x, y) \in F$ y existe z tal que $(y, z) \in G$. La propiedad $(x, y) \in F$ para algún y es equivalente a $x \in \mathrm{dom}(F)$ e $y = F(x)$, mientras que la propiedad $(y, z) \in G$ para algún z es equivalente a $y \in \mathrm{dom}(G)$ (como $z = G(y)$, esto demuestra ya $(G \circ F)(x) = G(F(x))$). Por tanto, las dos propiedades anteriores equivalen a $x \in \mathrm{dom}(F)$ y $F(x) \in \mathrm{dom}(G)$, es decir, $x \in \mathrm{dom}(F) \cap F^{-1}[\mathrm{dom}(G)]$. Esto demuestra la igualdad $\mathrm{dom}(G \circ F) = \mathrm{dom}(F) \cap F^{-1}[\mathrm{dom}(G)]$. □

Definición. Se llama *restricción de una función* F a un conjunto Z al conjunto

$$F \restriction Z := \{(x, y) \in F \mid x \in Z\}.$$

Evidentemente, $F \restriction Z$ es una nueva función con dominio $Z \cap \mathrm{dom}(F)$, y para cada $z \in Z \cap \mathrm{dom}(F)$ se tiene que $(F \restriction Z)(z) = F(z)$.

Teorema 1.20. *Sea Φ un conjunto de funciones tales que para cada $F, G \in \Phi$ se tiene*

$$F \restriction (\mathrm{dom}(F) \cap \mathrm{dom}(G)) = G \restriction (\mathrm{dom}(F) \cap \mathrm{dom}(G)).$$

Entonces $\bigcup \Phi$ es una función cuyo dominio es la unión de los dominios de las funciones de Φ.

Demostración: Es evidente que $\bigcup \Phi$ es una relación binaria, ya que sus elementos son elementos de alguna $F \in \Phi$, y por tanto pares ordenados. Supongamos que tenemos ahora $(x, y_1), (x, y_2) \in \bigcup \Phi$. Entonces existen $F, G \in \Phi$ tales que $(x, y_1) \in F$ y $(x, y_2) \in G$. En particular, $x \in \mathrm{dom}(F) \cap \mathrm{dom}(G)$. Como por hipótesis se tiene $F \restriction (\mathrm{dom}(F) \cap \mathrm{dom}(G)) = G \restriction (\mathrm{dom}(F) \cap \mathrm{dom}(G))$, entonces $F(x) = G(x)$, es decir, $y_1 = y_2$. Por tanto, $\bigcup \Phi$ es una función.

Que el dominio de $\bigcup \Phi$ sea la unión de los dominios de las funciones de Φ es prácticamente evidente, salvo que habría que ver que tal unión tiene sentido, para lo que es

necesario construir el conjunto de todos los dominios de las funciones de Φ. Pero esto es cierto porque cada dominio de una función de Φ es un subconjunto de $\mathrm{dom}(\bigcup \Phi)$, luego podemos construir una función $\mathrm{dom}: \Phi \to \mathcal{P}(\mathrm{dom}(\bigcup(\Phi)))$ que asocia a cada función $F \in \Phi$ su dominio. La unión se hace entonces como en la Observación 1.18. □

Ejercicio 1.21. Demostrar que, si X, Y son conjuntos, entonces existe el conjunto Y^X de funciones cuyo dominio es X y cuyo recorrido está contenido en Y.

Ejercicio 1.22. Demostrar que, dados conjuntos X, Y, Z, la función

$$Z^{X\times Y} \to (Z^Y)^X$$

que manda cada función $f : X \times Y \to Z$ a la función $\phi_f : X \to Z^Y$ definida por

$$(\phi_f(x))(y) = f(x, y)$$

es una biyección.

Ejercicio 1.23. Sea $\{S_i\}_{i\in I}$ un sistema de conjuntos. Demostrar que existe el conjunto $\prod_{i\in I} S_i$ (que llamaremos *producto*) formado por las funciones F de dominio I tales que $F(i) \in S_i$ para todo $i \in I$.

Definición. Sea R una relación binaria sobre un conjunto X. Se dice que R es:

(i) *reflexiva* si xRx para todo $x \in X$;

(ii) *simétrica* si xRy implica yRx;

(iii) *antisimétrica* si xRy e yRx implica $x = y$;

(iv) *asimétrica* si xRy e yRx nunca ocurre;

(v) *transitiva* si xRy e yRz implica xRz.

Se dice que R es una *relación de equivalencia* si es reflexiva, simétrica y transitiva. Se dice que es una *relación de orden* (a veces también diremos *relación de orden parcial*) si es reflexiva, antisimétrica y transitiva; en tal caso diremos que R es una *relación de orden* (o una *relación de orden parcial*) y que el par (X, R) es un *conjunto ordenado*. Se dice que R es un *orden estricto* si es una relación asimétrica y transitiva.

Lema 1.24. *Sea R una relación de equivalencia en un conjunto X. Para cada $x \in X$ sea $[x]_R = \{z \in X \mid xRz\}$. Entonces son equivalentes:*

(i) $[x]_R = [y]_R$.

(ii) $[x]_R \cap [y]_R \neq \emptyset$.

(iii) xRy.

Demostración: Demostramos las implicaciones de modo cíclico:

$(i) \Rightarrow (ii)$: Es evidente, ya que cada $[x]_R$ contiene al menos a x, por la propiedad reflexiva.

$(ii) \Rightarrow (iii)$: Sea $z \in [x]_R \cap [y]_R$. Entonces xRz e yRz. Por la propiedad simétrica podemos escribir xRz y zRy, y por la propiedad transitiva concluimos xRy.

$(iii) \Rightarrow (i)$: Veamos por ejemplo el contenido $[x]_R \subseteq [y]_R$, demostrándose el otro intercambiando de modo simétrico. Si $z \in [x]_R$, entonces xRz. Como, por la propiedad simétrica aplicada a la hipótesis, yRx, se obtiene de la propiedad transitiva que yRz, es decir, $z \in [y]_R$. □

Definición. Los conjuntos $[x]_R$ del lema anterior se llaman *clases de equivalencia módulo* R. El recorrido de la función $\pi : X \to \mathcal{P}(X)$ definida por $\pi(x) = [x]_R$ (se deja como ejercicio demostrar que es una función) se llama *cociente del conjunto* X *módulo la relación* R, y se denota X/R.

Definición. Se llama *partición de un conjunto* X a un subconjunto $S \subseteq \mathcal{P}(X)$ tal que:

(i) $Z \neq \emptyset$ para todo $Z \in S$.

(ii) Si $Z, Z' \in S$, entonces $Z = Z'$ o $Z \cap Z' = \emptyset$.

(iii) $X = \bigcup S$.

El siguiente resultado nos dice que es lo mismo hablar de relaciones de equivalencia en un conjunto que hablar de particiones de dicho conjunto:

Teorema 1.25. *Sea* X *es un conjunto. Entonces:*

(i) Para cada relación de equivalencia R, X/R *es una partición de* X.

(ii) Para cada partición S *de* X, *el conjunto*

$$R_S := \{(x, y) \in X \times X \mid \text{ existe } Z \in S \text{ tal que } x, y \in Z\}$$

es una relación de equivalencia en X. *Además, se tiene que* $X/R_S = S$.

(iii) Para cada relación de equivalencia, si $S = X/R$, *entonces* $R_S = R$.

Demostración: La parte (i) es una consecuencia inmediata del Lema 1.24. Veamos entonces que R_S es una relación de equivalencia, comprobando las tres propiedades:

–Propiedad reflexiva: Sea $x \in X$. Como S es una partición $x \in Z$ para algún $Z \in S$. Por tanto, $(x, x) \in R_S$.

–Propiedad simétrica: Si $(x, y) \in R_S$, entonces x, y están en el mismo subconjunto $Z \in S$, y por supuesto lo mismo es cierto para y, x, luego $(y, x) \in R$.

–Propiedad transitiva: Si $(x, y), (y, z) \in R_S$, entonces x, y están en el mismo Z de S, e y, z están en el mismo Z' de S. Como $Z \cap Z' \neq \emptyset$ (ya que y está en la intersección), se tiene que necesariamente $Z = Z'$. Por tanto, x, z están en el mismo $Z \in S$, luego $(x, z) \in R_S$.

Para terminar de demostrar (ii) hay que ver $X/R_S = S$, que demostraremos por doble contenido:

–$X/R_S \subseteq S$: Sea $[x]_{R_S} \in X/R_S$. Por definición de clase de equivalencia, $y \in [x]_{R_S}$ si y sólo si $(x, y) \in R_S$, y por definición de R_S esto es equivalente a que x, y estén en el mismo subconjunto $Z \in S$. Como x está sólo en un subconjunto $Z \in S$, necesariamente $[x]_{R_S} = Z$, luego $[x]_{R_S} \in S$.

–$S \subseteq X/R_S$: Sea $Z \in S$. Como es no vacío, podemos tomar $x \in Z$. Entonces, según acabamos de demostrar, $Z = [x]_{R_S}$, luego $Z \in X/R_S$.

Demostremos finalmente (iii). Por definición, $(x, y) \in R_S$ si y sólo si x, y están en el mismo Z de $S = X/R$, es decir, si y sólo si x, y están en el mismo $[z]_R$. Pero por el Lema 1.24, $x, y \in [z]_R$ es equivalente a zRx y zRy. Esto implica xRy, es decir $(x, y) \in R$. Pero el recíproco también es cierto ya que basta tomar por ejemplo $z = x$. □

Definición. Se llama *sistema de representantes de una partición* S de un conjunto X a un subconjunto $T \subset X$ tal que para cada $Z \in S$ la intersección $Z \cap T$ tiene exactamente un elemento.

Los dos ejemplos que hay que tener en mente a la hora de pensar en relaciones de orden son, dado un conjunto X, el conjunto $\mathcal{P}(X)$ con la relación $\subseteq$, que es un orden (parcial) y con la relación $\subset$, que es un orden estricto. El siguiente resultado nos dice que la relación entre estos dos tipos de órdenes es siempre como en el ejemplo:

Teorema 1.26. *Sea X un conjunto. Entonces:*

(i) Si R es una relación de orden en X, entonces la relación

$$xSy \text{ si y sólo si } xRy \text{ y } x \neq y$$

es un orden estricto en X.

(ii) Si S es una relación de orden estricto en X, entonces la relación

$$xRy \text{ si y sólo si } xSy \text{ o } x = y$$

es un orden parcial en X.

Demostración: Sea R un orden, y veamos que S definida en (i) es asimétrica y transitiva. Es asimétrica porque no puede ser a la vez xSy e ySx (en efecto, si ocurriera eso, necesariamente por definición $x \neq y$, mientras que además xRy e yRx, lo que implicaría $x = y$ por ser R antisimétrica.). Es transitiva porque, si xSy e ySz, entonces en particular xRz (por la transitividad de R; además, no puede ser $x = z$, porque ya hemos visto que S es asimétrica.

Sea ahora S un orden estricto y veamos que R es reflexiva, antisimétrica y transitiva. La reflexividad es inmediata de la definición de R. Para la antisimetría, supongamos xRy, yRx y, por reducción al absurdo, $x \neq y$; entonces xSy e ySx, en contra de la asimetría de S. Finalmente, R es transitiva porque, si xRy e yRz entonces:

–si $x = y$ o $y = z$, entonces automáticamente xRz;

–si $x \neq y$ e $y \neq z$, entonces xSy e ySz, luego (por la transitividad de S) xSz, por lo que xRz. □

Notación. Normalmente a una relación de orden la denotaremos por $\leq$ en lugar de R, y a la correspondiente relación de orden estricto $<$.

Definición. Una *cadena* de un conjunto ordenado es un subconjunto tal que para cada dos elementos suyos x, y se verifica $x \leq y$ o $y \leq x$. Un *orden total* o *lineal* en un conjunto X es un orden tal que todo X es una cadena.

Una de las cosas que necesitaremos demostrar es que ciertos conjuntos ordenados que construiremos (por ejemplo el de los naturales) están caracterizados por ciertas propiedades del orden. Estar caracterizados quiere decir, como es habitual en matemáticas, que son únicos "salvo isomorfismo", por lo que primero hay que definir qué quiere decir que dos conjuntos ordenados sean isomorfos:

Definición. Un *isomorfismo entre dos conjuntos ordenados* es una biyección $f : X \to Y$ entre ellos tal que $x_1 < x_2$ si y sólo si $f(x_1) < f(x_2)$.

Proposición 1.27. *Si X está totalmente ordenado, entonces una función $f : X \to Y$ es un isomorfismo si y sólo si $rec(f) = Y$ y $x_1 < x_2$ implica $f(x_1) < f(x_2)$.*

Demostración: La inyectividad sigue de que, al ser X totalmente ordenado, entonces $x_1 \neq x_2$ implica $x_1 < x_2$ (luego $f(x_1) < f(x_2)$) o $x_2 < x_1$ (luego $f(x_2) < f(x_1)$). En cualquier caso $f(x_1) \neq f(f_x 2)$.

Basta ver entonces que $f(x_1) < f(x_2)$ implica $x_1 < x_2$. Por reducción al absurdo, supongamos que no es cierto $x_1 < x_2$. Entonces, por ser X totalmente ordenado hay dos

posibilidades: o bien $x_1 = x_2$(luego $f(x_1) = f(x_2)$, lo que es absurdo) o bien $x_2 < x_1$ (luego $f(x_2) < f(x_1)$, que también es absurdo). □

Definición. Sea Y un subconjunto de un conjunto ordenado X.

- Se llama elemento *minimal* (resp. *maximal*) de Y a un elemento $y \in Y$ para el que no exista $y' \in Y$ tal que $y' < y$ (resp. $y < y'$).
- Se llama *cota inferior* (resp. *cota superior*) de Y a un elemento $x \in X$ tal que $x \leq y$ (resp. $y \leq x$) para todo $y \in Y$.
- Se llama *mínimo* (resp. *máximo*) de Y a una cota inferior (resp. superior) que esté en Y (si existe, es necesariamente único).
- Se llama *ínfimo* (resp. *supremo*) de Y al máximo (resp. mínimo) de las cotas inferiores (resp. superiores) de Y.

Todos estos elementos satisfacen las propiedades obvias que que aparecen en los distintos cursos de Análisis o Topología. Recordemos por ejemplo una:

Lema 1.28. *Sea Y un subconjunto de X. Entonces $y \in X$ es el mínimo de Y si y sólo si $y \in Y$ e y es el ínfimo de Y.*

Demostración: Supongamos en primer lugar que y es el mínimo de Y. Entonces, por definición será $y \in Y$ y además es una cota inferior. Para ver que es el máximo de las cotas inferiores, sea y' otra cota inferior de Y. Como $y \in Y$, entonces $y' \leq y$.

Si ahora suponemos que y está en Y y es el ínfimo de Y, veamos que es también el mínimo de y. Por ser el ínfimo de Y, en particular es una cota inferior de Y, y al estar en Y es necesariamente el mínimo. □

Ejercicio 1.29. Sea V un espacio vectorial, no necesariamente de dimensión finita. Un subconjunto $S \subseteq V$ se dice que es *linealmente independiente* si lo es cualquier subconjunto finito suyo, mientras que se dice que es *sistema de generadores* si cualquier vector de V es combinación lineal de una cantidad finita de vectores de S. Finalmente, se dice que S es una *base* de V si es linealmente independiente y sistema de generadores. Si ordenamos $\mathcal{P}(V)$ por la inclusión de subconjuntos, demostrar:

(i) Las bases de V son los elementos maximales del conjunto de los subconjuntos linealmente independientes.

(ii) Las bases de V son los elementos minimales del conjunto de los sistemas de generadores.

2. Los números naturales

Intuitivamente, un número natural es el número de elementos de un conjunto finito. Por tanto, el camino natural (valga la redundancia) para una definición de número natural sería definir primero que dos conjuntos finitos como equivalentes si tienen el mismo número de elementos (es decir, si hay una biyección entre ellos) y llamar número natural a cada una de las clases de equivalencia resultantes. Sin embargo, nos enfrentamos al problema de siempre: ¿existe el conjunto de todos los conjuntos finitos? Para evitar este problema, vamos a dar una definición alternativa, dando para cada posible número natural un conjunto con ese cardinal. Como ya vimos, existe un único conjunto sin elementos, así que definimos $0 = \emptyset$. El siguiente paso es escoger un conjunto con un elemento. Ya vimos en el Ejemplo 1.6 que el primer conjunto que podemos construir con un elemento es $\{\emptyset\}$, así que definimos $1 = \{\emptyset\}$. De la misma forma, el primer conjunto con dos elementos que construimos fue $\{\emptyset, \{\emptyset\}\}$, así que definimos $2 = \{\emptyset, \{\emptyset\}\}$. Nótese que cada número lo estamos definiendo a base de añadir al número anterior, visto como conjunto, un nuevo elemento que es precisamente tal conjunto. La definición general es:

Definición. Se llama *sucesor de un conjunto* X al conjunto $S(X) = X \cup \{X\}$.

Entonces está claro cómo construir los números naturales por recurrencia. Se empieza por construir el 0, y supuesto construido n definimos $n + 1 = S(n)$. El problema para constuir el conjunto de los números naturales es que necesitamos hacer la unión de todos los n, pero para poder aplicar el Axioma de la Unión necesitamos previamente que el conjunto de los naturales ya exista. Podemos intentar usar entonces el Axioma de Separación. Para ello necesitaríamos un conjunto que contuviera a los naturales. Un buen candidato a conjunto que contenga a los naturales sería uno que satisfaga sus mismas propiedades de construcción:

Definición. Un *conjunto inductivo* es un conjunto X tal que $0 \in X$ y, para todo $x \in X$ se tiene $S(x) \in X$.

Es claro que los números naturales estarían caracterizados por estar en todos los conjuntos inductivos, pero eso no permite dar una definición de conjunto. Pero si supiéramos la existencia de algún conjunto inductivo X, entonces podríamos definir $\mathbb{N}$ como el conjunto de elementos de X que están en todos los conjuntos inductivos. Sin embargo, nuestros axiomas no permiten concluir la existencia de conjuntos inductivos (de hecho hasta ahora sólo garantizan la existencia de conjuntos finitos), así que necesitamos un axioma nuevo:

Axioma de Infinitud. *Existe algún conjunto inductivo.*

Podemos ahora precisar las ideas que hemos enunciado antes (demostrando que el conjunto de los números naturales no depende del conjunto inductivo que exista):

Lema 2.1. *Dado un conjunto inductivo X, el conjunto*

$$\mathbb{N} = \{n \in X \mid n \text{ está en todos los conjuntos inductivos}\}$$

es un conjunto inductivo. Además, si X' es otro conjunto inductivo, también se tiene $\mathbb{N} = \{n \in X' \mid n \text{ está en todos los conjuntos inductivos}\}$.

Demostración: Claramente, $0 \in \mathbb{N}$, ya que por definición 0 está en cualquier conjunto inductivo. Por otra parte, si $n \in \mathbb{N}$, entonces $S(n)$ está en todos los conjuntos inductivos (en particular en X), con lo que también $S(n) \in \mathbb{N}$.

Si ahora X' es otro conjunto inductivo, está claro por la definición de $\mathbb{N}$ que $\mathbb{N} \subseteq X'$, luego $\mathbb{N} \subseteq \{n \in X' \mid n \text{ está en todos los conjuntos inductivos}\}$. Como X y X' juegan papeles simétricos, se tiene el otro contenido, lo que completa la demostración. □

Observación 2.2. Para demostrar la independencia de X a la hora de definir $\mathbb{N}$, uno podría tener la tentación de definir $\mathbb{N}$ como la intersección de todos los conjuntos inductivos. Sin embargo, no podemos garantizar que los conjuntos inductivos formen un conjunto (de hecho veremos en la sección 5 que no lo forman), por lo que no tiene sentido hablar de la intersección de todos ellos. Este hecho es constante y ya ha aparecido varias veces (por ejemplo, en el conjunto de todos los conjuntos, de existir, la relación $\subseteq$ sería un orden).

Definición. Los elementos del conjunto $\mathbb{N}$ definido en el Lema 2.1 se llaman *números naturales*. Si $n \in \mathbb{N}$, escribiremos frecuentemente $n+1$ para denotar al sucesor $S(n)$ de n.

La existencia de los números naturales nos permite definir ya de forma precisa la inducción:

Teorema 2.3 (Principio de Inducción)**.** *Sea P una propiedad y supongamos que*

(i) $P(0)$.

(ii) Para todo $n \in \mathbb{N}$, $P(n)$ *implica* $P(n+1)$.

Entonces P se satisface para todos los números naturales.

Demostración: Las hipótesis implican que $X = \{n \in \mathbb{N} \mid P(n)\}$ es un conjunto inductivo. Por tanto, el Lema 2.1 implica que $\mathbb{N}$ está contenido en X. □

Veamos un modo "astuto" de usar a veces la inducción (aunque cuando un proceso de inducción sale tan trivial uno se suele quedar con la mosca detrás de la oreja, en este caso todo es lo más natural: ¿acaso la construcción de los naturales como conjunto inductivo no dice precisamente que $\mathbb{N}$ consiste en el cero y a partir de él todos los números naturales son sucesores de otro?):

Lema 2.4. *Para cada $n \in \mathbb{N}$ distinto de 0 existe $m \in \mathbb{N}$ tal que $m + 1 = n$.*

Demostración: El problema a priori es definir la propiedad P, ya que para $n = 0$ no tiene sentido. Definimos entonces $P(n)$ como "existe $m \in \mathbb{N}$ tal que $m = n + 1$" sólo si $n \neq 0$, definiendo $P(0)$ como una propiedad siempre cierta, por ejemplo $0 = 0$. Se trata entonces de demostrar P usando el Principio de Inducción. Evidentemente $P(0)$ es cierta, así que hay que ver que $P(n)$ implica $P(n + 1)$ para todo n. Obsérvese en primer lugar que $n + 1 \neq 0$, ya que $n \in n + 1$, por lo que $n + 1$ no es el conjunto vacío. Por tanto, $P(n + 1)$ es la propiedad "existe $m \in \mathbb{N}$ tal que $m + 1 = n + 1$", que es automáticamente cierta (basta tomar $m = n$). □

Definición. Dados dos números naturales m, n, diremos $m < n$ si $m \in n$ (luego, siguiendo nuestra notación habitual, $m \leq n$ quiere decir $m \in n$ o $m = n$).

Ejercicio 2.5. Sea P una propiedad de los números naturales y supongamos que existe $k \in \mathbb{N}$ tal que:

(i) $P(k)$.

(ii) Para todo $n \geq k$ se tiene que $P(n)$ implica $P(n + 1)$.

Demostrar que entonces $P(n)$ es cierta para todo $n \geq k$.

Lema 2.6. *Sean m, n números naturales. Entonces:*

(i) $m < n + 1$ si y sólo si $m \leq n$, es decir, $m < n$ o $m = n$.

(ii) $m < n$ implica $m + 1 \leq n$ (y por (i) también $m + 1 < n + 1$).

Demostración: Por definición, $m < n + 1$ si y sólo si $m \in n + 1$. Como $n + 1 = n \cup \{n\}$, lo anterior es equivalente a $m \in n$ (es decir, $m < n$) o $m = n$, lo que demuestra (i).

Demostremos por inducción sobre n que $m < n$ implica $m + 1 \leq n$. El caso $n = 0$ es trivial ya que no hay ningún $m < 0$ (recordemos que $m < 0$ quiere decir $m \in \emptyset$). Supongamos entonces que $m < n$ implica $m + 1 \leq n$ y veamos que $m < n + 1$ implica $m + 1 \leq n + 1$. Por (i), $m < n + 1$ es equivalente a $m = n$ (en cuyo caso es inmediato $m + 1 \leq n + 1$) o $m < n$. En este segundo caso, por hipótesis de inducción tenemos $m + 1 \leq n$, y de nuevo por (i) tenemos $m + 1 < n + 1$. □

Lema 2.7. *Para todo número natural n se tiene $n \geq 0$.*

Demostración: Lo demostraremos por inducción sobre n, siendo evidente cuando $n = 0$. Supongamos ahora $n \geq 0$ y veamos que $n + 1 \geq 0$. Por el Lema 2.6(i), la desigualdad $0 \leq n$ es equivalente, por definición, a $0 < n + 1$, luego $n + 1 \geq 0$. □

Teorema 2.8. *La relación $\leq$ sobre $\mathbb{N}$ es un orden total.*

Demostración: Para demostrar que $\leq$ es un orden, veamos (usando el Teorema 1.26) que $<$ es un orden estricto, es decir, que satisface las propiedades transitiva y asimétrica.

Para demostrar la propiedad transitiva, hay que demostrar, para todo $n \in \mathbb{N}$ que, para cualesquiera $k, m \in N$ tales que $k < m$ y $m < n$ se tiene que $k < n$. Lo demostraremos por inducción sobre n, siendo trivial el caso $n = 0$ ya que no hay ningún $m \in \mathbb{N}$ con $m < 0$ (ya que no puede ser $m \in \emptyset$). Supongamos ahora que sea cierto para n y demostremos el caso $n + 1$, es decir, supongamos $k < m$ y $m < n + 1$ y demostremos $k < n + 1$. Según el Lema 2.6(i), de la desigualdad $m < n + 1$ tenemos dos posibilidades:

–O bien $m < n$, por lo que, por hipótesis de inducción $k < n$.

–O bien $m = n$, y por tanto $k < n$.

Como $k < n$ implica $k < n + 1$ (porque $n \subset n + 1$), queda demostrado el caso $n + 1$ y por tanto la propiedad transitiva.

Veamos ahora la propiedad asimétrica. Tenemos que ver que no puede ocurrir al mismo tiempo $m < n$ y $n < m$. Por la propiedad transitiva que acabamos de demostrar, esto implicaría $n < n$, así que basta ver que, para todo $n \in \mathbb{N}$, no es cierto $n < n$.

Veamos por inducción sobre n que no se da nunca $n < n$. El caso $n = 0$ es trivial, porque no puede ser $\emptyset \in \emptyset$. Supongamos que sabemos que $n < n$ no es cierto y veamos que tampoco lo es $n + 1 < n + 1$. Si fuera así, por el Lema 2.6(i), o bien $n + 1 < n$ o bien $n + 1 = n$ (luego también $n + 1 < n$). Como $n < n + 1$, por la propiedad transitiva $n < n$, lo que es absurdo por hipótesis de inducción.

Queda entonces probado que $<$ es un orden estricto, y por tanto que $\leq$ es un orden. Para ver que es un orden total, hay que ver que, para cada $n \in \mathbb{N}$, se tiene que cada $m \in \mathbb{N}$ satisface o bien $m < n$ o bien $m = n$ o bien $n < m$. De nuevo, la demostración será por inducción sobre n. El caso $n = 0$ viene de que $m \geq 0$ para todo m, por el Lema. Supongamos ahora el resultado para n, y veámoslo para $n + 1$. Tomamos pues cualquier $m \in \mathbb{N}$, y sabemos, por hipótesis de inducción que o bien $m < n$, o bien $m = n$ o bien $n < m$. Los dos primeros casos son equivalentes, por el Lema 2.6(i), a $m < n+1$, mientras que el caso $n < m$ implica, por el Lema 2.6(ii), $n + 1 \leq m$, es decir, $m = n + 1$ o bien $n + 1 < m$. □

Nótese que al final de la demostración anterior, en medio de la inducción, hemos usado el Lema 2.6(ii), que demostramos también por inducción. En realidad hemos usado de forma implícita un argumento de *doble inducción*, cuyo enunciado preciso es el siguiente:

Ejercicio 2.9. Sea P una propiedad de $\mathbb{N} \times \mathbb{N}$ que satisface:

$$\left(P(k,l) \text{ cierta para cada } k,l \text{ con } \begin{cases} k < m \\ \text{ o bien} \\ k = m \text{ y } l < n \end{cases} \right) \text{ implica } P(m,n)$$

Demostrar que $P(m,n)$ es cierta para todo $m, n \in \mathbb{N}$.

Ejercicio 2.10. Demostrar que, para cada $n \in \mathbb{N}$, se tiene $n = \{m \in \mathbb{N} \mid m < n\}$ (obsérvese que no está claro a priori que los elementos de n sean números naturales).

Ejercicio 2.11. Sean n, m números enteros. Demostrar:

(i) $m < n$ si y sólo si $m \subset n$.

(ii) $m < n$ si y sólo si $m + 1 \leq n$ (es decir, en el Lema 2.6(ii) se da la otra implicación también).

(iii) No puede ocurrir $n < m < n + 1$.

Definición. Se llama *buen orden* a un orden total en un conjunto en que cada subconjunto no vacío tiene mínimo. Un conjunto con un buen orden se dice que es un *conjunto bien ordenado.*

Para demostrar que un conjunto está bien ordenado basta ver si un subconjunto suyo no tiene mínimo entonces es el subconjunto vacío. Para $\mathbb{N}$, la estrategia para demostrar que $X \subseteq \mathbb{N}$ sin mínimo es el vacío parece clara. En efecto, como $0 \leq x$ para todo $x \in X$ (Lema 2.7), 0 es una cota inferior de X, luego $0 \notin X$ (en caso contrario 0 sería el mínimo de X). Entonces, podemos decir ahora $1 \leq x$ para todo $x \in X$, y como 1 no puede ser mínimo de X, también $1 \notin X$. Se tiene entonces que $2 \leq x$ para todo $x \in X$ y así sucesivamente. Parece pues que se puede demostrar por inducción que $n \notin X$ para todo $n \in \mathbb{N}$, pero hay un problema: Para poder concluir $n + 1 \leq x$ para todo $x \in X$ hace falta saber antes que $0, 1, \ldots, n$ no están en X, no basta sólo saber $n \notin X$. Hace falta por tanto mejorar el Principio de Inducción:

Teorema 2.12 (Segunda versión del Principio de Inducción)**.** *Sea $P(n)$ una propiedad de los números naturales que satisface la condición*

Para todo $n \in \mathbb{N}$, si $P(m)$ es cierta para todo $m < n$ entonces $P(n)$ es cierta[(*)]*.*

[(*)] Obsérvese que, si en esta condición hacemos $n = 0$, al no haber ningún $m < 0$ la hipótesis se satisface siempre. Por tanto, $P(0)$ es cierta automáticamente, por lo que en esta versión también tenemos "primer paso de la inducción. De hecho, es por esto que se pasa del caso $m < n$ al caso n, en vez del caso $m \leq n$ al caso $n+1$, porque entonces sí que habría que suponer el caso $n = 0$

Entonces P es cierta para todo n.

Demostración: Observemos que basta demostrar que, para todo n, se satisface la propiedad $Q(n)$ definida como "P es cierta para todo $m < n$" (en efecto, entonces para todo n se satisface $Q(n+1)$, y como $n < n+1$ entonces $P(n)$ es cierta). Demostramos entonces $Q(n)$ por inducción, siendo trivial el caso $n = 0$ ya que $Q(0)$ es una condición vacía por no existir ningún $m < 0$.

Supongamos entonces que se satisface $Q(n)$. Para ver que se satisface $Q(n+1)$ hay que ver que $P(m)$ es cierta para todo $m < n+1$. Por el Lema 2.6(i), $m < n+1$ es equivalente a $m < n$ o $m = n$. Cuando $m < n$, $P(m)$ es cierta por la definición de $Q(n)$, mientras que para $m = n$, $P(m)$ es cierta por la hipótesis del enunciado. □

Teorema 2.13. *El conjunto de los números naturales es un conjunto bien ordenado.*

Demostración: Sea $X \subseteq \mathbb{N}$ un subconjunto y supongamos que no tiene mínimo. Demostremos que entonces X es el subconjunto vacío. Para ello, para cada número natural n definimos la propiedad $P(n)$ como $n \notin X$. Bastará ver que $P(n)$ es cierta para cada $n \in \mathbb{N}$, cosa que haremos usando la segunda versión del Principio de Inducción.

Supongamos entonces que $P(m)$ es cierta para todo $m < n$, es decir, que ningún $m < n$ está en X. Por tanto, como $\leq$ es un orden total, cualquier elemento $m \in X$ satisface $n \leq m$, es decir n es una cota superior de X. Como X no tiene mínimo, n no puede estar en X (porque si no sería un mínimo de X). Por tanto, $P(n)$ es cierta, luego el resultado se concluye por la segunda versión del Principio de Inducción. □

Ejercicio 2.14. Sean $<_1, <_2$ dos órdenes estrictos definidos respectivamente sobre los conjuntos X_1, X_2 y supongamos que $X_1 \cap X_2 = \emptyset$. Demostrar que la relación

$$<=<_1 \cup <_2 \cup (X_1 \times X_2)$$

es un orden estricto en $X_1 \cup X_2$. Además, si X_1, X_2 están bien ordenados, entonces también lo está $X_1 \cup X_2$.

Ejercicio 2.15. Demostrar que $\mathbb{N} \times \mathbb{N}$ con el orden lexicográfico es un conjunto bien ordenado.

Evidentemente, si cambiamos mínimo por máximo, no es cierto que todo conjunto no vacío de números naturales tenga máximo. Sin embargo, pidiendo que sea acotado, el resultado es cierto:

Teorema 2.16. *Sea $X \subset \mathbb{N}$ un subconjunto no vacío acotado superiormente. Entonces, X tiene máximo.*

Demostración: Sea $X' \subset \mathbb{N}$ el conjunto de cotas superiores de X. Por definición de máximo, basta encontrar un elemento de X' que esté en X. Para ello, el candidato natural es el mínimo de X'. Como $\mathbb{N}$ está bien ordenado y X' es no vacío por hipótesis, existe en efecto un mínimo n de X'. En particular, $k \leq n$ para todo $k \in X$. Supongamos, por reducción al absurdo, que n no está en X, y por tanto $k < n$ para todo $k \in X$. Como X es no vacío, necesariamente $n \neq 0$, y por el Lema 2.4 existe $m \in \mathbb{N}$ tal que $n = m + 1$. Además, la desigualdad $k < n = m + 1$ implica $k \leq m$ para todo $k \in X$, es decir, $m \in X'$, lo que es absurdo por la minimalidad de n. □

Nuestro próximo objetivo será ver que las propiedades que hemos ido demostrando de $\mathbb{N}$ lo caracterizan salvo isomorfismo. Nótese que dar un isomorfismo (o simplemente una función) de $\mathbb{N}$ a otro conjunto es lo mismo que dar una sucesión, que querremos dar de forma recursiva. Los siguientes resultados nos dirán cómo hacer todo esto de forma precisa.

Definición. Se llama *sucesión* a una función cuyo dominio es un número natural (la llamaremos entences *sucesión finita*) o $\mathbb{N}$ (en cuyo caso la llamaremos *sucesión infinita*). Si el recorrido de la sucesión está contenido en un conjunto X diremos que se trata de una sucesión en X. Si f es una sucesión, escribiremos normalmente f_n para indicar $f(n)$ y escribiremos $< f_n >$ para denotar a la sucesión (indicando como subíndice, si no es claro por el contexto, dónde varía n).

Ejercicio 2.17. Demostrar que existe el conjunto de las sucesiones finitas en X (que denotaremos por $\mathrm{Suc}(X)$).

Ejemplo 2.18. Hay sucesiones que parecen fáciles de definir a primera vista, y que sin embargo no es así. Por ejemplo, supongamos que ya hemos definido el producto de números naturales(*) y probemos a definir a partir de él la sucesión cuyo n-ésimo término es $f_n = n!$. Si no tenemos definida la noción de factorial ¿cómo se puede definir el subconjunto de $\mathbb{N}\times\mathbb{N}$ que consista en los pares $(n, n!)$? La respuesta canónica sería que "por recurrencia", ya que se puede definir $0! = 1$ y, conocido $n!$, se puede definir $(n+1)! = (n+1)n!$, en función del $n!$ previo y de n. En otras palabras, la función $f(n) = n!$ se puede definir dando el valor inicial $f(0) = 1$ y la fórmula de recurrencia $f(n+1) = g(f(n), n)$, donde en este caso

(*) De hecho, para definir el producto por un número fijo lo haremos definiendo una sucesión, y ya definir esta sucesión no será fácil en absoluto; no pondremos este ejemplo o el de la suma, ya que encontrar la definición en la construcción puede ser más sutil.

sería $g(m,n) = (n+1)m$. Nuestro objetivo es ver que tal recurrencia está bien definida y que define la función f que buscamos. Para ello necesitaremos ver primero que (como parece razonable) al menos tal función está bien definida para los números naturales hasta un valor fijo cualquiera n.

Lema 2.19. *Dado un conjunto X, un elemento $x_0 \in X$ y una función $g : X \times \mathbb{N} \to X$, entonces para todo $n \in \mathbb{N}$ existe una única función $h : n+1 \to X$ tal que*

(i) $h(0) = x_0$.

(ii) $h(m+1) = g(h(m), m)$ *para todo* $m < n$.

Demostración: Observemos en primer lugar que, por el Lema 2.6(ii), se tiene que $m < n$ implica $m+1 < n+1$ (de hecho son equivalentes, por el Ejercicio 2.11(ii)), por lo que la condición (ii) tiene sentido.

Demostraremos el resultado por inducción sobre n. El caso $n = 0$ es inmediato, ya que estamos buscando $h : \{0\} \to X$ tal que $h(0) = x_0$ (nótese que (ii) es una condición vacía). Por otra parte, si ya tenemos construida $h : n+1 \to X$ (única) satisfaciendo (i) y (ii), veamos cómo tiene que ser la $h' : (n+1)+1 :\to X$ que buscamos. Como $m < n+1$ es equivalente (por el Lema 2.6(i)) a $m < n$ o $m = n$, podemos escribir las propiedades que debe satisfacer h' como:

(i) $h(0) = x_0$.

(ii) $h(m+1) = g(h(m), m)$ para todo $m < n$.

(iii) $h(m+1) = g(h(m), m)$ para $m = n$.

Por la unicidad del caso n, las condiciones (i) y (ii) son equivalentes a $h' \restriction (n+1) = h$. Por otra parte, la condición (iii) es equivalente a $h'(n+1) = g(h_n(n), n)$. Como $(n+1)+1 = (n+1) \cup \{n+1\}$ y $n+1 \notin n+1$, es claro que existe h' y necesariamente $h' = h_n \cup \{(n+1, g(h_n(n), n))\}$. □

Observación 2.20. El lector posiblemente se estará preguntando por qué en el lema anterior no hemos denotado a la función h que existe para cada n como h_n, indicando a qué n corresponde y de paso evitando algunos engorros de notación tanto en el enunciado como sobre todo en la demostración. La respuesta es que tal notación podría inducir a pensar que en realidad tenemos un conjunto de sucesiones $\{h_n \mid n \in \mathbb{N}\}$ en que cada h_n es la sucesión $n+1 \to X$ que da el lema. A posteriori es cierto que existe tal conjunto, pero precisamente ahí está la dificultad(*) de la recurrencia y es justo lo que hemos demostrado

(*) Esta dificultad está de nuevo íntimamente relacionada con el Axioma de Elección que trataremos en la sección 7. Véase en concreto el Ejemplo 7.30

en el lema. De hecho, el único conjunto que podemos definir a priori (recordando que debemos acogernos a los axiomas que tenemos hasta ahora) es

$$R := \left\{ (n,h) \in \mathbb{N} \times \mathrm{Suc}(X) \;\middle|\; \begin{array}{l} \mathrm{dom}(h) = n+1 \\ h(0) = x_0 \\ h(m+1) = g(h(m), m) \text{ para todo } m < n \end{array} \right\}$$

y lo que demuestra el Lema 2.19 es que la relación R tiene dominio $\mathbb{N}$ (ya que para cada $n \in \mathbb{N}$ existe $h \in \mathrm{Suc}(X)$ tal que $(n,h) \in R$) y es una función (ya que el h que existe para cada n es único). Viendo R como una función $\mathbb{N} \to \mathrm{Suc}(X)$ ya podemos escribir las funciones h descritas en el lema como $\{h_n \mid n \in \mathbb{N}\}$.

Con todo esto ya podemos demostrar:

Teorema 2.21 (Principio de Recurrencia)**.** *Dado un conjunto X, un elemento $x_0 \in X$ y una función $g : X \times \mathbb{N} \to X$ existe una única sucesión infinita $f : \mathbb{N} \to X$ tal que*

(i) $f(0) = x_0$.

(ii) $f(n+1) = g(f(n), n)$.

Demostración: De acuerdo con la notación de la Observación 2.20, el Lema 2.19 nos da un conjunto de sucesiones finitas $\{h_n \mid n \in \mathbb{N}\}$ tal que cada h_n es una sucesión $h_n : n+1 \to X$ tal que:

(i') $h_n(0) = x_0$.

(ii') $h_n(m+1) = g(h_n(m), m))$ para todo $m < n$.

La idea ahora es usar el Teorema 1.20 para obtener que $\bigcup_{n\in\mathbb{N}} h_n$ es una función. En efecto, sean $h_n, h_{n'}$ dos de estas sucesiones. Como $\mathbb{N}$ está totalmente ordenado, podemos suponer, sin pérdida de generalidad $n \leq n'$. Por el Lema 2.6(ii), $n+1 \leq n'+1$ luego, por el Ejercicio 2.11(i), $n+1 \subseteq n'+1$. Entonces $\mathrm{dom}(h_n) \cap \mathrm{dom}(h_{n'}) = n+1$ y es claro, por la unicidad de h_n satisfaciendo (i') y (ii') que $h_{n'} \restriction (n+1) = h_n$. Entonces, por el Teorema 1.20, $f = \bigcup_{n\in\mathbb{N}} h_n$ es una función y $\mathrm{dom}(f) = \bigcup_{n\in\mathbb{N}} \mathrm{dom}(h_n) = \bigcup_{n\in\mathbb{N}} (n+1) = \mathbb{N}$.

Veamos ahora que f satisface (i) y (ii). Como $0 \in 1 = \mathrm{dom}(h_0)$, entonces $f(0) = h_0(0)$, y por (i') se tiene $h_0(0) = x_0$, lo que demuestra (i). Por otra parte, para todo $n \in \mathbb{N}$, se tiene $n, n+1 \in (n+1)+1 = \mathrm{dom}(h_{n+1})$, luego $f(n) = h_{n+1}(n)$, $f(n+1) = h_{n+1}(n+1)$, y por (ii') $h_{n+1}(n+1) = g(h_{n+1}(n), n) = g(f(n), n)$, lo que demuestra (ii).

Finalmente, para la parte de unicidad, supongamos que tenemos f, f' que satisfacen (i) y (ii), y veamos por inducción sobre n que entonces $f(n) = f'(n)$ para todo $n \in \mathbb{N}$. Para $n = 0$, es una consecuencia de (i), ya que $f(0) = x_0 = f'(0)$. Supongamos entonces por hipótesis de inducción que $f(n) = f'(n)$. Entonces, usando (ii):

$$f(n+1) = g(f(n), n) = g(f'(n), n) = f'(n+1)$$

lo que termina la demostración. □

Ejemplo 2.22. El Principio de Recurrencia es un modo de dar rigor a los puntos suspensivos. Por ejemplo, si tenemos una función $h : X \to X$, la función $h^n = h \circ \overset{n)}{\ldots} \circ h$ (es decir, componer h n veces consigo misma) se puede definir por recurrencia mediante $h^0 = id_X$ y $h^{n+1} = h^n \circ h$ (en realidad se define una función $f : \mathbb{N} \to X^X$ en que $f(n) = h^n$). De la misma forma, supuesta definida la suma, el producto $m \cdot n = m + \overset{n)}{\ldots} + m$ se define por recurrencia, y la exponenciación $m^n = m \cdots \overset{n)}{\ldots} \cdot m$ también. Sin embargo, querremos que las operaciones estén definidas como funciones $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, así que su definición la dejaremos para más adelante. En realidad, la suma también es una recurrencia, porque si interpretamos $n = 1 + \overset{n)}{\ldots} + 1$, entonces $m + n$ quiere decir que a m le aplicamos la función sucesor n veces, es decir, $m + n = S^m(n)$.

Ahora que ya tenemos la recurrencia bien fundamentada podemos finalmente caracterizar $\mathbb{N}$ mediante sus propiedades:

Teorema 2.23. *Sea X un conjunto no vacío con un orden total $\preceq$ que satisface las siguientes condiciones:*

(i) Para todo $x \in X$ existe algún $y \in X$ tal que $y \succ x$.

(ii) Todo subconjunto no vacío de X tiene mínimo.

(iii) Todo subconjunto no vacío y acotado superiormente de X tiene máximo.

Entonces $\mathbb{N}$ y X son conjuntos ordenados isomorfos.

Demostración: Sea o el mínimo elemento de X (que existe por (ii)). La forma natural de definir el "elemento sucesivo" de cualquier elemento de X es mediante la función $h : X \to X$ tal que

$$h(x) = \min\{y \in X \mid y \succ x\}$$

(que está bien definida por (i) y (ii)). A partir de h podemos definir $g : X \times \mathbb{N} \to X$ como $g(x, n) = h(x)$. Por el Principio de Recurrencia, existirá entonces $f : \mathbb{N} \to X$ tal que $f(0) = o$ y

$$f(n + 1) = h(f(n))$$

para todo $n \in \mathbb{N}$. Para ver que f es un isomorfismo usaremos la Proposición 1.27.

Veamos en primer lugar que $m < n$ implica $f(m) \prec f(n)$. Lo haremos por inducción sobre n, siendo trivial el caso $n = 0$ (ya que, como siempre, no existen naturales $m < 0$). Entonces, supuesto demostrado para n, consideremos $m < n + 1$ y demostremos $f(m) \prec f(n+1)$. Por el Lema 2.6(i), se tiene que o bien $m = n$ (luego $f(m) = f(n)$) o bien $m < n$ (luego por hipótesis de inducción $f(m) \prec f(n)$). Entonces, en cualquiera de los dos casos

(en el segundo por la transitividad de $\prec$), bastará demostrar $f(n) \prec f(n+1)$. Pero esto es evidente, ya que $f(n+1) = h(f(n))$, y por definición de h se tiene $f(n) \prec h(f(n))$.

Pasemos ahora a demostrar que $\mathrm{rec}(f) = X$. Si no lo fuera, por (ii), el conjunto $X - \mathrm{rec}(f)$ tendría un mínimo y. No puede ser $y = o$, ya que $o = f(0) \in \mathrm{rec}(f)$. Por tanto, como o es el mínimo de X, se tiene $o \prec y$. Esto implica que el conjunto $\{x \in X \mid x \prec y\}$ es no vacío, luego por la hipótesis (iii) tiene un máximo x. Como $x \prec y$, necesariamente existe $n \in \mathbb{N}$ tal que $x = f(n)$. Entonces $f(n+1) = h(x)$, con lo que si demostramos $y = h(x)$ habremos encontrado una contradicción, ya que y no estaba en el recorrido de f. Veamos por tanto que y es el mínimo elemento de X que satisface $x \prec y$. En efecto, dado cualquier otro $y' \in X$ tal que $x \prec y'$, por ser x máximo se tendrá que no puede ser $y' \prec y$. Como X está totalmente ordenado, se sigue entonces $y \preceq y'$, lo que completa la demostración. □

Ejercicio 2.24. Concluir del teorema anterior que, dado cualquier subconjunto $X \subset \mathbb{N}$ no acotado superiormente es isomorfo a $\mathbb{N}$. Si en cambio X está acotado superiormente, demostrar que existe $n \in \mathbb{N}$ tal que hay una biyección $n \to X$.

Ejemplo 2.25. Con el Principio de Recurrencia ocurre como con el Principio de Inducción: a veces para el caso $n+1$ no nos basta saber el caso anterior, sino todos (o parte de) los anteriores. Por ejemplo, es de todos conocida la sucesión de números de Fibonacci (que tendrá pleno sentido en cuanto definamos la suma de números naturales), dada por $t_0 = t_1 = 1$ y $t_{n+1} = t_n + t_{n-1}$. Como cada valor de la sucesión depende no sólo del inmediatamente anterior, sino de los dos anteriores, no puede usarse el Principio de Recurrencia. Cabe resaltar también que, si queremos dar una fórmula cerrada para el n-ésimo número de Fibonacci hay que "salirse" del conjunto de los números naturales, ya que la fórmula concreta es:

$$t_n = \frac{1}{\sqrt{5}}\Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^{n+1} - \Big(\frac{1-\sqrt{5}}{2}\Big)^{n+1}\Big] = \frac{5+\sqrt{5}}{10}\Big(\frac{1+\sqrt{5}}{2}\Big)^{n} + \frac{5-\sqrt{5}}{10}\Big(\frac{1-\sqrt{5}}{2}\Big)^{n}.$$

Es por ello por lo que los principios de recursión que estamos estudiando no son un mero formalismo, sino que dicen que las funciones existen aunque no "se pueden escribir explícitamente".

Imitemos pues para la recurrencia la segunda versión del Principio de Inducción. Recordemos que ahí se demostraba el caso n a partir de los anteriores. En nuestro caso, saber el valor de una sucesión $f : \mathbb{N} \to X$ para los naturales menores que n es conocer $f \restriction n$, que es una sucesión de longitud n. Por tanto, para determinar cada $f(n)$ a partir de $f \restriction n$ necesitaremos una función $g : \mathrm{Suc}(X) \to X$ que para cada sucesión finita nos dé un elemento de X. Recordemos también que la segunda versión del Principio de Inducción

no se pedía el caso 0, que pasaba a ser automático. En el caso de sucesiones el número de valores iniciales puede variar. Por ejemplo, para la sucesión de Fibonacci necesitamos dos valores iniciales. En este caso, la función $g : \mathrm{Suc}(\mathbb{N}) \to \mathbb{N}$ que necesitamos la podemos tomar como la que manda a cada sucesión de longitud menor o igual que uno a 1, mientras que cada sucesión $t : n \to \mathbb{N}$ de longitud $n \geq 2$ la manda a $t_{n-2} + t_{n-1}$. La sucesión de Fibonacci estará entonces definida por la fórmula de recurrencia $t_n = g(t \restriction n)$. Veamos que en general una recurrencia así define una sucesión:

Teorema 2.26 (Segunda versión del Principio de Recurrencia)**.** *Dados un conjunto X y una función $g : \mathrm{Suc}(X) \to X$, existe una única sucesión $f : \mathbb{N} \to X$ tal que $f_n = g(f \restriction n)$.*

Demostración: Definiremos por recurrencia las "sucesiones parciales" $F_n := \langle f_0, \ldots, f_{n-1} \rangle$. En otras palabras, queremos definir una función $F : \mathbb{N} \to \mathrm{Suc}(X)$, que tendrá que satisfacer $F_0 = \langle\rangle$ y $F_{n+1} = F_n \cup \{(n, g(F_n))\}$, y que existe por el Principio de Recurrencia, tomando como $G : \mathrm{Suc}(X) \times \mathbb{N} \to \mathrm{Suc}(X)$ la función que manda cada (t, n) a la sucesión vacía (o a cualquier otra, ya que es indiferente para nuestros objetivos) salvo si t tiene longitud n en que $G(t, n) = t \cup \{(n, g(t))\}$. Tomamos entonces $f = \bigcup_{n \in \mathbb{N}} F_n$, que es una función de dominio $\mathbb{N}$ (aplicando el Teorema 1.20 y teniendo en cuenta que se tiene $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$). Como cada $n \in \mathbb{N}$ está en el dominio de F_{n+1} se tiene

$$f_n = F_{n+1}(n) = g(F_n) = g(f \restriction n)$$

por lo que la f encontrada satisface la propiedad buscada.

Supongamos que tenemos otra $f' : \mathbb{N} \to X$ tal que $f'_n = g(f' \restriction n)$ y veamos por la segunda versión del Principio de Inducción que $f_n = f'_n$ para todo $n \in \mathbb{N}$. En efecto, supongamos $f_k = f'_k$ para todo $k < n$. Esto es equivalente a decir $f \restriction n = f' \restriction n$. Por tanto, se tendrá

$$f_n = g(f \restriction n) = g(f' \restriction n) = f'_n$$

lo que demuestra la unicidad de f y termina la demostración. □

Nuestro siguiente objetivo es definir las operaciones básicas entre números naturales. Una manera de definir la suma sería, por ejemplo, para cada número natural n definir la función $f_n : \mathbb{N} \to \mathbb{N}$ que consistiría en sumar n. Para ello necesitamos una versión del Principio de Recurrencia "con parámetros", es decir, en lugar de una función $f : \mathbb{N} \to X$ buscaremos una colección de funciones $\{f_i\}_{i \in I}$ parametrizadas por un conjunto I, para lo que necesitaremos dar para cada $i \in I$ el valor inicial a_i y la función $g_i : X \times \mathbb{N} \to X$. La forma rigurosa de poner eso será:

Teorema 2.27. *Sean X, I conjuntos y $a : I \to X$ y $g : I \times X \times \mathbb{N} \to X$ funciones. Entonces existe una única función $f : I \times \mathbb{N} \to X$ tal que*

(i) $f(i,0) = a(i)$ *para todo* $i \in I$.

(ii) $f(i,n+1) = g(i,f(i,n),n)$ *para todo* $i \in I$ *y todo* $n \in \mathbb{N}$.

Demostración: Por el Ejercicio 1.22, la función f buscada es equivalente a una función $F : \mathbb{N} \to X^I$, donde $F((n))(i) = f(i,n)$. Por tanto, las condiciones del enunciado son equivalentes a

(i) $F(0) = a$.

(ii) $F(n+1) = G(F(n),n)$,

donde $G : X^I \times \mathbb{N} \to X^I$ está definida mandando (h,n) a la función $G(h,n) : I \to X$ definida como

$$(G(h,n))(i) = g(i,h(i),n).$$

La existencia y unicidad de F (y por tanto de f) queda garantizada entonces por el Principio de Recurrencia. □

Podemos ahora definir las operaciones habituales entre números naturales

Corolario 2.28. *Existe una única función* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *tal que:*

(i) $f(m,0) = m$ *para todo* $m \in \mathbb{N}$.

(ii) $f(m,n+1) = f(m,n) + 1$ *para todo* $m,n \in \mathbb{N}$.

Además, $f(n,1) = n+1$ *para todo* $n \in \mathbb{N}$.

Demostración: Para la existencia y unicidad, basta tomar en el Teorema 2.27 las funciones $a : \mathbb{N} \to \mathbb{N}$ definida por $a(n) = n$ y $g : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $g(m,n,k) = n+1$. La igualdad $f(n,1) = n+1$ se demuestra por inducción sobre n. Para $n = 0$, se tiene, usando (ii) y luego (i)

$$f(0,1) = f(0,0+1) = f(0,0) + 1 = 0 + 1 = 1.$$

Supuesto $f(n,1) = n+1$, y usando de nuevo (ii) y (i) se tiene

$$f(n+1,1) = f(n+1,0+1) = f(n+1,0) + 1 = (n+1) + 1$$

lo que termina la demostración. □

Definición. A la función f del corolario anterior se le llama *suma de números naturales*, y se denota $m+n$ en lugar de $f(m,n)$ (obsérvese que la propiedad $f(n,1) = n+1$ indica que los dos sentidos de la escritura $n+1$ coinciden: el sucesor de n y la suma de n y 1).

Corolario 2.29. *Existe una única función* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *tal que:*

(i) $f(m, 0) = 0$ *para todo* $m \in \mathbb{N}$.

(ii) $f(m, n + 1) = f(m, n) + m$ *para todo* $m, n \in \mathbb{N}$.

Demostración: Basta tomar en el Teorema 2.27 las funciones $a : \mathbb{N} \to \mathbb{N}$ definida por $a(n) = 0$ y $g : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $g(m, n, k) = n + m$. □

Definición. A la función f del corolario anterior se le llama *producto de números naturales*, y se denota $m \cdot n$ (o simplemente mn) en lugar de $f(m, n)$.

Corolario 2.30. *Existe una única función* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *tal que:*

(i) $f(m, 0) = 1$ *para todo* $m \in \mathbb{N}$.

(ii) $f(m, n + 1) = f(m, n)m$ *para todo* $m, n \in \mathbb{N}$.

Demostración: Basta tomar en el Teorema 2.27 las funciones $a : \mathbb{N} \to \mathbb{N}$ definida por $a(n) = 1$ y $g : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $g(m, n, k) = nm$. □

Definición. A la función f del corolario anterior se le llama *exponenciación de números naturales*, y se denota m^n en lugar de $f(m, n)$.

Las operaciones apenas definidas satisfacen las propiedades habituales que conocemos. Demostramos la conmutatividad de la suma, dejando el resto como ejercicio.

Proposición 2.31. *Para todo* $m, n \in \mathbb{N}$ *se tiene* $m + n = n + m$.

Demostración: Demostraremos por inducción sobre n la propiedad $P(n)$: $m + n = n + m$ para todo $m \in \mathbb{N}$.

El caso $n = 0$ será $m+0 = 0+m$ para todo $m \in \mathbb{N}$. Como $m+0 = m$ por el Corolario 2.28(i), demostraremos por inducción sobre m que $0 + m = m$ para todo $m \in \mathbb{N}$. El caso $m = 0$ es de nuevo el Corolario 2.28(i). Y si suponemos $0 + m = m$, entonces usando el Corolario 2.28(ii) tendremos

$$0 + (m + 1) = (0 + m) + 1 = m + 1$$

lo que termina de demostrar $P(0)$.

Suponemos ahora $P(n)$ y demostremos $P(n+1)$, es decir $m+(n+1) = (n+1)+m$ para todo $m \in \mathbb{N}$. Esto es equivalente, por el Corolario 2.28(ii), a $(m+n)+1 = (n+1)+m$, y a su vez equivalente, por hipótesis de inducción, a $(n+m)+1 = (n+1)+m$, que demostraremos por inducción sobre m. El caso $m = 0$ es inmediato por el Corolario 2.28(i). Supongamos

entonces $(n+m)+1 = (n+1)+m$ y veamos qué pasa para $m+1$. Usando al principio y al final el Corolario 2.28 obtenemos entonces

$$(n+(m+1))+1 = ((n+m)+1)+1 = ((n+1)+m)+1 = (n+1)+(m+1)$$

lo que termina la demostración. □

El resto de propiedades se demuestra igual. Algunas demostraciones pueden ser especialmente largas, porque suele hacer falta hacer tantas inducciones como números naturales distintos aparecen en el enunciado. Enunciamos ahora como ejercicio tales propiedades (obsérvese que la propiedad (iv) permite hablar de *sustracción de números naturales*):

Ejercicio 2.32. Demostrar las siguientes propiedades de las operaciones de números naturales:

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

(ii) $m < n$ si y sólo si $m+k < n+k$.

(iii) $m = n$ si y sólo si $m+k = n+k$.

(iv) Dados números naturales $m \leq n$, existe un único $k \in \mathbb{N}$ tal que $m+k = n$.

(v) $mn = nm$

(vi) $(km)n = k(mn)$.

(vii)) $k(m+n) = km+kn$.

(viii) Si $k \neq 0$, $m < n$ si y sólo si $mk < nk$.

(ix) Si $k \neq 0$, $m = n$ si y sólo si $mk = nk$.

(x) $a^{m+n} = a^m a^n$.

(xi) $(a^m)^n = a^{mn}$.

(xii) $a^m = a^n$ si y sólo si $m = n$.

Finalizamos esta sección mencionando que la aritmética de los números naturales puede hacerse de forma axiomática. Concretamente, los *Axiomas de Peano* afirman que existe un conjunto $\mathbb{N}$ con un elemento 0, una función $S : \mathbb{N} \to \mathbb{N}$ y operaciones $+$ y $\cdot$ de forma que:

(i) Si $S(m) = S(n)$ entonces $m = n$.

(ii) $S(n) \neq 0$ para todo $n \in \mathbb{N}$.

(iii) $n+0 = n$ para todo $n \in \mathbb{N}$.

(iv) $m+S(n) = S(m+n)$ para todo $m, n \in \mathbb{N}$.

(v) $n \cdot 0 = 0$ para todo $n \in \mathbb{N}$.

(vi) $m \cdot S(n) = m \cdot n + m$ para todo $m, n \in \mathbb{N}$.

(vii) Si $n \neq 0$ entonces $n = S(m)$ para algún $m \in \mathbb{N}$.

(viii) Si P es una propiedad expresable en términos de 0, S, $+$ y $\cdot$ tal que $P(0)$ y $P(n)$ implica $P(S(n))$ entonces $P(n)$ es cierta para todo $n \in \mathbb{N}$.

3. Sistemas de números

En esta sección nos proponemos construir los conjuntos de los números enteros, racionales y reales, recordando sus propiedades más importantes. Empezamos por los enteros. La idea es que los números enteros deben ser el conjunto de todas las "diferencias" $m - n$. Como un mismo entero puede venir de distintas diferencias, la definición precisa debe ser:

Definición. Llamaremos *número entero* a una clase de equivalencia en $\mathbb{N} \times \mathbb{N}$ módulo la relación R

$$(m, n)R(m', n') \text{ si y sólo si } m + n' = m' + n$$

(que se demuestra fácilmente que es de equivalencia: para la transitividad, úsese el Ejercicio 2.32(iii)). El conjunto de los números enteros se denotará por $\mathbb{Z}$.

Lema 3.1. *Cada número entero $a \in \mathbb{Z}$ se puede escribir de forma única de alguna de las siguientes maneras:*

(i) $a = [(n, 0)]_R$ *con* $n > 0$

(ii) $a = [(0, n)]_R$ *con* $n > 0$.

(iii) $a = [(0, 0)]_R$.

Demostración: Escribimos $a = [(m', n')]_R$. Supongamos por ejemplo $m' \leq n'$. Entonces por el Ejercicio 2.32(iv), existirá un único $n \in \mathbb{N}$ tal que $n' = m' + n$, lo que es equivalente a $a = [(0, n)]_R$. Análogamente, si $n' \leq m'$ se podrá poner $a = [(n, 0)]_R$ para un único $n \in \mathbb{N}$. Además, si fuera $a = [(0, n)]_R = [(m, 0)]_R$, entonces $m + n = 0$, lo que implica $m = n = 0$ (ya que si, por ejemplo, $n > 0$, el Ejercicio 2.32(ii) implicaría $m + n > m$, luego $m + n \neq 0$). Esto implica que los casos (i) y (ii) no se dan simultáneamente. □

Notación. El lema anterior nos dice que la función $\mathbb{N} \to \mathbb{Z}$ que manda n a $[(n, 0)]_R$ es inyectiva. Consideraremos por tanto $\mathbb{N}$ como subconjunto de $\mathbb{Z}$, y escribiremos n en vez de $[(n, 0)]_R$. Del mismo modo, si $n > 0$, escribiremos $-n$ en vez de $[(0, n)]_R$. Llamaremos *valor absoluto de un número entero* a al único $n \in \mathbb{N}$ tal que $a = [(n, 0)]_R$ o $a = [(0, n)]_R$. En otras palabras, $|n| = n$ y $|-n| = n$.

Proposición 3.2. *La relación $<$ en $\mathbb{Z}$ definida por*

$$[(m_1, n_1)]_R < [(m_2, n_2)]_R \text{ si y sólo si } m_1 + n_2 < m_2 + n_1$$

está bien definida, es un orden estricto, el correspondiente orden $\leq$ es total y, restringido a $\mathbb{N}$, coincide con el orden en los naturales.

Demostración: Que el orden es total y que la restricción a $\mathbb{N}$ es el orden de los naturales es inmediato, así que sólo hay que demostrar que está bien definido y es un orden estricto.

Supongamos en primer lugar $[(m_1, n_1)]_R = [(m_1', n_1')]_R$ y $[(m_2, n_2)]_R = [(m_2', n_2')]_R$, es decir $m_1 + n_1' = m_1' + n_1$ y $m_2 + n_2' = m_2' + n_2$. Usando el Ejercicio 2.32(ii) se tiene que

$$m_1 + n_2 < m_2 + n_1$$

es equivalente a

$$(m_1 + n_2) + (n_1' + n_2') < (m_2 + n_1) + (n_1' + n_2')$$

que, reagrupando y usando las igualdades $m_1 + n_1' = m_1' + n_1$ y $m_2 + n_2' = m_2' + n_2$ queda

$$(m_1' + n_2') + (n_1 + n_2) < (m_2' + n_1') + (n_1 + n_2)$$

y de nuevo por el Ejercicio 2.32(ii) es equivalente a

$$m_1' + n_2' < m_2' + n_1'$$

luego $<$ está bien definido al no depender de los representantes.

Es claro que no puede ocurrir a la vez $[(m_1, n_1)]_R < [(m_2, n_2)]_R$ y $[(m_2, n_2)]_R < [(m_1, n_1)]_R$, porque no puede ocurrir a la vez $m_1 + n_2 < m_2 + n_1$ y $m_2 + n_1 < m_1 + n_2$ en $\mathbb{N}$, luego $<$ es asimétrica en $\mathbb{Z}$.

Finalmente, la transitividad de $<$ se demuestra porque, si $[(m_1, n_1)]_R < [(m_2, n_2)]_R$ y $[(m_2, n_2)]_R < [(m_3, n_3)]_R$, entonces por definición $m_1 + n_2 < m_2 + n_1$ y $m_2 + n_3 < m_3 + n_2$. Entonces

$$(m_1 + n_3) + n_2 < m_2 + n_3 + n_1 < (m_3 + n_1) + n_2$$

y $[(m_1, n_1)]_R < [(m_3, n_3)]_R$ se deduce entonces del Ejercicio 2.32(ii). □

Dejamos como ejercicio la demostración de los siguientes resultados (que es del todo análoga a las hechas hasta ahora), que dan la estructura de anillo de $\mathbb{Z}$:

Proposición 3.3. *La operación*

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

$$[(m, n)]_R + [(m', n')]_R = [(m + m', n + n')]_R$$

está bien definida y da a $\mathbb{Z}$ estructura de grupo abeliano. Además, esta suma restringida a $\mathbb{N} \times \mathbb{N}$ es la suma de números naturales. □

Proposición 3.4. *La operación*

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$[(m, n)]_R \cdot [(m', n')]_R = [(mm' + nn', mn' + m'n)]_R$$

está bien definida y da a $\mathbb{Z}$, junto con la suma de la Proposición 3.3, estructura de anillo conmutativo unitario. Además, este producto restringido a $\mathbb{N}\times\mathbb{N}$ es el producto de números naturales. □

Pasamos a continuación a definir los números racionales. Ahora buscamos el conjunto de todos los cocientes de números enteros, por lo que la definición debe ser:

Definición. Llamaremos *número racional* a una clase de equivalencia en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ módulo la relación R definida por

$$(m, n)R(m', n') \text{ si y sólo si } mn' = m'n$$

(que se demuestra fácilmente que es de equivalencia). La clase $[(m, n)]_R$ la escribiremos $\frac{m}{n}$. El conjunto de los números racionales se denotará por $\mathbb{Q}$.

Notación. Es claro que la función $\mathbb{Z} \to \mathbb{Q}$ que manda n a $\frac{n}{1}$ es inyectiva, por lo que podemos identificar $\mathbb{Z}$ como un subconjunto de $\mathbb{Q}$. Normalmente escribiremos n en vez de $\frac{n}{1}$. Nótese también que $\frac{m}{n} = \frac{-m}{-n}$, por lo que podemos siempre suponer que el denominador de un número racional es positivo.

Extendemos ahora a $\mathbb{Q}$ todos los conceptos que teníamos en $\mathbb{Z}$. Ahorramos al lector las demostraciones, que a estas alturas no aportan ya nada nuevo.

Proposición 3.5. *La relación $<$ en $\mathbb{Q}$ definida por*

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \text{ si y sólo si } m_1 n_2 < m_2 n_1$$

(considerando siempre $n_1, n_2 > 0$) está bien definida, es un orden estricto, el correspondiente orden $\leq$ es total y, restringido a $\mathbb{Z}$, coincide con el orden en los enteros. □

Proposición 3.6. *La operación*

$$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$$

$$\frac{m}{n} + \frac{m'}{n'} = \frac{mn' + m'n}{nn'}$$

está bien definida y da a $\mathbb{Q}$ estructura de grupo abeliano. Además, esta suma restringida a $\mathbb{Z} \times \mathbb{Z}$ es la suma de números enteros. □

Proposición 3.7. *La operación*

$$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$$

$$\frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'}$$

está bien definida y da a $\mathbb{Q}$, junto con la suma de la Proposición 3.6, estructura de cuerpo. Además, este producto restringido a $\mathbb{Z} \times \mathbb{Z}$ es el producto de números enteros. □

Definición. Sea X un conjunto totalmente ordenado. Se dice que un subconjunto $Y \subseteq X$ es *denso* (por supuesto se puede tomar $Y = X$) si, para cada dos elementos $x_1 < x_2$ de X existe $y \in Y$ tal que $x_1 < y < x_2$. Se dice que X *no tiene extremos* si no tiene ni máximo ni mínimo.

Ejercicio 3.8. Demostrar que $\mathbb{Q}$ es un conjunto denso (dados $r, s \in \mathbb{Q}$ tales que $r < s$, demostrar $r < \frac{r+s}{2} < s$) y sin extremos (demostrar que, para todo $r \in \mathbb{Q}$, se tiene $r - 1 < r < r + 1$). Veremos más adelante que es esencialmente el único conjunto con esta propiedad (y que tenga "el mismo número de elementos").

Queremos ahora definir de forma precisa el hecho de que $\mathbb{Q}$ tenga "huecos", para estudiar cómo taparlos. Por ejemplo ¿qué quiere decir que a $\mathbb{Q}$ le falte $\sqrt{2}$? Una forma de decirlo es que el conjunto de los racionales menores que $\sqrt{2}$ no se puede escribir como el conjunto de racionales menores que un número racional. Para describir esto de forma más concreta, veamos cómo son los conjuntos de esta forma

Lema 3.9. *Sea X un conjunto totalmente ordenado, y sea $x \in X$. Si llamamos $A_x = \{x' \in X \mid x' < x\}$, entonces:*

(i) A_x es subconjunto propio y, para todo $x' \in A_x$, se tiene que todos los elementos $x'' < x'$ están también en A_x.

(ii) A_x no es vacío si y sólo si x no es el mínimo de X.

(iii) $x = \min(X - A_x)$.

(iv) Si X es denso, A_x no tiene máximo; en tal caso, $x = \sup(A_x)$.

(v) La función $f : X \to \mathcal{P}(X)$ satisface que $x < x'$ si y sólo si $A_x \subset A_{x'}$, luego en particular es una función inyectiva.

Demostración: Claramente A_x es un subconjunto propio, ya que $x \notin A_x$. Además, si $x' \in A_x$, entonces $x' < x$, luego por la transitividad de $<$ se tiene que si $x'' < x'$, también $x'' < x$, es decir, $x'' \in A_x$. Esto prueba (i).

Por definición, A_x es no vacío si y sólo si existe $x' \in X$ tal que $x' < x$, lo que es claramente equivalente a que x no sea el mínimo de X, demostrando (ii).

Para demostrar (iii), por ser X totalmente ordenado, $X - A_x$ es el conjunto de elementos de X mayores o iguales que x. De aquí se deduce inmediatamente $x = \min(X - A_x)$, demostrando (iii).

Para demostrar (iv), supongamos que es X es denso. Entonces, para todo $x' \in A_x$ (es decir, $x' < x$) existe $x'' \in X$ tal que $x' < x'' < x$. Es decir, ningún $x' \in A_x$ es cota superior (porque existe $x'' \in A_x$ con $x' < x''$), luego A_x no tiene máximo. Claramente x es una cota superior de A_x, y veamos que es el supremo si A_x no tiene máximo. Para demostrar que es el supremo de A_x, hay que ver que es la mínima cota superior. En efecto, si x' es otra cota superior de A_x y no fuese $x \leq x'$, como X está totalmente ordenado se tendrá $x' < x$, es decir $x' \in A_x$, lo que implicaría que x' es el máximo de A, en contra de la hipótesis. Por tanto, x es el supremo de A_x.

Finalmente, (v) es evidente usando que $x \in A_{x'} - A_x$ y que X está totalmente ordenado. □

Pensando de nuevo en los racionales, es claro que los menores de $\sqrt{2}$ satisfacen la propiedad (i) del Lema 3.9. Damos entonces la siguiente:

Definición. Se llama *segmento inicial* de un conjunto totalmente ordenado X a un subconjunto propio $A \subset X$ tal que para todo $x' \in A$ se tiene que todos los elementos $x'' < x'$ están también en A (como $x' \in A$, podemos cambiar en la definición $x'' < x'$ por $x'' \leq x'$). Claramente, esto es equivalente a que A es propio y que $x' \in A$, $x'' \in X - A$ implica $x' < x''$, es decir, que cada elemento de A es menor que cada elemento de $X - A$.

Podemos dar inmediatamente un criterio para decidir qué segmentos iniciales son de la forma A_x.

Lema 3.10. *Sea X un conjunto totalmente ordenado y A un segmento inicial. Entonces $A = A_x$ para algún $x \in X$ si y sólo si $X - A$ tiene mínimo. En particular, si X está bien ordenado, todo segmento inicial es de la forma A_x.*

Demostración: Si $A = A_x$, entonces el Lema 3.9(iii) implica que $X - A$ tiene a x como mínimo. Recíprocamente, si existe $x = \min(X - A)$, entonces veamos que $A = A_x$. En efecto, por una parte, si $x' \in A$ entonces al ser A un segmento inicial y $x \in X - A$, se tiene $x' < x$, es decir, $x' \in A_x$. Y por otra parte, si $x' \in A_x$, entonces $x' < x$, y por ser x mínimo en $X - A$ no podrá ser $x' \in X - A$, es decir, $x' \in A$.

Finalmente, supongamos que X está bien ordenado. Como todo segmento inicial es propio, se tendrá que $X - A$ es un subconjunto no vacío. Por tanto, al ser X bien ordenado, $X - A$ tiene un mínimo x, luego $A = A_x$, como acabamos de demostrar. □

Es claro que se podría repetir todo el estudio anterior con los conjuntos $A'_x = \{x' \in X \mid x' \leq x\}$, que en particular seguirán siendo un segmento inicial, y un segmento inicial

A será de la forma A'_x si y sólo si A tiene máximo(*). Para excluir segmentos iniciales de este tipo (que "cortan" X de la misma forma que los A_x) damos la siguiente definición:

Definición. Se llama *corte* en un conjunto totalmente ordenado a un segmento inicial no vacío $A \subset X$. Se llama *corte de Dedekind* en un conjunto totalmente ordenado a un segmento inicial no vacío $A \subset X$ que no tiene máximo(**).

Podemos dar ya finalmente la definición precisa de hueco:

Definición. Un *hueco* en un conjunto totalmente ordenado X es un corte de Dedekind A que no es de la forma A_x (y por el Lema 3.10, es equivalente a decir que $X - A$ no tiene mínimo).

Ejercicio 3.11. Demostrar que $A = \{x \in \mathbb{Q} \mid x \leq 0 \text{ o } (x > 0,\ x^2 < 2)\}$ es un hueco de $\mathbb{Q}$.

Parece entonces natural completar los huecos de un conjunto bien ordenado considerando el conjunto de cortes de Dedekind. Cabe preguntarse entonces si tal conjunto ya no tendrá huecos. Dicho así, habría que estudiar los cortes de Dedekind del conjunto de cortes de Dedekind. Aparte de parecer un trabalenguas, parece una tarea complicada. Vamos a intentar entonces dar un criterio para decidir si un conjunto tiene huecos. Necesitamos previamente un lema (que da una generalización de los conjuntos A_x, cambiando x por un conjunto no vacío):

Lema 3.12. *Sea S un subconjunto no vacío de un conjunto totalmente ordenado X y definamos $A_S = \bigcup_{x \in S} A_x$. Entonces:*

(i) Si S es acotado, entonces A_S es un segmento inicial.

(ii) Si S es acotado y no tiene máximo, entonces A_S es un corte de Dedekind.

(iii) Si S tiene supremo x, entonces $A_S = A_x$.

(iv) Si S es un corte de Dedekind, entonces $A_S = S$.

Demostración: Veamos primero que, si $x' \in A_S$ y $x'' < x'$, entonces $x'' \in A_S$. En efecto, $x' \in A_S$ quiere decir $x' \in A_x$ para algún $x \in S$; entonces $x' < x$, luego por la transitividad $x'' < x$, de donde $x'' \in A_x$ y por tanto $x'' \in A_S$. Para terminar de demostrar (i), sea $y \in X$

(*) El lector puntilloso habrá caído en la cuenta de que hay que imponer que A'_x sea propio para que pueda ser segmento inicial, y que para que un segmento inicial pueda ser de la forma A'_x hay que pedirle también que sea no vacío. De todas formas, ambas hipótesis las vamos a poner a partir de ahora en la definición de corte

(**) En realidad, se suele llamar corte o corte de Dedekind al par $(A, X - A)$, pero hemos preferido abreviar la notación.

una cota superior de S, y veamos que $y \notin A_S$, lo que implicará que A_S es un subconjunto propio. En efecto, para todo $x' \in A_S$ se tiene que $x' < x$ para algún $x \in S$. Por ser y cota superior de S, $x \leq y$, luego $x' < y$, y por tanto $x' \neq y$. Por tanto, A_S es un segmento inicial.

Para demostrar (ii) hay que ver que, si S no tiene máximo, entonces A_S es no vacío y no tiene máximo. Como S no tiene máximo, no puede constar de un solo elemento (pues sería máximo). Entonces tendrá al menos dos elementos x, x', y podemos suponer por ejemplo $x' < x$. Entonces $x' \in A_x$, luego $x' \in A_S$, lo que demuestra que A_S es no vacío. Para ver que A_S no tiene máximo, veamos que ningún elemento suyo es cota superior. En efecto, sea $x' \in A_S$. Entonces $x' \in A_x$ para algún $x \in S$. Como x no puede ser máximo de S, existirá $x'' \in S$ tal que $x < x''$. Por tanto, $x \in A_{x''}$, luego $x \in A_S$, lo que implica (porque $x' < x$) que x' no es máximo de A_S. Esto completa la demostración de (ii).

Para demostrar (iii), sea $x = \sup(S)$ y veamos por doble contenido $A_S = A_x$. Si $x' \in A_S$, entonces $x' < x''$ para algún $x'' \in S$. Como x es cota superior de S, entonces $x'' \leq x$ y por tanto también $x' < x$, es decir, $x' \in A_x$. Recíprocamente, si $x' \in A_x$, entonces $x' < x$. Por ser x el mínimo de las cotas superiores de S, se tendrá que x' no es cota superior de S, luego existirá $x'' \in S$ tal que $x' < x''$. Por tanto $x' \in A_{x''}$, luego $x' \in A_S$, demostrando (iii)

Finalmente, si S es un corte de Dedekind, veamos la igualdad $A_S = S$ de (iv) mediante el doble contenido. Primero, si $x' \in A_S$, entonces $x' < x$ para algún $x \in S$, y por ser S segmento inicial se tiene $x' \in S$. Recíprocamente, si $x' \in S$, como S no tiene máximo existe $x \in S$ tal que $x' < x$, luego $x' \in A_x$, y por tanto $x' \in A_S$. □

Proposición 3.13. *Sea X un conjunto totalmente ordenado. Entonces X no tiene huecos si y sólo si cada subconjunto no vacío acotado superiormente tiene supremo.*

Demostración: Supongamos primero que X no tiene huecos, y sea S un subconjunto no vacío de X. Consideramos $A_S = \bigcup_{x \in S} A_x$ y, por el Lema 3.12(ii), o bien S tiene máximo (en cuyo caso tiene supremo) o bien A_S es un corte de Dedekind. En este último caso, como A_S no puede ser un hueco, necesariamente $X - A_S$ (que es claramente el conjunto de cotas superiores de S) tiene un mínimo, que por definición será el supremo de S.

Recíprocamente, supongamos ahora que cada subconjunto no vacío acotado superiormente de X tiene supremo. Hay que demostrar que cada corte de Dedekind A es de la forma A_x. Por definición, un corte de Dedekind A es no vacío y cualquier elemento de $X - A$ (que es no vacío) es cota superior de A, luego por hipótesis A tendrá un supremo x. Aplicamos entonces las partes (iv) y (iii) de Lema 3.12, tomando $S = A$, para concluir $S = A_S = A_x$, lo que termina la demostración. □

Definición. Diremos que un conjunto totalmente ordenado X es *completo* si es denso y cada subconjunto no vacío y acotado superiormente tiene supremo (es decir, X no tiene huecos).

Teorema 3.14. *Sea X un conjunto totalmente ordenado, denso y sin extremos. Sea $\bar{X} = \{A \in \mathcal{P}(X) \mid X \text{ es un corte de Dedekind}\}$. Entonces:*

(i) La función $X \to \bar{X}$ que asocia a cada $x \in X$ el elemento $A_x = \{x' \in X \mid x' < x\}$ es inyectiva y, considerando X como subconjunto de $\bar{X}$, el orden $\subseteq$ de $\bar{X}$ restringido a X es el orden de X y además X es denso en $\bar{X}$.

(ii) La relación $\subseteq$ en $\bar{X}$ es una relación de orden total que hace de $\bar{X}$ un conjunto completo sin extremos.

Demostración: La parte (i) excepto la densidad es consecuencia del Lema 3.9 (como X no tiene extremos, x no puede ser el mínimo de X). Para demostrar que X es denso en $\bar{X}$, consideremos dos cortes de Dedekind $A \subset A'$ y veamos que podemos intercalar un A_x entre ellos. Sea $x' \in A' - A$ y, como x' no puede ser el máximo de A', existirá $x \in A'$ tal que $x' < x$. Se tiene entonces $A \subset A_x \subset A'$ (ya que $x' \in A_x - A$ y $x \in A' - A_x$).

Para la parte (ii), veamos primero que el orden es total. En efecto, si $A \not\subseteq A'$, entonces existe un elemento $x \in A - A'$. Entonces, para todo $x' \in A'$, por ser A' un segmento inicial debe ser $x' < x$. Pero entonces, por ser A un segmento inicial se tiene $x' \in A$. Esto demuestra que el orden es total.

Para ver que $\bar{X}$ es completo, debemos ver (aparte de la densidad de $\bar{X}$, que es consecuencia de que ya sólo X es denso en $\bar{X}$) que si $\bar{S} \subset \bar{X}$ es no vacío y acotado (es decir, existe un corte de Dedekind A'' tal que $A' \subseteq A''$ para todo $A' \in \bar{S}$) entonces $\bar{S}$ tiene supremo. Consideramos entonces $A = \bigcup \bar{S}$ y veamos que es el supremo de $\bar{S}$. Para ello, primero hay que ver que es un corte de Dedekind. En primer lugar, es fácil ver que es un segmento inicial (es propio porque está contenido en A'', que es propio). Además es no vacío por serlo los $A' \in \bar{S}$ y ser $\bar{S}$ no vacío. Finalmente, no puede tener un máximo , ya que tendría que pertenecer a algún $A' \in \bar{S}$, y sería entonces también máximo de A'. Por tanto, A es un corte de Dedekind, y es claro que es el supremo de $\bar{S}$.

Para finalizar (ii), veamos que $\bar{X}$ no tiene extremos. En efecto, sea A un corte de Dedekind cualquiera. Como A es no vacío, podemos tomar $x \in A$, y claramente se tiene $A_x \subset A$ (porque $x \notin A_x$), luego A no puede ser mínimo de $\bar{X}$. Por otra parte, $X - A$ también es no vacío, luego existe $x' \in X - A$ (y por ser A segmento inicial $x'' < x'$ para todo $x'' \in A$). Como X no tiene máximo, se tendrá que existe $x > x'$. Entonces claramente $A \subset A_x$ (ya que $x' \in A_x - A$), luego A tampoco es máximo de $\bar{X}$. □

Definición. Dado un conjunto totalmente ordenado X, denso y sin extremos, llamaremos

compleción de X a un conjunto ordenado $\bar{X}$ tal que:

(i) $X \subset \bar{X}$, el orden de $\bar{X}$ restringido a X es el orden de X y además X es denso en $\bar{X}$.

(ii) $\bar{X}$ es un conjunto totalmente ordenado, completo y sin extremos.

El Teorema 3.14 nos dice que el conjunto de cortes de Dedekind es una compleción de un conjunto totalmente ordenado, denso y sin extremos. Cabe preguntarse si es la única posible (salvo isomorfismo, por supuesto). En principio uno sólo espera unicidad cuando ha impuesto alguna condición para que la compleción sea el conjunto completo más pequeño que contiene a X. Aunque de forma encubierta, tal condición está implícita en el hecho de que X tiene que ser denso en su compleción. De hecho, la propiedad de densidad va a ser clave en la demostración de cada uno de los pasos del siguiente resultado, que será clave para la demostración de la unicidad, y que afirma que dos conjuntos uno denso del otro tienen los mismos cortes de Dedekind:

Teorema 3.15. *Sea X un subconjunto denso de un conjunto totalmente ordenado X' y supongamos que ni X ni X' tienen extremos. Entonces existe un isomorfismo $f : \bar{X} \to \bar{X}'$ que, restringido a X, es la inclusión de X en X'.*

Demostración: Para ver que f es biyectiva vamos a construir una inversa $g : \bar{X}' \to \bar{X}$, definida mediante $g(A') = A' \cap X$. Primero habrá que ver que cada $A' \cap X$ es un corte de Dedekind de X:

–$A' \cap X$ no es todo X, ya que existe $x' \in X' - A'$, y al no tener máximo X', existirá $x'' > x'$ también en X'; finalmente, la densidad de X en X' implica que existe $x \in X$ tal que $x' < x < x''$. Como A' es un segmento inicial, $x > x'$ y $x' \notin A'$, no puede ser $x \in A'$. Por tanto, $x \in X - (A' \cap X)$.

–Si $x' \in A' \cap X$ y tomamos $x'' \in X$ tal que $x'' < x'$, por ser A' un segmento inicial se tiene $x'' \in A$, luego $x'' \in A' \cap X$.

–$A' \cap X$ es no vacío, porque, tomando $x' \in A'$, que es no vacío, y otro $x'' < x'$ en X' (que existe porque X' no tiene mínimo), entonces por la densidad de X en X' existirá $x \in X$ tal que $x'' < x < x'$. Como A' es un segmento inicial, entonces $x \in A'$, luego $x \in A' \cap X$.

–Finalmente, $A' \cap X$ no tiene máximo. En efecto, dado cualquier $x \in A' \cap X$, veamos que no puede ser cota superior de $A' \cap X$. Como A' no tiene máximo, existirá $x' \in A'$ tal que $x < x'$. Por la densidad de X en X', existirá $x'' \in X$ tal que $x < x'' < x'$. Como A' es un segmento inicial y $x'' < x'$, entonces $x'' \in A'$. Por tanto x no es cota superior de $A' \cap X$, porque $x < x''$ con $x'' \in A \cap X$.

Antes de ver que definir f, resolveremos primero un problema de notación. Cuando escribamos $A'_{x'}$ querrá decir el segmento inicial de los $x'' \in X'$ tales que $x'' < x'$, reservando la notación A_x (con $x \in X$) para el segmento inicial de X de los $x' \in X$ tales que $x' < x$.

Con esta notación, definimos la función $f : \bar{X} \to \bar{X}'$ mediante $f(A) = \bigcup_{x\in A} A'_x$, es decir, lo que sería el A'_A del Lema 3.12. Por tanto, por ser A un segmento inicial, no tiene máximo (ni como subconjunto de X ni como subconjunto de X', por lo que el Lema 3.12 implica que $f(A)$ es en efecto un corte de Dedekind de X'.

Veamos entonces primero $g(f(A)) = A$ para todo $A \in \bar{X}$. En efecto, por definición, y aplicando al final el Lema 3.12(iv):

$$g(f(A)) = f(A) \cap X = (\bigcup_{x\in A} A'_x) \cap X = \bigcup_{x\in A} (A'_x \cap X) = \bigcup_{x\in A} A_x = A_A = A.$$

Para ver ahora $f(g(A')) = A'$ para todo $A' \in \bar{X}'$. Usando la definición de f y g para el primer miembro de la igualdad y el Lema 3.12(iv) para el segundo debemos demostrar

$$\bigcup_{x\in A'\cap X} A'_x = \bigcup_{x'\in A'} A'_{x'}.$$

Evidentemente el segundo término es mayor porque es unión de más subconjuntos. Sin embargo, para cada $x' \in A'$, usando que A' no tiene máximo, existe $x'' \in A'$ tal que $x'' > x'$, y usando una vez más la densidad de X en X' se tiene que existe $x \in X$ tal que $x' < x < x''$. Como A' es un segmento inicial, de $x < x''$ y $x'' \in A'$ se deduce $x \in A'$. Luego $x \in A' \cap X$, y además $A'_{x'} \subset A'_x$ (porque $x' < x$), luego cada $A'_{x'}$ está contenido en un A'_x con $x \in A' \cap X$. Esto demuestra el otro contenido de la igualdad, luego $f(g(A')) = A'$ para todo $A' \in \bar{X}'$.

Es obvio que f (y los mismo g) preserva inclusiones. Además, como es biyectiva, preserva también los contenidos estrictos. Por tanto (ver Proposición 1.27) f es un isomorfismo.

Finalmente, demostrar que la restricción de f a X es la inclusión de X en X' es equivalente a decir $f(A_x) = A'_x$ para todo $x \in X$. Como g es la inversa de f, es equivalente a decir $g(A'_x) = A_x$, que es evidente. □

Teorema 3.16. *Sea X' una compleción de un conjunto totalmente ordenado X denso y si extremos. Entonces existe un isomorfismo $\bar{X} \to X'$ que restringido a X es la identidad.*

Demostración: Aplicando el Teorema 3.15, tenemos un diagrama conmutativo

$$\begin{array}{ccc} X & \to & X' \\ \downarrow & \nearrow & \downarrow \\ \bar{X} & \to & \bar{X}' \end{array}$$

en que las flechas verticales son las dadas para X y X' por el Teorema 3.14 la flecha superior es la inclusión de X en X' y la flecha inferior es el isomorfismo del Teorema 3.15. Por

otra parte, el hecho de que X' sea completo es equivalente a que la flecha vertical derecha sea un isomorfismo. Podemos construir entonces la flecha diagonal como composición del isomorfismo inferior y la inversa del isomorfismo de la derecha, que será el isomorfismo buscado. □

Definición. Llamaremos $\mathbb{R}$ al conjunto $\bar{\mathbb{Q}}$, compleción del conjunto de los números racionales. Los elementos de $\mathbb{R}$ los llamaremos *números reales*. Como todas las compleciones de $\mathbb{Q}$ son isomorfas, esta compleción será isomorfa, por ejemplo, a la obtenida a través de sucesiones de Cauchy, que igual resulta más familiar al lector.

Ejercicio 3.17. Sea $a : \mathbb{N} \to 2 = \{0, 1\}$ una sucesión y llamemos

$$A_a = \bigcup_{n\in\mathbb{N}} \Big\{ x \in \mathbb{Q} \mid x < \frac{a_0}{3^0} + \frac{a_1}{3^1} + \ldots + \frac{a_n}{3^n} \Big\}.$$

Demostrar que, para cada $a \in 2^{\mathbb{N}}$, el conjunto A_a es un corte de Dedekind en $\mathbb{Q}$ y que la función $2^{\mathbb{N}} \to \mathbb{R}$ que manda cada sucesión a a A_a es inyectiva.

Ahora que tenemos un conjunto completo $\mathbb{R}$ que contiene a $\mathbb{Q}$, podemos definir las operaciones suma y producto en $\mathbb{R}$ a partir de las de $\mathbb{Q}$. Por ejemplo, la suma se definiría como

$$x + y = \sup\{p + q \mid p, q \in \mathbb{Q},\ p \le x,\ q \le y\}$$

(el supremo existe por tratarse de un conjunto no vacío acotado superiormente y ser $\mathbb{R}$ completo). Claramente, la suma restringida a $\mathbb{Q}$ es la suma en $\mathbb{Q}$. Que la suma es conmutativa es evidente por serlo la suma en $\mathbb{Q}$. Como ejemplo de cómo se demuestra el resto de propiedades de las operaciones en los números reales demostraremos la asociatividad (como se verá, se deben usar fuertemente las propiedades de las operaciones en $\mathbb{Q}$, así como la densidad):

Proposición 3.18. *Sean $x, y, z \in \mathbb{R}$. Entonces $(x + y) + z = x + (y + z)$.*

Demostración: Llamaremos $\alpha = (x + y) + z$ y demostraremos que es el supremo del conjunto

$$S = \{p + q + r \mid p, q, r \in \mathbb{Q},\ p \le x,\ q \le y,\ r \le z\}$$

(nos ahorramos los paréntesis en la suma de racionales, que ya sabemos que es asociativa). De forma análoga se demuestra que el supremo de ese conjunto es $x + (y + z)$, lo que terminaría la demostración.

Veamos primero que α es una cota superior de S. Sea entonces $p + q + r \in S$. Como $p \le x$ y $q \le y$, entonces $p + q$ es menor o igual que el supremo de todas las posibles sumas

$p' + q'$ en estas condiciones, que por definición es $x + y$. Entonces, $p + q + r$ será menor o igual que el supremo del conjunto de sumas $s' + r'$ con $s' \leq x + y$ y $r' \leq z$, es decir, $p + q + r \leq \alpha$.

Queda entonces por ver que α es el mínimo de las cotas superiores de S. Para ello veamos que ningún $\alpha' < \alpha$ puede ser cota superior de S. Por la densidad de $\mathbb{Q}$ en $\mathbb{R}$, existe $a \in \mathbb{Q}$ tal que $\alpha' < a < \alpha$. Como $a < \alpha = \sup\{s + r \mid s, r \in \mathbb{Q},\ s \leq x + y,\ r \leq z\}$, existirán $s, r \in \mathbb{Q}$ tales que $s \leq x + y$, $r \leq z$ y $s + r > a$. Tendremos entonces $a - r < s \leq x + y = \sup\{p + q \mid p, q \in \mathbb{Q},\ p \leq x,\ q \leq y\}$, luego existirán $p, q \in \mathbb{Q}$ tales que $p \leq x$, $q \leq y$ y $p + q > a - r$. Por tanto, $p + q + r > a > \alpha'$ y, como $p + q + r \in S$, α' no es cota superior de S. □

Para definir el producto hay que tener más cuidado, porque los signos pueden influir. En efecto, para multiplicar $x, y > 0$ no podemos decir que sea el supremo de los productos $p, q \in \mathbb{Q}$ tales que $p \leq x$ y $q \leq y$, puesto que entonces podríamos tomar p, q arbitrariamente negativos y su producto sería arbitrariamente grande. La definición se hace entonces distinguiendo casos. En primer lugar, si $x, y \geq 0$, se define

$$x \cdot y = \sup\{p \cdot q \mid p, q \in \mathbb{Q},\ 0 \leq p \leq x,\ 0 \leq q \leq y\}.$$

Entonces, mediante las definiciones naturales

$$-x = \sup\{p \in \mathbb{Q} \mid x \leq -p\}$$

y

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0 \end{cases}$$

podemos definir en general

$$x \cdot y = \begin{cases} |x| \cdot |y| & \text{si } x, y \geq 0 \text{ o } x, y \leq 0 \\ -|x| \cdot |y| & \text{si } (x \geq 0 \text{ e } y \leq 0) \text{ o } (x \leq 0 \text{ e } y \geq 0) \end{cases}$$

Ejercicio 3.19. Demostrar que $\mathbb{R}$, con estas dos operaciones, es un cuerpo del que $\mathbb{Q}$ es subcuerpo.

Ejercicio 3.20. Definamos en $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ las operaciones

$$(x_1, y_1) + (x_2, y_2) = (x_1 + y_1, x_2 + y_2)$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 y_1 - x_2 y_2, x_1 y1 + x_2 y_1).$$

Demostrar que $\mathbb{C}$ es un cuerpo del que $\mathbb{R}$ es un subcuerpo ($\mathbb{C}$ es el cuerpo de los *números complejos*).

4. Comparabilidad de conjuntos

Nuestro objetivo sería definir la noción de cardinal de un conjunto como número de elementos que contiene. Como en principio eso no es nada fácil, lo que vamos a imaginar es que existiera ese concepto y que estuviera bien definido. Todas las definiciones y notaciones irán en ese sentido, pero serán en principio meros nombres formales o notaciones. En primer lugar, es fácil imaginar lo que debería ser que dos conjuntos tuvieran el mismo número de elementos:

Definición. Dos conjuntos X, Y se dice que son *equipotentes* o que *tienen el mismo cardinal* si existe una biyección $X \to Y$. Escribiremos entonces $|X| = |Y|$. Si existiera el conjunto de todos los conjuntos, la relación de equipotencia sería de equivalencia:

Lema 4.1. *La equipotencia satisface las siguientes propiedades:*

(i) Para cualquier conjunto X se tiene $|X| = |X|$.

(ii) Si X, Y son conjuntos tales que $|X| = |Y|$, entonces $|Y| = |X|$.

(iii) Si X, Y, Z son conjuntos tales que $|X| = |Y|$, $|Y| = |Z|$, entonces $|X| = |Z|$.

Demostración: Para (i), basta tomar la identidad $id_X : X \to X$, que evidentemente es biyectiva. Para (ii), si $f : X \to Y$ es una biyección entre X e Y, entonces $f^{-1} : Y \to X$ es una biyección entre Y y X. Finalmente, para (iii), si $f : X \to Y$ es una biyección entre X e Y y $g : Y \to Z$ es una biyección entre Y y Z, entonces $g \circ f$ es una biyección entre X y Z. □

Como ejemplo de equipotencia damos el siguiente resultado, que será muy útil:

Teorema 4.2. *Sea X un conjunto cualquiera. Entonces $|\mathcal{P}(X)| = |2^X|$.*

Demostración: Definimos $f : \mathcal{P}(X) \to 2^X$ asociando a cada subconjunto S de X la función $\chi_S : X \to 2$ definida por

$$\chi_S(x) = \begin{cases} 1 & \text{si } x \in S \\ 0 & \text{si } x \notin S \end{cases}$$

(la llamada *función característica de S*). Es claro que f es una biyección, ya que la función $2^X \to \mathcal{P}(X)$ que manda cada función $\chi : X \to 2$ a $\chi^{-1}[\{1\}]$ se comprueba fácilmente que es la inversa de f. □

Dejamos como ejercicio las propiedades obvias de la equipotencia:

Ejercicio 4.3. Sean X_1, X_2, Y_1, Y_2 conjuntos tales que $|X_1| = |X_2|$ e $|Y_1| = |Y_2|$. Demostrar:

(i) Si $X_1 \cap Y_1 = X_2 \cap Y_2 = \emptyset$, entonces $|X_1 \cup Y_1| = |X_2 \cup Y_2|$.

(ii) $|X_1 \times Y_1| = |X_2 \times Y_2|$.

(iii) $|X_1^{Y_1}| = |X_2^{Y_2}|$.

(iv) $|\mathrm{Suc}(X_1)| = |\mathrm{Suc}(X_2)|$.

(v) $|\mathcal{P}(X_1)| = |\mathcal{P}(X_2)|$.

Es fácil definir también cuándo el cardinal de un conjunto es como mucho el de otro (aunque podría haber una definición alternativa, según el Ejercicio 4.4, aunque en realidad sólo será equivalente suponiendo el Axioma de Elección):

Definición. Diremos que *el cardinal de un conjunto X es menor o igual que el cardinal de un conjunto Y* si existe una función inyectiva $X \to Y$. Escribiremos $|X| \leq |Y|$. Diremos también que *el cardinal de un conjunto X es menor que el cardinal de un conjunto Y*, y escribiremos $|X| < |Y|$ si $|X| \leq |Y|$ y no se tiene $|X| = |Y|$.

Ejercicio 4.4. Demostrar que, si $|X| \leq |Y|$ y $X \neq \emptyset$, entonces existe una función $Y \to X$ cuyo recorrido es X.

En este caso, sólo es fácil demostrar las "propiedades" reflexiva y transitiva de $\leq$.

Lema 4.5. *El símbolo $\leq$ satisface:*

(i) Para cualquier conjunto X, se tiene $|X| \leq |X|$.

(ii) Para cualesquiera conjuntos tales que $|X| \leq |Y|$, $|Y| \leq |Z|$, se tiene $|X| \leq |Z|$.

Demostración: Para (i), basta tomar la identidad $id_X : X \to X$, que evidentemente es inyectiva. Para (ii), si $f : X \to Y$ y $g : Y \to Z$ son funciones inyectivas, entonces $g \circ f : X \to Z$ es una función inyectiva. □

La "propiedad antisimétrica" es también cierta, pero requiere más trabajo:

Teorema 4.6 (de Cantor-Bernstein)**.** *Si $|X| \leq |Y|$ e $|Y| \leq |X|$, entonces $|X| = |Y|$.*

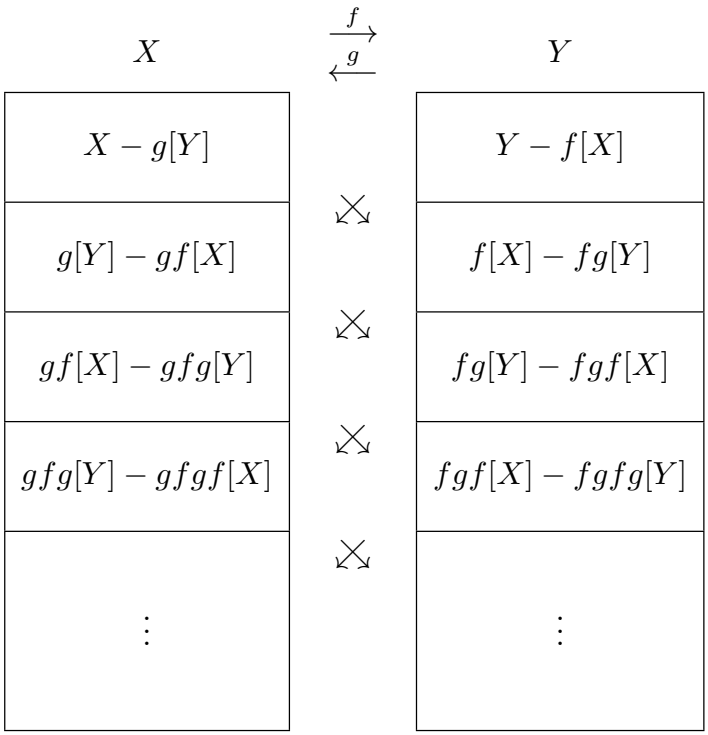
Demostración: Por hipótesis, existen funciones inyectivas $f : X \to Y$ y $g : Y \to X$. Como $g[Y] \subseteq X$ y $f[X] \subseteq Y$, tenemos, aplicando alternativamente f y g y reiterando, obtendremos cadenas

$$X \supseteq g[Y] \supseteq gf[X] \supseteq gfg[Y] \supseteq gfgf[Y] \supseteq \dots$$

$$Y \supseteq f[X] \supseteq fg[Y] \supseteq fgf[X] \supseteq fgfg[X] \supseteq \dots$$

Si a cada subconjunto le quitamos el inmediatamente sucesivo, obtendremos una descomposición de X y de Y en (infinitos) subconjuntos distintos. Ilustramos esto estas descomposiciones en el diagrama siguiente, en que las cajas horizontales representan cada uno de

estos trozos (el dibujo es muy engañoso, porque nadie asegura que las cajas horizontales rellenen los conjuntos X e Y[*]).



Obsérvese que, con esta descomposición, f manda (biyectivamente) cada caja horizontal a la caja inmediatamente inferior de Y, mientras que g manda cada caja horizontal a la caja inmediatamente inferior de X. La idea entonces es mandar mediante f las cajas impares de X a las cajas pares de Y y, mediante g^{-1}, las cajas pares de X a las cajas impares de Y, lo que nos dará una biyección entre X e Y.

Para formalizar esta idea, definimos primero lo que sería la unión de las cajas impares de X, es decir:

$$S := \bigcup_{n\in\mathbb{N}} (g \circ f)^n [X - g[Y]]$$

(recuérdese que en el Ejemplo 2.22 vimos que $(g \circ f)^n$ se puede definir con rigor). Nótese que el elemento de la unión correspondiente a $n = 0$ es $X - g[Y]$, luego los elementos de fuera de S están en la imagen de g (y son imagen de un solo elemento de Y por ser g inyectiva. Esto permite definir la siguiente función $h : X \to Y$:

$$x \mapsto h(x) = \begin{cases} f(x) & \text{si } x \in S \\ g^{-1}(x) & \text{si } x \notin S \end{cases}$$

[*] Para el lector que crea que el dibujo anterior ya es una demostración, recordamos las palabras de Henri Poincaré: "La geometría es el arte de razonar bien sobre figuras mal hechas" (en "Dernières Pensées", accesible en http://www.ac-nancy-metz.fr/enseign/philo/textesph/Dernierespensees.pdf)

que veremos que es una biyección.

Para ver que es inyectiva, supongamos que $h(x) = h(x')$. Si fuera $x, x' \in S$, entonces $x = x'$ sigue de la inyectividad de f, mientras que si fuera $x, x' \notin S$, entonces $g^{-1}(x) = g^{-1}(x')$, lo que implica también $x = x'$ (basta aplicar g). Veamos finalmente que no puede ocurrir, por ejemplo $x \in S$ y $x' \notin S$ (el otro caso es simétrico). En efecto, en tal caso tendríamos $f(x) = g^{-1}(x')$, y por tanto $x' = g(f(x))$. Como $x \in S$, existen $x'' \in X - g[Y]$ y $n \in \mathbb{N}$ tales que $x = (g \circ f)^n(x'')$ con lo que $x' = (g \circ f)^{n+1}(x'')$, luego $x' \in S$, que es absurdo.

Veamos finalmente que el recorrido de h es Y. Sea $y \in Y$, y consideramos dos posibilidades. Si $g(y) \notin S$, entonces $y = h(g(y))$, y por tanto está en la imagen. Si en cambio $g(y) \in S$, entonces existen $n \in \mathbb{N}$ y $x \in X - g[Y]$ tales que $g(y) = (g \circ f)^n(x)$ (necesariamente $n > 0$, pues en caso contrario $g(y) = x$, en contra de $x \in X - g[Y]$). Por la inyectividad de g, se tendrá $y = f((g \circ f)^{n-1}(x))$. Pero entonces $x' = (g \circ f)^{n-1}(x) \in S$ y $f(x') = y$, luego y está en la imagen de h. □

La pregunta natural ahora es si "el orden entre cardinales es total", es decir, si dados dos conjuntos cualesquiera X, Y, necesariamente $|X| \leq |Y|$ o $|Y| \leq |X|$. Sin embargo, a esto no vamos a poder contestar afirmativamente más que usando el Axioma de Elección.

Otra propiedad obvia de los cardinales es que existe el mínimo, que es el cardinal del conjunto vacío. Sin embargo, no hay máximo, ya que se tiene el siguiente resultado:

Teorema 4.7 (Cantor)**.** *Para cada conjunto X se tiene $|\mathcal{P}(X)| > |X|$.*

Demostración: La desigualdad $|X| \leq |\mathcal{P}(X)|$ se deduce inmediatamente de la función inyectiva $f : X \to \mathcal{P}(X)$ definida por $f(x) = \{x\}$. Para ver que no se da la igualdad, veamos que no existe ninguna función $X \to \mathcal{P}(X)$ cuyo recorrido sea $\mathcal{P}(X)$. Para ello demostraremos que, dada cualquier función $g : X \to \mathcal{P}(X)$, el subconjunto $S = \{x \in X \mid x \notin g(x)\}$ no puede estar en el recorrido. En efecto, si existiera $x \in X$ tal que $g(x) = S$, entonces no puede ser $x \in S$ (porque entonces, por definición de S, sería $x \notin g(x) = S$, lo que es absurdo) ni puede ser $x \notin S$ (porque entonces $x \notin g(x)$ y por tanto $x \in S$). □

Parece natural empezar a definir los cardinales de los conjuntos finitos y que sean los números naturales. Antes de hacerlo, como hemos definido las nociones de igualdad y desigualdad para cardinales y para naturales, debemos demostrar que coinciden. Para ello, demostramos un lema previo, que será la base de buena parte de la teoría de cardinales finitos:

Lema 4.8. *Para todo $n \in \mathbb{N}$, toda función inyectiva $n \to n$ es biyectiva.*

Demostración: Lo demostraremos por inducción sobre n, siendo trivial el caso $n = 0$ (sólo hay una función $\emptyset \to \emptyset$, que es biyectiva). Supongamos ahora que el resultado es cierto para n, y sea $f : n + 1 \to n + 1$ una función inyectiva. Sea $f' : n \to n$ la función definida como

$$f'(m) = \begin{cases} f(m) \text{ si } f(m) \neq n \\ f(n) \text{ si } f(m) = n \end{cases}$$

(nótese que si existe un $m < n$ tal que $f(m) = n$, por la inyectividad de f no puede ser $f(n) = n$, luego $f'(m) = f(n) \in n$, luego f' está bien definida). Claramente f' es inyectiva por serlo f, luego por hipótesis de inducción es biyectiva. Eso implica inmediatamente que $n \subseteq \text{rec}(f)$. Basta ver entonces que $n \in \text{rec}(f)$. Pero esto se sigue de estudiar quién es $f(n)$. Si es $f(n) = n$, entonces inmediatamente $n \in \text{rec}(f)$. Si en cambio $f(n) < n$, entonces $f(n) \in n = \text{rec}(f')$; por tanto, existe $m \in n$ tal que $f'(m) = f(n)$, y veamos que entonces $f(m) = n$. Efectivamente, si fuera $f(m) \neq n$, por la definición de f' se tendría $f'(m) = f(m)$, luego sería $f(m) = f(n)$, contradiciendo la inyectividad de f (ya que $m < n$). Por tanto, $f(m) = n$, luego también en este caso $n \in \text{rec}(f)$. □

Proposición 4.9. *Sean $m, n \in \mathbb{N}$. Entonces:*

(i) $|n| = |m|$ si y sólo si $n = m$.

(ii) $n \leq m$ si y sólo si $|n| \leq |m|$.

Demostración: Veamos primero (i). Ya sabemos que $|n| = |n|$ (Lema 4.1(i)), así que sólo hay que ver que $|n| = |m|$ implica $n = m$. Supongamos que no fuera así. Entonces, como $\mathbb{N}$ está totalmente ordenado, podemos suponer sin pérdida de generalidad $m < n$, y por tanto $m \subset n$ (Ejercicio 2.11(i)). Componiendo entonces la biyección $n \to m$ con la inclusión estricta $m \subset n$, tendremos una función inyectiva $n \to n$ que no es biyectiva, en contradicción con el Lema 4.8.

Para demostrar (ii), supongamos primero $n \leq m$, es decir, $n \subseteq m$ (Ejercicio 2.11(i)). Entonces, la inclusión da una función inyectiva $n \to m$, lo que implica $|n| \leq |m|$.

Recíprocamente, supongamos $|n| \leq |m|$, es decir, que existe una función inyectiva $n \to m$. Por el Lema 4.8, no puede ser $m \subset n$, es decir, no puede ser $m < n$. Como el orden de $\mathbb{N}$ es total, necesariamente $n \leq m$. □

Podemos ya dar entonces la siguiente:

Definición. Un *conjunto finito* es un conjunto equipotente a un número natural. En caso contrario, se dice que es un *conjunto infinito*. Si X es equipotente a n, diremos que X *tiene cardinal finito* n y escribiremos $|X| = n$.

Observación 4.10. Como un conjunto finito es biyectivo con un conjunto n, muchas veces bastará, a la hora de demostrar algo para conjuntos finitos, demostrarlo para los conjuntos n. Por ejemplo, el Lema 4.8 demuestra que, si X es un conjunto finito, no hay ninguna función inyectiva de X a un subconjunto propio $Y \subset X$. Una primera consecuencia de esto es que $\mathbb{N}$ es un conjunto infinito, ya que la función sucesor $S : \mathbb{N} \to \mathbb{N}$ tiene como recorrido el subconjunto propio $\mathbb{N} - \{0\}$ y es inyectiva (Ejercicio 2.32(iii) con $k = 1$).

Pasamos ahora a demostrar las principales propiedades de los conjuntos finitos. La primera es que los cardinales finitos son los menores que hay.

Teorema 4.11. *Si X es un conjunto tal que $|X| \leq n$ para algún $n \in \mathbb{N}$, entonces X es finito (en particular, los subconjuntos de conjuntos finitos son también finitos).*

Demostración: Si tenemos una función inyectiva $f : X \to n$, entonces $|X| = |f[X]|$. Basta demostrar entonces que, para todo $n \in \mathbb{N}$ se tiene que todo subconjunto $X \subseteq n$ es finito. Lo demostraremos por inducción, siendo trivial el caso $n = 0$ (ya que el único subconjunto de 0 es el vacío, que es finito). Si suponemos cierto el caso n, tomemos ahora $X \subseteq n + 1$. Distinguimos dos posibilidades:

–Si $n \notin X$, entonces $X \subseteq n$, y por hipótesis de inducción X es finito.

–Si $n \in X$, consideramos $X' = X - \{n\} \subseteq n$. Por hipótesis de inducción X es finito y, si escribimos $|X'| = m$, luego existe una biyección $f' : m \to X'$. Podemos definir entonces $f : m + 1 \to X$ mediante $f(k) = f'(k)$ si $k < m$ y $f(m) = n$. Entonces f es una biyección, lo que implica que X es finito. □

Teorema 4.12. *Si X es finito y $f : X \to Y$ es una función, entonces $|f[X]| \leq |X|$ (y por tanto $f[X]$ es también finito).*

Demostración: Podemos suponer (ver la Observación 4.10) que $X = n$. Por el Teorema 4.11, basta encontrar una función inyectiva $g : f[n] \to n$. La definimos simplemente mediante

$$g(y) = \min\{m \in n \mid f(m) = y\}.$$

Obsérvese que g está bien definida, porque $\mathbb{N}$ está bien ordenado y, para cada $y \in f[n]$ es evidente que el conjunto $\{m \in n \mid f(m) = y\}$ es no vacío. Además, g es inyectiva, porque $g(y) = m = g(y')$ implica, por la definición de g, $y = f(m) = y'$. □

Observación 4.13. El resultado anterior está diciendo entonces que, si X es finito, $|Y| \leq |X|$ es equivalente (salvo que Y sea el conjunto vacío) a que exista $f : X \to Y$ tal que $\mathrm{rec}(f) = Y$ (que $|Y| \leq |X|$ implica la existencia de f es el Ejercicio 4.4). El motivo por el que esto no se puede generalizar cuando X no es finito es que, aunque sepamos que para

cada $y \in f[X]$ exista algún $x \in X$ tal que $f(x) = y$, ¿como hacemos para elegir tal x de forma que la asignación $y \mapsto x$ sea una función? Recordemos que una función $g : Y \to X$ no es más que un cierto subconjunto de $\mathcal{P}(Y \times X)$, y que estamos siendo muy rigurosos a la hora de admitir qué es un conjunto. De hecho, g necesita de una definición precisa. Por eso, cuando X es un conjunto finito, y por tanto con una biyección prefijada con n, podemos dar una definición precisa de $g(y)$ tomando el mínimo del conjunto de los x cuya imagen es y (es claro que el truco se puede generalizar a cualquier conjunto X que esté bien ordenado). En un caso más general, admitir que podemos admitir como función una g que "elija" para cada y un elemento x es lo que llamaremos Axioma de Elección.

Lema 4.14. *Sean X, Y dos conjuntos finitos. Entonces*

$$|X \cup Y| \leq |X| + |Y|$$

(y en particular $X \cup Y$ es finito), y se da la igualdad si $X \cap Y = \emptyset$.

Demostración: Si llamamos $m = |X|$ y $n = |Y|$, entonces tenemos biyecciones $f : m \to X$ y $g : n \to Y$. Definimos entonces $h : n + m \to X \cup Y$ mediante

$$h(k) = \begin{cases} f(k) & \text{si } k \in m \\ g(k - m) & \text{si } k \in (m + n) - m \end{cases}$$

Es claro que el recorrido de h es $X \cup Y$, luego por el Teorema se tiene $|X \cup Y| \leq m + n$. Además, si $X \cap Y = \emptyset$, la función h es biyectiva, con lo que se tiene la igualdad. □

Teorema 4.15. *La unión finita de conjuntos finitos es finita. Además, si los conjuntos son disjuntos dos a dos, entonces el cardinal de la unión es la suma de los cardinales.*

Demostración: Si S es un conjunto finito de conjuntos finitos, podemos tomar una biyección $f : n \to S$. Escribiremos $f(n) = X_n$, que será un conjunto finito. Haremos la demostración por inducción sobre n. Si $n = 0$, entonces $\bigcup S = \emptyset$, que es finito y tiene cardinal 0 (que por convenio decimos que es la suma de cero sumandos).

Supongamos que ahora tenemos una biyección $f : n + 1 \to S$ con cada $f(i) = X_i$ un conjunto finito. Por hipótesis de inducción, $\bigcup f[n]$ (es decir, $\bigcup_{i<n} X_i$) es un conjunto finito, luego por el Lema 4.14 el conjunto $\bigcup S = (\bigcup f[n]) \cup X_n$ es finito. Además, decir que los elementos de S son disjuntos dos a dos es equivalente a

(i) $\bigcup f[n]$ y X_n son disjuntos: luego por el Lema 4.14 el cardinal de $\bigcup S = (\bigcup f[n]) \cup X_n$ es $|\bigcup f[n]| + |X_n|$;

(ii) y los elementos de $f[n]$ son disjuntos dos a dos: luego por hipóteis de inducción $|\bigcup f[n]| = \sum_{i<n} |X_i|$.

Poniendo juntas ambas cosas, se concluye $|\bigcup S| = \sum_{i<n+1} |X_i|$. □

De forma más sencilla se ve el cardinal del producto y del conjunto potencia, y se ve mejor el motivo de la definición inductiva del producto y potencia de números naturales:

Teorema 4.16. *Si X, Y son conjuntos finitos, entonces $X \times Y$ es finito y $|X \times Y| = |X| \cdot |Y|$.*

Demostración: Podemos suponer $X = m$ e $Y = n$, así que hay que demostrar $|m \times n| = mn$ (ver Ejercicio 4.3(ii)). Lo demostraremos por inducción sobre n. El caso $n = 0$ es trivial, ya que $m \times 0$ es el conjunto vacío, y por la definición inductiva de producto se tiene $m \cdot 0 = 0$.

Supongamos ahora $|m \times n| = mn$ y veamos $|m \times (n+1)| = m(n+1)$. Escribiendo $n + 1 = n \cup \{n\}$, que es una unión disjunta, se tiene $m \times (n+1) = (m \times n) \cup (m \times \{n\})$, que es también una unión disjunta. Por el Teorema 4.14, se tiene

$$|m \times (n+1)| = |m \times n| + |m \times \{n\}|.$$

Por hipótesis de inducción, el primer sumando es mn, mientras que claramente $|m \times \{n\}| = m$, ya que existe una biyección $m \times \{n\} \to m$ mandando (k, n) a k. Por tanto, $|m \times (n+1)| = mn + m$ que, por la definición inductiva de producto, es precisamente $m(n+1)$. □

Teorema 4.17. *Si X, Y son conjuntos finitos, entonces X^Y es finito y $|X^Y| = |X|^{|Y|}$.*

Demostración: Como en el teorema anterior, usando el Ejercicio 4.3(iii), basta demostrar $|m^n| = m^n$, lo que haremos de nuevo por inducción sobre n. Para $n = 0$, la única función del conjunto vacío en m el la función vacía, luego $|m^0| = 1$, que es precisamente m^0 por la definición inductiva de la exponenciación.

Supuesto ahora $|m^n| = m^n$, veamos $|m^{n+1}| = m^{n+1}$. Para ver eso, observemos que existe una biyección $m^{n+1} \to m^n \times m$ que manda cada $f : n + 1 \to m$ al par $(f \restriction n, f(n))$. Por tanto, por el Teorema 4.16, se tiene $|m^{n+1}| = m^n m$ que, por la definición inductiva de la exponenciación, es precisamente m^{n+1}. □

Corolario 4.18. *Si X es un conjunto finito, entonces $\mathcal{P}(X)$ es un conjunto finito, y además $|\mathcal{P}(X)| = 2^{|X|}$.*

Demostración: Sabemos por el Teorema de Cantor (Teorema 4.7) que $|\mathcal{P}(X)| = |2^X|$ y, por el Teorema 4.17 se tiene $|2^X| = 2^{|X|}$. □

El siguiente resultado indica que cada conjunto infinito es comparable con cada conjunto finito (y de la forma natural, es decir, que el cardinal de los infinitos es mayor que el de los finitos). Esto da un primer indicio de que los cardinales de conjuntos pueden formar un conjunto totalmente ordenado.

Teorema 4.19. *Si X es un conjunto infinito, entonces para cada $n \in \mathbb{N}$ se tiene $|X| > n$.*

Demostración: Por definición de conjunto infinito, no puede de $|X| = n$, así que basta demostrar $|X| \geq n$. Lo demostramos por inducción sobre n, siendo trivial el caso $n = 0$ (ya que $\emptyset \subseteq X$). Si suponemos ahora $|X| \geq n$, esto quiere decir que existe una función inyectiva $f : n \to X$. Como no puede ser biyectiva, existe $x \in X$ que no está en la imagen de f. Podemos definir entonces $f' : n+1 \to X$ como $f' = f \cup \{(n, x)\}$, que es claramente inyectiva, luego $|X| \geq n + 1$. □

En la demostración uno podría estar tentado a pegar todas las funciones $n \to X$ para obtener una función inyectiva $f : \mathbb{N} \to X$. De nuevo, esto no es posible sin el Axioma de Elección. Por tanto, no podemos decir que el cardinal de $\mathbb{N}$ sea el cardinal infinito más pequeño. De momento, vamos a dar un nombre a tal cardinal:

Definición. Diremos que un conjunto X es numerable si es equipotente con $\mathbb{N}$. Escribiremos $|X| = \aleph_0$.

El siguiente enunciado dice que entre los cardinales finitos y $\aleph_0$ no hay más cardinales (luego si los cardinales estuvieran totalmente ordenados, $\aleph_0$ sería el menor cardinal infinito):

Teorema 4.20. *Si $|X| \leq \aleph_0$, entonces o bien X es numerable o bien es finito.*

Demostración: Como $|X| \leq \aleph_0$, existe una función inyectiva $f : X \to \mathbb{N}$. Si llamamos X' a la imagen de f, basta ver que X' es finito o numerable. Suponemos por tanto que X' no es finito, y construyamos $h : \mathbb{N} \to X'$ por recurrencia. Concretamente, definiremos $h(n+1) = \min(X' - h[n])$ (obsérvese que, como X' no es finito, no puede ser $h[n] = X'$). Claramente h es inyectiva y, aunque tampoco es difícil demostrar que es biyectiva, de la inyectividad sacamos ya $\aleph_0 \leq |X'|$. Como por otra parte tenemos $|X'| \leq \aleph_0$, se sigue del Teorema de Cantor-Bernstein que $|X'| = \aleph_0$ □

Teorema 4.21. *Sea $f : X \to Y$ una función entre conjuntos. Entonces, si $|X| = \aleph_0$, se tiene $|f[X]| \leq \aleph_0$.*

Demostración: Imitamos la demostración del Teorema 4.12 para el caso finito, empezando por suponer $X = \mathbb{N}$. Construimos $h : f[\mathbb{N}] \to \mathbb{N}$ mediante $h(y) = \min\{n \in \mathbb{N} \mid f(n) = y\}$. Como h es claramente inyectiva, se concluye el resultado. □

Teorema 4.22. *La unión finita (no vacía) de conjuntos numerables es numerable.*

Demostración: Aquí imitaremos la demostración del Teorema 4.15, es decir, basta demostrarlo para la unión de dos conjuntos, haciéndose el resto por inducción. Sean entonces

X, Y conjuntos con biyecciones $f : \mathbb{N} \to X$ y $g : \mathbb{N} \to Y$. Definimos $h : \mathbb{N} \to X \cup Y$ como

$$h(n) = \begin{cases} f(k) & \text{si } n = 2k \\ g(k) & \text{si } n = 2k+1 \end{cases}$$

cuyo recorrido es claramente $X \cup Y$. Por el Teorema 4.21, $|X \cup Y| \leq \aleph_0$. Por tanto, por el Teorema 4.20, o bien $X \cup Y$ es finito (lo que es absurdo, ya que contiene a X, que es infinito) o bien $|X \cup Y| = \aleph_0$, como queríamos. □

Corolario 4.23. *El conjunto $\mathbb{Z}$ de los números enteros es numerable.*

Demostración: Basta escribir $\mathbb{Z} = \mathbb{N} \cup \mathbb{Z}_-$, donde $\mathbb{Z}_- = \{a \in \mathbb{Z} \mid a < 0\}$. Como $f : \mathbb{N} \to \mathbb{Z}_-$ definida por $f(n) = -1 - n$ es una biyección, se tiene que $\mathbb{Z}$ es la unión de dos conjuntos numerables, y por tanto numerable por el Teorema 4.22. □

Teorema 4.24. *Si X, Y son conjuntos numerables, entonces $X \times Y$ es también numerable.*

Demostración: Basta encontrar una biyección $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. La definimos como $f(m, n) = 2^m(2n + 1) - 1$. Es una biyección ya que, para cada $a \in \mathbb{N}$, el número $a + 1$ factoriza, de forma única, como producto de una potencia de 2 por un número impar. □

Corolario 4.25. *El producto cartesiano de una cantidad finita no vacía de conjuntos numerables es numerable.*

Demostración: Basta hacerlo por inducción sobre el número de factores usando el Teorema 4.24. □

Corolario 4.26. *El conjunto $\mathbb{Q}$ de los números racionales es numerable.*

Demostración: Claramente $\aleph_0 \leq |\mathbb{Q}|$, ya que $\mathbb{N} \subseteq \mathbb{Q}$. Por otra parte, tenemos la función $\mathbb{Z} \times (\mathbb{Z} - \{0\}) \to \mathbb{Q}$ que manda (m, n) a $\frac{m}{n}$, cuyo recorrido es $\mathbb{Q}$. Como $\mathbb{N} \subseteq \mathbb{Z} - \{0\} \subseteq \mathbb{Z}$ y $|\mathbb{N}| = |\mathbb{Z}| = \aleph_0$, se sigue del Teorema de Cantor-Bernstein que $\mathbb{Z} - \{0\}$ es numerable (también es fácil demostrarlo a mano), luego por el Teorema 4.24 el producto $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ es numerable. Se sigue entonces del Teorema 4.21 que $|\mathbb{Q}| \leq \aleph_0$, luego, por el Teorema de Cantor-Bernstein $|\mathbb{Q}| = \aleph_0$. □

Observación 4.27. El lector puede preguntarse por qué no hemos dicho hasta ahora nada de uniones numerables de conjuntos. El motivo es que, incluso para la unión de una cantidad numerable de conjuntos de dos elementos no se puede decir nada sin el Axioma de Elección. En efecto, si $\{X_n\}$ es una colección de conjuntos de dos elementos, el

escribirlos de la forma $X_n = \{a_n, b_n\}$ (lo que permitiría numerarlos fácilmente como unión de dos conjuntos a lo más numerables, $\{a_n\}$ y $\{b_n\}$) supone ya hacer, para cada $n \in \mathbb{N}$, una elección para escoger, de cada conjunto X_n, quién hace el papel de a_n. Por tanto, para obtener resultados sobre unión numerable de conjuntos hace falta que los conjuntos "vengan ya numerados".

Teorema 4.28. *Sea $\{X_n\}$ una colección de conjuntos numerables para los que existe una función $h : \mathbb{N} \to (\bigcup_{n\in\mathbb{N}} X_n)^{\mathbb{N}}$ de forma que cada h_n sea una biyección $\mathbb{N} \to X_n$. Entonces $\bigcup_{n\in\mathbb{N}} X_n$ es numerable.*

Demostración: La función h es equivalente, por el Ejercicio 1.22, a una función $\mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} X_n$, cuyo recorrido es claramente $\bigcup_{n\in\mathbb{N}} X_n$. Por el Teorema 4.21, se tendrá entonces $|\bigcup_{n\in\mathbb{N}} X_n| \leq \aleph_0$. Por otra parte, como $X_0 \subset \bigcup_{n\in\mathbb{N}} X_n$, se sigue $\aleph_0 \leq |\bigcup_{n\in\mathbb{N}} X_n|$, y el resultado se sigue del Teorema de Cantor-Bernstein. □

Teorema 4.29. *Si X es numerable, el conjunto $Suc(X)$ es numerable.*

Demostración: Bastará demostrar que $\mathrm{Suc}(\mathbb{N})$ es numerable. Para ello observamos primero que $\mathrm{Suc}(\mathbb{N}) = \bigcup_{n\in\mathbb{N}} \mathbb{N}^n$. Como $\mathbb{N}^0$ tiene un solo elemento (la sucesión vacía), es claro que basta ver que $\bigcup_{n>0} \mathbb{N}^n$ es numerable. Claramente, cada $\mathbb{N}^n$ es numerable (ya que es equipotente con el producto cartesiano n veces de $\mathbb{N}$), luego por el Teorema 4.28 bastará precisar una numeración de cada $\mathbb{N}^n$. Para ello fijamos una biyección $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ (que existe por el Teorema 4.24) y escribiremos, para cada $m \in \mathbb{N}$, $g(m) = (m_1, m_2)$. Entonces definimos por recurrencia biyecciones $h_n : \mathbb{N} \to \mathbb{N}^n$ para cada $n > 0$ de la siguiente forma (cada sucesión de n elementos la escribiremos como $< a_0, \ldots, a_{n-1} >$):

$$h_1(m) =< m >$$

$$h_{n+1}(m) =< h_n(m_1), m_2 > .$$

Se comprueba fácilemente por inducción que las funciones h_n son biyecciones, lo que concluye la demostración. □

Corolario 4.30. *Si X es numerable, el conjunto de subconjuntos finitos de X es numerable.*

Demostración: Como el recorrido de la función inyectiva $X \to \mathcal{P}(X)$ definida por $x \mapsto \{x\}$ está contenido en el conjunto de subconjuntos finitos de X, el cardinal de tal conjunto es mayor o igual que $\aleph_0$. Por otra parte, la función $\mathrm{Suc}(X) \to \mathcal{P}(X)$ que asocia a cada sucesión finita su recorrido tiene como recorrido el conjunto de conjuntos finitos de $\mathcal{P}(X)$,

luego, por los Teoremas 4.29 y 4.21, tal conjunto es a lo más numerable. El Teorema de Cantor-Bernstein termina la demostración. □

Teorema 4.31. *Dos conjuntos cualesquiera numerables, totalmente ordenados, densos y sin extremos son necesariamente isomorfos. En particular, cada conjunto totalmente ordenado denso y sin extremos que sea numerable es isomorfo a* $\mathbb{Q}$.

Demostración: Sean X, Y conjuntos numerables, totalmente ordenados, densos y sin extremos. Si $x : \mathbb{N} \to X$ e $y : \mathbb{N} \to Y$ son biyecciones, escribiremos $x(n) = x_n$ e $y(n) = y_n$. Dado que no hay peligro de confusión escribiremos $\leq$ tanto para el orden de X como para el orden de Y. Construyamos por recurrencia funciones h_n inyectivas tales que:

(i) $h_0 = \emptyset$.

(ii) $\mathrm{dom}(h_n)$ es finito y $\{x_0, \ldots, x_{n-1}\} = x[n] \subseteq \mathrm{dom}(h_n) \subseteq X$.

(iii) $\{y_0, \ldots, y_{n-1}\} = y[n] \subseteq \mathrm{Im}(h_n) \subseteq Y$.

(iv) $h_{n+1} \restriction \mathrm{dom}(h_n) = h_n$.

(v) Para cada $x, x' \in \mathrm{dom}(h_n)$ se tiene $x < x'$ si y sólo si $h_n(x) < h_n(x')$.

(con lo que es claro entonces que $h = \bigcup_{n\in\mathbb{N}} h_n$ será el isomorfismo buscado).

Nótese que, para usar la recurrencia, no basta demostrar que existe h_{n+1} supuesto que existe h_n (eso sería usar el Axioma de Elección), sino que debemos dar una definición precisa de cómo construir h_{n+1} a partir de h_n. Procedemos de la siguiente forma:

–Si x_n está en el dominio de h_n, entonces definimos $h'_n = h_n$. Si en cambio x_n no está en el dominio de h_n, entonces nos fijamos en qué lugar ocupa entre los elementos de $\mathrm{dom}(h_n)$ (si es menor que todos ellos, está entre dos consecutivos de ellos o es mayor que todos ellos). Como Y es denso y no tiene extremos, existirá algún elemento de Y que ocupe el mismo lugar que x_n respecto de las imágenes de los elementos de $\mathrm{dom}(h_n)$. Definimos y'_n como $y'_n = y_m$, donde m es el mínimo natural tal que y_m está en dicha posición. Definimos entonces $h'_n = h_n \cup \{(x_n, y'_n)\}$.

–Análogamente, si y_n está en la imagen de h_n, definimos $h_{n+1} = h'_n$. Si en cambio y_n no está en la imagen de h_n, nos fijamos en qué lugar ocupa entre los elementos de $\mathrm{Im}(h_n)$. Como antes, al ser X denso y sin extremos, podemos encontrar $x'_n = x_l$, donde l es el mínimo natural tal que x_l está en la misma posición respecto de los elementos del dominio de h_n. Definimos entonces $h_{n+1} = h'_n \cup \{(x'_n, y_n)\}$. □

Observación 4.32. La mitad de la demostración anterior (tomando en la recurrencia como h_{n+1} la función h') muestra que, si X, Y son conjuntos numerables totalmente ordenados e Y es denso y sin extremos, entonces existe una función inyectiva $h : X \to Y$ tal que $x < y$ si y sólo si $h(x) < h(y)$.

Un corolario inmediato del teorema es el siguiente:

Corolario 4.33. *El conjunto $\mathbb{R}$ de los números reales no es numerable.*

Demostración: Si lo fuera, como es totalmente ordenado, denso y sin extremos, tendría que ser isomorfo a $\mathbb{Q}$. Pero esto es imposible, ya que $\mathbb{R}$ es completo y $\mathbb{Q}$ no. □

El cardinal preciso de $\mathbb{R}$ viene dado por el siguiente resultado:

Teorema 4.34. $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}|$.

Demostración: Por la definición de $\mathbb{R}$ como el conjunto de cortes de Dedekind de $\mathbb{Q}$, tenemos una inclusión $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, luego $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})|$ y, como $|\mathbb{N}| = |\mathbb{Q}|$, se sigue del Ejercicio 4.3(v) que $|\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$, es decir, que tenemos $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$.

Por otra parte, el Ejercicio 3.17 muestra $|2^{\mathbb{N}}| \leq |\mathbb{R}|$. Como $|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}|$ por el Teorema 4.2, el Teorema de Cantor-Bernstein concluye el resultado. □

Notación. A la vista del resultado anterior, escribiremos $2^{\aleph_0}$ para indicar el cardinal de $\mathbb{R}$, y lo llamaremos *cardinal del continuo*.

Finalizamos con la caracterización de $\mathbb{R}$ a partir de su orden:

Teorema 4.35. *Sea X un conjunto totalmente ordenado, completo y sin extremos. Entonces, si X contiene un conjunto numerable $Y \subseteq X$ denso, necesariamente X es isomorfo a $\mathbb{R}$.*

Demostración: Veamos primero que Y no tiene extremos. En efecto, para cada $y \in Y$, como X no tiene extremos, existen $x_1, x_2 \in X$ tales que $x_1 < y < x_2$; y como Y es denso en X, entonces existen $y_1, y_2 \in Y$ tales que $x_1 < y_1 < y < y_2 < x_2$.

Podemos aplicar entonces el Teorema 4.31 para concluir que Y es isomorfo a $\mathbb{Q}$. Por otra parte, como X es una compleción de Y, entonces es isomorfo a una compleción de $\mathbb{R}$. Por el Teorema 3.16, se sigue que X es isomorfo a $\mathbb{R}$. □

5. Números ordinales e inducción transfinita

Recordemos que cada número natural n estaba definido como el conjunto de los números naturales anteriores, y que por tanto, el número natural sucesivo $S(n) = n + 1$ estaba definido como $S(n) = n \cup \{n\}$. Dado que parece que el "primer número después de todos los naturales" es $\mathbb{N}$, podemos darle un nombre, por ejemplo ω, y continuar definiendo sucesivos $S(\omega) = \omega + 1 = \omega \cup \{\omega\} = \{0, 1, \ldots, \omega\}$ y así sucesivamente.

Nótese que de esta forma obtenemos nuevos conjuntos bien ordenados (lo que es clave para argumentos de inducción), pero que ya no son isomorfos a $\mathbb{N}$ (por ejemplo, ω no tiene un elemento precedente). De hecho, dos cualesquiera de estos conjuntos no son nunca isomorfos, y demostraremos que cada conjunto bien ordenado es isomorfo exactamente a uno de ellos. Empezamos primero con la definición precisa de los números que queremos considerar:

Definición. Un conjunto X se dice que es *transitivo* si cada elemento de X es un subconjunto de X. En otras palabras, para cada $x \in X$ se tiene que, si $y \in x$, entonces $y \in X$ (de ahí el nombre de "transitivo"). Un *número ordinal* (o simplemente un *ordinal*) es un conjunto transitivo para el que la relación "$y < x$ si y sólo si $y \in x$" define una relación de buen orden.

Ejemplo 5.1. Cada número natural (incluido el 0, es decir, el conjunto vacío) es un ordinal, y también $\mathbb{N}$ es un ordinal. Cuando nos refiramos a $\mathbb{N}$ como ordinal escribiremos ω (en general, denotaremos a los ordinales por letra minúsculas griegas). Nótese que un conjunto como $\{0, 1, 3, 4\}$ no es un ordinal, ya que $3 \in \{0, 1, 3, 4\}$, pero $3 \not\subset \{0, 1, 3, 4\}$, ya que $3 = \{0, 1, 2\}$.

Observación 5.2. Que la relación $<$ defina un buen orden en un ordinal α quiere decir en primer lugar que es un orden estricto. Por tanto, se tiene la propiedad asimétrica, y en particular no puede existir ningún $x \in \alpha$ tal que $x < x$ (en particular $\alpha \notin \alpha$). Además, por cómo está definido el orden, se sigue que para cada $x \in \alpha$ se tiene $x = \{y \in \alpha \mid y < x\}$, es decir, x es el segmento inicial A_x del conjunto α (recordemos del Lema 3.10 que todos los segmentos iniciales de un conjunto bien ordenado son de esta forma).

Volvemos de nuevo a la necesidad de estudiar segmentos iniciales, pero esta vez en un contexto distinto, ya que en la sección 3 nos interesaban para conjuntos densos, mientras que ahora nos interesan para conjuntos bien ordenados:

Ejercicio 5.3. Sea X totalmente ordenado, denso y con al menos dos elementos. Demostrar que X no está bien ordenado.

Veamos en primer lugar que el hecho de ser un conjunto bien ordenado es muy rígido:

Lema 5.4. *Sea X un conjunto bien ordenado. Entonces:*

(i) Si $f : X \to X$ satisface que $x_1 < x_2$ implica $f(x_1) < f(x_2)$, entonces $f(x) \geq x$ para todo $x \in X$.

(ii) X no es isomorfo a ningún segmento inicial suyo.

(iii) El único isomorfismo $X \to X$ es la identidad.

(iv) Para cada conjunto bien ordenado X', existe como mucho un isomorfismo $X \to X'$.

Demostración: Para demostrar (i), sea $S = \{x \in X \mid f(x) < x\}$, y queremos ver $S = \emptyset$. Si S fuera no vacío, tendría mínimo x. En particular $f(x) < x$ y, por la propiedad de f, también $f(f(x)) < f(x)$. Pero esto es absurdo, porque entonces $f(x) \in S$ y es menor que el mínimo x de S.

Si existiera un isomorfismo $f : X \to A_x$ para algún $x \in X$, entonces $f(x) \in A_x$, por lo que $f(x) < x$, lo que contradice (i). Esto prueba (ii).

Para ver (iii), sea $f : X \to X$ un isomorfismo. Por tanto, tanto f como f^{-1} satisfacen la hipótesis de (i). Entonces, para cualquier $x \in X$ la propiedad (i) aplicada a f^{-1} implica $f^{-1}(x) \geq x$, y si aplicamos ahora f a esa desigualdad tendríamos $x \geq f(x)$. Pero como por (i) también se tiene $f(x) \geq x$, se sigue que $f(x) = x$, luego f es la identidad.

Finalmente (iv) se sigue de (iii), ya que si $f, g : X \to Y$ son dos isomorfismos, entonces $g^{-1} \circ f$ es un isomorfismo de X en X, luego es la identidad. Por tanto, $f = g$. □

De lo anterior obtenemos ya el primer resultado relevante sobre conjuntos bien ordenados (básicamente que dos conjuntos bien ordenados son siempre comparables):

Teorema 5.5. *Sean X, Y dos conjuntos bien ordenados. Entonces ocurre exactamente una de las siguientes posibilidades:*

(i) X e Y son isomorfos.

(ii) X es isomorfo a un segmento inicial de Y.

(iii) Y es isomorfo a un segmento inicial de X.

Además, el isomorfismo es único.

Demostración: Está claro por el Corolario que las tres posibilidades son excluyentes dos a dos y que el isomorfismo es único. Veamos entonces que se da alguna de las tres posibilidades. Para ello, definimos

$$f := \{(x, y) \in X \times Y \mid A_x \text{ es isomorfo a } A_y\}$$

y veamos que define el isomorfismo buscado. Observemos primero que tanto f como f^{-1} son funciones inyectivas (luego f define un isomorfismo entre su dominio y su recorrido).

Por simetría, bastará ver que $(x,y),(x,y') \in f$ implica $y = y'$. En efecto, si A_x es isomorfo tanto a A_y como a $A_{y'}$, entonces A_y y $A_{y'}$ son isomorfos. Como Y está totalmente ordenado, o bien $y = y'$, o bien $y < y'$ o bien $y' < y$. Pero los dos últimos casos son imposibles, ya que si, por ejemplo, $y < y'$, entonces A_y es un segmento inicial de $A_{y'}$, luego ambos no pueden ser isomorfos por el Corolario 5.4.

Veamos además que f conserva el orden. Para ello, dados $x < x'$, sean $y = f(x)$, $y' = f(x'))$ y veamos que $y < y'$. Como $(x,y),(x',y') \in f$, existen isomorfismos $A_x \to A_y$ y $h : A_{x'} \to A_{y'}$. Restringiendo h a A_x (nótese que $A_x \subset A_{x'}$, pues $x < x'$) tenemos un isomorfismo $A_x \to A_{h(x)}$. Por tanto A_y y $A_{h(x)}$ son isomorfos, por lo que necesariamente $h(x) = y$. Como $\mathrm{rec}(h) \subseteq A_{y'}$ se sigue $y \in A_{y'}$, es decir, $y < y'$, como queríamos.

Observemos además que, si $x \in \mathrm{dom}(f)$, entonces existe un isomorfismo $h : A_x \to A_y$ para algún $y \in Y$. Por tanto, para todo $x' < x$ la restricción de h define un isomorfismo entre $A_{x'}$ y $A_{h(x')}$, con lo que también x' está en el dominio de f. De forma análoga se demuestra que, si y está en el recorrido de f, entonces también lo está cualquier $y' < y$. Estas propiedades indican que el dominio y el recorrido de f o son propios o son segmentos iniciales. Como f define un isomorfismo entre su dominio y su recorrido, el teorema quedará probado si demostramos que no puede ocurrir que tanto el dominio como el recorrido de f sean subconjuntos propios de X e Y, respectivamente. Si fuera así, por el Lema 3.10, existirían $x \in X$ e $y \in Y$ tales que A_x es el dominio de f y A_y es el recorrido de f. Por tanto, f sería un isomorfismo entre A_x y A_y, lo que implica, por definición, $(x,y) \in f$. Pero entonces x estaría en el dominio de f, lo que es absurdo, ya que $x \notin A_x$. □

Nuestro objetivo ahora es ver que los números ordinales sirven como representantes de los conjuntos bien ordenados. Para ello vamos a estudiar en profundidad sus propiedades.

Lema 5.6. *Si α es un ordinal, entonces $S(\alpha) = \alpha \cup \{\alpha\}$ es también un ordinal (que denoteremos a menudo como $\alpha + 1$).*

Demostración: Claramente $S(\alpha)$ es transitivo, ya que sus elementos son o bien elementos de α (que son subconjuntos de α y por tanto subconjuntos de $S(\alpha)$) o bien α, que también es un subconjunto de $S(\alpha)$. Además, como $\beta < \alpha$ para todo $\beta \in \alpha$ (recuérdese que $\alpha \notin \alpha$), se sigue inmediatamente que $S(\alpha)$ está bien ordenado (ver Ejercicio 2.14). □

Lema 5.7. *Cada elemento de un ordinal es un ordinal.*

Demostración: Sea α un ordinal y sea $x \in \alpha$. Entonces, como subconjunto de α, será $x = A_x$. Por tanto, x es transitivo, ya que para cada $y \in x$, se tendrá que y es un elemento de α, es decir un segmento inicial A_y, que es un subconjunto de A_x (ya que $y < x$ por ser $y \in x$).

Para ver que el orden en x (dado por la pertenencia) es un buen orden basta ver que es la restricción del orden en α. Pero esto es evidente, porque dados $y, z \in x$, decir $y < z$ como elementos de x es equivalente a decir que y es un elemento de z, que el lo mismo que decir $y < z$ como elementos de α. □

El lema anterior nos dice entonces que los elementos de un ordinal β son ordinales (que además, como subconjuntos, están estrictamente contenidos en β, ya que sabemos que $\beta \notin \beta$). El siguiente resultado nos dice que el recíproco es cierto, en el sentido de que todos los ordinales contenidos propiamente en β son elementos de β:

Lema 5.8. *Si α, β son ordinales, entonces $\alpha \subset \beta$ si y sólo si $\alpha \in \beta$ (por tanto, un número ordinal es el conjunto formado por todos sus subconjuntos propios que son números ordinales).*

Demostración: Supongamos $\alpha \subset \beta$ es decir, $\beta - \alpha \neq \emptyset$, que tendrá un primer elemento γ, por ser β un conjunto bien ordenado. Veamos que $\gamma = \alpha$, lo que terminará la demostración (ya que $\gamma \in \beta$). Veamos el doble contenido como subconjuntos de β:

Por una parte, sea $x \in \gamma$, es decir, $x < \gamma$. Como γ era mínimo en $\beta - \alpha$, necesariamente $x \in \alpha$.

Por otra parte, si $x \in \alpha$, no puede ser $\gamma \leq x$ porque entonces o bien $\gamma = x$ (luego $\gamma = x \in \alpha$) o bien $\gamma < x$ (luego $\gamma \in x$, y por la transitividad de α se tendrá $\gamma \in \alpha$), lo que es absurdo porque γ no está en α. Entonces, por ser el orden total, necesariamente $x < \gamma$, es decir, $x \in \gamma$. □

Observación 5.9. El lema anterior ya nos está diciendo que los números ordinales tienen el aspecto que dábamos al principio de la sección. En efecto, si un ordinal α es distinto del vacío, entonces se tiene $\emptyset \subset \alpha$, luego $0 = \emptyset \in \alpha$. Por tanto, tendremos, $1 = \{0\} \subseteq \alpha$, de donde se deduce que o bien $\alpha = \{0\} = 1$ o bien $1 = \{0\} \subset \alpha$. En este segundo caso tendremos, aplicando de nuevo el lema, $1 \in \alpha$, luego $2 = \{0, 1\} \subseteq \alpha$. Reiterando este proceso, se llegaría a que o bien α es un número natural o bien todos los naturales están en α. En este segundo caso, $\omega \subseteq \alpha$, luego podemos seguir el argumento concluyendo que o bien $\alpha = \omega$ o bien $\omega \subset \alpha$, luego $\omega \in \alpha$, es decir, $\omega + 1 \subseteq \alpha$. Más adelante veremos el modo riguroso de cómo hacer un proceso de recurrencia de este estilo.

Lo que vamos a hacer ahora es tratar a los números ordinales como si formaran un conjunto. En tal supuesto conjunto podemos definir un orden mediante $\alpha < \beta$ si y sólo si $\alpha \in \beta$ (que por el Lema 5.8 es equivalente a $\alpha \subset \beta$). Definimos también $\alpha \leq \beta$ si y sólo si $\alpha < \beta$ o $\alpha = \beta$ (lo que ahora es equivalente a $\alpha \subseteq \beta$). Veamos que con este orden los números ordinales se comportan como un conjunto bien ordenado, excepto por el hecho

de no formar un conjunto (de hecho la propiedad (v) siguiente demuestra que no existe el conjunto de todos los ordinales):

Teorema 5.10. *Si α, β, γ son ordinales, entonces:*

(i) $\alpha < \beta$ *y* $\beta < \gamma$ *implica* $\alpha < \gamma$.

(ii) Si $\alpha < \beta$, *entonces* $\beta \not< \alpha$.

(iii) O bien $\alpha \leq \beta$, *o bien* $\beta \leq \alpha$.

(iv) Si S es una colección (no necesariamente un conjunto) no vacía de ordinales, entonces existe el "mínimo" de S, es decir un σ de S tal que $\sigma \leq \sigma'$ para todo σ' de S.

(v) Si X es un conjunto de ordinales, entonces $\alpha = \bigcup X$ es el "supremo" de X, es decir, es un ordinal tal que $\beta \leq \alpha$ para todo $\beta \in X$ (luego en particular el ordinal $\alpha + 1$ no puede estar en X), y es el mínimo entre los ordinales α' tales que $\beta \leq \alpha'$ para todo $\beta \in X$.

Demostración: La parte (i) es la transitividad del conjunto γ, mientras que la parte (ii) sigue de (i), ya que si fuera $\alpha < \beta < \alpha$ entonces $\alpha < \alpha$. Estas dos propiedades son también consecuencia del Lema 5.8.

Para la parte (iii), consideramos $\alpha \cap \beta$, que se demuestra inmediatamente que es un ordinal. Como, por la Observación 5.2, no puede ser $\alpha \cap \beta \in \alpha \cap \beta$, entonces o bien $\alpha \cap \beta \notin \alpha$ o bien $\alpha \cap \beta \notin \beta$. Usamos ahora la caracterización del Lema 5.8. Si, por ejemplo, $\alpha \cap \beta \notin \alpha$, es decir, $\alpha \cap \beta \not\subset \alpha$, como claramente $\alpha \cap \beta \subseteq \alpha$, se deduce $\alpha \cap \beta = \alpha$, luego $\alpha \subseteq \beta$, es decir, $\alpha \leq \beta$. De forma simétrica, $\alpha \cap \beta \notin \beta$ llevaría a $\beta \leq \alpha$.

Demostramos ahora (iv). Fijamos en primer lugar un σ_0 de S. Entonces, por el Axioma de Separación, ya es un conjunto $S' = \{\sigma' \in \sigma_0 \mid \sigma \text{ está en } S\}$. Distinguiremos dos casos. Si $S' = \emptyset$, para cada $\sigma' \in S$ se tiene $\sigma' \notin \sigma_0$, es decir, $\sigma' \not< \sigma_0$, luego por (iii) será $\sigma_0 \leq \sigma'$; entonces $\sigma = \sigma_0$ cumple la condición buscada. Si en cambio $S' \neq \emptyset$, entonces el buen orden de σ_0 implica que S' tiene un primer elemento σ (y necesariamente $\sigma < \sigma_0$, por ser $\sigma \in \sigma_0$). Veamos que éste es el σ buscado. En efecto, dado σ' de S, o bien $\sigma' \in \sigma_0$ (y por tanto $\sigma \leq \sigma'$ por la minimalidad de σ y ser $\sigma' \in S'$) o bien $\sigma' \notin \sigma_0$ (y por tanto $\sigma_0 \leq \sigma'$, como antes, lo que junto a $\sigma < \sigma_0$ implica $\sigma < \sigma'$).

Finalmente, para demostrar (v), observamos que $\alpha = \bigcup X$ es un conjunto claramente transitivo(*). Además, sus elementos son ordinales por el Lema 5.7, luego por (iii) y (iv), está bien ordenado, y por tanto es un ordinal. Veamos para terminar que α es el "supremo" de X. En primer lugar, si $\beta \in X$, entonces por la definición de α se tendrá $\beta \subset \alpha$, es decir, $\beta \leq \alpha$. Y por otra parte, ningún $\alpha' < \alpha$ puede ser cota superior de X, ya que al

(*) Para toda esta demostración, piénsese en el ejemplo $X = \{1, 2, 4\}$. Entonces $\bigcup X = 1 \cup 2 \cup 4 = 4 = \{0, 1, 2, 3\}$. Mientras que $4 \in X$, sin embargo $4 + 1 = 5 \notin X$

ser $\alpha' \in \alpha = \bigcup X$, se tendrá $\alpha' \in \beta$ (que es equivalente a $\alpha' < \beta$) para algún $\beta \in X$. Por tanto, ningún α' que satisfaga $\beta \leq \alpha'$ para todo $\beta \in X$ puede satisfacer $\alpha' < \alpha$, y por (iii) será entonces $\alpha \leq \alpha'$. □

Teorema 5.11. *Los números naturales son exactamente los ordinales finitos.*

Demostración: Ya sabemos (Ejemplo 5.1) que cada número natural es un ordinal y es finito. Así que tenemos que ver que un ordinal finito es necesariamente un número natural. Para ello, veamos que, si un ordinal α no es natural, es necesariamente infinito. Que α no sea natural quiere decir $\alpha \notin \omega$, es decir, $\alpha \not< \omega$. Por el Teorema 5.10(ii), entonces $\omega \leq \alpha$, es decir, $\omega \subseteq \alpha$. Por tanto, α contiene al conjunto infinito de los números naturales, luego no puede ser finito. □

Incluimos a continuación el resultado fundamental que buscábamos sobre conjuntos bien ordenados y ordinales, pero con un punto delicado en la demostración (que, por otra parte, es calcada de la demostración del Teorema 5.5, con la salvedad de que no existe el conjunto Y de todos los ordinales):

Teorema 5.12. *Cada conjunto bien ordenado es isomorfo a un único ordinal.*

Demostración: Por el Teorema 5.10(iii), dados dos ordinales distintos, uno es un segmento inicial del otro, luego no hay dos ordinales isomorfos. Por tanto, cada conjunto bien ordenado es isomorfo como mucho a un único ordinal. Lo que hay que ver es que es isomorfo a alguno.

Sea entonces X un conjunto bien ordenado, y consideremos $A \subseteq X$ el subconjunto de los elementos $x \in X$ tales que A_x es isomorfo a algún ordinal. Para cada $x \in A$, sea α_x el único ordinal al que es isomorfo. Entonces, el isomorfismo $A_x \to \alpha_x$ manda también isomorfamente los segmentos iniciales de A_x en los segmentos iniciales de α_x (que son precisamente los elementos de α_x). Esto demuestra dos cosas:

1) Cada $y < x$ está también en A porque A_y es isomorfo al ordinal correspondiente de α_x. Por tanto, o bien A es un segmento inicial de X o bien $A = X$

2) Cada $\beta \in \alpha_x$ es también de la forma α_y para algún $y \in X$. Esto quiere decir que, si $\{\alpha_x \mid x \in A\}$ fuera un conjunto, sería un ordinal, puesto que es transitivo (estamos diciendo que cada α_x está contenido en él como subconjunto) y está bien ordenado por ser un conjunto de números ordinales.

Dando por descontado que $\alpha := \{\alpha_x \mid x \in A\}$ es un conjunto, tendríamos entonces un isomorfismo $A \to \alpha$ definido por $x \mapsto \alpha_x$. Esto implica también que $A = X$, porque si no sería un segmento inicial, y por tanto (Lema 3.10) de la forma A_x. Pero por definición de A, se tendría entonces $x \in A = A_x$, lo que es absurdo. □

La demostración anterior estará completa si demostramos que α es en realidad un conjunto. Parece evidente, ya que está parametrizado por un conjunto, pero no se puede obtener de ninguno de los axiomas que tenemos hasta ahora. Por tanto, necesitamos un nuevo axioma, que aadiremos a partir de ahora a los axiomas precedentes:

Axioma de Sustitución. *Si $P(x, y)$ es una propiedad tal que para cada x existe un único y tal que $P(x, y)$, entonces ocurre que, para cada conjunto X, existe un conjunto Y con la propiedad de que si $x \in X$ entonces existe $y \in Y$ tal que $P(x, y)$ es cierta.*

En el teorema anterior, la propiedad P es: o bien $x \in A$ e $y = \alpha_x$ o bien $x \notin A$ e $y = \emptyset$.

Teorema 5.13 (Principio de Inducción Transfinita)**.** *Sea P una propiedad de los números ordinales que satisface la siguiente condición:*

"Para cada ordinal α, si $P(\alpha')$ es cierta para todo $\alpha' < \alpha$, entonces $P(\alpha)$ es cierta".

Entonces $P(\alpha)$ es cierta para todo ordinal α.

Demostración: Supongamos que P no fuera cierta para algún ordinal. Entonces, la colección S de ordinales para los que P no es cierta sería no vacía. Por el Teorema 5.10(iv), S tiene un mínimo α. Por tanto, cada $\alpha' < \alpha$ no está en S, es decir, $P(\alpha')$ es cierto. Por la hipótesis de inducción del enunciado, se seguiría entonces que $P(\alpha)$ es cierta, es decir, $\alpha \in S$, lo que es absurdo. □

El lector igual se pregunta por qué hemos empezado por lo que, en el caso de inducción sobre los naturales llamábamos segundo principio de inducción, en lugar de empezar por la clásica inducción de que cada caso implica el sucesivo. El motivo es que, de ese modo y empezando del caso 0, a base de ir de cada caso al sucesivo nunca llegaríamos a ω, ya que no es el ordinal sucesivo de ninguno. De hecho, los ordinales así hay que tratarlos aparte:

Definición. Se llama *ordinal límite* a un ordinal $\alpha \neq 0$ para el que no existe un ordinal β tal que $\alpha = \beta + 1$.

Lema 5.14. *Sean α, β números ordinales. Entonces:*

(i) $\beta < \alpha + 1$ *si y sólo si* $\beta \leq \alpha$.

(ii) $\beta < \alpha$ *si y sólo si* $\beta + 1 \leq \alpha$.

Demostración: Por definición, $\beta < \alpha + 1$ si y sólo si $\beta \in \alpha \cup \{\alpha\}$, que es equivalente a $\beta \in \alpha$ o $\beta = \alpha$, es decir, $\beta < \alpha$ o $\beta = \alpha$, lo que prueba (i).

Para demostrar (ii), observemos que $\beta < \alpha$ es equivalente a $\beta \in \alpha$ y $\beta \subset \alpha$ (en realidad estas dos últimas propiedades son equivalentes entre sí). Esto último es claramente equivalente a $\beta \cup \{\beta\} \subseteq \alpha$, es decir, $\beta + 1 \leq \alpha$. □

Proposición 5.15. *Si $\alpha \neq 0$ es un ordinal, son equivalentes:*

(i) α *es un ordinal límite.*

(ii) Para cada $\beta < \alpha$ *se tiene* $\beta + 1 < \alpha$.

(iii) α *no tiene máximo.*

(iv) $\alpha = \sup \alpha$.

(v) $\alpha = \bigcup_{\alpha' \in \alpha} \alpha'$.

Demostración: Demostramos las equivalencias de modo cíclico:

$(i) \Rightarrow (ii)$: Por el Lema 5.14(ii), $\beta < \alpha$ es equivalente a $\beta + 1 \leq \alpha$. Como $\beta + 1 \neq \alpha$ por ser α un ordinal límite, se sigue $\beta + 1 < \alpha$.

$(ii) \Rightarrow (iii)$: La hipótesis (ii) implica que ningún $\beta \in \alpha$ puede ser cota superior de α, luego α no tiene máximo.

$(iii) \Rightarrow (iv)$: Recordando que α es el segmento inicial formado por los ordinales menores que α, esta implicación está demostrada en el Lema 3.9(iv).

$(iv) \Rightarrow (v)$: Si en el Lema 3.12(iii) tomamos $S = \alpha$, tendremos $A_S = A_\alpha$. Pero, por definición, $A_S = \bigcup_{\alpha' \in \alpha} \alpha'$, mientras que $A_\alpha = \alpha$.

$(v) \Rightarrow (i)$: Supongamos que fuera $\alpha = \beta + 1$. Entonces $\beta \in \alpha$, con lo que llegaremos a un absurdo si demostramos que β no pertenece a ningún α' con $\alpha' < \alpha$. En efecto, si $\alpha' < \alpha = \beta + 1$, por el Lema 5.14(i) se tiene $\alpha' \leq \beta$, luego no puede ser $\beta < \alpha$, es decir, no puede ser $\beta \in \alpha'$. □

Observación 5.16. A la vista del resultado anterior cabe preguntarse qué ocurre cuando α no es un ordinal límite, es decir, $\alpha = \beta + 1$. En tal caso, decir $\alpha' \in \alpha$ es equivalente (por definición y aplicando el Lema 5.14(i)) a decir $\alpha' \leq \beta$, por lo que obviamente α tiene máximo (y por tanto supremo), que es β, y también (como $\alpha' \leq \beta$ quiere decir $\alpha \subseteq \beta$), se tiene $\bigcup_{\alpha' \in \alpha} \alpha' = \beta$. El modo de obtener cualquier α como unión de ordinales menores es

$$\alpha = \bigcup_{\alpha' < \alpha} (\alpha' + 1)$$

ya que cada $\alpha' \in \alpha$ está obviamente en $\alpha' + 1$, mientras que por otra parte $\alpha' < \alpha$ es equivalente, por el Lema 5.14(ii), a $\alpha' + 1 \subseteq \alpha$.

Teorema 5.17 (Segundo Principio de Inducción Transfinita)**.** *Sea P una propiedad que satisface:*

(i) $P(0)$ *es cierta.*

(ii) $P(\alpha)$ *implica* $P(\alpha + 1)$.

(iii) Si α es un ordinal límite y $P(\alpha')$ es cierta para todo $\alpha' < \alpha$, entonces $P(\alpha)$ es cierta.

Entonces $P(\alpha)$ es cierta para todo ordinal α.

Demostración: Es inmediato del Teorema 5.13. En efecto, supongamos que $P(\alpha')$ sea cierta para todo $\alpha' < \alpha$, y necesitamos ver que entonces también $P(\alpha)$ es cierta. Distinguimos tres casos:

–Si $\alpha = 0$, entonces $P(0)$ es cierta por (i).

–Si fuera $\alpha = \alpha' + 1$, entonces $P(\alpha')$ es cierta por hipótesis ya que $\alpha' < \alpha$. Entonces, (ii) implica que $P(\alpha' + 1)$ es cierta, es decir, $P(\alpha)$ es cierta.

-Finalmente, si $\alpha \neq 0$ y no es sucesor de ningún ordinal α', entonces es un ordinal límite. Por tanto, (iii) implica que $P(\alpha)$ es cierta. □

Queremos extender ahora a los ordinales el principio de recurrencia. Para ello, visto que los ordinales no son conjuntos, necesitamos extender el concepto de función:

Definición. Sea $P(x, y)$ una propiedad tal que para cada x existe un único y tal que $P(x, y)$ es cierta. Se llama *operación* (asociada a la propiedad P) a la asignación F que asocia a cada x el único $y = F(x)$ tal que $P(x, y)$. Si X es un conjunto, entonces el Axioma de Sustitución garantiza que existe el conjunto formado por los pares $(x, F(x))$ cuando x varía en X. Tal conjunto es una función que denotaremos por $F \restriction X$.

En realidad, la noción de operación la venimos usando desde el principio:

Ejemplo 5.18. Si $P(x, y)$ es la propiedad

$$z \in y \text{ si y sólo si } z \subset x$$

entonces la operación asociada es $F(X) = \mathcal{P}(X)$.

Lema 5.19. *Sea G una operación. Entonces, para todo ordinal α existe una única función f_α con dominio $\alpha + 1$ tal que $f_\alpha(\beta) = G(f_\alpha \restriction \beta)$ para todo $\beta \leq \alpha$.*

Demostración: Lo demostraremos por inducción transfinita. Suponemos entonces que para todo $\alpha' < \alpha$ existe una única $f_{\alpha'}$ y tal que $f'_\alpha(\beta) = G(f_{\alpha'} \restriction \beta)$ para todo $\beta \leq \alpha'$. Por el Axioma de Sustitución, existe entonces el conjunto $\{f_{\alpha'} \mid \alpha' < \alpha\}$. Entonces $\bigcup_{\alpha' < \alpha} f_{\alpha'}$ es un conjunto, que define una relación de dominio $\bigcup_{\alpha' < \alpha}(\alpha' + 1)$, que es α por la Observación 5.16. Para ver que es una función, supongamos que β está en el dominio de α' y α'', veamos que entonces $f_{\alpha'}(\beta) = f_{\alpha''}(\beta)$. Lo demostraremos por inducción transfinita sobre β (aunque β tome valores hasta $\min\{\alpha, \alpha'\}$, se puede hacer este tipo

de inducción poniendo cualquier propiedad cierta para β mayor). Suponemos entonces $f_{\alpha'}(\beta') = f_{\alpha''}(\beta')$ para todo $\beta' < \beta$, es decir, $f_{\alpha'} \restriction \beta = f_{\alpha''} \restriction \beta$. Por tanto,

$$f_{\alpha'}(\beta) = G(f_{\alpha'} \restriction \beta) = G(f_{\alpha''} \restriction \beta) = f_{\alpha''}(\beta)$$

como queríamos.

Definimos entonces $f_\alpha = (\bigcup_{\alpha'<\alpha} f_{\alpha'}) \cup \{(\alpha, G(\bigcup_{\alpha'<\alpha} f_{\alpha'})\}$ (cuyo dominio es evidentemente $\alpha+1$), y veamos que es la función buscada. Veamos en primer lugar la propiedad $f_\alpha(\beta) = G(f_\alpha \restriction \beta)$ para todo $\beta \leq \alpha$, distinguiendo dos casos:

–Si $\beta = \alpha$, entonces $f_\alpha(\alpha) = G(\bigcup_{\alpha'<\alpha} f_{\alpha'}) = G(f_\alpha \restriction \alpha)$.

–Si $\beta < \alpha$, entonces $f_\alpha(\beta) = f_\beta(\beta) = G(f_\beta \restriction \beta) = G(f_\alpha \restriction \beta)$.

Finalmente, debemos probar la unicidad de f_α en esas condiciones. Supongamos que existe g en las mismas condiciones, y veamos $f_\alpha(\beta) = g(\beta)$ para todo $\beta \leq \alpha$. Lo demostraremos por inducción transfinita sobre β. Supongamos entonces $f_\alpha(\beta') = g(\beta')$ para todo $\beta' < \beta$, es decir, $f_\alpha \restriction \beta = g \restriction \beta$. Tendremos entonces

$$f_\alpha(\beta) = G(f_\alpha \restriction \beta) = G(g \restriction \beta) = g(\beta)$$

como queríamos. □

Ejemplo 5.20. Existe el conjunto $\omega + \omega$. Para ello tomamos la operación G que asocia a cada función f el conjunto $\big(\omega \cup (\bigcup \mathrm{rec}(f))\big) + 1$ y aplicamos el Lema para $\alpha = \omega$. Esto permite construir una función f_ω con dominio $\omega + 1$ tal que $f_\omega(n) = \omega + n$. Entonces $\omega + \omega = f_\omega(\omega)$.

Teorema 5.21 (Principio de Recurrencia Transfinita)**.** *Sea G una operación. Entonces existe una única operación F tal que, para todo ordinal α, se tiene $F(\alpha) = G(F \restriction \alpha)$ y $F(x) = \emptyset$ si x no es un ordinal.*

Demostración: Para demostrar la existencia, definimos la operación buscada como $F(x) = \emptyset$ si x no es un ordinal y $F(\alpha) = f_\alpha(\alpha)$ si α es un ordinal. Como $f_\alpha(\alpha) = G(f_\alpha \restriction \alpha)$, para ver que es igual –como necesitamos– a $G(F \restriction \alpha)$ bastará ver que $f_\alpha \restriction \alpha = F \restriction \alpha$. En otras palabras, hay que demostrar que, para cada $\alpha' < \alpha$ se tiene que $f_\alpha(\alpha')$ coincide con $F(\alpha')$, es decir, con $f_{\alpha'}(\alpha')$. Para ello es suficiente demostrar $f_\alpha \restriction (\alpha'+1) = f_{\alpha'}$. Pero eso es consecuencia de la unicidad de $f_{\alpha'}$ que garantiza el Lema 5.19, ya que para cada $\beta \leq \alpha' < \alpha$, se tiene $f_\alpha(\beta) = G(f_\alpha \restriction \beta)$.

Para la unicidad, basta ver que si otra F' satisface lo mismo entonces $F'(\alpha) = F(\alpha)$ para cada ordinal α. Lo demostramos por inducción sobre α. Si $F'(\alpha') = F(\alpha')$ para todo $\alpha' < \alpha$, entonces $F' \restriction \alpha = F \restriction \alpha$, luego

$$F'(\alpha) = G(F' \restriction \alpha) = G(F \restriction \alpha) = F(\alpha)$$

como queríamos. □

Teorema 5.22. *Sean G', G'' operaciones. Entonces existe una única operación F tal que:*

(i) $F(0) = x_0$.

(ii) $F(\alpha + 1) = G'(F(\alpha))$ *para cualquier ordinal* α.

(iii) $F(\alpha) = G''(F \restriction \alpha)$ *para cualquier ordinal límite* α.

(iv) $F(x) = \emptyset$ *si* x *no es un ordinal.*

Demostración: Definimos la operación G tal que

$$G(x) = \begin{cases} x_0 & \text{si } x = \emptyset \\ G'(x(\alpha)) & \text{si } x \text{ es una función con dominio } \alpha + 1 \\ G''(x) & \text{si } x \text{ es una función cuyo dominio es un ordinal límite} \\ \emptyset & \text{si } x \text{ no está en ningún caso anterior} \end{cases}$$

y aplicamos el Teorema 5.21. □

Supongamos ahora que las operaciones dependieran de dos parámetros en vez de una. De la misma forma que en el Ejercicio 1.22, una operación $F(x, y)$ puede verse como asignar a cada x una operación F_x definida por $F_x(y) = F(x, y)$. Podemos dar entonces las versiones paramétricas del Principio de Recurrencia.

Teorema 5.23. *Sean G, G', G'' operaciones. Entonces existe una única operación F tal que para todo x:*

(i) $F(x, 0) = G(x)$.

(ii) $F(x, \alpha + 1) = G'(x, F(x, \alpha))$ *para cualquier ordinal* α.

(iii) $F(x, \alpha) = G''(x, F_x \restriction \alpha)$ *para cualquier ordinal límite* α.

(iv) $F(x, y) = \emptyset$ *si* y *no es un ordinal.*

Teorema 5.24. *Sea G una operación. Entonces existe una única operación F tal que, para todo ordinal α, se tiene $F(x, \alpha) = G(x, F_x \restriction \alpha)$ y $F(x, y) = \emptyset$ si y no es un ordinal.*

6. Aritmética de ordinales

Si en el Teorema 5.24 tomamos $G(x) = x$, $G'(x,y) = y+1$ y $G'(x,y) = \bigcup \mathrm{rec}(y)$, podremos definir por recurrencia una operación $F(\beta,\alpha)$ que será la suma y que escribiremos $\beta + \alpha = F(\beta,\alpha)$):

Definición. Se llama *suma de ordinales* $\beta+\alpha$ a la operación definida por recurrencia sobre α mediante:

(i) $\beta + 0 = \beta$.

(ii) $\beta + (\alpha+1) = (\beta+\alpha)+1$.

(iii) $\beta + \alpha = \bigcup_{\alpha'<\alpha}(\beta+\alpha')$ si α es un ordinal límite.

(recuérdese que, por el Teorema 5.10(v), $\bigcup_{\alpha'<\alpha}(\beta+\alpha')$ es el supremo de $\{\beta+\alpha' \mid \alpha' < \alpha\}$, que es un conjunto por el Axioma de Sustitución).

En la definición anterior hay en principio una pequeña ambigüedad de notación, ya que cuando escribimos $+1$ detrás de un ordinal denotamos el ordinal sucesivo, no la suma con 1. La siguiente observación nos indica que ambas cosas coinciden, con lo que no hay ambigüedad.

Observación 6.1. Cuando α, β son números naturales, las propiedades (i) y (ii) son exactamente las que definen la suma de naturales. Por tanto, la suma restringida a $\mathbb{N}$ coincide con la suma de números naturales. Además, para todo ordinal β, la suma $\beta+1$ coincide con el ordinal sucesivo $\beta+1$ (basta hacer $\alpha = 0$ en (ii) y aplicar (i)).

Ejemplo 6.2. Para ver cómo funciona la parte (iii) de la definición, calculemos $\omega+\omega$ (que coincidirá con el conjunto del Ejemplo 5.20). En primer lugar, aplicando reiteradamente (ii), tendremos

$$\omega + n = \{0, 1, 2, \ldots, \omega, \omega+1, \ldots, \omega+(n-1)\}$$

de donde se deduce que

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

Veamos también ahora cómo se pueden demostrar propiedades de la suma a partir de la definición inductiva:

Ejemplo 6.3. Veamos que $0+\alpha = \alpha$ para cualquier ordinal α. Lo haremos por inducción transfinita. Para $\alpha = 0$ es la propiedad (i). Por otra parte, si sabemos $0+\alpha = \alpha$, entonces por (ii)

$$0 + (\alpha+1) = (0+\alpha)+1 = \alpha+1.$$

Y finalmente, si α es un ordinal límite y $0 + \alpha' = \alpha'$, entonces, por (iii),

$$0 + \alpha = \bigcup_{\alpha' < \alpha} (0 + \alpha') = \bigcup_{\alpha' < \alpha} (\alpha') = \alpha$$

donde la última igualdad es por la Proposición 5.15.

Observación 6.4. Si n es un número natural, entonces, por definición de suma para ordinales límite, se tiene

$$n + \omega = \bigcup_{m \in \mathbb{N}} (n + m) = \omega$$

que es distinto de $\omega + n$ (Ejemplo 6.2). Por tanto, la suma de ordinales no es conmutativa, ni cancelativa (ya que $n + \omega = m + \omega$ no implica $n = m$). Sin embargo, este mal comportamiento ocurre sólo al sumar a la izquierda (el motivo es que la definición de suma por inducción está hecha por la derecha):

Lema 6.5. *Sean $\alpha_1, \alpha_2, \beta$ ordinales. Entonces:*

(i) $\alpha_1 < \alpha_2$ *si y sólo si* $\beta + \alpha_1 < \beta + \alpha_2$.

(ii) $\alpha_1 = \alpha_2$ *si y sólo si* $\beta + \alpha_1 = \beta + \alpha_2$.

Demostración: Para ver (i), demostramos primero por inducción transfinita sobre α_2 que $\alpha_1 < \alpha_2$ implica $\beta + \alpha_1 < \beta + \alpha_2$:

–El caso $\alpha_2 = 0$ es trivial.

–Si es cierto para α_2, supongamos $\alpha_1 < \alpha_2 + 1$, que por el Lema 5.14(i) es equivalente a $\alpha_1 \leq \alpha_2$. Si es $\alpha_1 < \alpha_2$, entonces por hipótesis de inducción $\beta + \alpha_1 < \beta + \alpha_2$, mientras que si $\alpha_1 = \alpha_2$ obviamente se tiene $\beta + \alpha_1 = \beta + \alpha_2$. Entonces en cualquier caso se tiene $\beta + \alpha_1 \leq \beta + \alpha_2$. Por el Lema 5.14(i), esto es equivalente a $\beta + \alpha_1 < (\beta + \alpha_2) + 1$, luego por la parte (ii) de la definición de suma se tiene $\beta + \alpha_1 < \beta + (\alpha_2 + 1)$.

–Si α_2 es un ordinal límite, entonces $\alpha_1 < \alpha_2$ implica (por el Lema 5.15) que $\alpha_1 + 1 < \alpha_2$, y por tanto $\beta + (\alpha_1 + 1) \subseteq \bigcup_{\alpha' < \alpha_2} (\beta + \alpha')$, es decir, $\beta + (\alpha_1 + 1) \leq \beta + \alpha_2$. Como $\beta + (\alpha_1 + 1) = (\beta + \alpha_1) + 1$ por la definición de suma, se sigue del Lema 5.14(ii) que $\beta + \alpha_1 < \beta + \alpha_2$ (nótese que no hemos necesitado en este caso la hipótesis de inducción).

Para probar el recíproco en (i), supongamos $\beta + \alpha_1 < \beta + \alpha_2$. Entonces no puede ser ni $\alpha_1 = \alpha_2$ ni (usando la parte ya demostrada) $\alpha_2 < \alpha_1$. Por tanto, $\alpha_1 < \alpha_2$.

La parte (ii) es consecuencia de (i), usando que, si $\alpha_1 \neq \alpha_2$, entonces $\alpha_1 < \alpha_2$ o $\alpha_2 < \alpha_1$. □

De este lema sacamos que el comportamiento de la Observación 6.4 es más general:

Lema 6.6. *Si α es un ordinal límite, entonces $\beta+\alpha$ es un ordinal límite para todo ordinal β.*

Demostración: Sea $\gamma \in \beta+\alpha$; por el Lema 5.15 tendremos que ver que $\gamma+1$ también está en $\beta+\alpha$. Por definición, $\gamma \in \beta+\alpha$ quiere decir que $\gamma \in \beta+\alpha'$ para algún $\alpha' < \alpha$. Por una parte, de $\gamma < \beta+\alpha'$ se deduce, por el Lema 5.14(ii), que $\gamma+1 \leq \beta+\alpha'$. Y por otra parte, como $\beta+\alpha' < \beta+\alpha$ por el Lema 6.5(i), se sigue finalmente $\gamma+1 < \beta+\alpha$, como queríamos. □

Teorema 6.7. *Para cualesquiera ordinales α, β, γ se tiene $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.*

Demostración: Lo demostramos por inducción transfinita sobre γ:

–El caso $\gamma = 0$ es trivial.

–Si $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$, entonces (usando la parte (ii) de la definición de suma), se tiene $(\alpha+\beta)+(\gamma+1) = ((\alpha+\beta)+\gamma)+1 = (\alpha+(\beta+\gamma))+1 = \alpha+((\beta+\gamma)+1) = \alpha+(\beta+(\gamma+1))$.

–Si γ es un ordinal límite no nulo y cada $\gamma' < \gamma$ cumple la asociatividad, entonces $(\alpha+\beta)+\gamma = \bigcup_{\gamma'<\gamma}((\alpha+\beta)+\gamma') = \bigcup_{\gamma'<\gamma}(\alpha+(\beta+\gamma'))$. Como, por el Lema, $\beta+\gamma$ es un ordinal límite, tendremos $\alpha+(\beta+\gamma) = \bigcup_{\delta<\beta+\gamma}(\alpha+\delta)$. Basta demostrar entonces

$$\bigcup_{\gamma'<\gamma}(\alpha+(\beta+\gamma')) = \bigcup_{\delta<\beta+\gamma}(\alpha+\delta).$$

Es claro que, si $\epsilon \in \bigcup_{\gamma'<\gamma}(\alpha+(\beta+\gamma'))$, entonces $\epsilon < \alpha+(\beta+\gamma')$ para algún $\gamma' < \gamma$, y por el Lema(i) se tiene $\beta+\gamma' < \beta+\gamma$, luego $\epsilon \in \bigcup_{\delta<\beta+\gamma}(\alpha+\delta)$. Recíprocamente, si $\epsilon \in \bigcup_{\delta<\beta+\gamma}(\alpha+\delta)$, entonces $\epsilon \in \alpha+\delta$ para algún $\delta \in \beta+\gamma$. Como $\beta+\gamma = \bigcup_{\gamma'<\gamma}(\beta+\gamma')$, entonces $\delta < \beta+\gamma'$ para algún $\gamma' < \gamma$. Se sigue entonces, por el Lema 6.5(i), que $\alpha+\delta < \alpha+(\beta+\gamma')$, y por tanto $\epsilon \in \alpha+(\beta+\gamma')$, demostrando la inclusión que faltaba. □

De la misma forma que definíamos la suma por inducción, podemos definir también el producto de ordinales:

Definición. Se llama *producto de ordinales* $\beta \cdot \alpha$ a la operación definida por recurrencia sobre α mediante:

(i) $\beta \cdot 0 = 0$.

(ii) $\beta \cdot (\alpha+1) = (\beta \cdot \alpha)+\beta$.

(iii) $\beta \cdot \alpha = \bigcup_{\alpha'<\alpha}(\beta \cdot \alpha')$ si α es un ordinal límite no nulo.

Observación 6.8. Al ser la misma definición inductiva que para los números naturales, esta multiplicación es una generalización del producto de números naturales. Además, de

la definición (usando sucesivamente (ii) y (i)) sale inmediatamente $\beta \cdot 1 = \beta$ para todo ordinal β, mientras que hace falta usar inducción para demostrar $1 \cdot \alpha = \alpha$ para todo ordinal α. También se demuestra por inducción $0 \cdot \alpha = 0$ para todo α.

Ejemplo 6.9. Usando la observación anterior y la propiedad (ii), para todo ordinal β se tiene

$$\beta \cdot 2 = \beta(1+1) = \beta \cdot 1 + \beta = \beta + \beta$$

y, por inducción sobre n (y teniendo en cuenta la asociatividad del Teorema 6.7) se tiene $\beta \cdot n = \beta + \ldots + \beta$. En particular,

$$\omega \cdot n = \omega + \ldots + \omega = \{0, 1, \ldots, \omega, \omega+1, \ldots, \omega \cdot (n-1), \omega \cdot (n-1) + 1, \ldots\}$$

y por tanto

$$\omega \cdot \omega = \{0, 1, \ldots, \omega, \omega+1, \ldots, \omega \cdot n, \omega \cdot n + 1, \ldots\}$$

(donde ahora n puede tomar cualquier valor). Sin embargo

$$n \cdot \omega = \bigcup_{m \in \omega} (nm) = \omega$$

para todo $n \in \mathbb{N}$, luego el producto tampoco es conmutativo ni cancelativo.

Ejercicio 6.10. Demostrar la asociatividad del producto de ordinales y la distributividad con respecto a la suma.

Ejercicio 6.11. Demostrar que, si α es un ordinal límite, entonces $\beta \cdot \alpha$ es un ordinal límite para todo ordinal β no nulo.

Ejercicio 6.12. Sean $\alpha_1, \alpha_2, \beta$ ordinales con $\beta \neq 0$. Demostrar:

(i) $\alpha_1 < \alpha_2$ si y sólo si $\beta \cdot \alpha_1 < \beta \cdot \alpha_2$.

(ii) $\alpha_1 = \alpha_2$ si y sólo si $\beta \cdot \alpha_1 = \beta \cdot \alpha_2$.

Finalmente, definimos la exponenciación de ordinales:

Definición. Se llama *exponenciación de ordinales* β^α a la operación definida por recurrencia sobre α mediante:

(i) $\beta^0 = 1$.

(ii) $\beta^{\alpha+1} = \beta^\alpha \cdot \beta$.

(iii) $\beta^\alpha = \bigcup_{\alpha' < \alpha} \beta^{\alpha'}$ si α es un ordinal límite no nulo.

Observación 6.13. Como para la suma y el producto, la exponenciación que acabamos de definir, restringida a los naturales, es la exponenciación conocida de números naturales. En

particular, $0^0 = 1$. Además, se comprueba fácilmente $1^\alpha = 1$ para todo α y $\beta^n = \beta \cdot \ldots \cdot \beta$ para todo natural n y todo ordinal α.

Observación 6.14. Para todo $n \in \mathbb{N}$, se tiene

$$n^\omega = \bigcup_{m \in \omega} n^m = \omega.$$

Nótese en particular que entonces $2^\omega = w$ y, como conjunto, es numerable (sin embargo, $\omega^2 > \omega$, luego también $\omega^\omega > \omega$). Comparando con el Teorema de Cantor, esto muestra que la exponenciación no se comporta bien a la hora de estudiar el cardinal de los conjuntos. En realidad, la interpretación de suma, producto y exponenciación (que muestra por qué funcionan bien las dos primeras operaciones y explica mejor la tercera), es la siguiente:

Ejercicio 6.15. Sean α, β dos ordinales:

(i) Demostrar que $(\{0\} \times \beta) \cup (\{1\} \times \alpha)$, con el orden lexicográfico, es isomorfo a $\beta + \alpha$.

(ii) Demostrar que $\alpha \times \beta$, con el orden lexicográfico, es isomorfo a $\beta \cdot \alpha$.

(iii) En $S(\alpha, \beta) = \{f : \alpha \to \beta \mid f^{-1}[\beta - \{0\}] \text{ es finito}\}$ definimos una relación $\preceq$ mediante $f \prec g$ si y sólo si existe $\alpha' \in \alpha$ tal que $f(\alpha') < g(\alpha')$ y $f(\alpha'') = g(\alpha'')$ para todo $\alpha'' > \alpha'$. Demostrar que, con este relación, $S(\alpha, \beta)$ es un conjunto bien ordenado y que es isomorfo a β^α.

Ejercicio 6.16. Dados ordinales $\alpha_1, \alpha_2, \beta$, demostrar:

(i) $\beta^{\alpha_1 + \alpha_2} = \beta^{\alpha_1} \cdot \beta^{\alpha_2}$.

(ii) $(\beta^{\alpha_1})^{\alpha_2} = \beta^{\alpha_1 \cdot \alpha_2}$.

(iii) Si $\beta > 1$, entonces $\alpha_1 < \alpha_2$ si y sólo si $\beta^{\alpha_1} < \beta^{\alpha_2}$.

(iv) Si $\beta > 1$, entonces $\alpha_1 = \alpha_2$ si y sólo si $\beta^{\alpha_1} = \beta^{\alpha_2}$.

Aunque las operaciones con ordinales sólo funcionen bien por un lado, por el otro se puede decir lo siguiente:

Ejercicio 6.17. Dados ordinales α, β, demostrar:

(i) $\beta + \alpha \geq \alpha$.

(ii) $\beta \cdot \alpha \geq \alpha$ si $\beta > 0$.

(iii) $\beta^\alpha \geq \alpha$ si $\beta > 1$.

El siguiente resultado (que será fundamental para lo que sigue) indica que, operando con ordinales un ordinal dado, se puede superar cualquier otro ordinal (obviamente, en el caso de suma, el mínimo ordinal que hay que sumar a otro para superar un tercero es la diferencia: con el producto o la exponenciación es la mejor aproximación al cociente o al "logaritmo"):

Lema 6.18. *Sean β, α números ordinales tales que $\beta \leq \alpha$. Entonces:*

(i) Existe un único ordinal γ tal que $\alpha = \beta + \gamma$.

(ii) Si $\beta > 0$, existe un máximo ordinal γ tal que $\beta \cdot \gamma \leq \alpha$.

(iii) Si $\beta > 1$, existe un máximo ordinal γ tal que $\beta^\gamma \leq \alpha$.

Demostración: Para demostrar (i), consideremos los ordinales δ tales que $\beta + \delta > \alpha$ (hay alguno, por ejemplo $\delta = \alpha + 1$). Existe entonces un mínimo δ tal que $\beta + \delta > \alpha$. Si δ fuera un ordinal límite, entonces $\alpha \in \beta + \delta = \bigcup_{\delta' < \delta}(\beta + \delta')$, luego $\beta + \delta' > \alpha$ para algún $\delta' < \delta$, lo que contradiría la minimalidad de δ. Por tanto (como obviamente $\delta \neq 0$), $\delta = \gamma + 1$ para algún ordinal γ. Por tanto, $\alpha < \beta + (\gamma + 1) = (\beta + \gamma) + 1$ y, por el Lema 5.14(i) se tiene $\alpha \leq \beta + \gamma$. Por la minimalidad de δ no puede ser $\alpha < \beta + \gamma$, luego $\alpha = \beta + \gamma$. La unicidad de tal γ viene garantizada por el Lema 6.5(ii).

Para demostrar (ii), procedemos como en la primera parte de la demostración de (i), considerando ahora los ordinales δ tales que $\beta \cdot \delta > \alpha$. Como antes, el mínimo δ en esas condiciones es de la forma $\delta = \gamma + 1$. De aquí se sigue que $\beta \cdot \gamma \leq \alpha$, y es el máximo en esas condiciones, porque si $\gamma' > \gamma$, por el Lemma 5.14(ii) se tendrá $\delta = \gamma + 1 \leq \gamma'$, luego $\beta\delta \leq \beta\gamma'$, así que no puede ser $\beta\gamma' \leq \alpha$.

Finalmente, (iii) se obtiene de la misma forma consideranto los ordinales δ tales que $\beta^\delta > \alpha$. □

El lema anterior nos permite, en primer lugar, generalizar la división euclídea a los números ordinales:

Teorema 6.19. *Sean β, α números ordinales con $\beta \neq 0$. Entonces existen γ, δ únicos tales que $\delta < \beta$ y $\alpha = \beta \cdot \gamma + \delta$.*

Demostración: Para probar la existencia, distinguimos dos casos. Si $\beta > \alpha$, tomamos $\gamma = 0$ y $\delta = \alpha$. Si $\beta \leq \alpha$, tomamos el máximo γ tal que $\beta \cdot \gamma \leq \alpha$, que existe por el Lema(ii). Sea el único δ tal que $\alpha = \beta \cdot \gamma + \delta$, que existe por el Lema(i). Entonces se tiene $\delta < \beta$, ya que en caso contrario

$$\beta \cdot (\gamma + 1) = \beta \cdot \gamma + \beta \leq \beta \cdot \gamma + \delta = \alpha$$

contradiciendo la maximalidad de γ.

Para probar la unicidad, supongamos $\alpha = \beta \cdot \gamma + \delta = \beta \cdot \gamma' + \delta'$ y por ejemplo $\gamma' \leq \gamma$. Entonces existe ϵ tal que $\gamma = \gamma' + \epsilon$. y tendremos

$$\beta \cdot \gamma' + \delta' = \beta \cdot \gamma + \delta = \beta \cdot (\gamma' + \epsilon) + \delta = \beta \cdot \gamma' + \beta \cdot \epsilon + \delta$$

luego $\delta' = \beta \cdot \epsilon + \delta$. Si fuera $\epsilon \neq 0$, entonces $\delta' \geq \beta \cdot \epsilon \geq \beta$, lo que es absurdo. Por tanto, $\epsilon = 0$, es decir, $\gamma = \gamma'$, lo que implica también $\delta = \delta'$. □

De la misma forma en que la división euclídea permite escribir los números naturales en cualquier base (en particular en la escritura habitual en base 10), la división euclídea de ordinales permite escribir cada ordinal "en base ω":

Teorema 6.20. *Cada ordinal $\alpha > 0$ se puede escribir de forma única como*

$$\alpha = \omega^{\gamma_1} \cdot n_1 + \omega^{\gamma_2} \cdot n_2 + \ldots + \omega^{\gamma_r} \cdot n_r$$

con $\gamma_1 > \gamma_2 > \ldots > \gamma_r$ y $n_1, \ldots, n_r$ naturales no nulos.

Demostración: Demostramos la existencia por inducción transfinita sobre α. Si $\alpha = 1$ basta escribir $\alpha = \omega^0 \cdot 1$. Supongamos entonces que sabemos la existencia para todos los ordinales $0 < \alpha' < \alpha$ y demostrémosla para α.

Para ver qué γ_1 debemos tomar, observamos primero que, si podemos encontrar una expresión como la que buscamos, necesariamente

$$\omega^{\gamma_1} \leq \omega^{\gamma_1} \cdot n_1 \leq \alpha,$$

$$\omega^{\gamma_2} \cdot n_2 + \ldots + \omega^{\gamma_r} \cdot n_r \leq \omega^{\gamma_2} \cdot n_2 + \omega^{\gamma_2} + \ldots + \omega^{\gamma_2} = \omega^{\gamma_2} \cdot (n_2 + 1 + \ldots + 1) < \omega^{\gamma_1}$$

y

$$\omega^{\gamma_1 + 1} > \omega^{\gamma_1} \cdot (n_1 + 1) \geq \omega^{\gamma_1} \cdot n_1 + \omega^{\gamma_2} \cdot n_2 + \ldots + \omega^{\gamma_r} \cdot n_r = \alpha.$$

Por tanto, γ_1 es el mayor ordinal tal que $\omega^{\gamma_1} \leq \alpha$ y n_1 es el cociente de dividir α entre ω^{γ_1}.

Por tanto, aplicamos el Lema(iii) y tomamos el máximo γ_1 tal que $\omega^{\gamma_1} \leq \alpha$. Aplicando el Teorema, existirán n_1 y δ tales que $\alpha = \omega^{\gamma_1} \cdot n_1 + \alpha'$ con $\alpha' < \omega^{\gamma_1}$.

Veamos en primer lugar que n_1 es finito. En efecto, si fuera $n_1 \geq \omega$, entonces

$$\alpha \geq \omega^{\gamma_1} \cdot n_1 \geq \omega^{\gamma_1} \cdot \omega = \omega^{\gamma_1 + 1}$$

contradiciendo la maximalidad de γ_1. Además, $n_1 \neq 0$, porque si no $\alpha = \alpha' < \omega^{\gamma_1}$, en contra de la elección de γ_1. Podemos escribir entonces $\alpha = \omega^{\gamma_1} \cdot n_1 + \alpha'$, con $n_1 \in \mathbb{N} - \{0\}$

y $\alpha' < \omega^{\gamma_1} \leq \alpha$(*). Si fuera $\alpha' = 0$, ya habríamos terminado. Si en cambio $\alpha' > 0$, por hipótesis de inducción tendremos

$$\alpha' = \omega^{\gamma_2} \cdot n_2 + \ldots + \omega^{\gamma_r} \cdot n_r$$

con $\gamma_2 > \ldots > \gamma_r$ y $n_2, \ldots, n_r$ naturales no nulos. Basta ver entonces $\gamma_1 > \gamma_2$, lo que se sigue de

$$\omega^{\gamma_2} \leq \omega^{\gamma_2} \cdot n_2 \leq \alpha' < \omega^{\gamma_1}$$

y el Ejercicio 6.16(iii).

Demostramos la unicidad también por inducción sobre α, siendo clara la unicidad para $\alpha = 1$. Supongamos entonces que tenemos dos descomposiciones distintas $\alpha = \omega^{\gamma_1} \cdot n_1 + \omega^{\gamma_2} \cdot n_2 + \ldots + \omega^{\gamma_r} \cdot n_r = \omega^{\gamma_1'} \cdot n_1' + \omega^{\gamma_2'} \cdot n_2' + \ldots + \omega^{\gamma_r'} \cdot n_r'$. Ya hemos observado antes que tanto γ_1 como γ_1' deben ser el mayor ordinal tal que $\omega^{\gamma_1} \leq \alpha$ (por tanto $\gamma_1 = \gamma_1'$) y n_1 y n_1' deben ser el cociente de dividir α entre ω^{γ_1} (luego $n_1 = n_1'$). De aquí sacamos $\omega^{\gamma_2} \cdot n_2 + \ldots + \omega^{\gamma_r} \cdot n_r = \omega^{\gamma_2'} \cdot n_2' + \ldots + \omega^{\gamma_r'} \cdot n_r'$ y, por hipótesis de inducción se concluye. □

Definición. La escritura que da el Teorema 6.20 de un número ordinal se llama *forma normal del número ordinal*.

Observación 6.21. Al contrario que en la escritura de naturales en base 10, para calcular la forma normal de un ordinal no vale reiterar la división por ω para demostrar la existencia de forma normal. El motivo es que de la división entre ω, la igualdad $\alpha = \omega \cdot \gamma + \delta$ implica la desigualdad $\alpha \geq \omega \cdot \gamma$, pero esta última no implica $\alpha > \gamma$. Por ejemplo, podemos tener $\alpha = \omega^\omega$, y su división entre ω es $\omega^\omega = \omega \cdot \omega^\omega$, ya que $\omega \cdot \omega^\omega = \omega^{1+\omega} = \omega^\omega$.

(*) Obsérvese que no se puede deducir $\alpha' < \alpha$ directamente de la igualdad $\alpha = \omega^{\gamma_1} n_1 + \alpha'$ y $\omega^{\gamma_1} n_1 > 0$, ya que en general no es cierto que $\epsilon > \epsilon'$ implique $\epsilon + \alpha' > \epsilon' + \alpha'$ (ver Ejemplo 6.4)

7. Cardinales y el Axioma de Elección

En esta sección pretendemos averiguar cuántos cardinales distintos hay. Para ello empezamos a estudiar los cardinales que tienen los números ordinales. Observamos primero que los número naturales tienen cada uno de ellos cardinal distinto a cualquier otro ordinal (eso es lo que nos permitió usarlos como cardinales de los conjuntos finitos). Sin embargo, observamos que ya ω tiene el mismo cardinal que $\omega+1, \omega+2, \ldots$, por lo que para cardinales infinitos tenemos que hacer ahora algo más cuidadoso. Lo que haremos es escoger, para cada posible cardinal de ordinales, el mínimo ordinal que tenga tal cardinal (y más adelante estudiaremos si así hemos encontrado ya finalmente todos los cardinales posibles). Para ello damos la siguiente:

Definición. Un *ordinal inicial* es un ordinal α que no es equipotente a ningún $\beta < \alpha$.

Ejemplo 7.1. $0, 1, 2, \ldots, \omega$ son iniciales, mientras que ningún $\omega \cdot n + m$ es inicial.

Ejercicio 7.2. Demostrar que cualquier ordinal inicial infinito es un ordinal límite.

Los ordinales iniciales nos sirven para dar cardinales de conjuntos bien ordenados (incluso independientemente del buen orden que demos al conjunto):

Teorema 7.3. *Cada conjunto que admite un buen orden es equipotente a un único ordinal inicial.*

Demostración: Sea X un conjunto que admita un buen orden. Por el Teorema 5.12, sabemos que X, una vez fijado un buen orden, es isomorfo a un (único) ordinal, y por tanto es equipotente a algún ordinal. Entonces existe un ordinal mínimo al que X es equipotente, que necesariamente es un ordinal inicial. Además, el ordinal inicial al que X es equipotente es único, porque dos ordinales iniciales distintos nunca pueden ser equipotentes (ya que por el Teorema 5.10(iii) uno de ellos será necesariamente mayor que el otro). □

Definición. Llamaremos *número cardinal* de un conjunto bien ordenado X al único ordinal inicial equipotente a X.

Veamos a continuación que el cardinal de los números ordinales no está acotado:

Teorema 7.4. *Dado cualquier conjunto X, existe un ordinal α tal que $|\alpha| \not\leq |X|$.*

Demostración: Cada función inyectiva de un ordinal α en X define una buen orden en la imagen de la función. Recíprocamente, cada subconjunto bien ordenado de X es, por el Teorema 5.12, isomorfo a un único ordinal α, y tal isomorfismo será un una función inyectiva de α en X. Por tanto, los ordinales α tales que $|\alpha| \leq |X|$ son los ordinales que provienen de un buen orden de un subconjunto de X. Hagamos esto más explícito:

Un buen orden en un subconjunto de X es un elemento de $\mathcal{P}(X \times X)$, por tanto, por el Axioma de Separación, existe el conjunto de todos los buenos órdenes en subconjuntos de X. Tenemos además una operación que a cada buen orden en un subconjunto de X le asocia el único ordinal isomorfo a tal subconjunto con ese orden. Por el Axioma de Sustitución, existirá entonces el conjunto de los ordinales que son isomorfos a un subconjunto bien ordenado de X, es decir, el conjunto de ordinales α tales que $|\alpha| \leq |X|$. Por el Teorema 5.10(v), existe entonces un ordinal que no está en dicho conjunto, que es lo que queríamos demostrar. □

Definición. Se llama *número de Hartogs de un conjunto* X al menor ordinal $h(X)$ tal que $|h(X)| \not\leq |X|$.

(Obsérvese que en la definición y en el teorema hemos puesto "$\not\leq$" en vez de ">", porque en principio no hay por qué suponer que "los cardinales están totalmente ordenados", luego ambas cosas no son equivalentes).

Lema 7.5. *El número de Hartogs de un conjunto es un ordinal inicial.*

Demostración: Hay que ver que, si $\alpha < h(X)$, entonces $|\alpha| \neq |h(X)|$. Por la minimalidad del número de Hartogs, $\alpha < h(X)$ implica $|\alpha| \leq |X|$. Por tanto, no puede ser $|\alpha| = |h(X)|$, porque entonces sería $|h(X)| \leq |X|$, en contra de la definición de número de Hartogs. □

El Teorema 7.4 y el Lema 7.5 nos van a permitir definir una sucesión creciente de ordinales iniciales:

Definición. Llamaremos ω_α al ordinal definido por recurrencia como sigue:

(i) $\omega_0 = \omega$.

(ii) $\omega_{\alpha+1} = h(\omega_\alpha)$.

(iii) $\omega_\alpha = \bigcup_{\alpha' < \alpha} \omega_{\alpha'}$ si α es un ordinal límite.

Ejercicio 7.6. Demostrar $\omega_\alpha \geq \alpha$ para cualquier α. [Aunque parezca una acotación poco fina, puede demostrarse (Proposición 8.14) que existen valores de α arbitrariamente altos para los que se da la igualdad].

Veamos en primer lugar que los ordinales que hemos definido forman una sucesión creciente, y que el orden corresponde al orden entre cardinales. Esto es lo que pasaba para los números naturales (Proposición 4.9), lo que nos permitió usar los naturales como cardinales finitos. Nuestro objetivo ahora es usar los ω_α como cardinales infinitos, en la esperanza de que nos den luego todos los posibles cardinales infinitos.

Lema 7.7. *Sean α, β dos ordinales. Entonces son equivalentes:*

(i) $\beta < \alpha$.

(ii) $\omega_\beta < \omega_\alpha$.

(iii) $|\omega_\beta| < |\omega_\alpha|$.

Demostración: Demostraremos cíclicamente las implicaciones.

$(i) \Rightarrow (ii)$: Veamos por inducción sobre α que $\omega_\beta < \omega_\alpha$ para todo $\beta < \alpha$, siendo trivial el caso $\alpha = 0$.

Supongamos entonces que es cierto para α y sea $\beta < \alpha + 1$. Entonces o bien $\beta < \alpha$ (y por hipótesis de inducción $\omega_\beta < \omega_\alpha$) o bien $\beta = \alpha$ (y entonces $\omega_\beta = \omega_\alpha$). En cualquier caso, tenemos $\omega_\beta \leq \omega_\alpha$, con lo que el caso $\alpha+1$ estará demostrado si vemos que $\omega_\alpha < \omega_{\alpha+1}$. Pero esto es inmediato, ya que $\omega_{\alpha+1} = h(\omega_\alpha)$, luego no puede ser un subconjunto de ω_α; en otras palabras, no es $\omega_{\alpha+1} \leq \omega_\alpha$, y por tanto $\omega_\alpha < \omega_{\alpha+1}$.

Sea ahora α un ordinal límite no nulo y sea $\beta < \alpha$. Por ser α ordinal límite, $\beta+1 < \alpha$. Entonces, como $\omega_\alpha = \bigcup_{\alpha'<\alpha} \omega_{\alpha'}$, en particular tendremos $\omega_{\beta+1} \subseteq \omega_\alpha$. Como $\omega_\beta < \omega_{\beta+1}$ (según hemos demostrado en el párrafo anterior), se sigue $\omega_\beta < \omega_\alpha$.

$(ii) \Rightarrow (iii)$: Evidentemente $\omega_\beta < \omega_\alpha$ implica $|\omega_\beta| \leq |\omega_\alpha|$. Para ver que no puede ser $|\omega_\alpha| = |\omega_\beta|$ distinguimos dos casos.

–Si α no es un ordinal límite, entonces ω_α es un número de Hartogs (o $\alpha = 0$ y $\omega_\alpha = \omega$), luego es un ordinal inicial por el Lema 7.5. Por tanto, como $\omega_\beta < \omega_\alpha$, no puede ser $|\omega_\alpha| = |\omega_\beta|$.

–Si α es un ordinal límite, entonces como $\beta < \alpha$ (del hecho que ya sabemos que (i) implica (ii), luego no puede ser $\alpha < \beta$) se tiene también $\beta + 1 < \alpha$. Entonces por el caso anterior $|\omega_\beta| < |\omega_{\beta+1}|$, y como $|\omega_{\beta+1}| \leq |\omega_\alpha|$ (ya que $\omega_{\beta+1} \leq \omega_\alpha$), se sigue también $|\omega_\beta| < |\omega_\alpha|$.

$(iii) \Rightarrow (i)$: Como $|\omega_\beta| < |\omega_\alpha|$, no puede ser $\alpha = \beta$. Además, si fuera $\alpha < \beta$, como ya hemos visto que (i) implica (iii), sería $|\omega_\alpha| < |\omega_\beta|$, lo que es absurdo. Por tanto, sólo queda la posibilidad $\beta < \alpha$. □

A continuación demostramos no sólo que los ω_α son ordinales iniciales, sino que son todos los posibles ordinales iniciales infinitos. En otras palabras, cada número ordinal infinito (y por tanto cada conjunto infinito que admita un buen orden) es equipotente a un ω_α:

Teorema 7.8. *Los ordinales iniciales infinitos son exactamente los ordinales de la forma ω_α.*

Demostración: Como $\omega_\alpha \geq \omega_0 = \omega$ para todo α (por el Lema 7.7), se sigue que ω_α es infinito. Además, si α no es un ordinal límite es un número de Hartogs, por lo que es un ordinal inicial (Lema 7.5). Veamos que también ω_α es un ordinal inicial cuando α es un ordinal límite. Sea entonces $\gamma < \omega_\alpha$ y veamos que no puede ser equipotente a ω_α. En efecto, como $\gamma \in \omega_\alpha = \bigcup_{\alpha'<\alpha} \omega_{\alpha'}$, entonces $\gamma \in \omega_{\alpha'}$ para algún $\alpha' < \alpha$, luego $\gamma \subset \omega_{\alpha'}$ y $|\gamma| \leq |\omega_{\alpha'}|$. Además, como $\alpha' < \alpha$, el Lema 7.7 implica $|\omega_{\alpha'}| < |\omega_\alpha|$. Por tanto, $|\gamma| < |\omega_\alpha|$ y γ no es equipotente a ω_α.

Recíprocamente, sea γ un ordinal inicial infinito. Como (por el Ejercicio 7.6) $\gamma \leq \omega_\gamma < \omega_{\gamma+1}$, basta demostrar que, para todo ordinal α, los ordinales iniciales infinitos $\gamma < \omega_\alpha$ son de la forma $\gamma = \omega_\beta$ para algún β. Demostramos esa afirmación por inducción sobre α, siendo trivial el caso $\alpha = 0$ (ya que no hay ordinales infinitos $\gamma < \omega_0$, por lo que no hay nada que demostrar).

Supongamos entonces el enunciado demostrado para los ordinales iniciales infinitos menores que ω_α, y sea ahora $\gamma < \omega_{\alpha+1}$ un ordinal inicial infinito. Como $\gamma < h(\omega_\alpha)$, se sigue, por la definición de número de Hartogs, que $|\gamma| \leq |\omega_\alpha|$. Si fuera $\gamma < \omega_\alpha$ terminaríamos por hipótesis de inducción, así que suponemos $\omega_\alpha \leq \gamma$. Por tanto, $|\omega_\alpha| \leq |\gamma|$, lo que implicaría, por el Teorema de Cantor-Bernstein, $|\omega_\alpha| = |\gamma|$. Ahora bien, como tanto γ como ω_α son ordinales iniciales, se sigue $\gamma = \omega_\alpha$.

Para completar la inducción, sea finalmente α un ordinal límite tal que para todo $\alpha' < \alpha$ los ordinales menores que $\omega_{\alpha'}$ son de la forma ω_β. Tomemos entonces un ordinal inicial infinito $\gamma < \omega_\alpha$, es decir, $\gamma \in \omega_\alpha = \bigcup_{\alpha'<\alpha} \omega_{\alpha'}$. Por tanto, $\gamma \in \omega_{\alpha'}$ para algún $\alpha' < \alpha$. Por hipótesis de inducción, de $\gamma < \omega_{\alpha'}$ se sigue que $\gamma = \omega_\beta$ para algún ordinal β, como queríamos. □

Lema 7.9. *Sea $\{\alpha_i\}_{i\in I}$ un conjunto de ordinales. Si $\alpha = \bigcup_{i\in I} \alpha_i$, entonces $\omega_\alpha = \bigcup_{i\in I} \omega_{\alpha_i}$. En particular, la unión de ordinales iniciales es un ordinal inicial.*

Demostración: Para todo $i \in I$ se tiene $\alpha_i \leq \alpha$, luego $\omega_{\alpha_i} \leq \omega_\alpha$. Esto demuestra $\bigcup_{i\in I} \omega_{\alpha_i} \subseteq \omega_\alpha$, así que sólo hay que ver el otro contenido. Sea entonces $\beta \in \omega_\alpha$, que supondremos infinito (ya que, si β fuera finito, $\beta \in \omega_{\alpha_i}$ para cualquier $i \in I$, y no hay nada que demostrar). Por tanto, por el Teorema 7.3, γ es equipotente a un ordinal inicial infinito, luego por el Teorema 7.8 será $|\beta| = |\omega_{\alpha'}|$ para algún α'. Como $\beta < \omega_\alpha$, necesariamente $|\omega_{\alpha'}| < |\omega_\alpha|$, y por el Lema 7.7 se tendrá $\alpha' < \alpha$. Entonces $\alpha' \in \bigcup_{i\in I} \alpha_i$, es decir, existirá $i \in I$ tal que $\alpha' < \alpha_i$, y por tanto $|\beta| = |\omega_{\alpha'}| < |\omega_{\alpha_i}|$. Esto implica que no puede ser $\omega_{\alpha_i} \leq \beta$, luego $\beta < \omega_{\alpha_i}$, y por tanto $\beta \in \bigcup_{i\in I} \alpha_i$. □

Una vez que tenemos que los ordinales iniciales nos determinan los cardinales de conjuntos ordenados infinitos, podemos definir operaciones de suma, producto y exponenciación que correspondan al cardinal de la unión disjunta, del producto o del conjunto de

funciones. Mientras que para los números naturales tales operaciones coincidían considerada como números o como cardinales, en el caso de los ordinales iniciales esto ya no es cierto. Escogemos por tanto una letra distinta para designar a los cardinales de los ordinales iniciales:

Definición. Escribiremos $\aleph_\alpha = |\omega_\alpha|$.

Obsérvese que en principio no podemos garantizar que existan las operaciones entre los $\aleph_\alpha$. Por ejemplo, sabemos que el cardinal de $2^{\mathbb{N}}$ es mayor que $\aleph_0$, pero no sabemos que sea ningún $\aleph_\alpha$ (la Hipótesis del Continuo afirma que es $\aleph_1$), luego en principio no podemos determinar el valor de $2^{\aleph_0}$. Sin embargo, en muchos casos sí que es posible efectuar la operación. El resultado central sobre las operaciones de cardinales es la siguiente:

Teorema 7.10. $|\omega_\alpha \times \omega_\alpha| = \aleph_\alpha$ *para todo ordinal* α.

Demostración: Lo demostramos por inducción transfinita, suponiendo que $|\omega_{\alpha'} \times \omega_{\alpha'}| = \aleph_{\alpha'}$ para todo $\alpha' < \alpha$ y demostrándolo a partir de ahí para α.

Daremos primero una estrucura de conjunto bien ordenado a $\omega_\alpha \times \omega_\alpha$ que no sea la del orden lexicográfico. Concretamente, podemos considerar la función inyectiva

$$\begin{array}{ccc} \omega_\alpha \times \omega_\alpha & \to & \omega_\alpha \times \omega_\alpha \times \omega_\alpha \\ (\beta_1, \beta_2) & \mapsto & (\max\{\beta_1, \beta_2\}, \beta_1, \beta_2) \end{array}$$

que identifica $\omega_\alpha \times \omega_\alpha$ con un subconjunto de $\omega_\alpha \times \omega_\alpha \times \omega_\alpha$. Como $\omega_\alpha \times \omega_\alpha \times \omega_\alpha$ es un conjunto bien ordenado con el orden lexicográfico, entonces también lo es $\omega_\alpha \times \omega_\alpha$ con el orden $\prec$ restringido a su imagen.

Sabemos que entonces por el Teorema 5.5 que tenemos tres posibilidades:

–O bien $\omega_\alpha \times \omega_\alpha$ es isomorfo a ω_α, en cuyo caso $|\omega_\alpha \times \omega_\alpha| = \aleph_\alpha$, como queríamos.

–O bien $\omega_\alpha \times \omega_\alpha$ es isomorfo a un segmento inicial de ω_α, es decir, a un ordinal $\beta < \omega_\alpha$. Esto es absurdo, porque entonces sería $|\omega_\alpha \times \omega_\alpha| = |\beta| < |\omega_\alpha|$, mientras que claramente $|\omega_\alpha| \leq |\omega_\alpha \times \omega_\alpha|$.

–O bien ω_α es isomorfo a un segmento inicial de $\omega_\alpha \times \omega_\alpha$. Veamos que esto es imposible demostrando que, para todo $(\beta_1, \beta_2) \in \omega_\alpha \times \omega_\alpha$, el segmento inicial

$$A_{(\beta_1,\beta_2)} = \{(\beta_1', \beta_2') \in \omega_\alpha \times \omega_\alpha \mid (\beta_1', \beta_2') \prec (\beta_1, \beta_2)\}$$

tiene cardinal $|A_{(\beta_1,\beta_2)}| < \aleph_\alpha$, con lo que en particular no puede ser isomorfo a ω_α. Como la definición del orden $\prec$ implica$A_{(\beta_1,\beta_2)} \subseteq (\beta+1) \times (\beta+1)$, donde $\beta = \max\{\beta_1, \beta_2\}$, bastará demostrar que $|(\beta+1) \times (\beta+1)| < \aleph_\alpha$. Esta desigualdad es inmediata si $\beta+1$ es finito, así que supondremos que $\beta+1$ es infinito, luego por el Teorema 7.8 existirá α' tal que $|\beta+1| = |\omega_{\alpha'}|$. Al ser $\beta < \omega_\alpha$ y ser ω_α un ordinal límite (ver Ejercicio 7.2), se tiene

también $\beta+1<\omega_\alpha$, luego $|\beta+1|<|\omega_\alpha|$. Por el Lema 7.7 será $\alpha'<\alpha$, luego por hipótesis de inducción

$$|(\beta+1)\times(\beta+1)|=|\omega_{\alpha'}\times\omega_{\alpha'}|=\aleph_{\alpha'}<\aleph_\alpha$$

como queríamos demostrar. □

Introducimos a continuación la *aritmética de cardinales*, es decir, las operaciones con cardinales. Se trata de generalizar los resultados para conjuntos finitos (Lema 4.14, Teorema 4.16 y Teorema 4.17) en que el cardinal de la suma disjunta, producto cartesiano y exponenciación de conjuntos finitos vienen dados respectivamente por la suma, producto y exponenciación de números naturales. En principio la definición se puede considerar formal porque no sabemos si conocemos ya todos los posibles cardinales.

Definición. Se llama *suma de dos cardinales* λ,μ, y lo denotaremos por $\lambda+\mu$, al cardinal de $|X\cup Y|$, donde X,Y son conjuntos distintos de cardinales respectivos λ y μ (esta definición es independiente de la elección de X,Y por el Ejercicio 4.3(i))

Definición. Se llama *producto de dos cardinales* λ,μ, y lo denotaremos por $\lambda\cdot\mu$ (o simplemente $\lambda\mu$), al cardinal de $|X\times Y|$, donde X,Y son conjuntos de cardinales respectivos λ y μ (esta definición es independiente de la elección de X,Y por el Ejercicio 4.3(ii)).

Definición. Se llama *exponenciación de dos cardinales* λ,μ, y lo denotaremos por λ^μ, al cardinal de $|X^Y|$, donde X,Y son conjuntos de cardinales respectivos λ y μ (esta definición es independiente de la elección de X,Y por el Ejercicio 4.3(iii))

Observación 7.11. Nótese la conveniencia de no haber usado para cardinales infinitos la notación que usamos para los cardinales finitos, en que llamamos con el mismo nombre n al cardinal del conjunto finito n. En efecto, con la exponenciación de cardinales, el Teorema de Cantor afirma $2^{\aleph_0}>\aleph_0$, mientras que $2^{\omega_0}=\omega_0$ (ver Observación 6.14).

La suma y producto de los cardinales que ya conocemos funciona bien, en el sentido de que el resultado vuelve a ser un cardinal conocido:

Proposición 7.12. *Si α,β son ordinales, $\gamma=\max\{\alpha,\beta\}$ y n es un número natural, entonces:*

(i) $\aleph_\alpha\cdot\aleph_\beta=\aleph_\gamma$.

(ii) $n\cdot\aleph_\alpha=\aleph_\alpha$ *si* $n\neq 0$.

(iii) $\aleph_\alpha+\aleph_\beta=\aleph_\gamma$.

(iv) $n+\aleph_\alpha=\aleph_\alpha$.

(v) $\aleph_\alpha^n = \aleph_\alpha$.

Demostración: Veamos primero (i). La desigualdad $|\omega_\alpha \times \omega_\beta| \geq \aleph_\gamma$ se sigue de la función inyectiva $\omega_\gamma \to \omega_\alpha \times \omega_\beta$ definida, si $\alpha \geq \beta$ como $\delta \mapsto (\delta, 0)$, y si $\alpha < \beta$ como $\delta \mapsto (0, \delta)$.

Por otra parte, de la inclusión $\omega_\alpha \times \omega_\beta \hookrightarrow \omega_\gamma \times \omega_\gamma$ se sigue $|\omega_\alpha \times \omega_\beta| \leq |\omega_\gamma \times \omega_\gamma|$, y como $|\omega_\gamma \times \omega_\gamma| = \aleph_\gamma$ por el Teorema 7.10, se deduce $|\omega_\alpha \times \omega_\beta| \leq \aleph_\gamma$

La parte (ii) la vemos también usando la doble desigualdad. Obviamente $n \cdot \aleph_\alpha \geq 1 \cdot \aleph_\alpha = \aleph_\alpha$. La otra desigualdad se obtiene de la cadena de la desigualdad $n \cdot \aleph_\alpha \leq \aleph_\alpha \cdot \aleph_\alpha$ y de (i).

Para la parte (iii) observamos que $\aleph_\gamma \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\gamma + \aleph_\gamma = 2 \cdot \aleph_\gamma$. Como la parte (ii) implica $2 \cdot \aleph_\gamma = \aleph_\gamma$, las desigualdades son todas igualdades.

La parte (iv) se obtiene de la (iii), ya que se tiene una cadena de desigualdades $\aleph_\alpha \leq n + \aleph_\alpha \leq \aleph_0 + \aleph_\alpha = \aleph_\alpha$.

Finalmente, la parte (v) se obtiene fácilemente por inducción sobre n a partir de (i). □

Aparte de (v) en la proposición anterior), para la exponenciación se pueden dar de momento sólo resultados parciales (ver el Teorema 8.15 para el resultado completo supuesto el Axioma de Elección). Indicamos como muestra el siguiente:

Proposición 7.13. *Si* $\alpha \leq \beta$, *entonces* $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$.

Demostración: Primero observamos que, como $\aleph_\alpha > 2$ se sigue $\aleph_\alpha^{\aleph_\beta} \geq 2^{\aleph_\beta}$. Por otra parte, usando $\aleph_\alpha < 2^{\aleph_\alpha}$ se deduce

$$\aleph_\alpha^{\aleph_\beta} \leq (2^{\aleph_\alpha})^{\aleph_\beta} = 2^{\aleph_\alpha \cdot \aleph_\beta}.$$

Como por la parte (i) se tiene $\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$ (ya que $\max\{\alpha, \beta\} = \beta$ por ser $\alpha \leq \beta$), se sigue el resultado. □

Sin embargo, el resultado de tal operación no se conoce ni para $\alpha = 0$. Si supiéramos que los $\aleph_\alpha$ son todos los cardinales, entonces $2^{\aleph_0} = \aleph_\alpha$ para algún $\alpha > 0$. Supongamos además:

Hipótesis del Continuo. *No existe ningún conjunto* X *tal que* $\aleph_0 < |X| < 2^{\aleph_0}$.

Entonces, como $\aleph_0 < \aleph_1 \leq \aleph_\alpha$, necesariamente $\alpha = 1$, es decir, $2^{\aleph_0} = \aleph_1$.

Observación 7.14. Hemos visto que los conjuntos bien ordenados satisfacen todas las buenas propiedades que queremos respecto a cardinalidad, comparabilidad,... Cabe

entonces preguntarse: ¿Y no ocurrirá que cada conjunto admite un buen orden? Para responder a ello, dado un conjunto X, la forma natural de ordenarlo parece bastante sencilla en principio: tomo como primer elemento cualquier $x_0 \in X$, como siguiente elemento cualquier elemento de $X - \{x_0\}$ y así sucesivamente. Ya sabemos que este "y así sucesivamente" debe tomarse como una recurrencia (transfinita), es decir, que debemos construir una sucesión x_α que ordene los elementos de X. Un primer obstáculo es que no sabemos "en qué α debemos parar". En realidad esto no es un obstáculo serio, ya que basta tomar como x_α un elemento fijo $y \notin X$ si "al llegar a α se nos han terminado los elementos de X". Dicho ya de forma más precisa, buscamos definir una operación F mediante

$$F(\alpha) = \begin{cases} \text{algún } x_\alpha \in X - \operatorname{Im}(F \restriction \alpha) & \text{si } X - \operatorname{Im}(F \restriction \alpha) \neq \emptyset \\ y & \text{en caso contrario.} \end{cases}$$

Ahora bien, para que esto sea posible, necesitamos una operación G que asocie a cada conjunto $F \restriction \alpha$ un elemento $x_\alpha \in X - \operatorname{Im}(F \restriction \alpha)$ (si este conjunto no es vacío). Esto sería posible, por ejemplo, si tuviéramos una función $g : \mathcal{P}(X) \to X$ de forma que $g(S) \in S$ para todo $S \in \mathcal{P}(X)$ tal que $S \neq \emptyset$. En tal caso, definiríamos $G(F \restriction \alpha) = g(X - \operatorname{Im}(F \restriction \alpha))$. El problema es que la existencia de tal función no se puede deducir de los axiomas que tenemos hasta el momento.

Definición. Se llama *función de elección* de un sistema de conjuntos S a una función con dominio S que asocia a cada conjunto no vacío de S un elemento suyo.

Teorema 7.15. *Cualquier sistema finito de conjuntos tiene una función de elección.*

Demostración: Los demostramos por inducción sobre el número de conjuntos, siendo trivial el enunciado para el sistema vacío de conjuntos. Supongamos entonces todos los sistemas de n conjuntos tienen una función de elección y sea S un sistema de $n+1$ conjuntos. Si fijamos entonces X un elemento de S, el sistema $S - \{X\}$ tiene ahora n elementos, por lo que tiene una función de elección g'. Si fijamos un elemento x, pidiendo que esté en X si $X \neq \emptyset$ (si $X = \emptyset$ vale cualquier x), entonces $g' \cup \{(X, x)\}$ es una función de elección de S. □

Teorema 7.16. *Un conjunto X admite un buen orden si y sólo si $\mathcal{P}(X)$ tiene una función de elección.*

Demostración: De la Observación 7.14 se sigue que, si $\mathcal{P}(X)$ tiene un función de elección, entonces X admite un buen orden.

Supongamos entonces recíprocamente que X tiene un buen orden dado por $<$. Definimos g con dominio $\mathcal{P}(X)$ mediante

$$g(Z) = \begin{cases} \min Z & \text{si } Z \neq \emptyset \\ \emptyset & \text{si } Z = \emptyset \end{cases}$$

que claramente es una función de elección de $\mathcal{P}(X)$. □

Enunciamos entonces el axioma más significativo de toda la teoría de conjuntos, en el sentido de que se puede admitir tanto su veracidad como su falsedad (en breve discutiremos las consecuencias, no todas positivas, de admitirlo como cierto).

Axioma de Elección. *Cada sistema de conjuntos tiene una función de elección.*

Observación 7.17. Son equivalentes:

(i) El Axioma de Elección es cierto.

(ii) Para cada conjunto X, el conjunto $\mathcal{P}(X)$ tiene una función de elección.

(iii) Cada sistema de conjuntos no vacíos tiene una función de elección.

Evidentemente, (i) implica (ii), y (iii) implica (i), ya que las funciones de elección no tienen en cuenta los conjuntos vacíos. Por tanto, basta ver que (ii) implica (iii). Esto es así porque, si S es un sistema de conjuntos no vacíos, tomando $X = \bigcup S$, se tiene que S es un subconjunto de $\mathcal{P}(X)$; por tanto, la restricción a S de una función de elección de $\mathcal{P}(X)$ es una función de elección de S.

La observación anterior, junto con el Teorema 7.16, implica que el Axioma de Elección es equivalente al:

Principio del Buen Orden. *Todo conjunto admite un buen orden.*

En los resultados que siguen a continuación supondremos cierto el Axioma de Elección (de hecho, lo daremos siempre por cierto salvo que digamos lo contrario).

Teorema 7.18. *Todo conjunto infinito tiene como cardinal algún $\aleph_\alpha$ y contiene un subconjunto numerable.*

Demostración: Si X es un conjunto infinito, por el Principio del Buen Orden, tiene un buen orden, luego por el Teorema 7.3 su cardinal es el de algún ordinal inicial. Por el Teorema 7.8, el cardinal de X es entonces algún $\aleph_\alpha$. Como $\aleph_0 \leq \aleph_\alpha$, se tiene entonces que hay una función inyectiva $\mathbb{N} \to X$, luego X contiene al conjunto numerable formado por la imagen de la función. □

Corolario 7.19. *Los posibles cardinales de un conjunto son los números naturales o los $\aleph_\alpha$.*

Demostración: Por definición, si un conjunto es finito su cardinal es un número natural. Si es infinito, por el Teorema 7.18 su cardinal es un $\aleph_\alpha$. □

Teorema 7.20. *Dados dos conjuntos cualesquiera X, Y, necesariamente $|X| \leq |Y|$ o $|Y| \leq |X|$.*

Demostración: Como por el Principio del Buen Orden X, Y son conjuntos bien ordenados, el resultado se sigue del Teorema 5.5 (también puede demostrarse directamente usando el Corolario 7.19). □

Teorema 7.21. *Si X, Y son conjuntos y $X \neq \emptyset$, entonces $|X| \leq |Y|$ si y sólo si existe una función $Y \to X$ cuyo recorrido es X.*

Demostración: Una implicación ya la sabemos (Ejercicio 4.4). Basta entonces ver que, si existe $f : Y \to X$ con $\text{rec}(f) = X$, necesariamente $|X| \leq |Y|$. Para ello vamos a construir una inversa parcial de f. En concreto, consideramos el sistema de conjuntos no vacíos $S = \{f^{-1}[\{x\}] \mid x \in X\}$ y tomamos una función de elección $g : S \to Y$. Entonces, la función $h : X \to Y$ definida por $h(x) = g(\{f^{-1}[\{x\}])$ es una función inyectiva (ya que $f \circ h = id_X$), luego $|X| \leq |Y|$. □

Teorema 7.22. *Sea S un sistema de conjuntos tal que $|S| \leq \aleph_\alpha$ y $|Z| \leq \aleph_\beta$ para todo $Z \in S$. Entonces $|\bigcup S| \leq \aleph_\gamma$, con $\gamma = \max\{\alpha, \beta\}$. Además, si $\beta \geq \alpha$ y $|Z| = \aleph_\beta$ para algún $Z \in S$, entonces $|\bigcup S| = \aleph_\beta$.*

Demostración: Claramente, podemos suponer que S es un sistema no vacío de conjuntos no vacíos. Por el Teorema 7.21, podemos definir una función $f : \omega_\alpha \to S$ con $\text{rec}(f) = S$. Además, por el mismo resultado, para cada $Z \in S$, si llamamos Y_Z al conjunto de funciones $\omega_\beta \to Z$ cuyo recorrido es Z, se tiene que Y_Z es no vacío. Si g es una función de elección del sistema $\{Y_Z \mid Z \in S\}$, tenemos entonces una función

$$\begin{aligned} \omega_\alpha \times \omega_\beta &\to \bigcup S \\ (\gamma, \delta) &\mapsto \big(g(Y_{f(\gamma)})\big)(\delta) \end{aligned}$$

(en palabras sencillas, el valor de γ nos da un conjunto $f(\gamma)$ del sistema S, y tomamos el elemento en el lugar δ de ese conjunto) cuyo recorrido es claramente $\bigcup S$. El resultado sigue ahora de los Teoremas 7.21 y 7.10. □

Teorema 7.23. *El Axioma de Elección es equivalente a que cada partición de cada conjunto tenga un sistema de representantes.*

Demostración: Supongamos en primer lugar el Axioma de Elección, y sea $S \subset \mathcal{P}(X)$ una partición de un conjunto X. Entonces, si $g : S \to X$ es una función de elección de S, veamos la imagen de g es un sistema de representantes de S. En efecto, para cada $Z \in S$,

un elemento $x \in X$ están en $\mathrm{rec}(g) \cap Z$ si y sólo si $x \in Z$ y además $x = g(Z')$ para algún $Z' \in S$. Por ser g una función de elección, $x = g(Z') \in Z'$, luego $x \in Z \cap Z'$, y por ser S una partición necesariamente $Z = Z'$. Por tanto, cada $\mathrm{rec}(g) \cap Z$ consiste sólo en el elemento $g(Z)$, lo que prueba que $\mathrm{rec}(g)$ es un sistema de representantes de S.

Recíprocamente, supongamos ahora que cada partición de cada conjunto tiene un sistema de representantes, y sea S cualquier sistema de conjuntos (que supondremos no vacíos por la Observación). Queremos ver que S tiene una función de elección. Pero entonces $S' = \{\{Z\} \times Z \mid Z \in S\}$ es claramente una partición de $\bigcup S'$. Por tanto, S' tiene un sistema de representantes T'. Entonces, para cada $Z \in S$, la intersección de $\{Z\} \times Z$ con T' consiste en un único elemento (Z, z), con $z \in Z$. Claramente, la asignación $Z \mapsto z$ define una función de elección de S (de hecho, la función, vista como conjunto de pares, es T'). □

Recordemos ahora el siguiente resultado tan ampliamente usado en Matemáticas:

Lema de Zorn. *Si X es un conjunto no vacío con un orden (parcial) tal que cada cadena de subconjuntos tiene una cota superior, entonces X tiene elementos maximales.*

A pesar de su uso tan extendido, el Lema de Zorn es equivalente al Axioma de Elección, que ya hemos dicho que no hay que admitirlo necesariamente:

Teorema 7.24. *El Axioma de Elección es equivalente al Lema de Zorn.*

Demostración: Supongamos primero el Axioma de Elección, y sea X un conjunto no vacío con un orden parcial tal que cada cadena de subconjuntos tiene una cota superior. La idea es actuar como en la Observación 7.14, pero ahora construyendo una sucesión transfinita que no abarque necesariamente todos los elementos de X, sino simplemente que sea creciente (es decir, una cadena) hasta donde se pueda. Para ello, escogemos también un $y \notin X$ al que mandar los elementos de la sucesión cuando ya no pueda ser más creciente. Consideramos entonces $g : \mathcal{P}(X) \to X$ una función de elección de $\mathcal{P}(X)$, y definimos por recurrencia una sucesión x_α mediante:

$$x_\alpha = \begin{cases} g(Z_\alpha) & \text{si } Z_\alpha := \{x \in X \mid x_{\alpha'} < x \text{ para todo } \alpha' < \alpha\} \neq \emptyset \\ y & \text{en caso contrario.} \end{cases}$$

Obsérvese que, como $Z_\beta \subset Z_\alpha$ si $\beta > \alpha$, en cuanto la sucesión tome el valor y para algún α, a partir de ahí ya vale constantemente y. Además, en algún momento la sucesión debe valer y, ya que, en caso contrario, para cada ordinal α la función $\alpha \to X$ definida por $\alpha' \mapsto x_{\alpha'}$ sería una función inyectiva, es decir, $|\alpha| \leq |X|$, lo que contradice el Teorema 7.4. Podemos tomar por tanto el mínimo α tal que $x_\alpha = y$ (en particular, $Z_\alpha = \emptyset$). Entonces

los elementos $x_{\alpha'}$ con $\alpha' < \alpha$ forman una cadena en X (no vacía, puesto que al ser X no vacío al menos $x_0 \in X$). Por hipótesis del Lema de Zorn, existirá una cota superior x' para los elementos de la cadena, es decir, $x_{\alpha'} \leq x'$ para todo $\alpha' < \alpha$. Veamos que x' es un elemento maximal de X. En efecto, no puede haber ningún $x > x'$, porque sería $x > x_{\alpha'}$ para todo $\alpha' < \alpha$, con lo que $x \in Z_\alpha$, lo que es absurdo.

Recíprocamente, supongamos ahora que es cierto el Lema de Zorn, y sea S un sistema de conjuntos no vacíos. Necesitamos ver que S tiene una función de elección. Para ello, consideramos el conjunto X de todas las funciones g tales que $\mathrm{dom}(g) \subseteq S$ y tales que $g(Z) \in Z$ para todo $Z \in \mathrm{dom}(g)$ (obviamente, X es no vacío, ya que existe al menos la función vacía). Vistos los elementos de X como pares, podemos definir un orden mediante la inclusión. En el lenguaje de funciones, esto querrá decir que $g \leq g'$ si y sólo si g es la restricción de g' al dominio de g. Por tanto, está claro que toda cadena de elementos de X tiene cota superior, precisamente la unión de las funciones (ver Teorema 1.20). Por tanto, ya que suponemos cierto el Lema de Zorn, existe un elemento maximal g en X, que será una función con dominio contenido en S tal que para cada $Z \in S$ se tiene $g(Z) \in Z$. Si demostramos que necesariamente $\mathrm{dom}(g) = S$, entonces g será la función de elección de S que buscábamos. Si, por reducción al absurdo, suponemos que existe $Z \in S$ que no está en $\mathrm{dom}(g)$, basta entonces tomar cualquier $z \in Z$ y definir $g' = g \cup \{(Z, z)\}$. Se tendría entonces $g' \in X$ y $g \subset g'$, lo que es absurdo. □

Veamos ahora algunos de los usos típicos en Matemáticas del Lema de Zorn.

Ejemplo 7.25. Todo espacio vectorial V distinto de 0 tiene una base. Para ello, se considera el conjunto X de los subconjuntos linealmente independientes de V (X es no vacío, ya que si v es un vector no nulo, entonces $\{v\} \in X$). Es fácil ver que toda cadena en X tiene una cota superior (ya que la unión de una cadena de conjuntos linealmente independientes es un conjunto linealmente independiente). Por tanto, por el Lema de Zorn, el conjunto X tendrá un elemento maximal. Por el Ejercicio 1.29(i), tal elemento será una base de V.

Ejemplo 7.26. Todo ideal propio $I \subset A$ está contenido en un ideal maximal. En efecto, considerando el conjunto X de los ideales propios de A que contienen a I (X es no vacío, ya que $I \in X$), cada cadena en X tiene cota superior (ya que la unión de una cadena de ideales propios que contienen a I es un ideal propio que contiene a I). Por tanto, X tendrá un elemento maximal, que necesariamente es un ideal maximal que contiene a I.

Ejemplo 7.27. El radical de un ideal I es la intersección de todos los ideales primos que contienen a I. Es claro que el radical de I está contenido en cada ideal primo que lo contiene. Para terminar la demostración habrá que ver que, si f no está en el radical de I

entonces no está en algún primo que contenga a I. Para ello, consideramos el conjunto X de los ideales que contienen a I a cuyo radical no pertenezca f (claramente $I \in X$). Como en el ejemplo anterior, toda cadena de elementos en X tiene cota superior, luego el Lema de Zorn implica que X tiene un elemento maximal J. Si vemos que J es primo habremos terminado. Para verlo, tomamos $g, h \notin J$. Por la maximalidad de J, f estará entonces en el radical de $J + (g)$ y de $J + (h)$, luego existirán $m, n \in \mathbb{N}$ tales que $f^m \in J + (g)$ y $f^n \in J + (h)$. Multiplicando, se obtiene $f^{m+n} \in J + (gh)$. Por tanto, $J + (gh)$ no puede coincidir con J, es decir, $gh \notin J$. Esto demuestra que J es un ideal primo.

Observación 7.28. Por la longitud de la demostración omitimos los dos teoremas más importantes en los que se usa el Lema de Zorn: el Teorema de Hahn-Banach de Análisis Funcional y la existencia de la clausura algebraica de cualquier cuerpo. Cabe añadir también que el Teorema de los Ceros de Hilbert implica que, para anillos de la forma $K[X_1, \ldots, X_n]/J$ con K algebraicamente cerrado, los resultados de los Ejemplos 7.26 y 7.27 se pueden demostrar sin usar el Lema de Zorn.

Los siguientes ejemplos muestran otras situaciones típicas en que se usa directamente el Axioma de Elección (aunque suela hacerse sin avisar).

Ejemplo 7.29. Un elemento $x_0 \in \mathbb{R}$ está en la clausura de $X \subseteq \mathbb{R}$ si y sólo si existe una sucesión $\{x_n\}$ de elementos de X que tiende a x_0. Si existe tal sucesión, entonces para cada $\epsilon > 0$ existe $n \in \mathbb{N}$ tal que $|x_n - x_0| < \epsilon$, luego x_0 está en la clausura de X. Para la otra implicación hace falta ya el Axioma de Elección, ya que para cada $n \in \mathbb{N}$ el conjunto $X_n = \{x \in X \mid |x - x_0| < \frac{1}{n}\}$ es no vacío, y para encontrar la sucesión buscada hace falta tener una función de elección para el sistema de conjuntos $\{X_n \mid n \in \mathbb{N}\}$ (cosa que en un curso de Análisis de primer año suele hacerse sin más).

Ejemplo 7.30. Una función $f : \mathbb{R} \to \mathbb{R}$ es continua en un punto x_0 si y sólo si para cada sucesión $\{x_n\}$ que tienda a x_0 se tiene que $\{f(x_n)\}$ tiende a $f(x_0)$. Como antes, una implicación no necesita el Axioma de Elección. En efecto, supongamos que f sea continua en x_0. Tomamos una sucesión $\{x_n\}$ que tiende a x_0, y veamos que $\{f(x_n)\}$ tiende a $f(x_0)$. Para cada $\epsilon > 0$ existirá $\delta > 0$ tal que $|f(x) - f(x_0)| < \epsilon$ si $|x - x_0| < \delta$. Por tender $\{x_n\}$ a x_0, existirá $n_0 \in \mathbb{N}$ tal que $|x_n - x_0| < \delta$ si $n \geq n_0$, luego también se tendrá $|f(x_n) - f(x_0)| < \epsilon$ si $n \geq n_0$, lo que demuestra que $\{f(x_n)\}$ tiende a $f(x_0)$.

Recíprocamente, supongamos que f no sea continua en x_0. Entonces existe $\epsilon > 0$ tal que para cada $\delta > 0$ existe un x' tal que $|x' - x_0| < \delta$ y $|f(x') - f(x_0)| \geq \epsilon$. Por tanto, para cada $n \in \mathbb{N}$, el conjunto $X_n = \{x' \in \mathbb{R} \mid |x' - x_0| < \frac{1}{n} \text{ y } |f(x') - f(x_0)| \geq \epsilon\}$ es no vacío. Escogiendo una función de elección de la familia $\{X_n\}$, se obtiene un $x_n \in X_n$ para todo $n \in \mathbb{N}$, y claramente la sucesión $\{x_n\}$ tiende a x_0 mientras que la sucesión $\{f(x_n)\}$ no tiende a $f(x_0)$.

Los problemas de los dos ejemplos anteriores pueden resolverse suavizando el Axioma de Elección:

Axioma de Elección Numerable. *Todo sistema numerable de conjuntos tiene una función de elección.*

Pasamos ahora a las consecuencias negativas de suponer el Axioma de Elección:

Ejemplo 7.31. No existe ninguna función $\mu : \mathcal{P}(\mathbb{R}) \to [0, \infty) \cup \{\infty\}$ que satisfaga:

(i) $\mu([a, b]) = b - a$.

(ii) $\mu(\emptyset) = 0$, $\mu(\mathbb{R}) = \infty$.

(iii) Si $\{Z_n \mid n \in \mathbb{N}\}$ es un sistema de conjuntos mutuamente disjuntos, entonces

$$\mu(\bigcup_{n\in\mathbb{N}} Z_n) = \sum_{n\in\mathbb{N}} \mu(Z_n).$$

(iv) Para todo $x \in X$ y todo $Z \subseteq \mathbb{R}$, si $x + Z = \{x + z \mid z \in Z\}$ se tiene $\mu(x + Z) = \mu(Z)$.

En efecto, consideramos en $\mathbb{R}$ la relación de equivalencia dada por xRy si y sólo si $x - y \in \mathbb{Q}$. Entonces, suponiendo el Axioma de Elección, por el Teorema 7.23 existirá un sistema de representantes X de $\mathbb{R}/R$. Se demuestra fácilmente que $\mathbb{R}$ es la unión disjunta

$$\mathbb{R} = \bigcup_{q\in\mathbb{Q}} (X + q)$$

donde $X + q = \{x + q \mid x \in X\}$. Entonces, si suponemos que existe μ, entonces por (iv) se tendrá $\mu(X + q) = \mu(X)$ para todo $q \in \mathbb{Q}$, luego por (iii) debe ser $\mu(X) > 0$ (ya que si no sería $\mu(\mathbb{R}) = 0$, en contra de (ii)). Usando de nuevo (ii) y (iii) y que

$$X = \bigcup_{n\in\mathbb{Z}} (X \cap [n - 1, n)),$$

se sigue que existe un intervalo $[n - 1, n]$ tal que $\mu(X \cap [n - 1, n)) > 0$. Entonces, de la igualdad

$$\bigcup_{q\in\mathbb{Q}\cap[0,1]} ((X \cap [n - 1, n]) + q) \subset [n - 1, n + 1]$$

se seguirá que el conjunto de la izquierda tiene medida infinita (por ser unión numerable de conjuntos disjuntos de igual medida positiva), mientras que el de la derecha tiene medida 2 (por (i)), lo que es absurdo (ver el Ejercicio 7.32(vi)).

Ejercicio 7.32. Demostrar que, si una función $\mu : \mathcal{P}(\mathbb{R}) \to [0, \infty) \cup \{\infty\}$ satisface las propiedades (i)-(iv) anteriores, satisface también las propiedades:

(v) Si $Z \cap Z' = \emptyset$, entonces $\mu(Z \cup Z') = \mu(Z) + \mu(Z')$.

(vi) Si $Z \subseteq Z' \subseteq \mathbb{R}$, entonces $\mu(Z) \leq \mu(Z')$.

(vii) Para cualesquiera $Z, Z' \subseteq \mathbb{R}$, se tiene $\mu(Z \cup Z') = \mu(Z) + \mu(Z') - \mu(Z \cap Z')$.

(viii) Si $\{Z_n \mid n \in \mathbb{N}\}$ es un sistema de conjuntos, entonces $\mu(\bigcup_{n\in\mathbb{N}} Z_n) \leq \sum_{n\in\mathbb{N}} \mu(Z_n)$.

8. Aritmética de cardinales y últimos axiomas

Retomamos finalmente la aritmética de cardinales a partir del Axioma de Elección. La suma y el producto ya están completos por la Proposición 7.12 (aunque enseguida ampliaremos la definición a sumas y productos infinitos), así que empezamos por volver a la situación de la Proposición 7.13.

Teorema 8.1. $2^{\aleph_\alpha} \geq \aleph_{\alpha+1}$ *para todo ordinal* α.

Demostración: Por el Teorema de Cantor, $2^{\aleph_\alpha} > \aleph_\alpha$. Por tanto, usando el Teorema 7.18, necesariamente $2^{\aleph_\alpha} = \aleph_\beta$ con $\beta > \alpha$, es decir, $2^{\aleph_\alpha} \geq \aleph_{\alpha+1}$. □

Como en el caso $\alpha = 0$, podemos enunciar (aunque sin tomar como axioma):

Hipótesis del Continuo Generalizada. $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Si damos por buenos el Axioma de Elección y la Hipótesis del Continuo Generalizada se obtiene:

Proposición 8.2. *Sean* α, β *ordinales. Entonces:*

(i) Si $\alpha \leq \beta$, *se tiene* $\aleph_\alpha^{\aleph_\beta} = \aleph_{\beta+1}$.

(ii) Si $\beta \leq \alpha$, *se tiene* $\aleph_\alpha \leq \aleph_\alpha^{\aleph_\beta} \leq \aleph_{\alpha+1}$.

Demostración: La parte (i) es consecuencia inmediata de la Proposicion 7.13 y de la Hipótesis del Continuo Generalizada. Para la parte (ii), basta considerar la cadena de desigualdades

$$\aleph_\alpha = \aleph_\alpha^1 \leq \aleph_\alpha^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\alpha} = \aleph_{\alpha+1}.$$

□

Observación 8.3. En realidad, se sabe (ver Teorema 8.15) cuándo $\aleph_\alpha^{\aleph_\beta}$ toma uno de los dos valores posibles si $\beta \leq \alpha$, y depende de si ω_α es regular o singular (explicaremos brevemente esa noción más adelante). Si ω_α es regular, entonces

$$\aleph_\alpha^{\aleph_\beta} = \begin{cases} \aleph_{\alpha+1} & \text{si } \beta = \alpha \\ \aleph_\alpha & \text{si } \beta < \alpha. \end{cases}$$

Sin embargo, si ω_α es singular, existe un cardinal $cf(\omega_\alpha) < \omega_\alpha$ (llamado la *cofinalidad del cardinal* ω_α) tal que

$$\aleph_\alpha^{\aleph_\beta} = \begin{cases} \aleph_{\alpha+1} & \text{si } cf(\omega_\alpha) \leq \aleph_\beta \leq \aleph_\alpha \\ \aleph_\alpha & \text{si } \aleph_\beta < cf(\aleph_\alpha). \end{cases}$$

Para terminar de determinar el valor de esas operaciones, podemos observar que $\aleph_\alpha^{\aleph_\beta}$ se puede interpretar como el producto $\aleph_\beta$ veces del cardinal $\aleph_\alpha$. Para ello, ampliaremos la aritmética de cardinales considerando sumas y productos infinitos. Las definiciones naturales de estas operaciones serían las siguientes (recuérdese la definición de producto arbitrario dada en el Ejercicio 1.23):

Definición. Sea $\{\lambda_i\}_{i\in I}$ una familia de cardinales. Se llama *suma de la familia de cardinales* al cardinal $\sum_{i\in I}\lambda_i$ de $\bigcup_{i\in I} X_i$, donde $\{X_i \mid i\in I\}$ es una familia de conjuntos disjuntos dos a dos tales que $|X_i|=\lambda_i$ para todo $i\in I$. Se llama *producto de la familia de cardinales* al cardinal $\prod_{i\in I}\lambda_i$ de $\prod_{i\in I} X_i$, donde $\{X_i \mid i\in I\}$ es una familia de conjuntos tales que $|X_i|=\lambda_i$ para todo $i\in I$.

Sin embargo, para ver que esta noción está bien definida necesitaremos el Axioma de Elección:

Lema 8.4. *Sean $\{X_i\}_{i\in I}$ y $\{X'_i\}_{i\in I}$ dos familias de conjuntos tales que $|X_i|=|X'_i|$ para todo $i\in I$. Entonces:*

(i) Si tanto los conjuntos X_i como X'_i son disjuntos dos a dos, $|\bigcup_{i\in I} X_i| = |\bigcup_{i\in I} X'_i|$.

(ii) $|\prod_{i\in I} X_i| = |\prod_{i\in I} X'_i|$.

Demostración: Para cada $i\in I$, el conjunto Y_i de las biyecciones de X_i a X'_i es no vacío. Por el Axioma de Elección, podemos definir una función de dominio I que asocia a cada $i\in I$ un elemento de Y_i, es decir, una biyección $f_i : X_i \to X'_i$.

En las hipótesis de (i), es fácil ver que entonces que $\bigcup_{i\in I} f_i$ (viendo las funciones como conjuntos de pares) es una biyección de $\bigcup_{i\in I} X_i$ a $\bigcup_{i\in I} X'_i$.

Para ver (ii), basta definir $f : \prod_{i\in I} X_i \to \prod_{i\in I} X'_i$ que manda a cada elemento $\{x_i\}_{i\in I}\in\prod_{i\in I} X_i$ a $\{f_i(x_i)\}_{i\in I}$. Claramente f es una biyección. □

Empezamos estudiando las sumas, que son las que son más fáciles. Comenzamos con una observación muy simple pero práctica.

Lema 8.5. *Si $\lambda_i=\lambda$ para todo $i\in I$, entonces:*

(i) $\sum_{i\in I}\lambda_i = \lambda|I|$.

(ii) $\prod_{i\in I}\lambda_i = \lambda^{|I|}$.

Demostración: Sea X un conjunto de cardinal λ. Entonces el producto cartesiano $X\times I$ se puede descomponer como unión disjunta $X\times I = \bigcup_{i\in I}(X\times\{i\})$. Como cada $X\times\{i\}$ tiene cardinal λ, se sigue

$$\lambda|I| = |X\times I| = |\bigcup_{i\in I}(X\times\{i\})| = \sum_{i\in I}\lambda$$

lo que demuestra (i).

Para demostrar (ii), basta observar que, por definición (ver Ejercicio 1.23) $\prod_{i\in I} X = X^I$. □

Obviamente, si I es un conjunto finito, la suma coincide con la suma de cardinales ya definida. Nos dedicaremos entonces sólo a sumas infinitas. Además, supondremos que ningún sumando es cero, ya que obviamente no aportan nada a la suma. Entonces, como el cardinal de I será algún $\aleph_\alpha$, podemos sustituir I por el correspondiente ω_α. Por otra parte, agrupando los sumandos finitos y los infinitos basta estudiar separadamente las sumas infinitas de cardinales finitos y las sumas infinitas de cardinales infinitos. Empecemos por las primeras:

Proposición 8.6. *Sea $\{n_{\alpha'}\}_{\alpha'\in\omega_\alpha}$ una colección infinita de números naturales no nulos. Entonces $\sum_{\alpha'\in\omega_\alpha} n_{\alpha'} = \aleph_\alpha$.*

Demostración: Se sigue del Teorema de Cantor-Bernstein y de la cadena de desigualdades (en donde usamos el Lema 8.5(i)):

$$\aleph_\alpha = 1\aleph_\alpha = \sum_{\alpha'\in\omega_\alpha} 1 \leq \sum_{\alpha'\in\omega_\alpha} n_{\alpha'} \leq \sum_{\alpha'\in\omega_\alpha} \aleph_0 = \aleph_0\aleph_\alpha = \aleph_\alpha$$

(en la última igualdad hemos usado la Proposición 7.12(i)). □

Teorema 8.7. *Sea $\{\beta(\alpha')\}_{\alpha'\in\omega_\alpha}$ una colección de ordinales, y sea $\beta = \bigcup_{\alpha'\in\omega_\alpha} \beta(\alpha')$. Entonces $\sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')} = \aleph_\alpha\aleph_\beta$.*

Demostración: Lo demostraremos usando el Teorema de Cantor-Bernstein. Está claro que se tiene $\sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')} \leq \sum_{\alpha'\in\omega_\alpha} \aleph_\beta = \aleph_\alpha\aleph_\beta$ (usando el Lema 8.5(i)). Demostremos pues la otra desigualdad. Como por la Proposición 7.12(i) se tiene que $\aleph_\alpha\aleph_\beta = \aleph_{\max\{\alpha,\beta\}}$, bastará ver $\aleph_\alpha, \aleph_\beta \leq \sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')}$. Evidentemente $\aleph_\alpha = \sum_{\alpha'\in\omega_\alpha} 1 \leq \sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')}$, así que falta ver $\aleph_\beta \leq \sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')}$.

Como $\sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')}$ es un cardinal infinito, podemos escribir $\sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')} = \aleph_\gamma$. Supongamos, por reducción al absurdo, $\aleph_\gamma < \aleph_\beta$. Por el Lema 7.7, esto es equivalente a $\gamma < \beta$, es decir, $\gamma \in \beta = \bigcup_{\alpha'\in\omega_\alpha} \beta(\alpha')$. Por tanto, existe $\alpha' \in \omega_\alpha$ tal que $\gamma < \beta(\alpha')$. Entonces se tendrá $\aleph_\gamma < \aleph_{\beta(\alpha')} \leq \sum_{\alpha'\in\omega_\alpha} \aleph_{\beta(\alpha')} = \aleph_\gamma$, lo que es absurdo. □

Ejemplo 8.8. Veamos cuánto vale $1 \cdot 2 \cdot \ldots$, es decir, $\prod_{n\in\mathbb{N}-\{0\}} n$. Por una parte es claro que (usando el Lema 8.5(ii))

$$\prod_{n\in\mathbb{N}-\{0\}} n \leq \prod_{n\in\mathbb{N}-\{0\}} \aleph_0 = \aleph_0^{\aleph_0} = 2^{\aleph_0}.$$

Pero por otra parte, también (usando de nuevo el Lema 8.5(ii))

$$\prod_{n\in\mathbb{N}-\{0\}} n \geq \prod_{n\in\mathbb{N}-\{0,1\}} 2 = 2^{\aleph_0}$$

de donde se deduce que $1 \cdot 2 \cdot \ldots = 2^{\aleph_0}$, que será igual a $\aleph_1$ si admitimos la Hipótesis del Continuo.

El ejemplo anterior es bastante significativo de lo difícil que es en general calcular productos infinitos. El resultado más importante, que nos servirá más adelante, es el siguiente:

Teorema 8.9 (König)**.** *Sean $\{\lambda_i\}_{i\in I}$ y $\{\mu_i\}_{i\in I}$ dos familias de cardinales tales que $\lambda_i < \mu_i$ para todo $i \in I$. Entonces $\sum_{i\in I} \lambda_i < \prod_{i\in I} \mu_i$.*

Demostración: Sean $\{X_i\}_{i\in I}$, $\{Y_i\}_{i\in I}$ familias de conjuntos tales que $|X_i| = \lambda_i < \mu_i = |Y_i|$. Podemos suponer que los Y_i son disjuntos dos a dos, y como tenemos (usando el Axioma de elección) funciones inyectivas que no son biyectivas de cada X_i a Y_i, podemos suponer que cada X_i es un subconjunto propio de Y_i. Entonces los X_i son disjuntos entre sí, y para demostrar $\sum_{i\in I} \lambda_i \leq \prod_{i\in I} \mu_i$ bastará encontrar una función inyectiva $f : \bigcup_{i\in I} X_i \to \prod_{i\in I} Y_i$.

De nuevo usando el Axioma de elección, para cada $i \in I$ podemos escoger $y_i \in Y_i - X_i$. Recordando la definición de $\prod_{i\in I} Y_i$ como conjunto de funciones (ver Ejercicio 1.23) definimos entonces $f(x_i)$ como la función $I \to \bigcup_{i\in I} Y_i$ que manda i a x_i y $j \neq i$ a y_i. Claramente f es inyectiva, lo que prueba $\sum_{i\in I} \lambda_i \leq \prod_{i\in I} \mu_i$.

Supongamos ahora por reducción al absurdo que fuera $\sum_{i\in I} \lambda_i = \prod_{i\in I} \mu_i$. Eso quiere decir que existe una familia de conjuntos $\{Y_i\}$ tal que $|Y_i| = \mu_i$ para todo i y que podemos escribir $\prod_{i\in I} Y_i = \bigcup_{i\in I} X'_i$, donde $|X'_i| = \lambda_i$ y los X'_i son disjuntos dos a dos. Para cada $i \in I$, llamamos X_i a la imagen de la composición $X'_i \hookrightarrow \prod_{i\in I} Y_i \to Y_i$ (donde la última función es la proyección), es decir X_i es el conjunto de posibles coordenadas i-ésimas de los elementos de X'_i. Por el Teorema 7.21$^{(*)}$ tendremos $|X_i| \leq |X'_i|$, luego X_i estará contenido estrictamente en Y_i ya que tiene cardinal estrictamente menor. Usando el Axioma de Elección, tendremos un elemento en $y \in \prod_{i\in I} Y_i$ cuya i-ésima coordenada sea un $y_i \in Y_i - X_i$ para cada $i \in I$. Pero no puede ser $y \in X'_i$ para ningún $i \in I$, ya que eso implicaría $y_i \in X_i$. Por tanto $y \notin \bigcup_{i\in I} X'_i$, lo que es absurdo. □

En la proposición siguiente queremos ver a qué es equivalente que un cardinal se pueda escribir como suma infinita de ordinales. Aunque por motivos prácticos escribamos

(*) Aunque de forma implícita, aquí estamos usando de nuevo el Axioma de Elección

el enunciado por medio de funciones, se entiende mejor el contenido si se consideran los conjuntos imagen de las mismas.

Proposición 8.10. *Sean α, β ordinales. Entonces son equivalentes:*

(i) Existe una función $f : \omega_\beta \to \mathcal{P}(\omega_\alpha)$ tal que

a) $|f(\beta')| < \aleph_\alpha$ para todo $\beta' \in \omega_\beta$.

b) $f(\beta'_1) \cap f(\beta'_2) = \emptyset$ si $\beta'_1 \neq \beta'_2$.

c) $\omega_\alpha = \bigcup_{\beta' \in \omega_\beta} f(\beta')$.

(ii) Existe una función $g : \omega_\beta \to \omega_\alpha$ tal que $\omega_\alpha = \bigcup_{\beta' \in \omega_\beta} g(\beta')$.

Demostración: El resultado es trivial si $\beta = \alpha$, ya que (i) y (ii) son ciertos: basta tomar $f(\beta') = \{\beta'\}$ y g la identidad (recordando la Proposición 5.15 y que ω_α es un ordinal límite). Y si $\beta > \alpha$, tomando cualquier $\omega_\beta \to \omega_\alpha$ de recorrido ω_α y componiendo con las f y g anteriores, (i) y (ii) siguen siendo ciertos. Supondremos por tanto $\beta < \alpha$.

Supongamos primero (i) y escribamos $\aleph_{\gamma(\beta')} = |f(\beta')|$ para cada $\beta' \in \omega_\beta$. El Teorema 8.7 implica $\aleph_\alpha = \aleph_\beta \aleph_\gamma$, donde $\gamma = \bigcup_{\beta' \in \omega_\beta} \gamma(\beta')$. Como hemos supuesto $\beta < \alpha$, entonces deberá ser, por la Proposición 7.12(i), $\aleph_\alpha = \aleph_\gamma$, es decir, $\alpha = \bigcup_{\beta' \in \omega_\beta} \gamma(\beta')$. El Lema 7.9 implica entonces $\omega_\alpha = \bigcup_{\beta' \in \omega_\beta} \omega_{\gamma(\beta')}$. Por tanto, definiendo $g(\beta') = \omega_{\gamma(\beta')}$ se demuestra (ii).

Supongamos ahora (ii) y definimos $f : \omega_\beta \to \mathcal{P}(\omega_\alpha)$ mediante

$$f(\beta') = \{\alpha' \in g(\beta') \mid \alpha' \notin g(\beta'') \text{ para todo } \beta'' < \beta'\}$$

y veamos que se cumplen a), b), c). Como $f(\beta')$ está contenido en el ordinal $g(\beta') < \aleph_\alpha$, entonces $|f(\beta')| < \aleph_\alpha$, con lo que se cumple a). Además, si $\beta'_1 \neq \beta'_2$, por ejemplo $\beta'_1 < \beta'_2$, está claro por la definición que si $\alpha'' \in f(\beta'_1)$ entonces $\alpha'' \notin g(\beta'_2)$, luego $\alpha'' \notin f(\beta'_2)$; por tanto $f(\beta'_1) \cap f(\beta'_2) = \emptyset$ y se cumple b). Finalmente, dado cualquier $\alpha' \in \omega_\alpha$, como $\omega_\alpha = \bigcup_{\beta' \in \omega_\beta} g(\beta')$, existirá $\beta' \in \omega_\beta$ tal que $\alpha'' \in g(\beta')$. Si tomamos β' mínimo tal que $\alpha' \in g(\beta')$, entonces por definición $\alpha'' \in f(\beta')$, luego $\alpha' \in \bigcup_{\beta' \in \omega_\beta} f(\beta')$. Esto demuestra c). □

Definición. Se llama *cofinalidad del cardinal* $\aleph_\alpha$ al mínimo cardinal $\aleph_\beta$ para el que existe $Y \subseteq \omega_\alpha$ tal que $|Y| = \aleph_\beta$ y $\bigcup_{\alpha' \in Y} \alpha' = \omega_\alpha$. Escribiremos la cofinalidad de $\aleph_\alpha$ como $cf(\aleph_\alpha)$.

Observación 8.11. Es claro que la cofinalidad de un cardinal $\aleph_\alpha$ es también el mínimo cardinal $\aleph_\beta$ tal que existe una función $g : \omega_\beta \to \omega_\alpha$ tal que $\omega_\alpha = \bigcup_{\beta' \in \omega_\beta} g(\beta')$. Por tanto, por la Proposición 8.10, es también el mínimo cardinal $\aleph_\beta$ tal que existe una función $f : \omega_\beta \to \mathcal{P}(\omega_\alpha)$ tal que

a) $|f(\beta')| < \aleph_\alpha$ para todo $\beta' \in \omega_\beta$.

b) $f(\beta'_1) \cap f(\beta'_2) = \emptyset$ si $\beta'_1 \neq \beta'_2$.

c) $\omega_\alpha = \bigcup_{\beta' \in \omega_\beta} f(\beta')$.

Esto implica fácilmente que la cofinalidad de $\aleph_\alpha$ es el mínimo cardinal $\aleph_\beta$ para el que existe una partición $S \subseteq \mathcal{P}(\omega_\alpha)$ de ω_α tal que $|S| = \aleph_\beta$ y $|Z| < \aleph_\alpha$ para cada $Z \in S$.

Proposición 8.12. *Sea α un ordinal. Entonces.*

(i) $cf(\aleph_\alpha) \leq \aleph_\alpha$.

(ii) Si α no es un ordinal límite, entonces $cf(\aleph_\alpha) = \aleph_\alpha$.

(iii) Si α es un ordinal límite y $cf(\aleph_\alpha) = \aleph_\alpha$, *entonces* $\omega_\alpha = \alpha$.

Demostración: La parte (i) es inmediata porque, al ser ω_α un ordinal límite, la Proposición 5.15 permite escribir $\omega_\alpha = \bigcup_{\alpha' \in \omega_\alpha} \alpha'$.

Para la parte (ii), hacemos primero el caso $\alpha = 0$, que sigue de que la unión finita de conjuntos finitos es finita, luego no puede ser $cf(\aleph_0) < \aleph_0$. Si en cambio $\alpha = \gamma + 1$ para algún γ, entonces sabemos que $\beta < \alpha$ es equivalente a $\beta \leq \gamma$. Por tanto, para todo $Y \subset \omega_\alpha$ de cardinal $\aleph_\beta < \aleph_\alpha$, como $|\alpha'| < \aleph_\alpha$ para todo $\alpha' \in \alpha$, el Teorema 7.22 nos dice que $\bigcup_{\alpha' \in Y} \alpha'$ tiene cardinal menor o igual $\aleph_\gamma$, luego no puede ser nunca ω_α.

Finalmente, (iii) es consecuencia en primer lugar de la definición de ω_α, que cuando α es un ordinal líimite es $\omega_\alpha = \bigcup_{\alpha' \in \alpha} \omega_{\alpha'}$, que implica $cf(\aleph_\alpha) \leq |\alpha|$, es decir, $\aleph_\alpha \leq |\alpha|$ por nuestra hipótesis. Como por el Ejercicio 7.6 tenemos $\alpha \subseteq \omega_\alpha$ y ω_α es un ordinal inicial, se tiene necesariamente $\omega_\alpha = \alpha$. □

Definición. Un cardinal $\aleph_\alpha$ se dice que es *regular* si $cf(\aleph_\alpha) = \aleph_\alpha$, y se dice *singular* si $cf(\aleph_\alpha) < \aleph_\alpha$.

Ejemplo 8.13. La Proposición 8.12 implica que sólo los cardinales $\aleph_\alpha$ con α ordinal límite pueden ser singulares. De hecho, es fácil conseguir cardinales singulares, ya que para todo ordinal α se tiene $\omega_{\alpha+\omega} = \bigcup_{n \in \mathbb{N}} \omega_{\alpha+n}$ (pruébese como ejercicio a partir del Lema 7.9). Esto implica que cada cardinal $\aleph_{\alpha+\omega}$ es un cardinal singular (de hecho su cofinalidad es $\aleph_0$), y por tanto existen cardinales singulares arbitrariamente grandes. Cabe entonces la duda de si existen cardinales regulares $\aleph_\alpha$ con α ordinal límite. La Proposición 8.12(iii) indica que deberá ser $\omega_\alpha = \alpha$. Dicha igualdad no parece en principio que pueda alcanzarse (de hecho, un cardinal límite $\aleph_\alpha$ en esas condiciones se llama *inaccesible*, y su existencia no puede demostrarse a partir de los Axiomas de Zermelo-Frenkel junto con el Axioma de Elección y la Hipótesis del Continuo Generalizada). Sin embargo, el siguiente resultado demuestra que cardinales (no necesariamente regulares) para los que se da dicha igualdad existen y pueden ser arbitrariamente grandes.

Proposición 8.14. *Para todo ordinal β existe un cardinal $\aleph_\alpha > \aleph_\beta$ tal que $\omega_\alpha = \alpha$.*

Demostración: Basta definir por recurrencia una sucesión de ordinales $\{\alpha_n\}$ mediante $\alpha_0 = \omega_\beta$ y $\alpha_{n+1} = \omega_{\alpha_n}$. Escribimos $\alpha = \bigcup_{n\in\mathbb{N}} \alpha_n$ y veamos que $\omega_\alpha = \alpha$. Por el Ejercicio 7.6, basta demostrar $\omega_\alpha \subseteq \alpha$.

Sea entonces $\beta \in \omega_\alpha$. Por ser ω_α un ordinal inicial, $|\beta| < \aleph_\alpha$, luego, $|\beta| = \aleph_{\alpha'}$ con $\alpha' < \alpha$. Esto último quiere decir $\alpha' \in \bigcup_{n\in\mathbb{N}} \alpha_n$, luego existe $n \in \mathbb{N}$ tal que $\alpha' \in \alpha_n$. Por tanto, $|\beta| < \aleph_{\omega_{\alpha_n}}$, lo que implica $\beta < \omega_{\alpha_n}$. En otras palabra, $\beta \in \alpha_{n+1}$, luego $\beta \in \alpha$. □

Con todo esto que hemos visto ya podemos decir con precisión el valor de las exponenciales que faltaban en la Proposición 8.2:

Teorema 8.15. *Sean $\beta \leq \alpha$ dos ordinales. Entonces:*

(i) Si $\aleph_\beta < cf(\aleph_\alpha)$, entonces $\aleph_\alpha^{\aleph_\beta} = \aleph_\alpha$.

(ii) Si $cf(\aleph_\alpha) \leq \aleph_\beta$, entonces $\aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}$.

Demostración: Para demostrar (i) basta demostrar $\aleph_\alpha^{\aleph_\beta} \leq \aleph_\alpha$ ya que la Proposición 8.2(ii) nos da la otra desigualdad. Observamos en primer lugar que $\aleph_\alpha^{\aleph_\beta}$ es el cardinal del conjunto de funciones de ω_β en ω_α, y cada función puede verse como un conjunto de pares de cardinal $\aleph_\beta$ en $\omega_\beta \times \omega_\alpha$. Por tanto, $\aleph_\alpha^{\aleph_\beta}$ es menor o igual que el cardinal del conjunto de los subconjuntos de $\omega_\beta \times \omega_\alpha$ que tienen cardinal ω_β. Como $\beta < \alpha$ (ya que $\aleph_\beta < cf(\aleph_\alpha) \leq \aleph_\alpha$), se sigue de la Proposición 7.12(i) que $\omega_\beta \times \omega_\alpha$ tiene cardinal $\aleph_\alpha$. Entonces, $\aleph_\alpha^{\aleph_\beta}$ será menor o igual que el cardinal del conjunto

$$X = \{Y \subseteq \omega_\alpha \mid |Y| = \omega_\beta\}.$$

Si demostramos que X tiene cardinal menor o igual que $\aleph_\alpha$ habremos terminado.

La observación fundamental es que, al ser $\aleph_\beta < cf(\aleph_\alpha)$, dado cualquier $Y \in X$, necesariamente $\gamma' := \bigcup_{\alpha'\in Y} \alpha' \subset \omega_\alpha$, luego Y es un subconjunto de $\gamma := \gamma' + 1 < \omega_\alpha$. Esto demuestra $X \subseteq \bigcup_{\gamma\in\omega_\alpha} \mathcal{P}(\gamma)$. Como $\gamma < \omega_\alpha$ implica $|\gamma| = \aleph_{\alpha'}$ con $\alpha' < \alpha$, suponiendo la Hipótesis del Continuo Generalizada tendremos $|2^\gamma| = \aleph_{\alpha'+1} \leq \aleph_\alpha$. La desigualdad buscada se obtiene entonces de

$$|X| \leq |\bigcup_{\gamma\in\omega_\alpha} \mathcal{P}(\gamma)| \leq \sum_{\gamma\in\omega_\alpha} 2^{|\gamma|} \leq \sum_{\gamma\in\omega_\alpha} \aleph_\alpha = \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha.$$

Finalmente, para demostrar (ii), como la Proposición 8.2(ii) implica que $\aleph_\alpha^{\aleph_\beta}$ vale $\aleph_\alpha$ o $\aleph_{\alpha+1}$, basta demostrar $\aleph_\alpha^{\aleph_\beta} \neq \aleph_\alpha$. Para ello veamos que $cf(\aleph_\alpha^{\aleph_\beta}) \neq cf(\aleph_\alpha)$. Como por hipótesis $cf(\aleph_\alpha) \leq \aleph_\beta$, bastará entonces demostrar $\aleph_\beta < cf(\aleph_\alpha^{\aleph_\beta})$.

Si llamamos $\aleph_\gamma = cf(\aleph_\alpha^{\aleph_\beta})$, existirá una partición $\aleph_\alpha^{\omega_\beta} = \bigcup_{\gamma' \in \omega_\gamma} X_{\gamma'}$ tal que $|X_{\gamma'}| < |\aleph_\alpha^{\aleph_\beta}|$ para todo $\gamma' \in \omega_\gamma$. Por tanto, se tendrá la igualdad

$$\aleph_\alpha^{\aleph_\beta} = \sum_{\gamma' \in \omega_\gamma} |X_{\gamma'}|$$

y, por el Teorema de König se obtiene $\aleph_\alpha^{\aleph_\beta} < \prod_{\gamma' \in \omega_\gamma} \aleph_\alpha^{\aleph_\beta}$ y por tanto

$$\aleph_\alpha^{\aleph_\beta} < (\aleph_\alpha^{\aleph_\beta})^{\aleph_\gamma} = \aleph_\alpha^{\aleph_\beta \aleph_\gamma}.$$

Esto implica que no puede ser $\aleph_\beta \aleph_\gamma = \aleph_\beta$, por lo que necesariamente $\aleph_\beta < \aleph_\gamma$, es decir, $\aleph_\beta < cf(\aleph_\alpha^{\aleph_\beta})$, como queríamos. □

Como cierre de estas notas, vamos a recopilar todos los axiomas que hemos ido incluyendo (con uno más que no hemos necesitado), y que son los llamados **Axiomas de Zermelo-Frenkel**:

Axioma de Existencia. *Existe un conjunto sin elementos.*

Axioma de Extensionalidad. *Si cada elemento de X es un elemento de Y y cada elemento de Y es un elemento de X, entonces $X = Y$.*

Axioma de Separación. *Dada una propiedad P y un conjunto X, existe un conjunto Z tal que $x \in Z$ si y sólo si $x \in X$ y x.*

Axioma del Par. *Dados X, Y, existe un conjunto Z tal que $x \in Z$ si y sólo si $x = X$ o $x = Y$.*

Axioma de la Unión. *Para todo conjunto S, existe un conjunto, que denotaremos $U = \bigcup S$, tal que $x \in \bigcup S$ si y sólo si $x \in X$ para algún $X \in S$.*

Axioma del Conjunto Potencia. *Dado cualquier conjunto X, existe un conjunto $\mathcal{P}(X)$ tal que $x \in \mathcal{P}(X)$ si y sólo si x es un subconjunto de X.*

Axioma de Infinitud. *Existe algún conjunto inductivo.*

Axioma de Sustitución. *Si $P(x, y)$ es una propiedad tal que para cada x existe un único y tal que $P(x, y)$, entonces ocurre que, para cada conjunto X, existe un conjunto Y con la propiedad de que si $x \in X$ entonces existe $y \in Y$ tal que $P(x, y)$ es cierta.*

Axioma de Fundación. *Cada conjunto no vacío X tiene un elemento $x \in X$ tal que $x \cap X = \emptyset$.*

Axioma de Elección. *Cada sistema de conjuntos tiene una función de elección.*

El Axioma de Fundación (también llamado Axioma de Regularidad) no lo hemos necesitado para ninguna de las construcciones y definiciones fundamentales. Su uso es más bien técnico para evitar situaciones atípicas. Por ejemplo, dado cualquier conjunto X, sabemos por el Axioma del Par que $\{X\}$ es un conjunto no vacío. Como tiene un único elemento X, el Axioma de Fundación implica que $X \cap \{X\} = \emptyset$, es decir, $X \notin X$. Como ya hemos visto en numerables ocasiones, el hecho de que un conjunto no se pueda contener a sí mismo como elemento evita muchos problemas. De la misma forma, dados dos conjuntos y considerando el conjunto $\{X, Y\}$, el Axioma de Fundación implica que no puede ocurrir simultáneamente $Y \in X$ y $X \in Y$.

Una última cuestión que es lícita (incluso saludable) plantearse es si existirá alguna definición precisa de conjunto con la que se cumplan todos estos axiomas. Indicamos aquí brevemente el primer modelo conocido. Se trata de ir describiendo por recurrencia transfinita los posibles conjuntos. El primer peldaño es claro, y definimos $L_0 = \omega$. Es decir, los primeros conjuntos que consideramos son los elementos de ω, i.e. los números naturales (definidos como conjuntos, que es como los hemos construido en la sección 2). Los conjuntos que consideramos en una segunda etapa L_1 serán los subconjuntos dados por los elementos de L_0 definidos por una propiedad $P(n)$. Obsérvese que cada número natural es entonces un elemento de L_1, es decir, $L_0 \subseteq L_1$. La definición completa de los L_α por recurrencia transfinita es:

(i) $L_0 = \omega$.

(ii) $L_{\alpha+1}$ es el conjunto de subconjuntos de L_α definidos por una propiedad $P(x)$ de los $x \in L_\alpha$.

(iii) Si α es un ordinal límite, $L_\alpha = \bigcup_{\alpha' < \alpha} L_{\alpha'}$.

Definición. Un *conjunto constructible* es un elemento de algún L_α.

El *modelo constructible* consiste en el modelo en que los conjuntos son los conjuntos constructibles. Obsérvese que todos los conjuntos que hemos construido hasta ahora son constructibles, ya que se basaban en funciones, relaciones y, en definitica, conjuntos de pares, y un par es también un subconjunto. Por tanto, conjuntos como $\mathbb{R}$ no son sino un elemento de las partes de las partes... de un conjunto formado por naturales (que por cierto se construyen todos a partir del conjunto vacío).

Una forma de imponer el modelo constructible es añadir el siguiente axioma:

Axioma de Constructibilidad. *Todo conjunto es constructible.*

Se puede demostrar que el Axioma de Constructibilidad implica la Hipótesis del Continuo Generalizada.