Benemérita Universidad Autónoma de Puebla

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

LICENCIATURA EN MATEMÁTICAS

DEL AXIOMA DE ELECCIÓN: SUSTITUYENDO A ZORN POR HAUSDORFF EN ÁLGEBRA

TESIS

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN MATEMÁTICAS

PRESENTA
BRUNO LÓPEZ GARCÍA

DIRECTOR DE TESIS
Dr. IVÁN FERNANDO VILCHIS MONTALVO

SINODALES
DR. JOSÉ JUAN ANGOA AMADOR
DR. AGUSTÍN CONTRERAS CARRETO
DR. CÉSAR CEJUDO CASTILLA

PUEBLA, PUE. JUNIO - 2019

A mis padres,
porque ellos siempre han creido en mi,
más que nadie.

Agradecimientos

Le agradezco a mi madre Rocío quien ha sido mi guía toda mi vida, quien me ha enseñado tanto y se volvió mi amiga.

Le agradezco a mi padre Gerardo, quien pienso que es el hombre más bueno que jamas conoceré, y es mi ejemplo a seguir.

Le agradezco a mi asesor, el doc Fernando, que me tuvo paciencia infinita, me escucho y me aconsejó.

Le agradezco a mis amigos por hacer este viaje realmente divertido, a Coco por enseñarme a pensar mejor, a Kike por enseñarme a trabajar más duro, a Brian por ser quien mejor me ha entendido, y en general a todos con quienes tengo buenos recuerdos.

Le agradezco a todos los profesores que nunca se rindieron tratando de enseñarme, particularmente al profesor Poisot que me dio la clave para estudiar mejor.

En fin le agradezco a la FCFM por ser un hogar para mi.

Introducción

Of course not, but I am told it works even if you don't believe in it.

Niels Bohr (cuando se le preguntó si creía que una herradura colgada sobre su puerta le daba suerte).

Después de crear su teoría de conjuntos, Cantor, dejó dos conjeturas: la Hipótesis del Continuo y el Teorema del Buen Orden. A principios del siglo XX, gracias a Ernst Zermelo, se postula el axioma de elección en su formalización de la prueba del Teorema del Buen Orden; y desde entonces las equivalencias del axioma de elección se dejan ver en muchas ramas de las matemáticas. No obstante se puede ver una gran aversión hacía el axioma de elección por una notable cantidad de matemáticos; la razón de esto es que no es constructivo y que tiene consecuencias contraintuitivas como por ejemplo la paradoja de Banach-Tarski o el buen ordenamiento de los números reales, como lo dicho por Luzin: "Para mí, usar el axioma de Zermelo en la prueba de un teorema, es valioso sólo como indicación de que es inútil gastar tiempo en una prueba exacta de la falsedad del teorema en cuestión". Sin embargo, para el desagrado de estos matemáticos, el axioma de elección también es equivalente a resultados que son de los más naturales, en particular la existencia de bases en los espacios vectoriales. Hoy día el axioma de elección y sus "creyentes"ganan terreno pues en algunas ocasiones es insalvable usar principios no constructivos, desastres pasan sin él y bellos teoremas no pueden ser probados. Dado el creciente desarrollo de las matemáticas se empezó a prescindir de los métodos constructivistas; un principio que usaron diversos matemáticos para reemplazar la inducción transfinita y el Teorema del Buen Orden, matemáticos como Zorn, Hausdorff, Kuratowski entre otros. Hoy día su forma más famosa es el Lema de Zorn (de acuerdo a Zorn, Artin y Chevalley se refirieron al principio como Lema de Zorn en 1933). Godel probó la relativa consistencia del axioma en 1939, este personaje es importante pues es uno de los creadores de la teoría de conjuntos NBG, la cual fue desarrollada por Von Neumann-Bernays-Gödel; en tal teoría está completamente determinada la relativa consistencia e independencia del axioma de elección, que se puede encontrar de manera clara en [6] y [7]. El axioma

de elección es uno de los axiomas más discutidos, quizá sólo seguido por el axioma de las paralelas de Euclides. En el primer capítulo de esta tesis sentaremos las bases necesarias mencionando los axiomas en los que nos basamos, una rapida introducción a los conjuntos ordinales y a la teoría de módulos, tan imperiosos para el desarrollo claro de muchos conceptos y resultados. En el segundo capítulo veremos equivalencias del axioma de elección en un esfuerzo por mostrar la diversidad de enunciados que hacen referencia a la necesidad de los matemáticos por crear de manera no constructiva, todos estos principios, acertadamente llamados principios de maximidad; llevan en su escencia el encontrar un máximo. Para el tercer capítulo de este trabajo, dada la variedad de principios de maximidad, sustituiremos el Lema de Zorn por el principio que nos regaló Hausdorff, y que a mi parecer es muy "poderoso", en pruebas clásicas del álgebra moderna.

Índice general

Capítulo 1

Preliminares

En este capítulo sentaremos las bases necesarias para el entendimiento de esta tesis. Como primer paso vamos a presentar algunos axiomas básicos de la teoría de conjuntos, así como algunos conceptos, entre ellos nuestros objetos primarios, los conjuntos que se pueden pensar como colecciones de "cosas" que tienen alguna característica en común; dada la vaguedad con la que podríamos pensar los conjuntos, es el por qué se enlistaran los axiomas necesarios para entender este trabajo. Por otro lado, la característica en común de la que hablamos la llamaremos propiedad y se denotara $P(x)$, y su veracidad o falsedad dependera del parametro x. Por último antes de empezar, necesitaremos algúnos símbolos básicos como: $=$, $($, $)$, $\in$ y letras del alfabeto español así como del alfabeto griego, que serán nuestras variables. Las fórmulas son cadenas de estos simbolo que cumplen:

1. $x \in y$, $x = y$ son fórmulas.

2. Si ϕ y ξ son fórmulas, entonces (ϕ y ξ), (es falso ϕ) y (existe x que cumple ϕ) son formulas.

1.1. Axiomatica

Los axiomas que se presentaran seran los de la teoría de conjuntos ZFC, para mayor información se pueden revisar [2] y [8].

Axioma de existencia: Existe un conjunto que no tiene elementos.
A este conjunto se le conoce como conjunto vacío y se denota $\emptyset$.

Axioma de extensión: Si todo elemento de X es un elemento de Y y todo elemento de Y es un elemento de X, entonces $X = Y$.

Esquema de axioma de comprensión: Sea $P(x)$ una propiedad de x. Para todo conjunto A, existe un conjunto B tal que $x \in B$ si y sólo si $x \in A$ y $P(x)$ se cumple.
Esto es un esquema de axiomas, i.e., para cada propiedad P, tenemos un axioma. Por ejemplo, si $P(x)$ es "$x = x$", el axioma dice:

Para cualquier conjunto A, existe un conjunto B
tal que $x \in B$ si y sólo si $x \in A$ y $x = x$.

En este caso $B = A$.

Axioma del par: Para cualesquiera A y B, existe un conjunto C tal que $A \in C$ y $B \in C$.

Axioma de unión: Para cualquier conjunto S, existe un conjunto U tal que $x \in U$ si y solo si $x \in A$ para algún $A \in S$

Esquema de axioma de reemplazo: Sea $P(x, y)$ una propiedad tal que para cada x existe una única y para la cual $P(x, y)$ se cumple.
Para cada conjunto A, existe un conjunto B tal que, para cada $x \in A$, existe $y \in B$ para la cual $P(x, y)$ se cumple.
Sea F la operación definida por la propiedad P, esto es, sea $F(x)$ que denota la única y para la cual $P(x, y)$ se cumple. El correspondiente axioma de reemplazo se puede expresar como sigue:

Para cada conjunto A, existe un conjunto B
tal que para toda $x \in A$, $F(x) \in B$.

Axioma del infinito: Existe un conjunto A que contiene al vacío ($\emptyset$) y para cada x elemento de A, $S(x)$ es elemento de A.

Axioma de regularidad: Para cualquier conjunto A no vacío, existe un conjunto B que es elemento de A tal que $A \cap B = \emptyset$.

1.1 Teorema. No existe conjunto que sea elemento de si mismo.

Demostración. Sea A un conjunto tal que $A \in A$ y sea $P(x)$ la propiedad "$x = A$", por el esquema de comprensión, existe un conjunto B tal que $B = \{x \in A : x = A\}$, B es diferente del vacío pues al menos $A \in B$. Ahora para toda $x \in B$ se cumple que $x = A$, así para toda $x \in B$ se cumple que $x \cap B = A \cap B$, como $A \in A$ y $A \in B$, entonces $A \cap B \neq \emptyset$. De lo último se deduce que para toda $x \in B$, $x \cap B \neq \emptyset$ lo que contradice el axioma de regularidad. Por lo tanto no existe conjunto que se contenga a si mismo como elemento. □

Por lo dicho en el anterior teorema podemos deducir que no existe "el conjunto de los conjuntos", pues si existiera entonces se contendría a si mismo como elemento, lo que es imposible. Se habla de colecciones de conjuntos o clases cuando pensamos en todos los conjuntos agrupados, esto es la clase de los conjuntos, así las clases se pueden pensar como toda propiedad expresada por una fórmula, estos conceptos no son de mayor relevancia para este trabajo,no se ahondara más en el tema.

Axioma de elección: Si S es un conjunto de conjuntos no vacíos, existe una función $f : S \to \cup S$ tal que, para cada $x \in S$, $f(x) \in x$.

Usando el axioma de unión, dada una familia de conjuntos F, definimos la unión de F ($\cup F$), como las $x \in A$ tal que existe $Y \in F$ con $x \in Y$. De igual manera, si $F \neq \emptyset$, definimos la intersección de F ($\cap F$), como las $x \in \cup F$ tal que para toda $Y \in F$ se tiene que $x \in Y$.
Como es usual definimos los siguientes conjuntos: $A \cup B = \cup\{A, B\}$, $A \cap B = \cap\{A, B\}$ y $A - B = \{x \in A : x \notin B\}$.

1.2. Conjuntos ordenados

1.2 Definición. Un conjunto R es una relación binaria si todos los elementos de R son parejas ordenadas, i.e., si para cada $z \in R$ existen x y y tales que $z = (x, y)$, y se dice que x está en relación R con y. Esta proposición se denota xRy.

1.3 Definición. Sea R una relación binaria.

1. El conjunto de todas las x que están en relación R con algún y se llama el dominio de R y se denota $Dom(R)$.

2. El conjunto de todas las y tal que, para algún x, x está en relación R con y se llama el rango de R, denotada por $Ran(R)$.

Así podemos ver que $R \subset Dom(R) \times Ran(R)$. Además dada una relación R podemos hablar de R^{-1}, y la definimos como el conjunto

$$\{(y, x) : (x, y) \in R\}.$$

1.4 Corolario. Sea R una relación, se cumple que:

1. $(R^{-1})^{-1} = R$;
2. $Dom(R^{-1}) = Ran(R)$ y $Ran(R^{-1}) = Dom(R)$.

Dado un conjunto A, si $Dom(R) = A$ y $Ran(R) \subseteq A$ diremos que R es una relación en A.

1.5 Definición. Se dice que una relación R es función si R es univalente, donde relación univalente significa que

$$(x, y) \in R \text{ y } (x, z) \in R \Rightarrow y = z.$$

Además R será función entre X y Y si $Dom(R) = X$ y $Ran(R) \subseteq Y$.

Si f es una función entre X y Y, tal hecho se denotará por $f : X \to Y$; además si x está en relación f con y se denotará $f(y) = x$. Diremos que f es una función inyectiva si f^{-1} es función. Diremos que f es una función sobreyectiva si $Ran(f) = Y$. Por último diremos que f es una función biyectiva si es inyectiva y sobreyectiva.

1.6 Corolario. Sea f una función entre X y Y, si f es biyectiva entonces f^{-1} también es una función biyectiva.

Demostración. Primero notemos que como f es inyectiva, f^{-1} es función entre Y y X, esto último por corolario 1.4 y de la definición 1.5, así se tiene que $Ran(f^{-1}) \subseteq X = Dom(f) = Ran(f^{-1})$ y además $(f^{-1})^{-1} = f$ es función, de nuevo por corolario 1.4, por tanto f^{-1} es una función biyectiva. □

1.7 Definición. Sean $f : X \to Y$ y $g : Y \to Z$ funciones, definimos la composición $f \circ g : X \to Z$ como las parejas (x, z) tal que existe $y \in Y$ tal que $(x, y) \in f$ y $(y, z) \in g$. Esto se denotara por $(f \circ g)(x) = g(f(x))$.

1.8 Definición. Sea $f : X \to Y$ una función y $Z \subseteq X$, se define la restricción de f en C como $f \cap Z \times Y$ y se denota por $f|_Z$.

1.9 Definición. (1) Las funciones f y g se dicen compatibles si $f(x) = g(x)$ para toda $x \in Dom(f) \cap Dom(g)$.

(2) Un conjunto de funciones F se llama sistema de funciones compatibles si cualesquiera dos funciones f y g de F son compatibles.

1.10 Lema. (1) Dos funciones f y g son compatibles si y solo si $f \cup g$ es una función.

(2) Dos funciones f y g son compatibles si y solo si $f|_{(Dom(f)\cap Dom(g))} = g|_{(Dom(f)\cap Dom(g))}$.

Demostración. (1)($\Rightarrow$) Sean f y g dos funciones compatibles, para mostrar que $f \cup g$ es función mostraremos que es univalente. Primero notemos que

$$Dom(f \cup g) = Dom(f) \cup Dom(g) \text{ y que } Dom(f \cap g) = Dom(f) \cap Dom(g).$$

Sea $x \in Dom(f \cup g)$ y supongamos que $(x, y), (x, z) \in f \cup g$; si $(x, y), (x, z) \in f$, entonces por ser f una función, $y = z$; lo mismo pasa si $(x, y), (x, z) \in g$. Por último, sin pérdida de generalidad, si $(x, y) \in f$ y $(x, z) \in g$ tenemos que $f(x) = y$, $g(x) = z$ y $x \in Dom(f) \cap Dom(g)$, como f y g son compatibles y $x \in Dom(f \cap g)$, entonces $f(x) = g(x)$, o sea, $y = z$; por lo tanto $f \cup g$ es univalente.

($\Leftarrow$) Supongamos que f y g no son compatibles, entonces existe $x \in Dom(f) \cap Dom(g)$ tal que $f(x) \neq g(x)$. Sean $y = f(x)$ y $z = g(x)$; se tiene que $(x, y), (x, z) \in f \cup g$, pero por ser $f \cup g$ una función obtenemos que $y = z$, o sea, $f(x) = g(x)$, pero esto no puede ocurrir. Por lo tanto f y g son compatibles.

(2)($\Rightarrow$) Sean f y g funciones compatibles. Sea $x \in Dom(f) \cap Dom(g)$ entonces $f(x) = g(x)$; como se cumple para cualquier $x \in Dom(f) \cap Dom(g)$ entonces $f|_{(Dom(f)\cap Dom(g))} = g|_{(Dom(f)\cap Dom(g))}$.
($\Leftarrow$)Supongamos que f y g no son compatibles, entonces existe $x \in Dom(f) \cap Dom(g)$ tal que $f(x) \neq g(x)$. Por otro lado

$$f|_{(Dom(f)\cap Dom(g))}(x) = g|_{(Dom(f)\cap Dom(g))}(x),$$

lo que significa que $f(x) = g(x)$, pero esto no puede ocurrir. Por lo tanto f y g son compatibles. □

1.11 Teorema. Si F es un sistema de funciones compatible, entonces $\cup F$ es una función con $Dom(\cup F) = \cup\{Dom(f) : f \in F\}$. La función $\cup F$ extiende todas las $f \in F$.

Demostración. Claramente $\cup F$ es una relación, solo falta probar que es univalente y total izquierda. Si $(a, b_1) \in \cup F$ y $(a, b_2) \in \cup F$, entonces existen funciones $f_1, f_2 \in F$ tal que $(a, b_1) \in f_1$ y $(a, b_2) \in f_2$. Pero f_1 y f_2 son compatibles y $a \in Dom(f_1) \cap Dom(f_2)$, así tenemos que $b_1 = f_1(a) = f_2(a) = b_2$. Ahora sea $a \in Dom(\cup F)$, existe $f \in F$ tal que $a \in Dom(f)$ entonces existe b tal que $(a, b) \in f$, si existe otra $g \in F$ tal que $a \in Dom(g)$ entonces por ser F un sistema de funciones compatibles, se tiene que $f(a) = g(a)$, así $(a, b) \in \cup F$ y $\cup F$ es función. Que $\cup F$ extiende a $f \in F$ es inmediato. □

1.12 Definición. Sean A y B conjuntos. El conjunto de todas las funciones de A en B se denota B^A.

No se mostrará la existencia de B^A en esta tesis.

1.13 Definición. Dada una relación R:

1. R se llama reflexiva si para cada $a \in Dom(R)$ se cumple aRa.

2. R se llama simétrica si para aRb se cumple que bRa, y se llama antisimétrica si dado que aRb y bRa se cumple si y solo si $a = b$.

3. Una relación R se llama transitiva si dado que aRb y bRc se cumple que aRc.

4. Si R es una relación en A reflexiva, antisimétrica y transitiva se llama un orden parcial de A. La pareja (A, R) se llama un conjunto parcialmente ordenado y R es un orden parcial en A.

1.14 Definición. Sean $a, b \in A$, y sea R un orden parcial en A. Decimos que a y b son comparables en el orden R si aRb o bRa. Decimos que a y b son incomparables si no son comparables.

1.15 Definición. Un orden parcial R de A es orden lineal o total, si cualesquiera dos elementos de A son comparables. La pareja (A, R) es entonces llamada conjunto linealmente ordenado.

1.16 Definición. Sea $B \subseteq A$, donde A está parcialmente ordenado por R. B es una cadena en A si cualesquiera dos elementos de B son comparables.

En lo siguiente ocuparemos el símbolo $\leq$, que se lee "menor o igual que", y el simbolo $<$, que se lee "menor que", para denotar elementos que están relacionados en un orden parcial.

1.17 Definición. Sea $\leq$ un orden parcial en A, y sea $B \subseteq A$.

(a) $b \in B$ es el elemento menor de B en el orden $\leq$ si $b \leq x$ para cada $x \in B$.

(b) $b \in B$ es elemento mínimo de B en el orden $\leq$ si para cada $x \in B$ tal que $x \leq b$ entonces $x = b$.

El elemento mayor y elemento máximo se definen de manera análoga.

1.18 Definición. Un conjunto que está linealmente ordenada por la inclusión conjuntista, $\subseteq$, es llamada un nido.

1.19 Definición. Un isomorfismo entre dos conjuntos parcialmente ordenados (A, R) y (B, S) es una función biyectiva $f : A \to B$ tal que para toda $a_1, a_2 \in A$

$$a_1 R a_2 \textit{ si solo si } f(a_1) S f(a_2).$$

Si un isomorfismo existe entre (A, R) y (B, S), entonces (A, R) y (B, S) son isomorfos y se denota por $(A, R) \cong (B, S)$.

1.20 Corolario. Sea f un isomorfismo entre (A, R) y (B, S) entonces, f^{-1} es un isomorfismo entre (B, S) y (A, R).

Demostración. Por corolario 1.6 tenemos que f^{-1} es biyectiva. Sean $b_1, b_2 \in B$ tal que $b_1 S b_2$, como f es inyectiva existen

$$a_1, a_2 \in A \textit{ tal que } (a_1, b_1), (a_2, b_2) \in f,$$

esto implica que $(b_1, a_1), (b_2, a_2) \in f^{-1}$. Como f es isomorfismo $a_1 R a_2$ si y solo si $b_1 S b_2$, que es lo que se quería demostrar, por tanto f^{-1} es isomorfismo. $\square$

1.21 Definición. Un orden lineal $\leq$ de un conjunto A es un buen orden si cada subconjunto no vacío de A tiene mínimo. Al conjunto $(A, \leq)$ se le llama conjunto bien ordenado.

1.22 Corolario. Sea $(L, <)$ un conjunto bien ordenado y sea $M \subseteq L$, entonces $(M, <)$ también es un conjunto bien ordenado.

Demostración. Es claro que $(M, <)$ es un conjunto parcialemnte ordenado. Sean $x, y \in M$, como están en M entonces están en L y por tanto son comparables respecto a $<$, entonces son comparables en $(M, <)$ y así $(M, <)$ es un conjunto linealmente ordenado. Por último sea $M_0 \subseteq M$, como M_0 es subconjunto de M también lo es de L y por ser $(L, <)$ bien ordenado, se cumple que M_0 tiene mínimo, por lo tanto $(M, <)$ es un conjunto bien ordenado. □

1.23 Definición. Sea $(L, \leq)$ un conjunto linealmente ordenado. Un conjunto $S \subsetneq L$ es segmento inicial de L si para cada $a \in S$, toda $x \leq a$ también es elemento de S.

Si a es un elemento de $(W, <)$, un conjunto bien ordenado, llamamos segmento inicial de W, dado por a, al conjunto

$$W[a] = \{x \in W : x < a\}.$$

1.24 Lema. Si $(W, <)$ es un conjunto bien ordenado y si S es un segmento inicial de $(W, <)$, entonces existe $a \in W$ tal que $S = W[a]$.

Demostración. Sea $X = W - S$. Por la definición 1.23 S es un subconjunto propio de W, entonces X es no vacío y así tiene mínimo en el buen orden $<$. Sea a el mínimo de X. Sea $x \in W$ tal que $x < a$, entonces x no puede pertenecer a X pues a es el mínimo, así $x \in S$. Sea $x \in W$ tal que $x \geq a$, si suponemos que $x \in S$, por la definición 1.23, a pertenecería a S pero $a \notin S$, por tanto $x \notin S$. Así $S = \{x \in W : x < a\} = W[a]$. □

1.25 Proposición. Si $(A, <)$ es bien ordenado, entonces para todo $a \in A$, se cumple que $(A, <)$ no es isomorfo a $(W[a], <)$.

Demostración. Supongamos que existe $a \in A$ tal que $(A, <)$ y $(W[a], <)$ son isomorfos, por tanto existe un isomorfismo

$$f : A \to W[a].$$

Sea C el conjunto de todas las $x \in A$ tal que $f(x) \neq x$, notemos que $C \neq \emptyset$ pues de lo contrario, si $f(x) = x$ para toda $x \in A$ se tendría que $f(a) = a$ y como $f(a) \in W[a]$ entonces $a = f(a) < a$, lo cual es una contradicción, por tanto $C \neq \emptyset$.
Sea x_0 el mínimo de C, es inmediato que $f(x_0) \neq x_0$ y además $f(x_0) < a$;

como f es isomorfismo se tiene que $f(f(x_0)) \neq f(x_0)$ y por tanto $f(x_0) \in C$, así $x_0 < f(x_0) < a$ lo que implica que $x_0 \in W[a]$. Como $x_0 \in W[a]$, existe $y_0 \in A$ tal que $f(y_0) = x_0$. Es claro que $y_0 \neq x_0$ pues si $y_0 = x_0$ se tendría que $x_0 = f(y_0) = f(x_0)$ pero $x_0 \in C$ y por ende $f(x_0) \neq x_0$, lo que es imposible, de ahí que $f(y_0) \neq y_0$. Por lo anterior tenemos que $y_0 \in C$ y así $x_0 < y_0$ y como f es isomorfismo se tiene que

$$f(x_0) < f(y_0) = x_0 < f(x_0),$$

una contradicción. Por tanto $(A, <)$ no es isomorfo a $(W[a], <)$. □

1.26 Teorema. Dados (A, R) y (B, S) conjuntos ordenados, se cumple una y solo una de las siguientes afirmaciones:

1. $(A, R) \cong (B, S)$;
2. existe $a \in A$ tal que $(W[a], R) \cong (B, S)$;
3. existe $b \in B$ tal que $(W[b], S) \cong (A, R)$.

Demostración. Empecemos la prueba definiendo la relación f como

$$f = \{(a, b) : a \in A, b \in B, (W[a], R) \cong (W[b], S)\},$$

y notemos que f es función. Sean $(a, b_1), (a, b_2) \in f$ y supongamos que $b_1 \neq b_2$, así tenemos que existen isomorfismos

$$g_1 : W[a] \to W[b_1] \text{ y } g_2 : W[a] \to W[b_2].$$

Por ser g_1 biyectiva se tiene que $(g_1)^{-1} : W[b_2] \to W[a]$ es una función biyectiva. Veamos que

$$(g_1)^{-1} \circ g_2 : W[b_1] \to W[b_2]$$

es una biyección. Para mostrar que es inyectiva sean

$$(x, z_1), (x, z_2) \in ((g_1)^{-1} \circ g_2)^{-1},$$

de esto se sigue que

$$(z_1, x), (z_2, x) \in (g_1)^{-1} \circ g_2,$$

y por tanto existen $y_1, y_2 \in W[a]$ tal que

$$(z_1, y_1), (z_2, y_2) \in (g_1)^{-1}(y_1, x), (y_2, x) \in g_2,$$

por ser g_2 inyectiva se tiene que $y_1 = y_2$, así $(z_1, y_1), (z_2, y_1) \in (g_1)^{-1}$, por ser $(g_1)^{-1}$ inyectiva se tiene que $z_1 = z_2$ y por tanto concluimos que $((g_1)^{-1} \circ g_2)^{-1}$ es función y por ende $(g_1)^{-1} \circ g_2$ es inyectiva.
Ahora para ver que es sobreyectiva sea $z \in W[b_2]$, por ser g_2 sobreyectiva existe

$$y \in W[a] \ tal \ que \ (y, z) \in g_2,$$

por ser $(g_1)^{-1}$ sobreyectiva existe

$$x \in W[b_1] \ tal \ que \ (x, y) \in (g_1)^{-1},$$

esto implica que $(x, z) \in (g_1)^{-1} \circ g_2$, así $y \in Ran((g_1)^{-1} \circ g_2)$, por tanto

$$W[b_2] \subseteq (g_1)^{-1} \circ g_2 \subseteq W[b_2],$$

por tanto $(g_1)^{-1} \circ g_2$ es sobreyectiva y biyectiva.
Por último sean $y_1, y_2 \in W[b_1]$ tal que

$$y_1 S y_2 \ y \ (y_1, z_1), (y_2, z_2) \in (g_1)^{-1} \circ g_2$$

y sean $x_1, x_2 \in W[a]$ tal que

$$(y_1, x_1), (y_2, x_2) \in (g_1)^{-1} \ y \ (x_1, z_1), (x_2, z_2) \in g_2.$$

Por corolario 1.20 sabemos que $(g_1)^{-1}$ es isomorfismo, así tenemos que

$$y_1 S y_2 \ si \ solo \ si \ x_1 R x_2 \ si \ solo \ si \ z_1 S z_2.$$

Concluimos que $(g_1)^{-1} \circ g_2$ es un isomorfismo entre $(W[b_1], S)$ y $(W[b_2], S)$. Sin perdida de generalidad sea $b_1 S b_2$ por ser (B, S) bien ordenado, entonces $b_1 \in W[b_2]$, por proposición 1.25 $W[b_2]$ no puede ser isomorfo a $W[b_1]$ pero habíamos visto que si, lo que es una contradicción. Por tanto $b_1 = b_2$ y así f es una función.
Ahora veamos que f es inyectiva, supongamos que no, esto es, existen $a_1, a_2 \in A$ diferentes entre si tal que para alguna $b \in B$, $(a_1, b), (a_2, b) \in f$, esto quiere decir que

$$(W[a_1], R) \cong (W[b], S) \cong (W[a_2], R).$$

Por un argumento análogo al anterior llegamos a que $(W[a_1], R) \cong (W[a_2], R)$, por ser A bien ordenada, a_1 y a_2 con comparables, por proposición 1.25 a_1 y a_2 no pueden ser diferentes, o sea, $a_1 = a_2$ pero habíamos dicho que si

eran diferentes, lo que nos lleva a una contradicción, por tanto $a_1 = a_2$ y f es inyectiva. De lo anterior se puede concluir que $f : Dom(f) \to Ran(f)$ es biyectiva.
Supongamos que $Dom(f) \subsetneq A$ y sea x_0 el mínimo de $A - Dom(f)$, es inmediato que $W[x_0] \subseteq Dom(f)$, veamos que $Dom(f) = W[x_0]$. Supongamos que no son iguales, esto es que existe $a \in Dom(f)$ tal que $a \notin W[x_0]$(i.e. $x_0 R a$), esto implica que existe $b \in B$ tal que $(a, b) \in f$ y sea

$$g : (W[a], R) \to (W[b], S)$$

el isomorfismo entre $(W[a], R)$ y $(W[b], S)$. Sea la restricción

$$g|_{W[x_0]} : (W[x_0], R) \to (W[g(x_0)], S),$$

mostraremos que es un isomorfismo, para ello es suficiente ver que $g|_{W[x_0]}$ es sobreyectiva. Sea $y \in W[g(x_0)]$, entonces $y S f(x_0) S b$ y de esto se sigue que existe $x \in W[a]$ tal que $y = g(x)$ por ser g sobreyectiva, además $y S g(x_0)$ si y solo si $x R x_0$ por ser g isomorfismo, de esto se sigue que para $y \in W[g(x_0)]$ cualquiera, existe $x \in W[x_0]$ tal que $(x, y) \in g|_{W[x_0]}$, y así $g|_{W[x_0]}$ es isomorfismo. De lo último se sigue que $(x_0, g(x_0)) \in f$ y por tanto $x_0 \in Dom(f)$, lo que es imposible, así $Dom(f) = W[x_0]$.
Ahora supongamos que $Ran(f) \subsetneq B$ y sea y_0 el mínimo de $B - Ran(f)$, es inmediato que $W[y_0] \subseteq Ran(f)$, mostraremos que $Ran(f) = W[y_0]$. Supongamos que no son iguales, entonces existe $b Ran(f)$ tal que $b \notin W[y_0]$(i.e. $y_0 S b$), así tenemos que existe $a \in Dom(f)$ tal que $(a, b) \in f$ y sea

$$h : (W[a], R) \to (W[b], S)$$

el isomorfismo entre $(W[a], R)$ y $(W[b], S)$. Como $y_0 S b$, entonces existe $x \in W[a]$ tal que $h(x) = y_0$. Sea la restricción

$$h|_{W[x]} : (W[x], R) \to (W[y_0], S),$$

igual que antes, mostrando que es sobreyectiva basta para ver que es un isomorfismo. Para mostrar la sobreyectividad se sigue un proceso análogo al anterior, no lo explicitaremos. Por lo anterior tenemos que $(x_0, y_0) \in f$, o sea, $y_0 \in Ran(f)$, pero habíamos dicho que $y_0 \notin Ran(f)$, lo que es una contradicción y por tanto $Ran(f) = W[y_0]$.
Para finalmente probar que f es isomorfismo sean $a, b \in W[x_0]$ tal que aRb, sabemos que $(b, f(b)) \in f$ y por tanto existe un isomorfismo

$$g : (W[b], R) \to (W[f(b)], S),$$

y $g(a) \in W[f(b)]$, así tenemos que $g(a)Sf(b)$. Sea la restricción

$$g|_{W[a]} : W[a] \to W[g(a)],$$

igual que en los parrafos anteriores, se puede mostrar que $g|_{W[a]}$ es un isomorfismo, entonces $(a, g(a)) \in f$ y así $f(a) = g(a)Sf(b)$, por tanto aRb implica que $f(a)Sf(b)$. Para mostrar que $f(a)Sf(b)$ implica aRb pensamos en $f(a) = a_0$, $f(b) = b_0$, $a = f^{-1}(a_0)$ y $b = f^{-1}(b_0)$ y realizando el mismo proceso anterior se obtiene que $f(a)Sf(b)$ implica aRb que es lo que se quería probar, por lo tanto $f : Dom(f) \to Ran(f)$ es isomorfismo.
Para finalizar la prueba veamos que no se cumple $Dom(f) \neq A$ y $Ran(f) \neq B$ al mismo tiempo, para ello supongamos que si, esto implica que

$$f : (W[x_0], R) \to (W[y_0], S)$$

es un isomorfismo y de esto se sigue que $(x_0, y_0) \in f$ lo que es imposible pues $x_0 \notin Dom(f)$ y $y_0 \notin Ran(f)$.
Concluimos que las únicas posibilidades son:

1. $Dom(f) = A$ y $Ran(f) = B$;
2. $Dom(f) = W[x_0]$ y $Ran(f) = B$;
2. $Dom(f) = A$ y $Ran(f) = W[y_0]$.

Quedando demostrado el teorema. □

1.3. Ordinales

1.27 Definición. Un conjunto T es transitivo si cada elemento de T es un subconjunto de T.

Para tener una idea clara de cómo luce un conjunto transitivo y sus elementos, sea $A = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$.

1. Para $\emptyset \in A$ siempre se cumple que $\emptyset \subseteq A$.
2. Ahora para $\{\emptyset\} \in A$ tenemos que su único elemeto tambien es elemento de A, pues $\emptyset \in A$, así $\{\emptyset\} \subseteq A$.
3. Por último, al igual que en el punto 2, podemos notar que $\{\{\emptyset\}\} \subseteq A$.

El conjunto A se puede contruir gracias al axioma del par.

1.28 Definición. Un ordinal es un conjunto α tal que:

(a) α es transitivo.

(b) α está bien ordenado por $\in$.

De aquí en adelante denotaremos a la colección de todos los ordinales por O. Cabe mencionar que O no es un conjunto (es una clase), esto último no se mostrará en esta tesis pero su demostración se puede encontrar en [8]. También es conveniente notar que ningun ordinal se puede contener a si mismo como elemento, esto gracias al teorema 1.1.

1.29 Teorema. 1. Si x es un ordinal e $y \in x$, entonces

   (a) y es ordinal;

   (b) $y = W[y]$ respecto a x.

2. Si x e y son ordinales tales que $(x, \in) \cong (y, \in)$, entonces $x = y$.

3. Si x e y son ordinales, entonces una y solo una de las siguientes afirmaciones es verdadera

   (a) $x = y$;

   (b) $x \in y$;

   (c) $y \in x$.

Demostración. 1.(a)Si x es ordinal e $y \in x$ entonces $y \subseteq x$. Sea $z \in y$, se busca demostrar que $z \subseteq y$, como $y \subseteq x$ entonces $z \in x$ pero por ser x ordinal se tiene que $z \subseteq x$. Sea $w \in z \subseteq x$, entonces $w \in x$ y así tenemos que $y, z, w \in x$, del hecho que $w \in z$ y $z \in y$ y por ser x se sigue que $w \in y$, concluimos que $z \subseteq y$. Por otro lado, como $(x, \in)$ es un conjunto bien ordenado, por corolario 1.22, $(y, \in)$ es un conjunto bien ordenado, quedando demostrado que y es ordinal.
1.(b)Por la definición $W[y] = \{a \in x : a \in y\} = x \cap y = y$ pues $y \subseteq x$.
2.Sea o_x el mínimo de x y sea o_y elmínimo de y. Afirmamos que $o_x = o_y = \emptyset$. Supongamos que o_x no es vacío, sea $z \in o_x$, como $o_x \subseteq x$, por ser x ordinal, entonces $z \in x$ y por tanto $o_x \in z$ o $z = o_x$, de cualquier forma obtenemos que $o_x \in o_x$, una contradicción, por tanto $o_x = \emptyset$. Análogamente se obtiene

que $o_y = \emptyset$.
Ahora supongamos que $x \neq y$, sea z_0 el mínimo de $x-y$. Por el argumento del parrafo anterior $\emptyset \in x \cap y$, entonces $z_0 \neq \emptyset$ y $z_0 \subseteq x$. Sea $z \in z_0$, $z \in x$, si $z \notin y$ se tiene que $z \in x - y$ y por tanto $z_0 \in z$ y así $z_0 \in z_0$, que es imposible, esto implica que $z \in y$, de esto se sigue que $z_0 \subseteq y$. Si suponemos que $y - z_0 \neq \emptyset$, sea l_0 el mínimo de $y - z_0$. Afirmamos que $W[l_0] = z_0$. Supongamos que existe $r \in W[l_0]$ y que $r \notin z_0$, esto quiere decir que $r \in y - z_0$, así $l_0 \in r$ pero $r \in l_0$, esto implica que $r \in r$, una imposibilidad, por tanto $r \in z_0$. Por otro lado sea $s \in z_0$, como $z_0 \subseteq y$, se sigue que $s, l_0 \in y$, así $s \in l_0$ o $l_0 \in s$ o $s = l_0$, si $l_0 = s$ o $l_0 \in s$ se llega a que $l_0 \in z_0$, una contradicción, entonces $s \in l_0$, o sea que $s \in W[l_0]$, mostrando que $W[l_0] = z_0$, por 1.(b), $W[l_0] = l_0$ y por tanto $z_0 = l_0$, esto implica $z_0 \in y$ pero $z_0 \in x - y$, lo que es imposible, por lo tanto $y - z_0 = \emptyset$, entonces $y \subseteq z_0$ y como $z_0 \subseteq y$ se tiene que $y = z_0$, pero $z_0 = W[z_0]$, de esto se sigue que $(x, \in) \cong (W[z_0], \in)$ y además $z_0 \in x$, por teorema 1.25 esto no puede pasar, por lo tanto $x - y = \emptyset$ y así $x \subseteq y$. Análogamente se muestra que $y \subseteq x$, mostrando que $x = y$.
3.Por teorema 1.26, solo pasa uno de los siguientes casos

(a) $(x, \in) \cong (y, \in)$;

(b) $(x, \in) \cong (W[l_0], \in)$ para algun $l_0 \in y$;

(c) $(y, \in) \cong (W[t_0], \in)$ para algun $t_0 \in x$.

Así $x = y$ o $(x, \in) \cong (l_0, \in)$ o $(y, \in) \cong (t_0, \in)$, lo que es lo mismo, $x = y$ o $x = l_0$ o $y = t_0$, entonces $x = y$ o $x \in y$ o $y \in x$. □

1.30 Teorema. Todo conjunto bien ordenado es isomorfo a un único número ordinal.

Demostración. Sea $(W, <)$ un conjunto bien ordenado. Sea A el conjunto de todos los $a \in W$ para los cuales $W[a]$ es isomorfo a algún número ordinal. Como dos ordinales distintos no pueden ser isomorfos (uno es segmento del otro) este número ordinal está determinado únicamente, y lo denotamos por α_a.
Ahora supongamos que existe un conjunto S tal que $S = \{\alpha_a : a \in A\}$. El conjunto S está bien ordenado por $\in$ por ser un conjunto de ordinales. También es un conjunto transitivo pues si $\gamma \in \alpha_a \in S$, y ϕ es el isomorfismo entre $W[a]$ y α_a, con $c = \phi^{-1}(\gamma)$; notemos que, como $\gamma \subseteq \alpha_a$, entonces $\phi^{-1}(\gamma) \subseteq W[a]$. Es fácil ver que $\phi|_c$ es un isomorfismo entre $W[c]$ y γ, por lo

que $\gamma \in S$. Por tanto, S es un número ordinal α.
Por un argumento similar se muestra que si $a \in A$ y $b < a$ entonces $b \in A$: sea ϕ el isomorfismo de $W[a]$ y α_a. Entonces $\phi|_{W[b]}$ es un isomorfismo entre $W[b]$ y un segmento inicial I de α_a. Por Lema 1.24, existe $\beta < \alpha_a$ tal que $I = \{\gamma \in \alpha_a : \gamma < \beta\} = \beta$, i.e., $\beta = \alpha_b$. Esto muestra que $b \in A$ y $\alpha_b < \alpha_a$. Concluimos que $A = W$ o $A = W[c]$ para algún $c \in W$ (por Lema 1.24 otra vez).
Ahora definimos una función $f : A \to S$ dada por $f(a) = \alpha_a$. De la definición de S y el hecho de que $b < a$ implica $\alpha_b < \alpha_a$ es claro que f es un isomorfismo entre $(A, <)$ y α. Si $A = W[c]$, entonces tendríamos que $c \in A$ y por tanto $f(c) = \alpha \in S = \alpha$, una contradicción. Así $A = W$, y f es un isomorfismo entre $(W, <)$ y el ordinal α.
Para terminar la prueba se debe justificar que exista tal conjunto S. Sea $P(x, y)$ la propiedad:

$$x \in W \text{ y } y \text{ es el único ordinal isomorfo a } W[x],$$
$$\text{o } x \notin W \text{ y } y = \emptyset.$$

Aplicando el axioma de reemplazo concluimos que (para $A = W$) existe un conjunto B tal que para toda $a \in W$ existe $\alpha \in B$ para la cual $P(a, \alpha)$ se cumple. Entonces sea

$$S = \{\alpha \in B : P(a, \alpha) \textit{ se cumple para algún } a \in W\} = F[W]$$

donde F es la operación definida por P. □

1.31 Teorema. (Principio de inducción transfinita) Sea $P(x)$ una propiedad. Supongamos que, para todo número ordinal α :

$$\textit{Si } P(\beta) \textit{ se cumple para toda } \beta < \alpha, \textit{ entonces } P(\alpha) \textit{ se cumple.}$$

Entonces $P(x)$ se cumple para todos los ordinales α.

Demostración. Supongamos que para algun ordinal γ no se cumple la propiedad P, y sea S el conjunto de todos los números ordinales $\delta \leq \gamma$ que no cumplen la propiedad P. Por ser S un conjunto de ordinales entonces está bien ordenado, sea α el mínimo. Como para cada $\beta < \alpha$ se cumple la propiedad P, se sigue que $P(\alpha)$ se cumple, una contradicción. □

Un resultado muy importante sobre ordinales es la recursión transfinita que nos habla de una función casi "divina", por lo que no será de gran

ayuda demostrar el resultado pues es muy abstracto, de todos modos si se tiene curiosidad acerca del resultado, este se puede encontrar en [2] y [8]. Denotaremos por V a la clase de todos los conjuntos, formalmente $V = \{x : x = x\}$. Veremos como se relacionan V y O.

1.32 Teorema. Si $F : V \to V$, entonces existe una única función $G : O \to V$, tal que para toda α

$$G(\alpha) = F(G|_\alpha.$$

1.33 Definición. Para cualquier A, sea $h(A)$ el número ordinal más pequeño que no es equipotente a ningún subconjunto de A. $h(A)$ es llamado el número de Hartogs de A. Por la definición, $h(A)$ es el menor ordinal α tal que $|\alpha| \nleq |A|$.

1.34 Lema. El número de Hartogs de A existe para toda A.

Demostración. Por el Teorema 1.30, para cada conjunto bien ordenado (W, R) donde $W \subseteq A$, existe un único ordinal α tal que $(\alpha, <)$ es isomorfo a (W, R). El Esquema de Axioma de Reemplazo implica que existe un conjunto H tal que, para cada buen ordenamiento $R \in P(A \times A)$, el ordinal α isomorfo a R está en H. Afirmamos que H contiene a todos los ordinales equipotentes a un subconjunto de A. De hecho, si f es una función inyectiva de α en A, fijamos

$$W = Im(f) \text{ y } R = \{(f(\beta), f(\gamma)) : \beta < \gamma < \alpha\}.$$

$R \subseteq A \times A$ es un buen ordenamiento isomorfo a α (por ser f isomorfismo). Estas consideraciones muestran que

$$h(A) = \{\alpha \in H : \alpha \text{ es un ordinal equipotente a un subconjunto de } A\},$$

y se justifica la existencia de $h(A)$ por el esquema de Axioma de Comprensión, tomando $A = H$, $B = h(A)$ y $P(x)$ dada por x es un ordinal equipotente a un subconjunto de A. □

1.4. Módulos

Otra parte importante de este trabajo trata sobre módulos, en particular el último teorema del capítulo 3. Enunciaremos algunas definiciones y resultados básicos de la teoría de módulos. En lo consecuente todos los anillos,

que denotaremos generalmente por R, tendrán elemento unitario 1. Se puede revisar con más detalles la teoria de modulos en [4].

1.35 Definición. Sea R un anillo. Un R-módulo derecho M es

(I) un grupo abeliano M con la suma

(II) una función

$$M \times R \to M \; con \; (m, r) \mapsto mr,$$

llamada producto por escalar, para la cual se tiene que

(1) Ley asociativa: $(mr_1)r_2 = m(r_1r_2)$.

(2) Leyes distributivas: $(m_1 + m_2)r = m_1r + m_2r,\ m(r_1 + r_2) = mr_1 + mr_2$.

(3) Ley unitaria: $m1 = 1$.

Donde m, m_1, m_2 son elementos arbitrarios de M y r, r_1, r_2 son elementos arbitrarios de R.

Si M es un R-módulo derecho lo denotaremos por M_R, para indicar que anillo está involucrado.

1.36 Definición. Sea M un R-módulo derecho. Un subconjunto A de M es llamado un submódulo de M, $A \leq M$ como notación (o también $A_r \leq M_R$) si A es un R-módulo derecho con respecto a la restricción de la adición y el producto por escalar de M a A.

Denotaremos

$$A \lneq M \text{ si y solo si } A \text{ es un submódulo propio de } M.$$

Todo módulo M tiene los submódulos triviales 0 y M, donde 0 es el submódulo que solo contiene al elemento cero de M.

Ahora enunciaremos un lema sin prueba dada su clara veracidad.

1.37 Lema. Sea M un R-módulo derecho. Si A es un subconjunto de M y $A \neq \emptyset$ entonces lo siguiente es equivalente:

(1) $A \leq M$.

(2) Para toda $a_1, a_2 \in A$, $a_1 + a_2 \in A$ (con respecto a la adición en M) y para toda $a \in A$ y toda $r \in R$, se tiene que $ar \in R$.

Obsérvese que se puede pensar R como un R-módulo derecho R_R. Dado lo anterior se llama ideal derecho de R a un submódulo de R_R.

1.38 Definición. A un submódulo $A \leq M$ se le llama submódulo máximo de M si y solo si A es submódulo propio y

$$A \lneq B \text{ implica que } B = M \text{ para todo } B \leq M.$$

De la misma manera hablamos de ideales máximos.

1.39 Lema. Sea X un subconjunto del módulo M_R. Entonces

$$A := \begin{cases} \{\sum_{j=1}^{n} x_j r_j | x_j \in X \text{ y } r_j \in R \text{ y } n \in \mathbb{N}\}, & si\ X \neq \emptyset \\ 0 & si\ X = \emptyset \end{cases}$$

es un submódulo de M.

Demostración. Para $X = \emptyset$ la afirmación es clara. Sea ahora $X \neq \emptyset$. La prueba ahora se sigue del Lema 1.37, sean $\sum_{i=1}^{m} x_i r_i,\ \sum_{j=1}^{n} x'_j r'_j \in A$, entonces

$$\sum_{i=1}^{m} x_i r_i \ + \ \sum_{j=1}^{n} x'_j r'_j \in A,$$

de igual manera, sea $\sum_{j=1}^{n} x_j r_j \in A$ y $r \in R$, entonces

$$\sum_{j=1}^{n} x_j r_j r \in A.$$

□

1.40 Definición. El módulo definido en el Lema 1.39 se llama el submódulo de M generado por X y se denota $\langle X \rangle$.

1.41 Definición. Sea el módulo M_R.

(1) Un subconjunto X del módulo M es un conjunto generador de $M :\Leftrightarrow \langle X \rangle = M$.

(2) Se dice que un módulo (o ideal derecho) es un módulo finitamente generado: si existe un conjunto generador finito de él.

1.42 Definición. Sean A y B ambos R-módulos derechos. Un homomorfismo α de A en B es una función

$$\alpha : A \to B$$

que satisface que

$$\alpha(a_1r_1 + a_2r_2) = \alpha(a_1)r_1 + \alpha(a_2)r_2 \text{ para toda } a_1, a_2 \in A \text{ y toda } r_1, r_2 \in R$$

1.43 Definición. Sea $\Gamma = \{A_i : i \in I\}$ un conjunto de submódulos $A_i \leq M$, entonces

$$\sum_{i\in I} A_i := \langle \cup_{i\in I} A_i \rangle$$

se llama la suma de los submódulos $\{A_i : i \in I\}$.

1.44 Definición. Se dice que M es la suma directa interna del conjunto $\{B_i | i \in I\}$ de submódulos $B_i \leq M$, en símbolos:

$$M = \oplus B_i :\Leftrightarrow \begin{cases} (1) M = \sum_{i\in I} B_i \\ (2) \forall j \in I [B_j \cap \sum_{i\in I,\ i\neq j} B_i = 0]. \end{cases}$$

1.45 Definición. Se dice que un submódulo $B \leq M$ es sumando directo de M:

si y solo si existe $C \leq M$ tal que $M = B \oplus C$.

Para dar una construcción de módulo cociente sea $C \leq M_R$. Entonces, en particular, C es un subgrupo del grupo aditivo M. Claramente el grupo cociente $M/C = \{m + C | m \in M\}$ existe bajo la adición

$$(m_1 + C) + (m_2 + C) := (m_1 + m_2) + C$$

Ahora se puede definir un producto de módulo sobre M/C tal que M/C se convierta en un módulo derecho denominado módulo cociente de M módulo C.

1.46 Definición.

$$(m + C)r := mr + C, \quad m \in M,\ r \in R$$

Para mostrar que M/C es en efecto un R-módulo derecho, es suficiente mostrar que

$$M/C \times R \to M/C \ \ con \ \ (m + C, r) \mapsto mr + C$$

es una función, ya que las otras propiedades de módulos se siguen directamente de las de M.
Sea $m_1 + C = m_2 + C$, entonces

$$m_1 = m_2 + c,\ c \in C,$$

lo que implica que

$$m_1 r + C = (m_2 + c)r + C = m_2 r + cr + C = m_2 r + C.$$

Capítulo 2

Equivalencias

En este capítulo mostraremos una serie de enunciados que se mostrará que son equivalencias del Axioma de Elección, primero mostrando que son equivalentes entre ellas y finalizando mostrando que realmente son equivalentes al Axioma de Elección.

2.1. Equivalencias débiles

M1: Si R es una relación de orden parcial sobre un conjunto no vacío X y si cada subconjunto de X que esté ordenado linealmente por R tiene una R-cota superior, entonces X tiene un R-elemento máximo.

M2: Si R es una relación de orden parcial sobre un conjunto no vacío X y si cada subconjunto de X que esté bien ordenado por R tiene una R-cota superior, entonces X tiene un R-elemento máximo.

M3: Si cada nido (como en la definición 1.18) no vacío subconjunto de un conjunto no vacío X tiene que su unión es un elemento de X, entonces X tiene un $\subseteq$-elemento máximo.

M4: Si cada nido no vacío bien ordenado subconjunto de un conjunto X no vacío tiene su unión como elemento de X, entonces X tiene un $\subseteq$-elemento máximo.

M5: Si R es una relación de orden parcial sobre $X \neq \emptyset$, entonces existe

un $\subseteq$-subconjunto máximo de X que está linealmente ordenado por R.

M6: Para cada conjunto $X \neq \emptyset$, existe un $\subseteq$-subconjunto máximo de X que es un nido.

2.1 Definición. $P(X)$ es una propiedad de carácter finito si:

(1) $P(\emptyset)$ se cumple.

(2) $P(X)$ se cumple para toda X si y solo si $P(x)$ se cumple para toda $x \subseteq X$, con x finito.

con X una clase.

2.2 Ejemplo. Veamos algunas propiedades de carácter finito, si $P(X)$ es cualquiera de las siguientes fórmulas entonces es una propiedad de carácter finito:

(1) X está parcialmente ordenado por R.

(2) X está linealmente ordenado por R.

(3) $u \notin X$

(4) Los elementos de X son disjuntos dos a dos.

Por otra parte, las siguientes no son propiedades de carácter finito:

(5) X puede ser linealmente ordenado (note la diferencia con 2).

(6) X está bien ordenado por R.

(7) $u \in X$.

(8) X es infinito.

M7: Para cada conjunto $X \neq \emptyset$ y cada propiedad P de carácter finito, existe un $\subseteq$-subconjunto máximo de X que tiene la propiedad P.
Ahora se muestran las pruebas de las equivalencias.

Demostración. (M2 $\Rightarrow$ M1)
Sea R una relación de orden parcial sobre un conjunto $X \neq \emptyset$ y supongamos que cada subconjunto de X que esté linealmente ordenado por R tiene una R-cota superior, de esto se sigue que los subconjuntos de X que estén bien ordenados por R tienen una R-cota superior. Ahora por M2, X tiene un R-elemento máximo, que es lo que queríamos probar. □

Demostración. (M1 $\Rightarrow$ M3)
Sea X un conjunto no vacío y supongamos que para cada nido no vacío subconjunto de X, la unión de tal nido es elemento de X. Sabemos que $\subseteq$ es relación de orden parcial sobre X y sea $A \subseteq X$ un nido tal que $\cup A \in X$. Veamos que $\cup A$ es $\subseteq$-cota superior de A, esto es inmediato pues para toda $a \in A$, $a \subseteq \cup A$, así $\cup A$ es $\subseteq$-cota superior de A, ahora como cada nido no vacío subconjunto de X tiene una $\subseteq$-cota superior, por M1, X tiene un $\subseteq$-elemento máximo, que es lo que se quería probar. □

Demostración. (M2 $\Rightarrow$ M4)
Sea X un conjunto no vacío y supongamos que cada nido no vacío subconjunto de X bien ordenado por $\subseteq$ tiene su unión como elemento de X. Sabemos que $\subseteq$ es una relación de orden parcial sobre X, sea $N \subseteq X$ un nido no vacío bien ordenado, veamos que tiene una $\subseteq$-cota superior, sea $M = \cup N$ y sabemos de la hipótesis de M4 que $M \in X$ y que para toda $n \in N$ se tiene que $n \subseteq M$, de esto se sigue que M es $\subseteq$-cota superior de N, así los nidos no vacíos bien ordenados subconjuntos de X están acotados superiormente, aplicando M2, X tiene un $\subseteq$-elemento máximo que es lo que se quería probar. □

Demostración. (M4 $\Rightarrow$ M3)
Sea X un conjunto no vacío tal que cada nido no vacío subconjunto de X tiene su unión en X, en particular los nidos no vacíos bien ordenados por $\subseteq$ tienen su unión en X, aplicando M4, tenemos que X tiene un $\subseteq$-elemento máximo, que es lo que se quería probar. □

Demostración. (M7 $\Rightarrow$ M5)
Sea X un conjunto parcialmente ordenado por R, y sea P la propiedad "ser linealmente ordenado por R", como sabemos, P es de carácter finito, por M7 existe un $\subseteq$-subconjunto máximo de X que tiene la propiedad P, esto es un $\subseteq$-subconjunto máximo de X que está linealmente ordenado por R. □

Demostración. (M5 $\Rightarrow$ M6)
Sea X un conjunto y $\subseteq$ relación de orden parcial sobre X, por M5 existe un $\subseteq$-subconjunto máximo de X que está linealmente ordenado por $\subseteq$, un nido. $\square$

Demostración. (M3 $\Rightarrow$ M7)
Sea X un conjunto y P una propiedad de carácter finito, sea

$$Y = \{t \subseteq X : P(t)\}.$$

Probaremos que si $n \subseteq Y$ es un nido diferente del vacío entonces $\cup n \in Y$. Claramente $\cup n \subseteq X$. Sea $u \subseteq \cup n$ finito. Veamos que u es subconjunto de un elemento de n, como u es finito podemos enumerar sus elementos, $u = \{u_1, ..., u_r\}$, y sea $n_i \in n$ tal que $u_i \in n_i$. Como n está linealmente ordenado se tiene que $n_i \subseteq n_j$ o $n_j \subseteq n_i$ para $i \neq j$ con $i, j \in \{1, ..., r\}$, sea $n_I = max\{n_i : i = 1, ..., r\}$, entonces

$$n_j \subseteq n_I \text{ para toda } j \in \{1, ..., r\},$$

de esto se sigue que

$$a \in n_I \text{ para toda } a \in u.$$

Por lo tanto u es subconjunto de un elemento de n. Ahora como $n_I \in Y$ entonces se cumple $P(n_I)$ y por tanto $P(u)$. De esta manera tenemos que $\cup n \subseteq X$ y cada subconjunto finito de $\cup n$ cumple P, de esto se sigue que $P(\cup n)$ se cumple y así $\cup n \in Y$. Por ser P de carácter finito, $P(\emptyset)$ se cumple, y así $\emptyset \in Y$ y por tanto $Y \neq \emptyset$. Ahora tenemos que cada nido $n \subseteq Y$, diferente del vacío, tiene su unión como un elemento de Y, aplicando M3 mostramos que Y tiene un $\subseteq$-elemento máximo. $\square$

Demostración. (M6 $\Rightarrow$ M5)
Sea R un orden parcial sobre un conjunto X. Sea Y el conjunto de todos los subconjuntos de X que están linealmente ordenados por R. Por M6 existe $n \subseteq Y$ nido máximo. Sea $m = \cup n$, veamos que m está linealmente ordenado por R. Sea $a \in m$, como $m = \cup n$ entonces existe $x \in n$ tal que $a \in x$, como x está linealmente ordenado por R se tiene que aRa, por tanto m cumple la reflexibilidad respecto a R. Ahora sean $a, b \in m$ tal que aRb y bRa, igual que antes, existen

$$x_1, x_2 \in n \text{ tal que } a \in x_1 \text{ y } b \in x_2,$$

por ser n nido, sin pérdida de generalidad, $x_1 \subseteq x_2$ y esto implica que $a, b \in x_2$, y como x_2 está linealmente ordenado por R entonces $a = b$, por tanto m cumple la anti-simetría respecto de R. Sean $a, b, c \in m$ tal que aRb y bRc, como antes, existen

$$x_1, x_2, x_3 \in n \text{ tal que } a \in x_1 \text{ y } b \in x_2 \text{ y } c \in x_3,$$

sin pérdida de generalidad, $a, b, c \in x_3$, de esto se sigue que como x_3 está linealmente ordenado por R, entonces aRc y así m cumple la transitividad respecto a R. Por último, sean $a, b \in m$, con $a \neq b$, entonces existen

$$x_1, x_2 \in n \text{ tal que } a \in x_1 \text{ y } b \in x_2,$$

por ser n nido, sin pérdida de generalidad,$x_1 \subseteq x_2 \Rightarrow a, b \in x_2$, y como x_2 está linealmente ordenado por R entonces aRb o bRa, cumpliendo que m está linealmente ordenado por R, además es inmediato que $m \subseteq X$, por lo tanto $m \in Y$.
Lo siguiente es probar que m es $\subseteq$-elemento máximo de Y. Supongamos que m no es máximo en Y; esto implica que existe $z \in Y$ tal que $m \subset z$. Observemos que $n \cup \{z\}$ es nido pues todos los elementos de n son subconjuntos de z. Como n es nido máximo entonces se tiene que $\{z\} \subseteq n$, esto implica que $z \in n$ y por tanto $z \subseteq m$, lo que contradice lo que asumimos de z. Por tanto, m es un $\subseteq$-subconjunto máximo de X linealmente ordenado por R. □

Demostración. (M5 $\Rightarrow$ M2)
Sea R un orden parcial sobre X. Sea Y el conjunto de todos los subconjuntos de X bien ordenados por R. Definimos la relación S sobre Y como sigue:

$$S = \{< t, u >: t \in Y,\ u \in Y \text{ y } t \text{ es un } R\text{-segmento inicial de } u\}.$$

Veamos que S es un orden parcial sobre Y.

i) Sea $a \in Y$, $a \subseteq a$ y sea $y \in a$ y $x \in a$ tal que xRy, como $x \in a$ se tiene que aSa y S cumple con la reflexividad.

ii) Sean $a, b \in Y$ tal que aSb y bSa, así por definición $a \subseteq b$ y $b \subseteq a$ y por tanto tenemos que $a = b$, por lo anterior s cumple la antisimetría.

iii) Por último sean $a, b, c \in Y$ tal que aSb y bSc, por la definición $a \subseteq b$ y $b \subseteq c$, por tanto $a \subseteq c$, ahora sea $y \in a \subseteq b$ y $x \in c$ tal que xRy,

esto implica que, por ser b segmento inicial de c, $x \in b$, así tenemos que $y \in a$ y $x \in b$ tal que xRy, y por ser a segmento inicial de b, $x \in a$, por tanto S cumple la transitividad.

Por tanto S es orden parcial sobre Y, así por M5 existe $n \subseteq Y$ $\subseteq$-máximo que está linealmenmte ordenado por S. Sea $m = \cup n$, mostraremos que m tiene una R-cota superior, y que tal elemento es un R-elemento máximo de X.
Primero mostraremos que $m \in Y$. Claramente $m \subseteq X$. Sea $z \subseteq m$ con $z \neq \emptyset$ y así tenemos que existe

$$x \in n \text{ tal que } z \cap x \neq \emptyset.$$

Como $z \cap x \subseteq x$ entonces se tiene que $z \cap x$ está bien ordenado por R, sea u el R-primer elemento de $z \cap x$. Veamos que u tambien es R-primer elemento en z. Sea $v \in z$ con $v \neq u$. Si $v \in x$ entonces $v \in x \cap z$, así tenemos que uRv y no vRu por ser $x \cap z$ bien ordenado. Ahora si $v \notin x$, tenemos que $v \in w$ para algún $w \in n$. Por la definición de S y la construcción de n, x es R-segmento inicial de w pues como $x, w \in n$ linealmente ordenado por S tenemos que xSw o wSx, si wSx entonces se tiene que $w \subseteq x$ y esto implica que $v \in x$ pero $v \notin x$, una contradicción. Por tanto xSw, esto implica que $u, v \in w$ que está bien ordenado por R, entonces tenemos que uRv o vRu, pero si vRu, como xSw, tendríamos que $u \in x$ y vRu implica que $v \in x$ pero $v \notin x$!, por lo tanto uRv y no vRu. Así, para cualquier otro elemento $v' \in z$ tendremos que uRv', por lo tanto u es el único R-primer elemento de z.
Por último veamos que m está linealmente ordenado por R. Sean $a, b \in m$, existen $x, y \in n$ tales que $a \in x$ y $b \in y$. Como n está linealmente ordenado por S, sin pérdida de generalidad digamos que, xSy, esto implica que $x \subseteq y$ y así $a, b \in y$, como y está bien ordenado por R, tenemos que aRb o bRa, mostrando que m está linealmente ordenado por R. Por tanto R bien ordena a m y $m \in Y$.
Ahora mostraremos que m es S-máximo en Y. Supongamos que m no es máximo, entonces para algún $t \in Y$ con $t \neq m$, tenemos que mSt, o sea que $m \subseteq t$. Sea

$$n^* := n \cup \{t\}.$$

Veremos que está linealmente ordenado por S. Primero, como $n^* \subseteq Y$ que está parcialmente ordenado por S, se tiene que n^* está parcialmente ordenado por S, falta ver que para cualesquiera $a, b \in n^*$ se cumple que aSb o bSa.

i) Si $a, b \in n$ se cumple pues n está linealmente ordenado por S.

ii) Si $a, b \in \{t\}$ entonces $a = b = t$ y como $t \in Y$ parcialmente ordenado por S, se tiene que tSt, o lo que es lo mismo, aSb cumpliendo lo que queríamos mostrar.

iii) Ahora sea $a \in n$ y $b = t$, como $a \subseteq m \subset t$ solo queda el caso posible que aSt, pues si pasara que tSa esto implicaría $t \subseteq a \subseteq m$, o sea, se tendría que $t \subseteq m$ y $m \subset t$, una contradicción.

Sea $\alpha \in a$ y $\lambda \in t$ tal que $\lambda R \alpha$, mostraremos que $\lambda \in a$. Como $\lambda \in t$ entonces $\lambda \in m$ o $\lambda \notin m$.

i) Si $\lambda \in m$ se tiene que existe $b \in n$ tal que $\lambda \in b$, ahora como $a, b \in n$ entonces aSb o bSa, si bSa se tiene que $b \subseteq a$ y por lo tanto $\lambda \in a$. Si aSb se tiene que $a \subseteq b$ y $\alpha \in a$ y $\lambda \in b$ y $\lambda R \alpha$ entonces $\lambda \in a$; por lo tanto aSt.

ii) Ahora supongamos que $\lambda \notin m$, como $a \subseteq m$ tenemos que $\alpha \in m$ y $\lambda \in t$ y $\lambda R \alpha$, por ser mSt, se sigue que $\lambda \in m$ pero $\lambda \notin m$, una contradicción, por lo tanto no es posible que $\lambda \notin m$.

Por lo tanto para toda $a, b \in n^*$ se tiene que aSb o bSa, entonces n^* está linealmente ordenado por S. Observemos que n es $\subseteq$-máximo en Y y como $n \subseteq n^*$ se tiene que $n^* = n$, de esto se sigue que $\{t\} \subseteq n$, o sea que $t \in n$, entonces $t \subseteq m$ pero dijimos que $m \subseteq t$, por lo tanto $m = t$ pero $m \neq t$!. Por lo tanto m es S-máximo en Y.
De esto se sigue que m no puede tener una R-cota superior estricta. Supongamos que b fuera una R-cota superior estricta para m, tendríamos $m \subset m' := m \cup \{b\} \subseteq X$. Probaremos que $m' \in Y$. Primero veamos que R es orden lineal, sean $x, y \in m'$:

i) si $x, y \in m$ entonces son comparables por estar m linealmente ordenado por R;

ii) si $x, y \in \{b\}$ entonces $x = b = y$ y como X está parcialmente ordenado por R se tiene que bRb, o lo que sería lo mismo, xRy;

iii) por último, sin pérdida de generalidad, sea $x \in m$ y $y = b$, como b es cota superior de m, xRy, por lo tanto m' está linealmente ordenado por R.

Ahora sea $l \subseteq m'$, esto implica que

$$b \in l \text{ o } b \notin l.$$

Si $b \notin l$, entonces $l \subseteq m$ y l tiene elemento mínimo, si $b \in l$ sea $l' := l - \{b\}$, así $l' \subseteq m$ y l' tiene elemento mínimo, digamos β, como $\beta \in m$ entonces βRb, se sigue que para toda $r \in l$, βRr, así l tiene mínimo, por lo tanto m' está bien ordenado por R y $m' \in Y$. Ahora veamos que mSm', primero tenemos que $m \subseteq m'$ y sean $v \in m$ y $w \in m'$ tal que wRv, si $w \neq b$ entonces $w \in m$, si $w = b$ esto implica que bRv pero como b es cota estricta solo se puede que vRb!, por lo tanto solo es posible el caso en el que $w \neq b$, cumpliendo que mSm' lo que contradice la S-maximidad de m en Y.
Para finalizar, como $m \in Y$, se sigue de la hipótesis de M2 que m tiene una R-cota superior. Sea b tal cota y supongamos que existe $z \in X$ tal que bRz. Si suponemos que zRb es falso se tiene que z sería una R-cota superior estricta para m, lo que es imposible. Por todo lo anterior, b es una R-elemento máximo de X. □

2.2. Equivalencias fuertes

M'1: Si R es una relación de orden parcial sobre un conjunto no vacío X y si cada subconjunto de X que esté ordenado linealmente por R tiene una R-cota superior y si $y \in X$, entonces X tiene un R-elemento máximo z tal que yRz.

M'2: Si R es una relación de orden parcial sobre un conjunto no vacío X y si cada subconjunto de X que esté bien ordenado por R tiene una R-cota superior y si $y \in X$, entonces X tiene un R-elemento máximo z tal que yRz.

M'3: Si cada nido no vacío subconjunto de un conjunto no vacío X tiene que su unión es un elemento de X y si $y \in X$, entonces X tiene un $\subseteq$-elemento máximo z tal que $y \subseteq z$.

M'4: Si cada nido no vacío bien ordenado subconjunto de un conjunto X no vacío tiene su unión como elemento de X y si $y \in X$, entonces X tiene un $\subseteq$-elemento máximo z tal que $y \subseteq z$.

M'5: Si R es una relación de orden parcial sobre $X \neq \emptyset$, para cada subconjunto $Y \subseteq X$ linealmente ordenado por R existe Z, un $\subseteq$-subconjunto máximo de X, que está linealmente ordenado por R y tal que $Y \subseteq Z$.

M'6: Para cada conjunto $X \neq \emptyset$ y cada subconjunto Y de X existe Z, un $\subseteq$-subconjunto máximo de X, que es un nido y tal que $Y \subseteq Z$.

M'7: Para cada conjunto $X \neq \emptyset$ y cada propiedad P de carácter finito y para cada subconjunto Y de X tal que $P(Y)$, existe un $\subseteq$-subconjunto máximo Z de X tal que $P(Z)$ y $Y \subseteq Z$.
Es evidente que por ser proposiciones más fuertes que su análogo, se cumple M'n $\rightarrow$ Mn para $n \in \{1, ..., 7\}$.

2.3 Teorema. Mn $\Rightarrow$ M'n para $n \in \{1, ..., 4\}$.

Demostración. Sea $y \in X$ y W el conjunto de las cotas superiores para $\{y\}$. Se aplica Mn a W para así obtener M'n. □

Para ver este proceso demostraremos que M1 $\Rightarrow$ M'1.

Demostración. (M1 $\Rightarrow$ M'1)
Sea R relación de orden parcial sobre X y supongamos las hipótesis de M'1. Sea W el conjunto de las cotas superiores de $\{y\}$. Como $W \subseteq X$ y X está parcialmente ordenado por R entonces W tambien lo está, además como cada subconjunto de W que esté linealmente ordenado por R también es un subconjunto de X que está linealmente ordenado por R entonces tales subconjuntos tienen R-cota superior.
Aplicando M1 a W, W tiene un R-elemento máximo, $z \in W \subseteq X$, tal que yRz. □

2.4 Teorema. M7 $\rightarrow$ M'n para $n \in \{5, 6, 7\}$.

Demostración. (M7 $\Rightarrow$ M'5)
Sea $Y \subseteq X$ linealmente ordenado por R. "Linealmente ordenado" es una propiedad de carácter finito, llamémosla P. Definimos una nueva propiedad Q como sigue:

$$\text{para toda } W \subseteq X,\ Q(W) \text{ si y solo si } P(W \cup Y).$$

Veamos que Q es de carácter finito, primero notemos que se cumple

$$P(Y) = P(Y \cup \emptyset) \text{ si y solo si } Q(\emptyset).$$

Ahora sea W_0 una clase y supongamos $Q(W_0)$. Lo que implica $P(W_0 \cup Y)$, sea $V_0 \subseteq W_0 \subseteq W_0 \cup Y$ con V_0 finito y como $P(W_0 \cup Y)$ se cumple entonces se tiene $P(V_0)$; por otro lado como $V_0 \cup Y \subseteq W_0 \cup Y$, que está linealmente ordenado, es cierto $P(V_0 \cup Y)$, por tanto se cumple $Q(V_0)$. Por lo tanto $Q(W_0)$ implica $Q(V_0)$ para $V_0 \subseteq W_0$ finito.
Ahora supongamos que para cada $V_0 \subseteq W_0$ finito se tiene $Q(V_0)$. Supongamos que $W_0 \cup Y$ no está linealmente ordenado por R, entonces existen $a, b \in W_0 \cup Y$ tal que a y b son incomparables.

i) Si $a, b \in Y$, como $P(Y)$ se cumple entonces aRb o bRa, una contradicción.

ii) Si $a, b \in W_0$, sea $V_1 = \{a, b\} \subseteq W_0$ finito, esto implica $Q(V_1)$ si y solo sí $P(V_1 \cup Y)$ y por tanto aRb o bRa, lo cual es imposible.

iii) Por último, sin pérdida de generalidad, si $a \in W_0$ y $b \in Y$, sea $V_2 = \{a\} \subseteq W_0$ finito, esto implica $Q(V_2)$ si y solo si $P(V_2 \cup Y)$ y por tanto aRb o bRa, pero esto no puede pasar.

Por lo tanto para cada subconjunto finito $V_0 \subseteq Q(V_0)$ si y solo si $Q(W_0)$ y así Q es de carácter finito.

Por M7 existe un subconjunto $\subseteq$-máximo Z de X que tiene la propiedad Q, o sea, $Q(Z)$ si y solo si $P(Z \cup Y)$. Para terminar veamos que $Z \cup Y$ es $\subseteq$-máximo en X, supongamos que no es máximo, esto es, existe

$$U \subseteq X \text{ tal que } Z \cup Y \subset U \text{ y } P(U).$$

Esto implica que $Y \subset U$, sea $U_0 := (U - Y) \cup Z$ y esto implica que $U = U_0 \cup Y$ entonces $P(U_0 \cup Y)$ si y solo si $Q(U_0)$. Por otro lado $Z \subset U_0$ pero Z es subconjunto $\subseteq$-máximo que cumple la propiedad Q, lo que es imposible. Por tanto $Z \cup Y$ es un subconjunto $\subseteq$-máximo de X que contiene a Y y está linealmente ordenado por R. □

Demostración. (M7 $\Rightarrow$ M'6)
Sea $Y \subseteq X$ un nido. "Ser nido" es una propiedad de caracter finito, llamemosla P y definimos una nueva propiedad Q como sigue: $\forall W \subseteq X : Q(W)$ si

y solo sí $P(W \cup Y)$. Como en la demostración anterior, Q es de carácter finito. Por M7 existe un subconjunto $\subseteq$-máximo Z de X que tiene la propiedad Q, esto es, $Q(Z)$ si y solo si $P(Z \cup Y)$, igual que antes, $Z \cup Y$ es $\subseteq$-subconjunto máximo de X que es nido y $Y \subseteq Z \cup Y$. □

Demostración. (M7 $\Rightarrow$ M'7)
Sea X un conjunto, P una propiedad de carácter finito y $Y \subseteq X$ tal que se cumple $P(Y)$. Definimos una nueva propiedad Q igual que antes. Veamos que Q es de carácter finito, como se cumple $P(Y) = P(\emptyset \cup Y)$ entonces se cumple $Q(\emptyset)$; ahora supongamos que para $W \subseteq X$ se cumple $Q(W)$, probaremos que para $V \subseteq W$ finito cumple Q, sea $V \subseteq W$ finito, como se cumple $Q(W)$ entonces se cumple $P(W \cup Y)$ y $V \subseteq W \cup Y$, así tenemos que se cumple $P(Y \cup W)$ que implica $P(V)$, falta ver que se cumple $P(V \cup Y)$. Supongamos que $P(V \cup Y)$ no se cumple, lo que significa que es falso que para todo $V_0 \subseteq V \cup Y$ finito se cumpla $P(V_0)$, esto es que existe $V_0 \subseteq V \cup Y$ finito, para el cual no se cumple $P(V_0)$, pero $V_0 \subseteq W \cup Y$ y como tenemos $P(W \cup Y)$ entonces se cumple $P(V_0)$, una contradicción. Por lo tanto se cumple $P(V \cup Y)$, lo que es lo mismo, se cumple $Q(V)$. Ahora supongamos que para cada $V \subseteq W$ finito se cumple $Q(V)$ y supongamos que $Q(W)$ no se cumple, o sea, $P(W \cup Y)$ no se cumple, esto significa que existe $V_1 \subseteq W \cup Y$ finito tal que $P(V_1)$ no se cumple. Si $V_1 \subseteq Y$ entonces $P(V_1)$ se cumple, una contradicción; si $V_1 \subseteq W$ entonces se cumple $Q(V_1)$, esto implica $P(V_1 \cup Y)$ y por tanto $P(V_1)$, lo cual es imposible; por último, si $V_1 \nsubseteq W$ y $V_1 \nsubseteq Y$ entonces sean $V_2 = V_1 \cap W$ y $V_3 = V_1 \cap Y$, como V_2 es finito se cumple $Q(V_2)$ y esto implica $P(V_2 \cup Y) = P(V_2 \cup Y \cup V_3) = P(V_1 \cup Y)$ y por tanto se cumple $P(V_1)$, pero esto no puede ocurrir. Por lo tanto se cumple $Q(W)$ y hemos mostrado que Q es de carácter finito. Por M7 existe un subconjunto Z $\subseteq$-máximo de X que cumple la propiedad Q, esto es, $Q(Z)$ que implica $P(Z \cup Y)$. Igual que antes, $Z \cup Y$ es subconjunto $\subseteq$-máximo de X y $Y \subseteq Z \cup Y$. □

2.3. Demostración de equivalencia con el Axioma de Elección

Para terminar este capítulo mostremos que M5 y el Axioma de Elección son equivalentes.

2.5 Teorema. El Axioma de Elección implica el Principio de Maximidad de Hausdorff (M5).

Demostración. Sea X un conjunto parcialmente ordenado tal que ninguno de sus subconjuntos linealmente ordenados sea $\subseteq$-máximo. Entonces para cada subconjunto linealmente ordenado $K \subseteq X$ definimos el conjunto

$$C(K) = \{x \in (X - K) : K \cup \{x\} \text{ está linealmente ordenado}\}.$$

Sea K como antes, veamos que $C(K) \neq \emptyset$, supongamos que $C(K) = \emptyset$ entonces tendríamos que es $\subseteq$-máximo, lo cual no puede pasar.
Por el axioma de elección, existe una función

$$g : P_0(X) \to X$$

($P_0(X)$ es el cojunto potencia de X quitando el conjunto vacío) con $g(A) \in A$ para cada $A \in P_0(X)$. Sea ξ el número de Hartogs de X, $h(X) = \xi$. Definimos, via recursión transfinita, una función

$$f : \xi \to X$$

dada por

$$f(\alpha) = g(C\{f(\beta) : \beta < \alpha\}).$$

Para ver que tiene sentido la definición de f veamos que $\{f(\beta) : \beta < \alpha\}$ es una cadena. Sean $f(\beta_1), f(\beta_2) \in \{f(\beta) : \beta < \alpha\}$, sin pérdida de generalidad, sea $\beta_1 < \beta_2$, esto implica que $f(\beta_1) \in \{f(\beta) : \beta < \beta_2\}$. Antes de seguir es conveniente notar que $f(\alpha) = g(C\{f(\beta) : \beta < \alpha\}) \notin \{f(\beta) : \beta < \alpha\}$ pues por su construcción, $f(\alpha)$, es justo un elemento que no está en $\{f(\beta) : \beta < \alpha\}$ tal que si se lo "pegamos", $\{f(\beta) : \beta < \alpha\} \cup \{f(\alpha)\}$, sigue siendo una cadena, en resumen $f(\alpha) \notin \{f(\beta) : \beta < \alpha\}$ y $\{f(\beta) : \beta < \alpha\} \cup \{f(\alpha)\}$ es una cadena. Continuando con lo anterior $f(\beta_1) \in \{f(\beta) : \beta < \beta_2\}$ y $f(\beta_2)$ es tal que $\{f(\beta) : \beta < \beta_2\} \cup \{f(\beta_2)\}$ es cadena, por lo tanto $f(\beta_1)$ y $f(\beta_2)$ son comparables y $\{f(\beta) : \beta < \alpha\}$ es una cadena.
Veamos que f es inyectiva, sean $\alpha_1, \alpha_2 \in \xi$ con $\alpha_1 \neq \alpha_2$ y supongamos que $f(\alpha_1) = f(\alpha_2)$, sin pérdida de generalidad sea $\alpha_1 < \alpha_2$, entonces $f(\alpha_1) \in \{f(\beta) : \beta < \alpha_2\}$, esto implica que $f(\alpha_2) \in \{f(\beta) : \beta < \alpha_2\}$ pero $f(\alpha_2) \notin \{f(\beta) : \beta < \alpha_2\}$, peroesto no puede ocurrir, por lo tanto f es inyectiva. De lo anterior se tiene que $|\xi| \leq |X|$, una contradicción, por lo tanto X tiene un subconjunto linealmente ordenado que es $\subseteq$-máximo. □

2.6 Teorema. El principio de máximidad de Hausdorff (M5) implica el Axioma de Elección.

Demostración. Sea S una colección de conjuntos no vacíos, y sea C la colección de todas las funciones de elección sobre subconjuntos de S, es claro que C está parcialmente ordenado por la inclusión, $\subseteq$. Por el Principio de Maximidad de Hausdorff, existe n, un subconjunto $\subseteq$-máximo de C que es un nido. Sea $m = \cup n$, m es una función de elección con $Dom(m) = U_{f\in n}Dom(f)$, $Im(m) = U_{f\in n}Im(f)$, es inmediato que $m \in n$. Afirmamos que m es la función de elección que estamos buscando, supongamos que no es, entonces existe $x \in S$ tal que $m(x) \notin x$. Sea $m^* = m \cup \{(x, m^*(x) \in x)\}$. Es claro que m^* es comparable con todos los elementos de n, así $n \cup \{m^*\}$ es un nido, como $m^* \notin n$ entonces $n \subsetneq n \cup \{m^*\}$, pero esto no puede pasar. Por lo tanto m es función de elección en S. $\square$

Capítulo 3

Pruebas sustituyendo Zorn

En este capítulo demostraremos resultados importantes del álgebra básica usando M6, un resultado importante postulado por Hausdorff antes de su Principio de Maximidad.

3.1. Algunos resultados clásicos en álgebra

Ahora probaremos un teorema importante del álgebra lineal.

3.1 Teorema. Todo espacio vectorial V sobre un campo F tiene base.

Demostración. Sea X el conjunto de los subconjuntos linealmente independientes de V. Es claro que X es diferente del vacío pues $\emptyset \in X$. Por M6 existe $n \subseteq X$ tal que es un nido $\subseteq$-máximo, y sea $m = \cup n$, veamos que $m \in X$. Supongamos que $m \notin X$, entonces existen

$$x_1, ..., x_k \in m \text{ tal que } a_1x_1 + ... + a_kx_k = 0 \text{ con algún } a_i \neq 0.$$

Sea $n_i \in n$ tal que $x_i \in n_i$ para $i \in \{1, ..., k\}$, además como n es un nido, para algún $j \in \{1, ..., k\}$, $n_i \subseteq n_j$, de esto se sigue que $x_i \in n_j$ para $i \in \{1, ..., k\}$. Como $a_1x_1 + ... + a_kx_k = 0$ con algún $a_i \neq 0$ entonces n_j es linealmente dependiente pero como $n_j \in n$ entonces es linealmente independiente!, por lo tanto $m \in X$.
Ahora veamos que $\langle m \rangle = V$. Supongamos que m no genera a V, entonces existe $v_0 \in V$ tal que v_0 no es combinación lineal de elementos de m, entonces

$v_0 \notin m$, sea $m^* := m \cup \{v_0\}$, es inmediato que m^* es linealmente independiente. Supongamos que $m^* \in n$, entonces $m^* \subseteq m$, de esto se sigue que $v_0 \in m$!, por lo tanto $m^* \notin n$. Sea $n^* = n \cup \{m^*\}$, veamos que es nido, sean $a, b \in n^*$, si $a, b \in n$ entonces $a \subseteq b$ o $b \subseteq a$; si $a, b \in \{m^*\}$ entonces $a = b = m^*$ y de esto se sigue que $a \subseteq b$; por último si $a \in n$ y $b = m^*$ como $a \subseteq m$ y $m \subseteq m^*$ entonces $a \subseteq b$, por lo tanto n^* es nido y además $n \subset n^*$ lo que contradice la maximidad de n, una contradicción.
Por lo tanto m genera a V y así m es base de V. □

3.2 Teorema. Sea V un espacio vectorial sobre un campo F y sean A y B bases, entonces $|A| = |B|$.

Demostración. Sea Q el conjunto de las funciones $G \in B^{A_0}$ tal que $A_0 \subseteq A$, G es inyectiva, $B - Im(G)$ y $Dom(G)$ son disjuntos y su unión $(B - Im(G)) \cup Dom(G)$ es linealmente independiente en V, en particular la función vacía está en Q. Por M6 existe un subconjunto $n \subseteq Q$ $\subseteq$-máximo que es un nido. Sea $m = \cup n$ y definimos:

$$Dom(m) = \bigcup_{n_\lambda \in n} Dom(n_\lambda) \wedge Im(m) = \bigcup_{n_\lambda \in n} Im(n_\lambda).$$

Veamos que $m \in Q$.
i)Sean $(x, y), (x, z) \in m$, entonces existen

$$n_1, n_2 \in n \text{ tal que } (x, y) \in n_1 \text{ y } (x, z) \in n_2,$$

como n es nido, sin pérdida de generalidad, $n_1 \subseteq n_2$ y de esto se sigue que $(x, y), (x, z) \in n_2$, como n_2 es función se tiene que $y = z$ y así m es una relación univalente, y por tanto función.

ii)Supongamos que m no es inyectiva, esto es que existen $(x, z), (y, z) \in m$ con $x \neq y$, por otro lado existen

$$n_1, n_2 \in n \text{ tal que } (x, z) \in n_1 \text{ y } (y, z) \in n_2,$$

sin pérdida de generalidad, $n_1 \subseteq n_2$ por ser n nido, de esto se sigue que $(x, z), (y, z) \in n_2$ y como n_2 es inyectiva tenemos que $x = y$, pero esto no puede pasar. Por lo tanto m es inyectiva.
iii)Para ver que $(B - Im(m)) \cap Dom(m) = \emptyset$, supongamos que existe $u \in (B - Im(m)) \cap Dom(m)$ y notemos que

$$B - Im(m) = B - \cup_{n_\lambda \in n} Im(n_\lambda) = \cap_{n_\lambda \in n} (B - Im(n_\lambda)) \subseteq B - Im(n_\alpha),$$

esto implica que para toda $n_\alpha \in n$

$$u \in B - Im(n_\alpha)$$

y que existe $n_\beta \in n$ tal que

$$u \in Dom(n_\beta),$$

pero esto nos dice que $u \in Dom(n_\beta) \cap (B - Im(n_\beta)) = \emptyset$, lo que es imposible. Por lo tanto $(B - Im(m)) \cap Dom(m) = \emptyset$.
iv)Ahora veamos que la unión es linealmente independiente. Sea $\{v_1, ..., v_r\} \subseteq (B - Im(m)) \cup (Dom(m))$ con $r \in \mathbb{N}$, podemos separar los elementos de la siguiente manera:

$$\{v_i : v_i \in Dom(m) \ \wedge \ i = 1, ..., r\} = \{w_1, ..., w_l\}$$

$$\{v_i : v_i \in B - Im(m) \ \wedge \ i = 1, ..., r\} = \{u_1, ..., u_t\}$$

Por ser nido n, existe

$$n_\alpha \in n \text{ tal que } \{w_1, ..., w_l\} \subseteq Dom(n_\alpha).$$

Veamos que $\{u_1, ..., u_t\} \subseteq B - Im(n_\alpha)$, sabemos que

$$B - Im(m) \subseteq B - Im(n_\alpha)$$

como $\{u_1, ..., u_t\} \subseteq B - Im(m)$ se tiene que $\{u_1, ..., u_t\} \subseteq B - Im(n_\alpha)$, por lo tanto $\{v_1, ..., v_r\} \subseteq (Dom(n_\alpha) \cup (B - Im(n_\alpha))$ que es linealmente independiente en V, por lo tanto $\{v_1, ..., v_r\}$ es linealmente independiente en V. Así tenemos que cualquier subconjunto finito de $(Dom(m) \cup (B - Im(m))$ es linealmente independiente y por lo tanto $(Dom(m) \cup (B - Im(m))$ es linealmente independiente en V. Por lo tanto $m \in Q$.
5)Por último veamos que $m \in n$. Para esto, primero notemos que $n \cup \{m\}$ es un nido, sean $n_1, n_2 \in n \cup \{m\}$:

i) si $n_1, n_2 \in n$, entonces $n_1 \subseteq n_2$ o $n_2 \subseteq n_1$ por ser n un nido;

ii) si $n_1, n_2 \in \{m\}$, entonces $n_1 = n_2 = m$ y $n_1 \subseteq n_2$;

iii) si $n_1 \in n$ y $n_2 \in \{m\}$, entonces $n_1 \subseteq n_2$.

Así vemos que $n \cup \{m\}$ es nido y que $n \subseteq n \cup \{m\}$, como n es nido $\subseteq$-máximo entonces $n \cup \{m\} = n$ y $m \in n$.
Para terminar la prueba supongamos que:

$$(\text{existe } v \in B - Im(m)) \text{ y } (A - Dom(m) \neq \emptyset).$$

Entonces

$$(B - (Im(m) \cup \{v\})) \cup Dom(m) \text{ es linealmente independiente en } V$$

además

$$\langle (B - (Im(m) \cup \{v\})) \cup Dom(m) \rangle \neq V$$

pues de lo contrario

$$v \in \langle (B - (Im(m) \cup \{v\})) \cup Dom(m) \rangle$$

y de eso se sigue que $(B - Im(m)) \cup Dom(m)$ no es linealmente independiente en V, una contradicción; además

$$A - Dom(m) \nsubseteq \langle (B - (Im(m) \cup \{v\})) \cup Dom(m) \rangle$$

supongamos que si, entonces:

$$A = (A - Dom(m)) \cup Dom(m) \subseteq \langle (B - (Im(m) \cup \{v\})) \cup Dom(m) \rangle$$

y esto implica que

$$V = \langle A \rangle \subseteq \langle (B - (Im(m) \cup \{v\})) \cup Dom(m) \rangle,$$

lo cual es imposible. Como

$$A - Dom(m) \nsubseteq \langle (B - (Im(m) \cup \{v\})) \cup Dom(m) \rangle,$$

entonces existe

$$w \in A - Dom(m) \text{ tal que } w \notin \langle (B - (Im(m) \cup \{v\})) \cup Dom(m) \rangle.$$

Definimos $\bar{m} := m \cup \{(w, v)\}$, es evidente que $w \notin Dom(m)$ y que $v \notin Im(m)$ y esto implica que $\bar{m}$ es una relación univalente, una relación total-izquierda y como función es inyectiva. Veamos que $\bar{m} \in Q$, para ello notemos que

$$Dom(\bar{m}) \cup (B - Im(\bar{m})) = (Dom(m) \cup \{w\}) \cup (B - (Im(m) \cup \{v\}))$$

es linealmente independiente pues

$$w \notin \langle Dom(m) \cup (B - (Im(m) \cup \{v\}))\rangle$$

y

$$Dom(m) \cup (B - (Im(m) \cup \{v\})$$

ya es linealmente independiente, además para ver que la intersección es vacía notemos que

$$Dom(m) \cap (B - (Im(m) \cup \{v\})) = \emptyset$$

y como

$$w \notin \langle Dom(m) \cup (B - (Im(m) \cup \{v\}))\rangle,$$

se tiene que

$$(Dom(m) \cup \{w\}) \cap (B - (Im(m) \cup \{v\})) = \emptyset$$

Por lo tanto $\bar{m} \in Q$ y $m \subsetneq \bar{m}$, lo que implica que $\bar{m} \notin n$. Sea $\bar{n} := n \cup \{\bar{m}\}$, se sigue del hecho de que n sea nido y que para cada $n_1 \in n$ sea tal que $n_1 \subseteq \bar{m}$ que $\bar{n}$ es nido. Por lo anterior tenemos que $n \subsetneq \bar{n}$ pero n es nido $\subseteq$-máximo, lo cual es imposible, la contradicción viene de suponer que

$$B - Im(m) \neq \emptyset \text{ y } A - Dom(m) \neq \emptyset.$$

Por lo tanto

$$A - Dom(m) = \emptyset \text{ o } B - Im(m) = \emptyset.$$

Tratemos ambos casos:
i)Si $A - Dom(m) = \emptyset$ se tiene que

$$A \subseteq Dom(m) \subseteq A,$$

por tanto

$$A = Dom(m),$$

de esto se sigue que $A \cup (B - Im(m))$ es linealmente independiente pero por ser A base, A ya es máximo linealmente independiente, entonces

$$B - Im(m) = \emptyset.$$

Así que

$$B \subseteq Im(m) \subseteq B.$$

Por lo que

$$Im(m) = B = Ran(m).$$

Entonces m es sobreyectiva y así existe una biyección entre A y B, por lo tanto $|A| = |B|$.
ii)Si $B - Im(m) = \emptyset$, m es sobreyectiva, entonces:

$$|B| = |Im(m)| \leq |Dom(m)| \leq |A|$$

y así

$$|B| \leq |A|$$

Haciendo todo el proceso de la prueba de forma análoga llegamos a que $|A| \leq |B|$ y por Teorema de Cantor-Schroeder-Bernstein, $|A| = |B|$. □

3.3 Teorema. Si M_R es un módulo finitamente generado entonces todo submódulo propio está contenido en un submódulo máximo de M.

Demostración. Sea $\{x_1, ..., x_n\}$ el sistema generador de M_R. Sea $A \lneq M_R$ y sea

$$C := \{B : A \leq B \lneq M_R\}$$

Notamos que en particular $A \in C$. Por M6 existe $N \subseteq C$ que es nido $\subseteq$-máximo, y sea $U = \cup N$. Veamos que U es submódulo, para esto es suficiente demostrar que para toda $a_1, a_2 \in U$ y toda $r \in R$ se cumple que $a_1 + a_2, a_1 r \in U$. Sean $a_1, a_2 \in U$, entonces existen

$$N_1, N_2 \in N \text{ tal que } a_1 \in N_1 \text{ y } a_2 \in N_2.$$

Como N es nido, sin pérdida de generalidad, $N_1 \subseteq N_2$, así $a_1, a_2 \in N_2$, como $N_2 \leq M$ se tiene que $a_1 + a_2, a_1 r \in N_2 \subseteq U$, por lo tanto $U \leq M$.
Queda ver que $U \lneq M$. Supongamos que $U = M$, entonces $\{x_1, ..., x_n\} \subseteq U$, así que existen

$$N_1, ..., N_n \in N \text{ tal que } x_i \in N_i \text{ con } i = 1, ..., n.$$

Como N es nido, sin pérdida de generalidad, $N_1, ..., N_n \subseteq N_j$ para $j \in \{1, ..., n\}$. Así que $\{x_1, ..., x_n\} \subseteq N_j$, por lo que $\langle\{x_1, ..., x_n\}\rangle \subseteq N_j$. Es decir $M \subseteq N_j$. Concluyendo que $N_j = M$, lo cual es imposible. Por lo tanto $U \lneq M$.
Falta ver que $A \leq U$, para esto solo necesitamos ver que $A \subseteq U$ pero dada la forma en que se construyo U es evidente que A es subconjunto, así tenemos que $A \leq U$ y por lo tanto $U \in C$.

Por último demostremos que U es submódulo máximo. Supongamos que no es máximo, entonces existe

$$U^* \lneq M \text{ tal que } U \lneq U^*,$$

en particular $A \leq U^*$, esto implica que $U^* \in C$, como $U^* \neq U$ entonces existe $u \in U^*$ tal que $u \notin U$, de esto se sigue que $U^* \notin N$. Sea $N^* := N \cup \{U^*\}$ y sean $D, E \in N^*$:
i)si $D, E \in N$ entonces $D \subseteq E$ o $E \subseteq D$;
ii)si $D, E \in \{U^*\}$ entonces $D = E$ y así $D \subseteq E$;
iii)si $D \in N$ y $E \in \{U^*\}$ entonces $D \subseteq E$. Por lo tanto N^* es nido, además $N \lneq N^*$, pero N es $\subseteq$-máximo en C, por lo tanto U es submódulo máximo. □

3.4 Corolario. Todo módulo distinto de cero finitamente generado tiene máximos.

3.5 Corolario. Todo anillo R tiene ideales máximos.

3.2. Criterio de Baer

3.6 Lema. Sea $\alpha : A \to B$ un homomorfismo. Entonces tenemos que:

(1) α es inyectivo si y solo si $Ker(\alpha) = 0$.

(2) $U \leq A$, entonces $\alpha^{-1}(\alpha(U)) = U + Ker(\alpha)$.

(3) $V \leq B$, entonces $\alpha(\alpha^{-1}(V)) = V \cap Im(\alpha)$.

(4) Sea también $\beta : B \to C$ un homomorfismo. Entonces

$$Ker(\beta\alpha) = \alpha^{-1}(Ker(\beta)) \text{ y } Im(\beta\alpha) = \beta(Im(\alpha)).$$

Demostración. (1)"$\Rightarrow$": Sea $x \in Ker(\alpha)$ entonces $\alpha(x) = 0 = \alpha(0)$, como α es inyectivo se tiene que $x = 0_A$ de ahí que $Ker(\alpha) = 0$.
"$\Leftarrow$": Sea $\alpha(a_1) = \alpha(a_2)$. Entonces $\alpha(a_1 - a_2) = 0$, así $a_1 - a_2 \in Ker(\alpha)$ y por tanto $a_1 = a_2$, se deduce que α es inyectivo.

(2)"$\alpha^{-1}(\alpha(U)) \leq U + Ker(\alpha)$": Sea $a \in \alpha^{-1}(\alpha(U))$. Entonces $\alpha(a) \in \alpha(U)$ y por tanto existe $u \in U$ tal que $\alpha(a) = \alpha(u)$. Entonces $\alpha(a - u) = 0$, luego $a - u \in Ker(\alpha)$ y así $a \in U + Ker(\alpha)$. "$\alpha^{-1}(\alpha(U)) \geq U + Ker(\alpha)$": Sean $u \in U$ y $k \in Ker(\alpha)$. Entonces

$$\alpha(u + k) = \alpha(u) + \alpha(k) = \alpha(u) + 0 = \alpha(u) \in \alpha(U),$$

y así $u + k \in \alpha^{-1}(\alpha(U))$.

(3)"$\alpha(\alpha^{-1}(V)) \leq V \cap Im(\alpha)$": Sea $b \in \alpha(\alpha^{-1}(V))$ entonces tenemos que existe $a \in \alpha^{-1}(V)$ tal que $\alpha(a) = b$ y por tanto $b \in Im(\alpha) \cap V$.
"$\alpha(\alpha^{-1}(V)) \geq V \cap Im(\alpha)$": Sea $b \in V \cap Im(\alpha)$ entonces existe $a \in A$ tal que $\alpha(a) = b$ y $\alpha^{-1}(b) \in \alpha^{-1}(V)$, entonces

$$\alpha(\alpha^{-1}(b)) \in \alpha(\alpha^{-1}(V)),$$

así que

$$b = \alpha(a) = \alpha(\alpha^{-1}(\alpha(a))) \in \alpha(\alpha^{-1}(V)).$$

(4)Tenemos que:

$$a \in Ker(\beta\alpha) \text{ sii } \beta\alpha(a) = 0 \text{ sii } \alpha(a) \in Ker(\beta) \text{ sii } a \in \alpha^{-1}(Ker(\beta)).$$

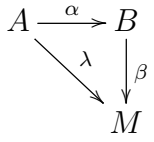
Además:

$$Im(\beta\alpha) = \beta\alpha(A) = \beta(\alpha(A)) = \beta(Im(\alpha)).$$

□

3.7 Definición. Se dice que un homomorfismo inyectivo $\alpha : A \to B$ se escinde si y solo si $Im(\alpha)$ es sumando directo en B.

3.8 Lema. Consideremos el siguiente diagrama



conmutativo, i.e. $\lambda = \beta\alpha$. Entonces

(1) $Im(\alpha) + Ker(\beta) = \beta^{-1}(Im(\lambda))$,

(2) $Im(\alpha) \cap Ker(\beta) = \alpha(Ker(\lambda))$.

Demostración. (1) $\lambda = \beta\alpha$, entonces $Im(\lambda) = Im(\beta\alpha) = \beta(Im(\alpha))$ por lo tanto $\beta^{-1}(Im(\lambda)) = \beta^{-1}(\beta(Im(\alpha))) = Im(\alpha) + Ker(\beta)$ por lema 3.6.

(2) $Ker(\lambda) = Ker(\beta\alpha) = \alpha^{-1}(Ker(\beta))$ por lema 3.6, entonces $\alpha(Ker(\lambda)) = \alpha(\alpha^{-1}(Ker(\beta))) = Im(\alpha) \cap Ker(\beta)$ por lema 3.6. □

3.9 Corolario. a) λ es un homomorfismo suprayectivo entonces $Im(\alpha) + Ker(\beta) = \beta^{-1}(M) = B$.
b) λ es un homomorfismo inyectivo entonces $Im(\alpha) \cap Ker(\beta) = \alpha(0) = 0$.
c) λ es un isomorfismo entonces $Im(\alpha) \oplus Ker(\beta) = B$.

Demostración. Consecuencia directa de lema 3.8. □

3.10 Corolario. Para $\alpha : A \to B$ las siguientes condiciones son equivalentes:

(a) α es un homomorfismo inyectivo que se escinde.

(b) Existe un homomorfismo $\beta : B \to A$ con $\beta\alpha = 1_A$.

Demostración. "(a) $\Rightarrow$ (b)": Sea $B = Im(\alpha) \oplus B_1$ y sea $\pi : B \to Im(\alpha)$ la proyección de B sobre $Im(\alpha)$ definida por

$$\pi(\alpha(a) + b_1) := \alpha(a), \quad \alpha(a) \in Im(\alpha), b_1 \in B_1.$$

Además sea $\alpha_0 : A \ni a \to \alpha(a) \in Im(\alpha)$, i.e. sea α_0 el isomorfismo definido por la restricción del codominio B de α a $Im(\alpha)$.
Definimos $\beta := \alpha_0^{-1}\pi$ entonces tenemos

$$\beta\alpha(a) = \alpha_0^{-1}\pi\alpha(a) = \alpha_0^{-1}(\alpha(a)) = a, \quad a \in A,$$

así $\beta\alpha = 1_A$.
"(b) $\Rightarrow$ (a)": Como $\beta\alpha = 1_A$ entonces por corolario 3.9 c) tenemos que $Im(\alpha) \oplus Ker(\beta) = B$. Para terminar la prueba notemos que si α no es inyectiva entonces deben existir $a_1 \neq a_2$ en A tal que su imagen bajo α es la misma y así tenemos que $a_1 = \beta\alpha(a_1) = \beta(\alpha(a_1)) = \beta(\alpha(a_2)) = \beta\alpha(a_2) = a_2$, una contradicción, por tanto α es un homomorfismo inyectivo que se escinde. □

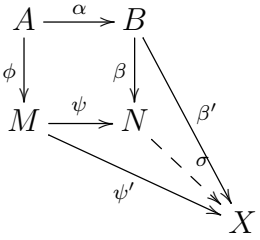
Sin ahondar mucho en el tema discutamos rápidamente lo que es un pushout lo que nos servirá para resultados más adelante. Sean $\alpha : A \to B$ y $\phi : A \to M$ dos homomorfismos con el mismo dominio y tengamos en cuenta el siguiente diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\beta} \\ M & \xrightarrow{\psi} & N \end{array}$$

deseamos ver de qué manera podemos integrar estos homomorfismos en un diagrama conmutativo y que para la pareja (ψ, β), si tenemos otra pareja que complete el diagrama de la misma manera, entonces de qué manera se relación con la primer pareja.

3.11 Definición. Consideremos el diagrama conmutativo dado antes. La pareja (ψ, β) es llamada el pushout de la pareja (ϕ, α): si y solo si para cada pareja (ψ', β') con $\psi' : M \to X$ y $\beta' : B \to X$ y $\psi'\phi = \beta'\alpha$ existe precisamente un $\sigma : N \to X$ con $\psi' = \sigma\psi$, $\beta' = \sigma\beta$.

Todo esto se ve claramente en el siguiente diagrama.



No nos dentendremos para probar la unicidad de los pushout, esto se puede encontrar sin ningún problema en cualquier libro de teoría de categorías; por otro lado demostraremos la existencia que nos servirá en lo posterior.
En lo siguiente denotamos a los elementos de $M \oplus B$ por (b, m) y a los elementos de $(M \oplus B)/U$ por $\overline{(m, b)}$.

3.12 Teorema. Sea la pareja (ϕ, α) dada por

$$\phi : A \to M, \quad \alpha : A \to B.$$

Sea

$$N := (M \oplus B)/U \quad \text{con} \quad U := \{(\phi(a), -\alpha(a)) : a \in A\}$$

y sean

$$\psi : M \ni m \mapsto \overline{(m, 0)} \in N, \quad \beta : B \ni b \mapsto \overline{(0, b)} \in N,$$

entonces (ψ, β) son un pushout de (ϕ, α).

Demostración. Antes que nada debe ser claro que $M \oplus B$ es un módulo, que U es submódulo de $M \oplus B$ y que N es un módulo cociente y que ψ y β son homomorfismos, solo nos dentendremos a verificar que ψ y β cumplen que $\psi\phi = \beta\alpha$. Sea $a \in A$

$$\psi\phi(a) = \beta\alpha(a) \text{ sii } \psi(\phi(a)) = \beta(\alpha(a)) \text{ sii } \overline{(\phi(a), 0)} = \overline{(0, \alpha(a))}$$
$$\text{sii } \overline{(\phi(a), 0)} - \overline{(0, -\alpha(a))} = 0 \text{ sii } \overline{(\phi(a), -\alpha(a))} = 0,$$

lo que es cierto pues $(\phi(a), -\alpha(a)) \in U$ y por ende $\overline{(\phi(a), -\alpha(a))}$ es quivalente a la clase del 0.
Sean ψ' y β' como en la definición 3.11. Definimos $\sigma : N \to X$ por $\sigma(\overline{(m, b)}) := \psi'(m) + \beta'(b)$. para ver que σ es función es suficiente con notar que para $(m, b) \in U$ se tiene que $\sigma(\overline{(m, b)}) = 0$:

$$\sigma(\overline{(\phi(a), -\alpha(a))}) = \psi'\phi(a) - \beta'\alpha(a) = 0$$

pues $\psi'\phi = \beta'\alpha$. De nuevo es claro que σ es un homomorfismo y que $\sigma\psi = \psi'$ y $\sigma\beta = \beta'$. Solo falta demostrar la unicidad de σ, para ellos supongamos que existe $\sigma_1 : N \to X$ tal que $\sigma_1\psi = \psi'$ y $\sigma_1\beta = \beta'$. De lo anterior se sigue que

$$(\sigma - \sigma_1)\psi = 0, \quad (\sigma - \sigma_1)\beta = 0,$$

así

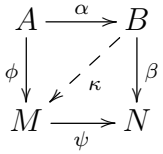
$$0 = (\sigma - \sigma_1)\psi(m) = (\sigma - \sigma_1)(\overline{(m,0)}),$$
$$0 = (\sigma - \sigma_1)\beta(b) = (\sigma - \sigma_1)(\overline{(0,b)}).$$

Como $\{\overline{(m,0)}, \overline{(0,b)} : m \in M \text{ y } b \in B\}$ es un conjunto generador de N, para el cual $\sigma - \sigma_1$ es el función cero, entonces $\sigma - \sigma_1 = 0$. Esto completa la prueba. □

3.13 Teorema. Sea (ψ, β) un pushout de (ϕ, α). Entonces tenemos:

(1) α es inyectivo entonces ψ es inyectivo;

(2) Sea α un homomorfismo inyectivo, entonces tenemos: $Im(\psi)$ es sumando directo en N, o sea que ψ se escinde si y solo si existe un $\kappa : B \to M$ tal que $\phi = \kappa\alpha$:



Demostración. (1)Sea α un homomorfismo inyectivo y sea $\psi(m) = \overline{(m,0)} = 0$ entonces existe $a \in A$ tal que $(m,0) = (\phi(a), -\alpha(a))$ y de esto se sigue que $-\alpha(a) = 0$, por tanto $a = 0$, por lo tanto $m = \phi(a) = 0$.

(2)Sea $Im(\psi)$ un sumando directo en N, entonces existe N_0 tal que $N = Im(\psi) \oplus N_0$. Como α es inyectivo, de (1) obtenemos que ψ también lo es y consecuentemente ψ induce una biyección

$$\psi_0 : M \to Im(\psi).$$

Sea

$$\pi : N \to Im(\psi)$$

la proyección que proviene del hecho que $N = Im(\psi) \oplus N_0$, entonces $\kappa := \psi_0^{-1}\pi\beta$ cumple lo que necesitamos

$$\kappa\alpha(a) = \psi_0^{-1}\pi\beta\alpha(a) = \psi_0^{-1}\pi\psi\phi(a) = \psi_0^{-1}\pi\overline{(\phi(a),0)} = \phi(a).$$

Inversamente sea κ tal que $\phi = \kappa\alpha$. Consideramos

$$\xi : N \ni \overline{(m, b)} \mapsto m + \kappa(b) \in M,$$

como $\xi(\overline{(\phi(a), -\alpha(a))}) = \phi(a) - \kappa\alpha(a) = 0$ entonces ξ es función y también homomorfismo. Como $\xi\psi(m) = \xi(\overline{(m, 0)}) = m$ tenemos que $\xi\psi = 1_M$, de lo anterior, por el corolario 3.10, se deduce la veracidad de que $N = Im(\psi) \oplus Ker(\xi)$.

□

3.14 Teorema. Lo siguiente es equivalente para un módulo Q_R:

(1) Cada homomorfismo inyectivo

$$\xi : Q \to B$$

se escinde(i.e. $Im(\xi)$ es sumando directo en B).

(2) Para cada homomorfismo inyectivo $\alpha : A \to B$ y para cada homomorfismo $\phi : A \to Q$ existe un homomorfismo $\kappa : B \to Q$ con $\phi = \kappa\alpha$.

Diagrama para (2):

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\phi}\downarrow & \swarrow_{\kappa} & \\ Q & & \end{array}$$

Demostración. "(1)⇒(2)":Completemos el diagrama de la definición, sabemos que existe el pushout de la pareja (ϕ, α), sean (ψ, β),

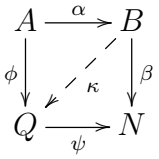
$$\beta : B \to N \text{ y } \psi : Q \to N,$$

tal pushout.

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\beta} \\ Q & \xrightarrow[\psi]{} & N \end{array}$$

Como α es inyectivo entonces ψ también lo es por el teorema 3.13(1) y de la hipótesis tenemos que ψ se escinde(es sumando directo en N), ahora por el teorema 3.13(2), existe

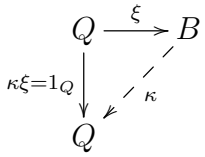
$$\kappa : B \to Q \text{ tal que } \phi = \kappa\alpha.$$



"(2)⇒(1)":Sean $\xi : Q \to B$ un homomorfismo inyectivo y $1_Q : Q \to Q$ un homomorfismo, de la hipótesis sabemos que existe

$$\kappa : B \to Q \text{ tal que } \phi = \kappa\alpha$$

ahora directo de el corolario 3.10 tenemos que ξ se escinde.



□

3.15 Definición. A un módulo que cumple lo anterior se le dice inyectivo.

3.16 Teorema. (Criterio de Baer) Un módulo Q_R es inyectivo si y solo si para cada ideal derecho $U \leq R_R$ y para cada homomorfismo $\rho : U \to Q$ existe un homomorfismo $\tau : R_R \to Q$ con $\rho = \tau\imath$, donde $\imath$ es la inclusión de U en R.

Demostración. Primero notemos que es claro de la definición de módulo inyectivo que la necesidad implica la suficiencia. El converso se sigue en dos pasos.
Paso 1: Sea $\alpha : A \to B$ un homomorfismo inyectivo y sea $\phi \in Hom_R(A, Q)$. Sea $C \lneq B$ con $Im(\alpha) \leq C$ y sea $\gamma : C \to Q$ con $\phi(a) = \gamma\alpha(a)$ para toda $a \in A$.
Afirmación. Existe un $C_1 \leq B$ con $C \lneq C_1$ y un $\gamma_1 : C_1 \to Q$ con $\gamma_1|_C = \gamma$ $(\phi(a) = \gamma_1\alpha(a))$.
Para probar esta afirmación sea $b \in B$, $b \notin C$, sea $C_1 = C + bR$. Si tuvieramos que $C \cap bR = 0$ entonces podríamos extender γ trivialmente a C_1. La dificultad yace en el hecho de que podemos tener $C \cap bR \neq 0$. ¿Cómo?. Si tuvieramos que $R = \mathbb{Z}$ y $C = 2b\mathbb{Z}$ se sigue que $b \notin C$ y también que

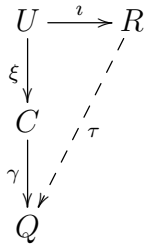
$C \cap bR \neq 0$.
Sea

$$U := \{u : u \in R \wedge bu \in C\},$$

veamos que $U \leq R_R$. Sean $u_1, u_2 \in U$, entonces

$$u_1 b, u_2 b \in C \Rightarrow u_1 b + u_2 b \in C \Rightarrow (u_1 + u_2)b \in C \Rightarrow u_1 + u_2 \in U.$$

Sea $r \in R$, como $u_1 b \in C$ se tiene que $u_1 br \in C$ y por tanto $u_1 r \in U$, así para toda $u_1, u_2 \in U$ y para toda $r \in R$ se cumple que $u_1 + u_2, u_1 r \in U$, por tanto $U \leq R_R$.
Sea $\xi : U \ni u \mapsto bu \in C$ un R-homomorfismo. Sea $\rho = \gamma\xi$, entonces tenemos que $\rho : U \to Q$ y por hipótesis tenemos que existe $\tau : R_R \to Q$ con $\rho = \tau\imath$ donde $\imath$ es la inclusión de U en R.



Ahora definimos $\gamma_1 : C_1 \to Q$ por

$$\gamma_1 : C + bR \ni c + br \mapsto \gamma(c) + \tau(r) \in Q,$$

para establecer que γ_1 es función sean $c + br = c_1 + br_1$ con $c, c_1 \in C$ y $r, r_1 \in R$, entonces $c - c_1 = b(r_1 - r) \in C \cap bR$ y por tanto $r_1 - r \in U$, luego $\gamma\xi(r_1 - r) = \tau(r_1 - r)$, dando como resultado que

$$\gamma(c - c_1) = \gamma(b(r_1 - r)) = \gamma\xi(r_1 - r) = \tau(r_1 - r),$$

se sigue que $\gamma(c) + \tau(r) = \gamma(c_1) + \tau(r_1)$, como γ y τ son R-homomorfismos entonces γ_1 también lo es y por la definición de γ_1, $\gamma_1|_C = \gamma$.

Paso 2: Ahora veamos que nos podemos "aproximar" a B y a un morfismo que vaya de B a Q. Sea $C_0 := Im(\alpha)$ y sea α_0 el isomorfismo de A sobre C_0 inducido por α. Más aun sea $\gamma_0 := \phi\alpha_0^{-1}$, entonces tenemos $\phi(a) = \gamma_0\alpha(a)$ para todo $a \in A$. Extendemos γ_0 a todo B con ayuda del paso 1 y M6. Para esto sea

$$\Gamma := \{\gamma : C \to Q : C_0 \leq C \lneq B \text{ y } \gamma|_{C_0} = \gamma_0\}$$

cabe mencionar que $C_0 \lneq B$ pues de lo contrario α sería una biyección y se obtendría de inmediato que el teorema es cierto, así el caso que nos interesa es cuando α no es biyección, entonces en particular $\gamma_0 \in \Gamma$. Recordemos que para dos homomorfismos μ y λ, $\mu \subseteq \lambda$ quiere decir que $Dom(\mu) \subseteq Dom(\lambda)$, $Im(\mu) \subseteq Im(\lambda)$ y

$$(a, \mu(a)) \in \mu \text{ entonces } (a, \mu(a)) \in \lambda \text{ y } \mu(a) = \lambda(a).$$

Sean $\gamma_1, \gamma_2 \in \Gamma$ con $\gamma_1 : C_1 \to Q$ y $\gamma_2 : C_2 \to Q$ tal que $\gamma_1 \subseteq \gamma_2$, esto implica que $C_1 \subseteq C_2$, es evidente que $\gamma_2|_{C_1} = \gamma_1$, notemos que $C_1 \leq C_2$.
Por M6 existe $n \subseteq \Gamma$ $\subseteq$-máximo que es un nido. Sea $\delta := \cup n$ donde

$$Dom(\delta) = \cup_{\gamma \in n} Dom(\gamma),\ Im(\delta) = \cup_{\gamma \in n} Im(\gamma) \subseteq Q,$$

llamemos $D = Dom(\delta)(\delta : D \to Q)$. Demostraremos que $\delta|_{C_0} = \gamma_0$. Sea $c \in C_0$, sea $\gamma \in n$, tenemos que $\gamma(c) = \gamma_0(c)$, como $\gamma(a) \in Im(\delta)$ entonces $\delta(c) = \gamma_0(c)$, por lo tanto $\delta|_{C_0} = \gamma_0$, de esto se sigue $\phi(a) = \delta\alpha(a)$, ahora bien nos debemos detener a pensar en como es D, si $D = B$ la prueba está completa y si $D \neq B$ entonces tenemos que $\delta \in \Gamma$. Ahora veamos que $\delta \in n$, para ello sea $n^* = n \cup \{\delta\} \subseteq \Gamma$, sean $\alpha, \beta \in n^*$:

i) si $\alpha, \beta \in n$ entonces $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$;

ii) si $\alpha, \beta \in \{\delta\}$ entonces $\alpha = \beta$ y por tanto $\alpha \subseteq \beta$;

iii) si $\alpha \in n$ y $\beta \in \{\delta\}$ entonces por la definición de δ tenemos que $\alpha \subseteq \beta$.

Por lo tanto n^* es un nido y como $n \subseteq n^*$, por la maximidad de n, $n^* = n$ y $\delta \in n$.
Por último veamos que δ es $\subseteq$-máximo en Γ. Supongamos que existe $\delta^* \in \Gamma$ tal que $\delta \lneq \delta^*$, sea $n^{**} := n \cup \{\delta^*\}$, igual que antes vemos que n^{**} es un nido, pero $\delta^* \notin n$, por lo tanto $n \lneq n^{**}$!, por la maximidad de n tenemos que δ es $\subseteq$-máximo en Γ. Ahora por paso 1) existe $B_1 \leq B$ con $D \lneq B_1$ y un $\kappa : B_1 \to Q$ con $\kappa|_D = \delta$.
Por demostrar que $B_1 = B$. Supongamos que $B_1 \neq B$, entonces

$$B_1 \lneq B \text{ y } \kappa|_{C_0} = (\kappa|_D)|_{C_0} = \delta|_{C_0} = \gamma_0,$$

por lo tanto $\kappa \in \Gamma$, además $\delta \subsetneq \kappa$, una contradicción, por ser δ máximo. Por tanto $B_1 = B$ y esto implica que $\kappa : B \to Q$ $(\phi(a) = \kappa\alpha(a))$.
Por lo tanto Q_R es un módulo inyectivo. $\square$

Bibliografía

[1] Rubin H., Rubin J. E., Equivalents of the axiom of choice, II, North Holland Publishing Co., 1985.

[2] Jech T., Hrbacek K., Introduction to set theory, Marcel Dekker, Inc., 1999.

[3] Herrlich H., Axiom of choice, Springer-Verlag, 2006.

[4] Kasch F., Modules and rings, Academic Press, 1982.

[5] Rincón Mejía H. A., Álgebra lineal, Publidisa Mexicana, 2006.

[6] Smullyan R. M., Fitting M., Set theory and the continuum problem, Claredon Press, 1996.

[7] Mendelson E., Introduction to mathematical logic, Chapman Hall, 1997.

[8] Angoa J., Arrazola J., Escobedo R., Topología y sus aplicaciones, Dirección de Fomento Editorial, 2012.