Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Algunos resultados del lema del ultrafiltro.

Tesis presentada al

Colegio de Matemáticas

como requisito parcial para la obtención del grado de

Licenciado en Matemáticas

por

Luis Enrique Aponte Pérez

Asesorado por

Iván Martínez Ruiz & Iván Fernando Vilchis Montalvo

Puebla Pue.
18 de agosto de 2022

Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Algunos resultados del lema del ultrafiltro.

Tesis presentada al

Colegio de Matemáticas

como requisito parcial para la obtención del grado de

Licenciado en Matemáticas

por

Luis Enrique Aponte Pérez

Asesorado por

Iván Martínez Ruiz & Iván Fernando Vilchis Montalvo

Puebla Pue.
18 de agosto de 2022

Título: Algunos resultados del lema del ultrafiltro.
Estudiante: Luis Enrique Aponte Pérez

COMITÉ

Presidente

Secretario

Vocal

Vocal

Iván Martínez Ruiz & Iván Fernando Vilchis Montalvo
Asesor

Dedicado con cariño a
Mis padres María Inés Peréz Martínez & Gustavo Alberto Aponte Barrientos
Por apoyarme todo este tiempo y darme la oportunidad de aprender.

Agradecimientos

A mis hermanos Gustavo Aponte Pérez por prestarme tu computadora para empezar a escribir esta tesis en tiempos de cuarentena, enseñarme a programar y Cristopher Aponte Pérez por brindarme tu tiempo cuando me sentía estresado en la universidad. A mi abuela, por su cariño incondicional, espero que estés en un mejor lugar.

A mis compañeros Miguel Eduardo Cabrera Linares, Abigail Alarcón Valdivia y Patricia Gonzáles León, por su amistad y mostrarme que una demostración es valida hasta que sea entendible para los demás.

A Esmeralda Zuñiga Gamboa por darme de comer cuando me terminada mi lunch :D, tenerme paciencia y ser una gran amiga. A Cesar Alonzo Moreno y Angel Rafael Barranco por escuchar mis locuras, ser unos grandes amigos.

A mis compañeros de la Tali-cueva por mostrarme la lógica matemática y mostrarme los fundamentos de las matematicas.

A mis asesores Iván Martínez Ruiz e Iván Fernando Vilchis Montalvo por mostrarme que las matemáticas son creativas y ayudarme con paciencia en la escritura de esta tesis.

A Zaida Garate Cahuatzi, por ser mi primer amiga de la universidad y aunque no nos vemos mucho, te quiero con demasiado cariño.

Introducción

La teoría de conjuntos es una rama de la lógica matemática que fue originada por *Georg Cantor* en el año 1874, quien al estudiar series trigonométricas extendió su interés en analizar la equipotencia de ciertos conjuntos. Por ejemplo mostró que el conjunto los números racionales tienen el mismo numero de elementos que el conjunto de los números enteros, además de probar la existencia de conjuntos infinitos mas grandes que otros conjuntos infinitos. Los primeros intentos para formalizar la teoría de conjuntos generaron en su tiempo controversia por la naturaleza paradójica de algunos resultados. Un ejemplo de ello es la conocida *paradoja de Rusell*. En consecuencia en el siglo XX *Ernest Zermelo* y *Adolf Fraenkel* se dieron a la tarea de dar una base aceptable de la teoría de conjuntos, cimentando los principios del modelo axiomático (ZF) que hoy conocemos.

Posteriormente *Ernest Zermelo* formuló el *Axioma de elección* para probar que todo conjunto puede ser bien ordenado, obteniendo así el sistema axiomático actual de la teoría de conjuntos ZFC (que son los axiomas de ZF agregando el *Axioma de elección*). Dicho principio tiene una gran variedad de aplicaciones en distintas áreas de la matemática como lógica, topología, álgebra, análisis, entre otras. Con el paso del tiempo del *Axioma de elección* generó discusiones por algunas de sus consecuencias como es el caso de la *Paradoja de Banach-Tarski*; que plantea de manera informal que... *uno puede cortar una bola en una cantidad finita de piezas y reordenar para tener dos bolas del mismo tamaño a la original.*

Después, en el año 1938 *Kurt Gödel* demostró que si se asume la consistencia de ZF es posible demostrar la consistencia de ZFC y, por otro lado en el año 1963 *Paul Cohen* creó un modelo matemático que cumplía los axiomas de ZF y la negación del *Axioma de elección* usando la *técnica de forzamiento*, con lo anterior se probo que el *Axioma de elección* no puede demostrarse por medio de los axiomas de la teoría de conjuntos. Usando ideas similares a las ya hechas por Gödel y Cohen, se crearon varios modelos de la teoría de conjuntos, en particular en un articulo de Miroslav Repický [16] se puede ver un modelo en el que se cumple el *Teorema del ideal booleano* (una equivalencia del *Lema del ultrafiltro*), pero que no cumple el *Axioma de elección*. Lo extraño aquí es que de manera similar el *Lema del ultrafiltro* no tiene una prueba en ZF y es necesario usar el *Axioma de elección* para poder probarlo.

Nuestro objetivo en esta tesis es analizar algunos resultados que usan el *Lema del ultrafiltro* (ó alguna de sus equivalencias) en vez del *Axioma de elección*. Esta tesis está organizada en tres capítulos que expondremos en breve.

En el primer capítulo se presentará una prueba simple de la equivalencia del *Lema de Zorn* con el *Axioma de elección*. Se introducirán también los conceptos de filtro y ultrafiltro, además de algunas de sus propiedades. Asimismo se demuestran algunos resultados que se usarán mas adelante para demostrar diversos resultados como el ya expuesto *Lema del ultrafiltro* y su equivalencia con el *Teorema del ideal primo*, el *Lema de Cowen-Engeler* ó que todo filtro finitamente generado es finito.

En el segundo capítulo se demostrara usando el *Lema de Cowen-Engeler*, que todo campo esta contenido en un campo algebraicamente cerrado. Para ello mostraremos que *Lema del ultrafiltro*, es equivalente a que todo todo ideal propio en un anillo conmutativo está contenido en un ideal primo. Al mismo tiempo se probara la unicidad (salvo isomorfismo) de una clausura algebraica de un campo, usando el *Teorema de Tychonoff para espacios Hausdorff*.

En el tercer capítulo estudiaremos la importancia del *Lema del ultrafiltro* en la lógica matemática, mostrando su equivalencia con el *Teorema de compacidad*. Mostraremos también que los siguientes resultados son consecuencias del *Lema del ultrafiltro*: los *Teoremas de Löwenheim-Skolem-Tarski*, la *Condición de Łos-Vaught*. Por ultimo se presentaran las bases para probar que el *teorema de Łos* y el *Lema del ultrafiltro* implican el *Axioma de elección*.

Índice general

Capítulo 1

Un poco de teoría de conjuntos

En este capitulo se presentaran los preliminares que se usaran en los resultados consecuentes en esta tesis, para ello veremos la axiomática de la teoría de conjuntos de Zermelo-Fraenkel (ZF).

Para entender la teoría axiomática de ZF, tenemos que entender qué es un conjunto. Usualmente entendemos por conjunto como una colección de elementos con alguna cualidad en común, pero con esta condición es complicado determinar un conjunto especifico. Para entender dicha dificultad, tomaremos como ejemplo a la *paradoja del montón de arena* la cual nos plantea hasta que punto un montón de arena al quitar granos de arena deja de ser un montón. En caso de que no existe un numero n de tal forma que n granos de arena forman un montón, entonces no podríamos definir que tanto es un montón, algo similar pasa con el conjunto de todos los colores oscuros hasta que punto un color deja de ser oscuro. Con ello es necesario determinar un sistema de axiomas que nos permitan decidir qué puede o no puede ser un conjunto.

1.1. Preliminares

En esta sección expondremos los principios del sistema axiomático ZF de la teoría de conjuntos, definiendo conceptos que usaremos en las secciones posteriores. Los conceptos primitivos de la teoría de conjuntos son los *conjuntos* y la relación de pertenencia *ser elemento de*. Representaremos a la relación binaria de pertenencia con el símbolo $\in$, de forma que $B \in A$ significa que B es un elemento de A. Abusando de la notación, representaremos (cuando sea necesario) a los conjuntos con letras mayúsculas y a sus elementos con letras minúsculas. Por otro lado, la negación de pertenencia la denotaremos por $\notin$, con lo cual $x \notin B$ significa que *x no es elemento de B*. A continuación enunciamos los axiomas de la teoría de conjuntos de Zermelo-Fraenkel:

Axioma 1. *(Axioma de extensión) Dos conjuntos A y B son iguales ($A = B$) si y solo sí tienen los mismos elementos.*

Axioma 2. *(Axioma del conjunto vacío) Existe un conjunto sin elementos.*

Axioma 3. *(Axioma del par) Dados dos conjuntos A y B, existe un conjunto Z tal que $A \in Z$ y $B \in Z$.*

Axioma 4. *(Axioma de la unión) Para cada conjunto X, existe un conjunto $\mathcal{U}$ tal que $x \in \mathcal{U}$ si y solo sí existe $A \in X$ con $x \in A$.*

Axioma 5. *(Axioma del conjunto potencia) Para cada conjunto X, existe un conjunto B, tal que si $A \subseteq X$, si y solo sí $A \in B$.*

Axioma 6. *(Esquema axiomático de especificación) Dada una propiedad $P(x)$ para cada conjunto X, existe un conjunto A tal que $a \in A$ si y solo sí $a \in X$ y se satisface $P(a)$.*

Axioma 7. *(Esquema axiomático de reemplazo) Sea $P(x, y)$ una propiedad tal que para cada x existe un único y, para el cual $P(x, y)$ se satisface. Para cada conjunto A, existe un conjunto B tal que para cada $x \in A$, existe un único $y \in B$ para el cual $P(x, y)$ se satisface.*

Axioma 8. *Existe un conjunto infinito.*

Decimos que A es subconjunto de B (denotado por $A \subseteq B$) si todo elemento de A también es elemento de B. Podemos reescribir el axioma de extensión de la siguiente manera: $A = B$ si y solo sí $A \subseteq B$ y $B \subseteq A$.

Se cumple que el conjunto que no tiene elementos es único. En efecto, si A, B son conjuntos que no tienen elementos (notemos que esto lo podemos suponer por el axioma del vacío), entonces todos los elementos de A pertenecen a B (la existencia de un elemento de A que no está en B, implicaría que A tiene al menos un elemento y esto contradice el hecho de que A no tiene elementos). Análogamente, se cumple que todo elemento de B está en A. Es decir que $A = B$. Al único conjunto que no tiene elementos se le llamara simplemente por *"conjunto vacío"* y lo denotaremos por $\emptyset$.

El *Esquema axiomático de especificación* nos dice que podemos construir nuevos conjuntos con un conjunto ya existente y con una propiedad, por ejemplo usando el *Axioma del par*, existe un conjunto Z que tiene como a elementos a dos conjunto A, B, luego definiendo a la propiedad $Q(x)$ tal que x satisface Q si y solo sí $x = A$ ó $x = B$, consecuentemente usando el *Esquema axiomático de especificación* podemos definir al conjunto $Z' = \{x \in Z \,|\, Q(x)\} = \{A, B\}$. De lo anterior dados a, b conjuntos podemos definir el conjunto $\{a\} = \{a, a\}$ y $\{a, b\}$, de manera similar se tiene que el conjunto $(a, b) = \{\{a\}, \{a, b\}\}$ existe. Al conjunto (a, b) lo llamaremos como el *par ordenado* cuyo primer elemento es a y segundo elemento es b.

Por el *Axioma del conjunto potencia* se tiene que para cada conjunto X, existe un conjunto B tal que si $A \subseteq X$, si y solo sí $A \in B$, suponiendo que existe otro conjunto B' con la misma propiedad, se obtiene que $A \in B'$ si y solo sí $A \in B$, luego por el *Axioma de extensión* $B = B'$ y en consecuencia se tiene que dicho conjunto es único al cuál lo denotaremos por $\mathcal{P}(X)$ que consiste de todos los subconjuntos del conjunto X.

Luego, usando lo anterior, si $a \in A$ y $b \in B$, entonces $\{a\} \subseteq A \subseteq A \cup B$ y $\{a, b\} \subseteq A \cup B$, entonces $\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$ y consecuentemente $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$.

Dados dos conjuntos A, B y $P(x)$ la propiedad tal que x se satisface si y solo sí $x \in B$, entonces podemos definir el conjunto de A intersección B como sigue $A \cap B = \{x \in A \,|\, P(x)\} = \{x \in A \,|\, x \in B\}$. Sea $Q(x)$ la propiedad tal que x se satisface si y solo sí $x \notin B$ (x no está en B), entonces podemos definir el conjunto diferencia entre A y B como sigue $A \backslash B = \{x \in A \,|\, Q(x)\} = \{x \in A \,|\, x \notin B\}$.

Con los axiomas anteriores, podemos definir el conjunto $A \times B = \{(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \,|\, a \in A,\, b \in B\}$ este conjunto conjunto recibe el nombre de *¨el producto cartesiano de A y B¨*.

Por ultimo, podemos definir *el producto cartesiano de una familia de conjuntos* $\{A_i\}_{i \in I}$, de la siguiente manera:

$$\prod_{i \in I} A_i = \{f : I \longrightarrow \bigcup_{i \in I} A_i \,|\, f(i) \in A_i \text{ para cada } i \in I\}.$$

El conjunto I, llamado conjunto de índices, puede ser finito o infinito. Cada elemento de $f \in \prod_{i \in I} A_i$ se puede representar como $(x_i)_{i \in I}$, donde $f(i) = x_i$.

Axioma 9. *(Axioma de regularidad) Para cada conjunto A, existe un conjunto $B \in A$ tal que $A \cap B = \emptyset$.*

Una consecuencia de este axioma, es que si A es un conjunto, entonces $A \notin A$.

Definición 1.1. *Sean A, B conjuntos una relación (binaria) $\mathcal{R}$ de A en B es un conjunto $\mathcal{R} \subseteq A \times B$.*

Para cada $z \in \mathcal{R}$, existen $a \in A$ y $b \in B$ tales que $z = (a, b)$. En este caso, diremos que a está en relación $\mathcal{R}$ con b y lo escribimos como $a\mathcal{R}b$.

Si $\mathcal{R}$ es una relación de A en A, solamente decimos que $\mathcal{R}$ es una relación en A.

Ejemplo 1.2. *Dado un conjunto X, tenemos que $\subseteq$ es una relación en $\mathcal{P}(X)$.*

Dada una relación $\mathcal{R}$ de X en Y, se definen el dominio de $\mathcal{R}$ y el rango de $\mathcal{R}$, denotados por $Dom(\mathcal{R})$ y $Rang(\mathcal{R})$ respectivamente como sigue $Dom(\mathcal{R}) = \{x \in X \mid x\mathcal{R}y \text{ para algún } y \in Y\}$ y $Rang(\mathcal{R}) = \{y \in Y \mid x\mathcal{R}y \text{ para algún } x \in X\}$.

Definición 1.3. *Una relación $\mathcal{R}$ en un conjunto X, se denomina un orden parcial si se cumplen las siguiente propiedades:*

- *(Reflexividad) Para cada $a \in X$, $a\mathcal{R}a$.*
- *(Antisimetría) Para cualesquiera $a, b \in X$, si $a\mathcal{R}b$ y $b\mathcal{R}a$ entonces $a = b$.*
- *(Transitividad) Para cualesquiera $a, b, c \in X$, si $a\mathcal{R}b$ y $b\mathcal{R}c$ entonces $a\mathcal{R}c$*

En este caso, decimos que $(X, \mathcal{R})$ es un conjunto parcialmente ordenado.

Ejemplo 1.4. *Dado un conjunto X, para cualquier familia de subconjuntos $\mathcal{A}$ de X con la relación contención $\subseteq$ forma un conjunto parcialmente ordenado $(\mathcal{A}, \subseteq)$, pues se cumple lo siguiente:*

- *(Reflexividad) Para cada elemento $A \in \mathcal{A}$, por el Axioma de extensión se obtiene que: $A \subseteq A$.*
- *(Antisimetría) Para A, $B \in \mathcal{A}$ si $A \subseteq B$ y $B \subseteq A$, por el Axioma de extensión se tiene que $A = B$.*
- *(Transitividad) Para A, B, $C \in \mathcal{A}$ tales que $A \subseteq B$ y $B \subseteq C$, entonces cada elemento de A es un elemento de B y como todo elemento de B es de C, entonces cada elemento de A es un elemento de C y así $A \subseteq C$.*

Definición 1.5. *Sea $(X, \mathcal{R})$ conjunto parcialmente ordenado:*

- *Un elemento $m \in X$ es máximo si para todo $x \in X$ se tiene que $x\mathcal{R}m$.*
- *Un elemento $m \in X$ es maximal si no existe un elemento $y \in X/\{m\}$ tal que $m\mathcal{R}y$.*
- *Un elemento $m \in X$ es mínimo si para todo $x \in X$ se cumple que $m\mathcal{R}x$.*
- *Decimos que un elemento $x \in X$ es una cota superior para un conjunto $A \subseteq X$, si para cada $a \in A$ $a\mathcal{R}x$. Decimos que $x \in X$ es una cota superior estricta para el conjunto A, si x es una cota superior y $x \notin A$.*

Ejemplo 1.6. *Para al conjunto parcialmente ordenado $(\mathcal{P}(X), \subseteq)$, se tiene que $X \in \mathcal{P}(X)$ es elemento máximo y $\emptyset \in \mathcal{P}(X)$ es el elemento mínimo.*

Definición 1.7. *Dados dos conjuntos A y B, una relación f de A en B es una función si para cada $a \in A$, existe un único $b \in B$ tal que afb. Si afb. En tal caso, escribiremos $f(a) = b$ para representar que afb.*

Si f es una relación de A en B. escribiremos $f : A \longrightarrow B$ si f es una función. Notemos que $A = Dom(f)$ y $Rang(f) \subseteq B$.

Dadas dos funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$, si $Rang(f) \subseteq Dom(g)$, definimos la función composición de f con g, denotada por $g \circ f : A \longrightarrow C$, como la función tal que para cada $a \in A$, $(g \circ f)(a) = g(f(a))$.

Dados una función $f : A \longrightarrow B$ y un conjunto $A' \subseteq A$, definimos la *función f restringida al conjunto A'* como la función $f|_{A'} : A' \longrightarrow B$, donde $Dom(f|_{A'}) = A'$, $Rang(f|_{A'}) \subseteq B$, y tal que $f|_{A'}(x) = f(x)$ para cada $x \in A'$.

Análogamente, si $Rang(f) \subseteq B' \subseteq B$, definimos a la *función f correstringida al conjunto B'* como la función $f|^{B'} : A \longrightarrow B'$ donde $Dom(f|^{B'}) = A$, $Rang(f|^{A'}) = B'$ y tal que para cada $x \in A$ se tiene que $f|^{B'}(x) = f(x) \in B'$.

Finalmente definimos a la función identidad de un conjunto A como la función $Id_A : A \longrightarrow A$, tal que $Id_A(a) = a$ para cada $a \in A$

Proposición 1.8. *Sea I un conjunto y para cada $i \in I$ sea $f_i : A_i \longrightarrow D$ una función. Entonces $\bigcup_{i\in I} f_i$ es una función si y solo sí para cada $k \neq j$ se tiene que $f_k|_{A_k\cap A_j} = f_j|_{A_k\cap A_j}$. En tal caso* $\bigcup_{i\in I} f_i : \bigcup_{i\in I} A_i \longrightarrow D$

Demostración: $\Rightarrow$] Para cada $k, j \in I$ distintos, sea $x \in A_k \cap A_j$, con ello $(x, f_k(x)) \in f_k$ y $(x, f_j(x)) \in f_j$, entonces $(x, f_k(x)), (x, f_j(x)) \in \bigcup_{i\in I} f_i : \bigcup_{i\in I} A_i \longrightarrow D$ y puesto que $\bigcup_{i\in I} f_i$ es una función se tiene que existe un único $d \in D$ tal que $\bigcup_{i\in I} f_i\,(x) = d$, así tenemos que $f_k(x) = d = f_j(x)$ para cada $x \in A_k \cap A_j$, por lo tanto $f_k|_{A_k\cap A_j} = f_j|_{A_k\cap A_j}$ para cada $i, j \in I$ distintos.

$\Leftarrow$] Por contrarrecíproca supongamos que existe $j, k \in I$ distintos tales que $f_k|_{A_k\cap A_j} \neq f_j|_{A_k\cap A_j}$, entonces existe un $x \in A_k \cap A_j$ tal que $f_k(x) = f_k|_{A_k\cap A_j}(x) \neq f_j|_{A_k\cap A_j}(x) = f_j(x)$, pero $(x, f_j(x)) \in \bigcup_{i\in I} f_i$ y $(x, f_k(x)) \in \bigcup_{i\in I} f_i$, por lo tanto $\bigcup_{i\in I} f_i$ no es una función □

Definición 1.9. *Dado un conjunto X, decimos que una relación $\mathcal{R}$, es una relación de equivalencia si se cumplen las siguientes propiedades:*

- *(Reflexividad) Para cualesquiera $a \in X$, se tiene que $a\mathcal{R}a$*
- *(Simetría) Para cualesquiera $a, b \in X$, $a\mathcal{R}b$ si y solo sí $b\mathcal{R}a$*
- *(Transitividad) Para cualesquiera $a, b, c \in X$, si $a\mathcal{R}b$ y $b\mathcal{R}c$ entonces $a\mathcal{R}c$*

Definimos a la clase de equivalencia de a como el conjunto $[a] = \{x \in X \mid x\mathcal{R}a\}$.

Lema 1.10. *Sea $\mathcal{R}$ una relación de equivalencia en X, si $a\mathcal{R}b$ entonces $[a] = [b]$*

Demostración: Sea $x \in [b]$, entonces $x\mathcal{R}b$ y por hipótesis tenemos que $a\mathcal{R}b$, por simetría tenemos que $b\mathcal{R}a$, luego por transitividad tenemos que $x\mathcal{R}a$. Es decir que $x \in [a]$ y así $[b] \subseteq [a]$. Análogamente tenemos que $[a] \subseteq [b]$ y por lo tanto $[a] = [b]$. □

Lema 1.11. *Sea $\mathcal{R}$ una relación de equivalencia en X. Entonces para cualesquiera $a, b \in X$, tenemos que $[a] \cap [b] = \emptyset$ ó bien $[a] = [b]$.*

Demostración: Sean $a, b \in X$ y supongamos que $[a] \cap [b] \neq \emptyset$. Entonces, existe un elemento $x \in [a] \cap [b]$, por definición tenemos que $x\mathcal{R}a$ y $x\mathcal{R}b$. Por la propiedad de simetría tenemos que $a\mathcal{R}x$ y por transitividad tenemos que $a\mathcal{R}b$. Por el *Lema 1.10*, se cumple que $[a] = [b]$. Por lo tanto para cada $a, b \in X$, tenemos que $[a] \cap [b] = \emptyset$ ó $[a] = [b]$. □

Definición 1.12. *Decimos que un conjunto $\{U_i\}_{i\in I} \subseteq \mathcal{P}(X)$ es una partición de X si:*

- $X = \bigcup_{i\in I} U_i$.

- *Para cada $i, j \in I$, si $i \neq j$ entonces $U_i \cap U_j = \emptyset$.*

Teorema 1.13. *Sea R un una relación de equivalencia sobre un conjunto no vacío X, entonces el conjunto $\{[x] \,|\, x \in X\}$ forma una partición de X.*

Demostración: Supongamos que R un una relación de equivalencia sobre un conjunto no vacío X. Denotemos al conjunto de clases de equivalencia como $\{[x_i]\}_{i\in I}$, Por el *Lema 1.11* si $i \neq j$, entonces $[x_i] \cap [x_j] = \emptyset$.

Probemos que $X = \bigcup_{i\in I}[x_i]$. Es claro que para cada $i \in I$, $[x_i] \subseteq X$, entonces $\bigcup_{i\in I}[x_i] \subseteq X$. Ahora sea $x \in X$, entonces por la reflexividad de $\mathcal{R}$, tenemos que $x\mathcal{R}x$ es decir que $x \in [x]$, luego existe $i \in I$ tal que $[x] = [x_i]$. Por lo tanto $X \subseteq \bigcup_{i\in I}[x_i]$. Así concluimos que el conjunto $\{[x] \,|\, x \in X\}$ forma una partición de X. □

Si $\mathcal{R}$ es una relación de equivalencia sobre el conjunto X, denotamos al conjunto de clases de equivalencias como el conjunto $X/\mathcal{R} := \{[x] \,|\, x \in X\}$.

1.2. Lema de Zorn

En esta sección abordaremos uno de los principios mas importantes de la teoría de conjuntos: el *Axioma de elección*. A finales del siglo XIX muchos resultados usaban de manera implícita el axioma de elección, hasta que en el año 1902 fue formulado por Zermelo para probar que todo conjunto está bien ordenado [1]. Para poder comprender dicho axioma veamos la siguiente definición.

Definición 1.14. *Una función $f : \mathcal{P}(X)\backslash\{\emptyset\} \longrightarrow X$, se dice que es una función de elección sí para cada $A \in \mathcal{P}(X)\backslash\{\emptyset\}$ se tiene que $f(A) \in A$.*

A continuación enunciaremos el *Axioma de elección*:

Axioma 10. *(Axioma de elección) Todo conjunto no vacío tiene una función de elección.*

Cabe señalar que nos aseguramos que las pruebas que anteceden a esta sección no ocupan elección.

Nuestro siguiente objetivo es exponer el *lema de Zorn*, junto a su equivalencia con el axioma de elección. Para ello veamos los siguientes conceptos.

Definición 1.15. *Sea $(X, \mathcal{R})$ un conjunto parcialmente ordenado:*

- *Decimos que $\mathcal{C} \subseteq X$ es una cadena si para cualesquiera $a, b \in \mathcal{C}$ se cumple que a y b son comparables; es decir se tiene que $a\mathcal{R}b$ ó bien $b\mathcal{R}a$.*

- *Dados un conjunto $\mathcal{C} \subset X$ y $x \in X$, se define el segmento inicial en $\mathcal{C}$ determinado por x, denotado por $\mathcal{C}_x$, de la siguiente forma:*

$$\mathcal{C}_x = \{y \in \mathcal{C} \,|\, y \leq x,\, x \neq y\}.$$

Decimos que $x < y$, si $x \neq y$ y $y \leq x$,

El *lema de Zorn*, también llamado *lema de Kuratowski-Zorn*, es una proposición importante en teoría de conjuntos que establece:

"Si $(X, \leq)$ es un conjunto no vacío y parcialmente ordenado tal que cada cadena en X tiene una cota superior, entonces X tiene un elemento maximal."

Este resultado fue formulado y demostrado por el matemático polaco Kazimierz Kuratowski en 1922, y de forma independiente por el matemático alemán Max Zorn en 1935, usando el *Principio maximal de Hausdorff*. Dicha proposición tiene una gran variedad de aplicaciones que van desde álgebra abstracta, análisis funcional, topología, entre otras áreas. En este caso, demostraremos la equivalencia del *Axioma de elección* y el *Lema de Zorn* usando otro concepto, a saber el de conjunto conforme. la demostración que se presenta en este trabajo esta basada en el articulo [5].

Definición 1.16. *Un conjunto parcialmente ordenado $(X, \leq)$ cumple la propiedad C^*, si para cada cadena $\mathcal{C} \subseteq X$, existe $x_{\mathcal{C}} \in X \backslash \mathcal{C}$ que es cota superior (estricta) de $\mathcal{C}$.*

Notemos que si $(X, \leq)$ es un conjunto parcialmente ordenado que cumple la propiedad C^*, el *axioma de elección* permite obtener una función f_X tal que para cada cadena $\mathcal{C}$, se cumple $f_X(\mathcal{C}) = x_{\mathcal{C}}$ es cota superior estricta de $\mathcal{C}$. A la función f_X la llamaremos una *C^*-función en X*.

Definición 1.17. *Sean $(X, \leq)$ un conjunto parcialmente ordenado que cumple la propiedad C^* y f una C^*-función en X. Un conjunto $A \subseteq X$ se denomina f-conforme si cumple:*

- *$(A, \leq)$ es bien ordenado (es decir que A es una cadena en la cual cada subconjunto tiene un elemento mínimo)*
- *Para cada $\alpha \in A$, se cumple que $\alpha = f(A_\alpha)$, si $A_\alpha \neq \emptyset$.*

Para ver la existencia de conjuntos f-conformes, tomemos a $x_1 \in X$, entonces no es difícil ver que $\{x_1\}$ es una cadena, luego $f(\{x_1\}) = x_2$ es una cota superior estricta de $\{x_1\}$, con lo cual $A = \{x_1, x_2\}$ forma un conjunto bien ordenado. Veamos que A es un conjunto f-conforme. Puesto que $A_{x_2} = \{x \in A \,|\, x < x_2\} = \{x_1\}$, entonces $f(A_{x_2}) = x_2$, por otro lado $A_{x_1} = \emptyset$ y terminamos. Por lo tanto $\{x_1, x_2\}$ es un conjunto f-conforme

Lema 1.18. *(De comparabilidad)*
Sean X un conjunto que cumple la propiedad C^* y f una C^*-función en X. Si A y B son conjuntos f-conformes en X distintos, entonces uno de los dos conjuntos es un segmento inicial del otro.

Demostración: Supongamos, sin pérdida de generalidad que $A \backslash B \neq \emptyset$. Puesto que A es f-conforme, entonces $A \backslash B$ tiene elemento mínimo, sea $x = \text{mín}\{A \backslash B\}$. Afirmamos que $A_x = B$:

Mostremos que $A_x \subseteq B$. Asumamos que existe $p \in A_x \backslash B$, entonces $p < x$ y $p \in A \backslash B$ lo cual contradice la minimalidad de x.

Ahora, probemos que $B \subseteq A_x$. Para ello, supongamos que $B \backslash A_x \neq \emptyset$. Sea $y = \text{mín}\{B \backslash A_x\}$. Dado que $A \backslash B \neq \emptyset$ y $B_y \subseteq B$, entonces $A \backslash B_y \neq \emptyset$. Consideremos a $z = \text{mín}\{A \backslash B_y\}$.

Probemos que $A_z = B_y$. Sea $w \in A_z$, luego por la minimalidad de z tenemos que que $w \in B_y$ y, en consecuencia $A_z \subseteq B_y$. Ahora sea $u \in B_y$, similarmente obtenemos que $u \in A_x$, en particular $u \in A$. Por definición de z, $z \in A$. Sin embargo, suponiendo que $z \leq u$ entonces $z < y$, lo cual implica que $z \neq y$. Además, puesto que $u \in A_x$, se cumple que $z \in A_x \subseteq B$ y entonces $z \in B$. Así obtenemos que $z \in B_y$, lo cual es una contradicción. Por lo tanto, $u < z$ y así $u \in A_z$. Esto prueba que $B_y \subseteq A_z$. En consecuencia, $A_z = B_y$.

Ya que A, B son f-conformes, entonces $z = f(A_z) = f(B_y) = y$. Dado que $x \notin B$, se cumple que $x \notin B_y$ y, por la minimalidad, de z se tiene que $z \leq x$. Por otro lado, notemos que $z \neq x$, pues si $z = x$ se tiene que $y = x \in B$, lo cual es una contradicción. Esto ultimo implica, dado que $z = y$, que $y < x$, es decir que $y \in A_x$. sin embargo, $y \notin A_x$, lo cual no puede suceder. Por lo tanto $B \subseteq A_x$. □

Proposición 1.19. *Si X es un conjunto que cumple la propiedad C^* y f es una C^*-función en X, entonces la unión de conjuntos f-conformes en X es un conjunto f-conforme en X.*

Demostración: Sea $\mathcal{U} = \bigcup\{A \mid A \text{ es } f \text{ -conforme}\}$. Mostremos que $\mathcal{U}$ es una cadena. Consideremos $x, y \in \mathcal{U}$, entonces existen A, B conjuntos f-conformes tales que $x \in A$ y $y \in B$. Si $A = B$, se tiene que x, y son comparables. En otro caso si $A \neq B$, por el Lema 1.18 podemos suponer que A es un segmento inicial de B, con ello $A \subseteq B$ y así $x, y \in B$. Por consiguiente, x, y son comparables. De aquí que $\mathcal{U}$ es una cadena.

Consideremos $V \subseteq \mathcal{U}$. Dado $v \in V$, existe un conjunto f-conforme A tal que $v \in A$. Puesto que A es f-conforme, $A \cap V$ tiene elemento mínimo. Sea $a = \text{mín}\{A \cap V\}$. Probemos que $\text{mín}\{V\} = a$. Para ello, supongamos que $\text{mín}\{V\} \neq a$, por lo cual existe $c \in V$ tal que $c < a$, Sea C un conjunto f-conforme tal que $c \in C$. Por el Lema 1.18, se cumple que A es un segmento inicial de C ó C es un segmento inicial de A. No se cumple que A es segmento inicial de C pues, de lo contrario, existe $x \in C$ tal que $C_x = A$, lo cual implica que $a \in C_x$. Como $c \leq a$, se tiene que $c \in C_x = A$, lo cual contradice la minimalidad de a. Por otro lado, dado que $a = \text{mín}\{A \cap V\}$, $c \in C$ y $c < a$, se cumple que C no puede ser un segmento inicial de A, lo cual es una contradicción. Por lo tanto, $\text{mín}\{V\} = a$. Hemos probado que $(\mathcal{U}, \leq)$ es un conjunto bien ordenado.

Dado $x \in \mathcal{U}$, existe un conjunto f-conforme C tal que $x \in C$. Veamos que $C_x = \mathcal{U}_x$. Para ello, sea $u \in C_x$. Entonces, $u \in C \subseteq \mathcal{U}$ y $u < x$, así que $u \in \mathcal{U}_x$. Por lo tanto, $C_x \subseteq \mathcal{U}_x$. Por otro lado, supongamos que $\mathcal{U}_x \nsubseteq C_x$. Elijase $v \in \mathcal{U}_x \backslash C_x$ y sea D un conjunto f-conforme tal que $v \in D$. Nuevamente por el Lema 1.18 D es un segmento inicial de C ó C es un segmento inicial de D. No se cumple que D sea un segmento inicial de C pues, de lo contrario existe $d \in D$ tal que $D_d = C$ y ya que $x \in C$. Lo cual implica que $v \in D_d = C$ es decir que $v \in C_x$, una contradicción. Tampoco sucede que C sea un segmento inicial de D pues, en caso contrario existe $c \in C$ tal que $C_c = D$, pero $v \in D = C_c \subseteq C$, lo cual contradice el hecho de que $v \in \mathcal{U}_x \backslash C_x$. Por lo tanto, $\mathcal{U}_x \backslash C_x = \emptyset$. Así concluimos que $\mathcal{U}_x = C_x$.

Finalmente, puesto que C es un conjunto f-conforme, concluimos que $x = f(C_x) = f(\mathcal{U}_x)$. □

Teorema 1.20. *El axioma de elección es equivalente al lema de Zorn*

Demostración: ⇒] Haremos la prueba por contradicción. Supongamos que existe un conjunto parcialmente ordenado $(X, \leq)$ tal que toda cadena no vacía tiene una cota superior, pero X no admite un elemento $\leq$-maximal. Notemos que lo anterior $(X, \leq)$ cumple la propiedad C^*. Entonces por el axioma de elección existe una C^*-función f que asigna a cada cadena una cota superior estricta.

Sea $U = \bigcup\{A \mid A \text{ es un conjunto } f\text{-conforme de } X\}$. Entonces, por la Proposición 1.19, se tiene que U es un conjunto f-conforme. Sea $D = U \cup \{x_U\}$, donde $f(U) = x_U$ es una cota superior estricta de la cadena U. Afirmamos que D es un conjunto f-conforme. Para demostrar esto notemos que se cumplen las siguientes condiciones:

a) D es una cadena. Sean $a, b \in D$ distintos, si $a, b \in U$ terminamos. Ahora si $a \notin U$, entonces $a = x_U$ y puesto que x_U es una cota superior de U, entonces $b \leq x_U = a$, por lo tanto a, b son comparables. Análogamente, si $a \in U$ y $b = x_U$, se prueba que a, b son comparables.

b) D es bien ordenado. Sea $V \subseteq D$ un conjunto no vacío. Puesto que U es conforme, se tiene que cada subconjunto de U tiene elemento mínimo, en particular existe $u = \text{mín}\{V \cap U\}$. Entonces, para cada $v \in V$, si $v \in U$ entonces $u \leq v$. Ahora, si $v \notin U$, entonces $v = x_U$ y como x_U es cota superior de U, obtenemos que $u \leq v$. Por lo tanto, V tiene elemento mínimo.

c) Para cada $d \in D$, $D_d = U_d$. Pues si $u \in U_d$, entonces $u \in U \subseteq D$ y $u \leq d$, entonces $u \in D_d$. Con lo cual $U_d \subseteq D_d$. Por otro lado supongamos que $D_d \nsubseteq U_d$. Sea $v \in D_d \backslash U_d$, por consiguiente $v \in D \backslash U$ y $v \leq d$, así $v = x_U$ y $v \leq d$ pero x_U es una cota superior de U, con ello $d \leq x_U$ y por la antisimetría de $\leq$ obtenemos que $x_U = d$. En consecuencia $d \in D_d$ una contradicción, por lo tanto $D_d = U_d$.

d) Por el inciso *c)*, si $d \in D$, entonces $d = f(U_d) = f(D_d)$. Por lo tanto D es un conjunto f-conforme.

Por los incisos anteriores D es un conjunto f-conforme, por lo que $D \subseteq U$. Entonces $f(U) = x_U \in U$ lo que contradice el hecho de que x_U sea una cota superior estricta de U. Por lo tanto X tiene un elemento maximal.

$\Leftarrow$] Sea X un conjunto no vacío. Definimos al siguiente conjunto:

$$\mathcal{F} = \{f : \mathcal{P}(A) \longrightarrow A \,|\, A \subseteq X \text{ y } f \text{ es una función de elección}\}$$

Notemos que $\mathcal{F} \neq \emptyset$. En efecto, $x \in X$, definimos la siguiente función de elección $f_x : \{\{x\}\} \longrightarrow \{x\}$ tal que $f(\{x\}) = x$. Por otra parte, no es difícil probar que $(\mathcal{F}, \subseteq)$ es un conjunto parcialmente ordenado.

Dada una cadena $\mathcal{C}$ en $\mathcal{F}$, para cada $f \in \mathcal{C}$, existe un conjunto A^f tal que $f : \mathcal{P}(A^f) \longrightarrow A^f$. Afirmamos que $F = \bigcup \mathcal{C} : \bigcup_{f\in\mathcal{C}} \mathcal{P}(A^f) \longrightarrow \bigcup_{f\in\mathcal{C}} A^f$ es una cota superior de $\mathcal{C}$. En efecto, F es una función pues dados $f, g \in \mathcal{C}$ distintos, existen $A^f, A^g \subseteq X$ tal que $f : \mathcal{P}(A^f) \longrightarrow A^f$ y $g : \mathcal{P}(A^g) \longrightarrow A^g$; también tenemos que $f \subseteq g$ ó bien $g \subseteq f$. Sin pérdida de la generalidad supongamos que $f \subseteq g$, luego $Dom(f) \subseteq Dom(g)$ y entonces $(x, f(x)) \in f \subseteq g$, puesto que g es una función y $(x, g(x)) \in g$, se tiene que $g(x) = f(x)$ para cada $x \in Dom(f)$. Esto implica que $f = f|_{Dom(f)} = g|_{Dom(f)}$ y $Dom(f) \subseteq Dom(g)$, por la *proposición 1.8* esto pasa si y solo sí $F = \bigcup \mathcal{C}$ es una función.

Por otro lado, sea $A^* = \bigcup_{f\in\mathcal{C}} A_f$, probemos que $\mathcal{P}(A^*) = \bigcup_{f\in\mathcal{C}} \mathcal{P}(A^f)$. En efecto, elijase $a \in \bigcup_{f\in\mathcal{C}} \mathcal{P}(A^f)$, entonces $a \in \mathcal{P}(A^g)$ para algún $g \in \mathcal{C}$. Esto implica que $a \subseteq A^g \subseteq A^*$, es decir que $a \in \mathcal{P}(A^*)$. Ahora sea $a \in \mathcal{P}(A^*)$, entonces $a \subseteq A^* = \bigcup_{f\in\mathcal{C}} A^f$ y puesto que $\mathcal{C}$ es una cadena, existe $g \in \mathcal{C}$ tal que $a \subseteq A^g$, con lo cual $a \in \mathcal{P}(A^g) \subseteq \mathcal{A}^*$.

Ahora mostremos que F es una función de elección. Para ello sea $a \in \mathcal{P}(A^*)$, entonces $F(a) = f(a)$ para algún $f \in \mathcal{C}$. Por lo tanto $F(a) = f(a) \in a$, es decir que F es una función de elección.

Por el *lema de Zorn* hay un elemento máximal, sea $F^* : \mathcal{P}(Y) \longrightarrow Y$ dicho elemento máximo. Afirmamos que F^* es una función de elección de X. Para ello supongamos que $X \neq Y$, entonces existe $x \in X \backslash Y$. Sea $Z = Y \cup \{x\}$ y $F' : \mathcal{P}(Z) \longrightarrow Z$ una función tal que:

$$F'(A) = \begin{cases} F^*(A) & si \quad A \subseteq Y \\ \\ x & si \quad x \in A \end{cases}$$

Lo cual contradice el hecho de que F^* sea el elemento máximo. Por lo tanto $Y = X$ y se obtiene que F^* es una función de elección para X □

1.3. Teorema del ideal primo

Definición 1.21. *Dado un conjunto X, decimos que f es una operación binaria cerrada o simplemente operación binaria sobre un conjunto X si f es una función tal que:*

$$f : X \times X \longrightarrow X.$$

Análogamente, definimos una operación unitaria cerrada g, o simplemente operación unitaria sobre un conjunto X, como una función:

$$g : X \longrightarrow X.$$

Omitiremos el uso de letras para referirnos a una operación (binaria ó unitaria), en su lugar usaremos símbolos tales como $(+, -, \cdot, *)$. Además escribiremos $*(a, b)$ para referirnos $a * b$. Si la operación es unitaria $*$, escribiremos $*(a)$ para referirnos a a^*.

Antes de establecer la definición de filtro, presentamos algunos resultados de las álgebras booleanas.

Definición 1.22. *Un álgebra booleana es un conjunto* $\mathbf{B}$ *con dos operaciones binarias cerradas* $\cdot, +$ *(producto y suma binarios), una operación unitaria cerrada* $-$ *(llamada complemento) y dos constantes* $\mathbf{1}$ *y* $\mathbf{0}$*, tales que para cualesquiera* $u, v, w \in \mathbf{B}$ *se cumple:*

a) $u + u = u = u \cdot u$

b) $u + v = v + u$ *y* $u \cdot v = v \cdot u$ *(Conmutatividad de la suma y el producto).*

c) $u + (v + w) = (u + v) + w$ *y* $u \cdot (v \cdot w) = (u \cdot v) \cdot w$ *(Asociatividad de la suma y el producto).*

d) $(u + v) \cdot w = (u \cdot w) + (v \cdot w)$ *y* $(u \cdot v) + w = (u + w) \cdot (v + w)$ *(Distribución del producto y la suma).*

e) $u + (u \cdot v) = u = u \cdot (u + v)$ *(Principio de absorción)*

f) $u + u^- = \mathbf{1}$ *y* $u \cdot u^- = \mathbf{0}$ *(Complemento de la suma y el producto)*

g) $(u + v)^- = u^- \cdot v^-$ *y* $(u \cdot v)^- = u^- + v^-$ *(Leyes de Morgan)*

h) $(u^-)^- = u$

i) $u \cdot \mathbf{1} = u$ *y* $u + \mathbf{0} = u$

Ejemplo 1.23. *Si* X *es un conjunto no vacío, sea* $\mathbf{B}_X = \mathcal{P}(X)$*. Si para cualesquiera* $A, B \in \mathbf{B}$ *se definen* $A + B = A \cup B$*,* $A \cdot B = A \cap B$ *y* $A^- = X \backslash A$*, entonces* $\mathbf{B}_X$ *con las operaciones* $+, \cdot, -$ *y con los elementos* $\mathbf{1} = X, \mathbf{0} = \emptyset$ *es un álgebra booleana.*

a) Para cada $A \in \mathbf{B}_X$*,* $A + A = A \cup A = A = A \cap A = A \cdot A$*. Por otro lado para cada* A*,* $B \in \mathbf{B}_X$*,* $A + B = A \cup B = B \cup A = B + A$ *y* $A \cdot B = A \cap B = B \cap A = B \cdot A$*.*

b) Para cada A*,* B*,* $C \in \mathbf{B}_X$*,* $A + (B + C) = A \cup (B \cup C) = (A \cup B) \cup C = (A + B) + C$ *y* $A \cdot (B \cdot C) = A \cap (B \cap C) = (A \cap B) \cap C = (A \cdot B) \cdot C$*.*

c) Para cada A*,* B*,* $C \in \mathbf{B}_X$*,* $(A + B) \cdot C = (A \cup B) \cap C = (A \cap C) \cup (B \cap C) = (A \cdot C) + (B \cdot C)$ *y* $(A \cdot B) + C = (A \cap B) \cup C = (A \cup C) \cap (B \cup C) = (A + C) \cdot (B + C)$*.*

d) Para cada A*,* $B \in \mathbf{B}_X$*,* $A + (A \cdot B) = A \cup (A \cap B) = A = A \cap (A \cup B) = A \cdot (A + B)$*.*

e) Para cada $A \in \mathbf{B}_X$*, se tiene que* $A + A^- = A \cup (X \backslash A) = X = \mathbf{1}$ *y* $A \cdot A^- = A \cap (X \backslash A) = \emptyset = \mathbf{0}$

f) Para cada A*,* $B \in \mathbf{B}_X$*,* $(A + B)^- = X \backslash (A \cup B) = (X \backslash A) \cap (X \backslash B) = A^- \cdot B^-$ *y* $(A \cdot B)^- = X \backslash (A \cap B) = (X \backslash A) \cup (X \backslash B) = A^- + B^-$*.*

g) $(A^-)^- = (X \backslash A)^- = X \backslash (X \backslash A) = A$

h) $A \cdot \mathbf{1} = A \cap X = A$ *y* $A + 0 = A \cup \emptyset = A$

Antes de establecer la noción de filtro, presentaremos algunas propiedades básicas de álgebras booleanas.

Proposición 1.24. *Sean* $\mathbf{B}$ *un álgebra booleana y* $u, u' \in \mathbf{B}$*. Si* $u \cdot u' = \mathbf{0}$ *y* $u + u' = \mathbf{1}$*, entonces* $u^- = u'$*. Además, si existen* $v, w \in \mathbf{B}$ *tales que para cada* $u \in \mathbf{B}$*,* $u \cdot v = u$ *y* $u + w = u$*, entonces* $v = \mathbf{1}$ *y* $\mathbf{0} = w$*.*

Demostración: Sea $u' \in \mathbf{B}$ tal que $u + u' = \mathbf{1}$ y $u \cdot u' = \mathbf{0}$. Notemos que $u^- = \mathbf{1} \cdot u^- = (u + u') \cdot u^- = (u \cdot u^-) + (u' \cdot u^-) = \mathbf{0} + (u' \cdot u^-) = (u' \cdot u^-)$, analogamente se tiene que $(u^- \cdot u') = u'$. Por lo tanto $u^- = u' \cdot u^- = u^- \cdot u' = u'$. Por otro lado $\mathbf{1} = \mathbf{1} \cdot v = v \cdot \mathbf{1} = v$ y de manera similar $\mathbf{0} = w$. □

Definición 1.25. *Para* $u, v \in \mathbf{B}$*, decimos que* $u \leq v$ *si y solo si* $u + v = v$*.*

Nótese que por el inciso *a*) de la *Definición 1.23*, que $u \leq u$ para todo $u \in \mathbf{B}$.

Mas adelante, se presentaran resultados que permitan concluir que $\leq$ es una relación de orden parcial.

Proposición 1.26. *Sean $u, v \in \mathbf{B}$, entonces $u \leq v$ si y solo si $u \cdot v = u$.*

Demostración: Por definición tenemos que $u \leq v$ si y solo sí $u + v = v$. Multiplicando por u en ambos lados de la igualdad, obtenemos que $u \leq v$ si y solo sí $(u + v) \cdot u = v \cdot u$. Ahora, por el *Principio de absorción* se tiene que $u = (u+v) \cdot u$ y, en consecuencia, $u = v \cdot u$. Finalmente, usando la *Conmutatividad del producto* obtenemos que $u = u \cdot v$. □

Proposición 1.27. *Sea $\mathbf{B}$ un álgebra booleana, entonces para cada $u, v, w \in \mathbf{B}$:*

a) $u \cdot v \leq u$ y $u \cdot v \leq v$

b) $u \leq u + v$ y $v \leq u + v$

c) Si $u \leq w$ y $v \leq w$, entonces $u + v \leq w$

d) Si $w \leq u$ y $w \leq v$, entonces $w \leq u \cdot v$

e) Si $v \leq u$ y $w \leq v$, entonces $v \cdot w \leq u \cdot v$

Demostración:

a) Notemos que $(u \cdot v) \cdot u = u \cdot (v \cdot u) = u \cdot (u \cdot v) = (u \cdot u) \cdot v = u \cdot v$, es decir $u \cdot v \leq u$. Análogamente $u \cdot v \leq v$.

b) Puesto que $(u+v)+u = u+(v+u) = u+(u+v) = (u+u)+v = u+v$, es decir $u \leq u+v$. Análogamente $v \leq u+v$.

c) Por hipótesis tenemos que $u \cdot w = u$ y $v \cdot w = v$. Entonces, $(u+v) \cdot w = (u \cdot w)+(v \cdot w) = u+v$.

d) Por hipótesis tenemos que $w \leq u$ y $w \leq v$. Entonces, $(u \cdot v) \cdot w = u \cdot (v \cdot w) = u \cdot w = w$.

e) Por hipótesis tenemos que $v \leq u$ y $b \leq a$. Entonces, $(u \cdot a) \cdot (b \cdot v) = u \cdot (a \cdot b) \cdot v = u \cdot (b \cdot v) = u \cdot (v \cdot b) = (u \cdot v) \cdot b = v \cdot b$. □

Proposición 1.28. *Para cada $u \in \mathbf{B}$, $u \cdot \mathbf{0} = \mathbf{0}$ (es decir que $\mathbf{0} \leq u$).*

Demostración: Puesto que $\mathbf{0} = u \cdot u^-$. Entonces $u \cdot \mathbf{0} = u \cdot (u \cdot u^-)$ por la *Asociatividad del producto* $u \cdot (u \cdot u^-) = (u \cdot u) \cdot u^- = u \cdot u^- = \mathbf{0}$. Por lo tanto para cada $u \in \mathbf{B}$, $u \cdot \mathbf{0} = \mathbf{0}$, es decir $\mathbf{0} \leq u$. □

Proposición 1.29. *Para cada $u \in \mathbf{B}$, $u + \mathbf{1} = \mathbf{1}$ (es decir que $u \leq \mathbf{1}$).*

Demostración: Puesto que $\mathbf{1} = u + u^-$, entonces $u + \mathbf{1} = u + (u + u^-)$ por la *Asociatividad de la suma* $u+(u+u^-) = (u+u)+u^- = u+u^- = u+u^- = \mathbf{1}$. Por lo tanto para cada $u \in \mathbf{B}$, $u \cdot \mathbf{1} = \mathbf{1}$, es decir $u \leq \mathbf{1}$. □

De las proposiciones *1.28* y *1.29*, podemos inferir que $\mathbf{0}$ es un elemento mínimo del conjunto $\mathbf{B}$ y $\mathbf{1}$ es un elemento máximo del conjunto $\mathbf{B}$.

Ahora, la siguiente proposición prueba que la relación $\leq$ es transitiva sobre el conjunto $\mathbf{B}$.

Proposición 1.30. *En un álgebra booleana $\mathbf{B}$ tenemos que $\mathbf{1}^- = \mathbf{0}$ y $\mathbf{0}^- = \mathbf{1}$.*

Demostración: Por el *Complemento del producto* $\mathbf{1} \cdot \mathbf{1}^- = \mathbf{0}$ y por el *Complemento de la suma* $\mathbf{1}+\mathbf{1}^- = \mathbf{1}$. Entonces $\mathbf{1}^- = \mathbf{1}^- \cdot \mathbf{1}^- = \mathbf{0}+(\mathbf{1}^- \cdot \mathbf{1}^-) = (\mathbf{1} \cdot \mathbf{1}^-)+(\mathbf{1}^- \cdot \mathbf{1}^-) = (\mathbf{1}+\mathbf{1}^-) \cdot \mathbf{1}^- = \mathbf{1} \cdot \mathbf{1}^- = \mathbf{0}$.

Por el *Complemento de la suma* es claro que $\mathbf{0}^- = \mathbf{0} + \mathbf{0}^- = \mathbf{1}$. □

Proposición 1.31. *Si $u \leq v$ y $v \leq w$. Entonces $u \leq w$.*

Demostración: Si $u \leq v$ y $v \leq w$, entonces por definición $u + v = v$ y $v + w = w$. Con lo cual $u + w = u + (v + w) = (u + v) + w = v + w = w$ y por lo tanto $u \leq w$. □

Definición 1.32. *Sea* $\mathbf{B}$ *un álgebra booleana. Decimos que* $\mathcal{F} \subseteq \mathbf{B}$ *es un filtro si:*

- $\mathbf{0} \notin \mathcal{F}$*, pero* $\mathbf{1} \in \mathcal{F}$
- *Si* $u \in \mathcal{F}$*,* $v \in \mathbf{B}$ *y* $u \leq v$*, entonces* $v \in \mathcal{F}$*.*
- *Si* u*,* $v \in \mathcal{F}$*, entonces* $u \cdot v \in \mathcal{F}$*.*

Ejemplo 1.33. *Sean* $\mathbf{B}$ *un álgebra booleana y* $u \in \mathbf{B}$ *fijo, con* $u \neq \mathbf{0}$*. Entonces,* $\mathcal{F}_u = \{v \in \mathbf{B} \mid u \leq v\}$ *es un filtro.*
Demostración:

No es difícil mostrar que $\mathbf{1} \in \mathcal{F}_u$*. Pues* $u \leq \mathbf{1}$*. Sabemos que para cada* $v \in \mathbf{B}$*,* $\mathbf{0} \leq v$*, además por hipótesis* $u \neq \mathbf{0}$*. Entonces es imposible que* $u \leq \mathbf{0}$*. por lo tanto* $\mathbf{0} \notin \mathcal{F}_u$*.*

Ahora, sean $v \in \mathcal{F}_u$ *y* $x \in \mathbf{B}$ *tales que* $v \leq x$ *(es decir* $v \cdot x = v$*). Puesto que* $u \leq v$*, se cumple que* $u \cdot v = u$*). Entonces, por Proposición 1.31,* $u \leq x$ *y así* $x \in \mathcal{F}_u$*.*

Por ultimo. Sean $x, y \in \mathcal{F}$*, entonces* $u \leq x$ *y* $u \leq y$ *(es decir* $u \cdot x = u$ *y* $u \cdot y = y$*), lo cual implica que* $u \cdot (x \cdot y) = (u \cdot x) \cdot y = u \cdot y = u$*. Por lo tanto* $x \cdot y \in \mathcal{F}_u$*.* □

Definición 1.34. *Sean* $\mathbf{B}$ *un álgebra booleana y* $\mathcal{A} \subseteq \mathbf{B}$*. Decimos que* $\mathcal{A}$ *tiene la propiedad de intersección finita si para cada familia finita de elementos*

$$\{u_1, \ldots, u_m\} \subseteq \mathcal{A} \text{ se cumple que } u_1 \cdot \ldots \cdot u_m \neq \mathbf{0}.$$

El concepto de propiedad de intersección finita puede consultarla en la pagina 202 en [12]. Sin embargo, en esta tesis modificamos la definición para que funcione de manera general en cualquier álgebra booleana.

Con la siguiente proposición, podemos demostrar la existencia de un filtro sobre un conjunto, solo bastaría encontrar una familia de conjuntos que cumpla la propiedad de intersección finita.

Proposición 1.35. *Sean* $\mathbf{B}$ *un álgebra booleana y* $\mathcal{A} \subseteq \mathbf{B}$ *una familia que cumple la propiedad de intersección finita. Entonces:*

$$\mathcal{F}_{\mathcal{A}} = \{u \in \mathbf{B} \mid (\exists m \in \mathbb{N})(\exists u_1, \ldots, u_m \in \mathcal{A})((u_1 \cdot \ldots \cdot u_m) \leq u)\}$$

es un filtro.

Demostración: Elíjase $u \in \mathcal{A}$*. Entonces, por Proposición 2.29,* $u \leq \mathbf{1}$*, lo cual implica que* $\mathbf{1} \in \mathcal{F}_{\mathcal{A}}$*. Por otro lado, si* $u_1 \cdot \ldots \cdot u_m \in \mathcal{A}$*, entonces* $(u_1 \cdot \cdots \cdot u_n) \neq \mathbf{0}$*. En particular, no ocurre que* $(u_1 \cdot \cdots \cdot u_n) \leq \mathbf{0}$*. En consecuencia,* $\mathbf{0} \notin \mathcal{F}_{\mathcal{A}}$*.*

Ahora, sean $v \in \mathcal{F}_{\mathcal{A}}$ *y* $x \in \mathbf{B}$ *tales que* $v \leq x$ *(es decir,* $v \cdot x = v$*). Puesto que* $v \in \mathcal{F}_{\mathcal{A}}$*, existen* $u_1, \ldots, u_m \in \mathcal{A}$ *tales que* $(u_1 \cdot \ldots \cdot u_m) \leq v$ *y por la Proposición 1.30, tenemos que* $(u_1 \cdot \ldots \cdot u_m) \leq x$*. Por consiguiente,* $x \in \mathcal{F}_{\mathcal{A}}$*.*

Finalmente, sean $x, y \in \mathcal{F}_{\mathcal{A}}$*. Entonces existen* $A = \{a_1, \ldots, a_m\} \subseteq \mathcal{A}$*,* $B = \{b_1, \ldots, b_n\} \subseteq \mathcal{A}$ *tales que* $(a_1 \cdot \ldots \cdot a_m) \leq x$ *y* $(b_1 \cdot \ldots \cdot b_n) \leq y$*. Entonces, por el inciso e) de la* Proposición 1.27*,* $((a_1 \cdot \ldots \cdot a_m) \cdot (b_1 \cdot \ldots \cdot b_n)) \leq (x \cdot y)$*. Por lo tanto* $x \cdot y \in \mathcal{F}_{\mathcal{A}}$ □

Definición 1.36. *Dada un álgebra booleana* $\mathbf{B}$*, diremos que un filtro* $\mathcal{F} \subseteq \mathbf{B}$ *es un filtro maximal si no existe* $\mathcal{F}' \subseteq \mathbf{B}$ *filtro tal que* $\mathcal{F} \subsetneq \mathcal{F}'$*. Por otro lado, diremos que* $\mathcal{F}$ *es un ultrafiltro, si para cada* $u \in \mathbf{B}$ *se tiene que* $u \in \mathcal{F}$ *o bien* $u^- \in \mathcal{F}$*.*

El siguiente resultado establece que estas dos nociones son equivalentes. Más aún, coinciden con una propiedad adicional, determinada por la suma.

Proposición 1.37. *Sean* $\mathbf{B}$ *un álgebra booleana y* $\mathcal{F}$ *un filtro en* $\mathbf{B}$. *Las siguientes condiciones son equivalentes:*

a) $\mathcal{F}$ *es un filtro maximal sobre* $\mathbf{B}$.

b) $\mathcal{F}$ *es un ultrafiltro sobre* $\mathbf{B}$.

c) Si $u+v \in \mathcal{F}$, *entonces* $u \in \mathcal{F}$ *ó* $v \in \mathcal{F}$.

Demostración: Sea $\mathcal{F}$ un filtro sobre $\mathbf{B}$;

a)* $\Rightarrow$ *b) Por contrarrecíproca. Supongamos que $u, u^- \notin \mathcal{F}$, entonces $\mathcal{F} \cup \{u\}$ cumple la propiedad de intersección finita. En efecto, pues suponiendo que $\mathcal{F} \cup \{u\}$ no cumple dicha propiedad, entonces existe $\{v_1, \ldots, v_m\} \subseteq \mathcal{F}$ tal que $v_1 \cdot \ldots \cdot v_m \cdot u = \mathbf{0}$. Por otro lado $u^- = u^- + \mathbf{0} = \mathbf{0} + u^- = (v_1 \cdot \ldots \cdot v_m \cdot u) + u^-$, por la *Distribución del suma sobre la producto* tenemos que $(v_1 \cdot \ldots \cdot v_m \cdot u) + u^- = ((v_1 \cdot \ldots \cdot v_m) + u^-) \cdot (u + u^-)$, pero $u + u^- = \mathbf{1}$ por lo que $((v_1 \cdot \ldots \cdot v_m) + u^-) \cdot (u + u^-) = ((v_1 \cdot \ldots \cdot v_m) + u^-) \cdot \mathbf{1} = (v_1 \cdot \ldots \cdot v_m) + u^-$. Por lo tanto $(v_1 \cdot \ldots \cdot v_m) \leq u^-$ y así $u^- \in \mathcal{F}$, una contradicción. Por lo tanto $\mathcal{F} \cup \{u\}$ cumple la propiedad de intersección finita y por la *Proposición 1.34*, $\mathcal{F} \cup \{u\}$ está contenido en un filtro $\mathcal{G} \neq \mathcal{F}$, entonces $\mathcal{F} \subset \mathcal{G}$. Por lo tanto $\mathcal{F}$ no es un filtro maximal.

b)* $\Rightarrow$ *c) Ahora supongamos que $u+v \in \mathcal{F}$, pero u, $v \notin \mathcal{F}$. Por ***b*** se tiene que $u^-, v^- \in \mathcal{F}$, por ser $\mathcal{F}$ un filtro tenemos que $u^- \cdot v^- \in \mathcal{F}$ y ya que $u+v \in \mathcal{F}$, entonces $\mathbf{0} = \mathbf{0}+\mathbf{0} = (v^- \cdot \mathbf{0}) + (\mathbf{0} \cdot u^-) = (\mathbf{0} \cdot v^-) + ((v \cdot v^-) \cdot u^-) = ((u \cdot u^-) \cdot v^-) + (v \cdot (v^- \cdot u^-)) = (u \cdot (u^- \cdot v^-)) + (v \cdot (u^- \cdot v^-)) = (u+v) \cdot (u^- \cdot v^-) \in \mathcal{F}$. Entonces $\mathcal{F}$ no es un filtro (Pues $\mathbf{0} \notin \mathcal{F}$), lo cual es absurdo. Por lo tanto $u \in \mathcal{F}$ ó $v \in \mathcal{F}$.

c)* $\Rightarrow$ *a) Ahora por contrarrecíproca. Supongamos que $\mathcal{F}$ es un filtro que no es maximal, entonces existe $\mathcal{F}'$ que contiene propiamente a $\mathcal{F}$. Sea $u \in \mathcal{F}'/\mathcal{F}$ y notemos que $u + u^- = \mathbf{1} \in \mathcal{F}$ ahora bastaría notar que $u^- \notin \mathcal{F}$, pues en caso contrario $u^- \in \mathcal{F}'$ y en consecuencia $\mathbf{0} = u \cdot u^- \notin \mathcal{F}'$, una contradicción. Por lo que existe un $u \in \mathbf{B}$ tal que $u, u^- \notin \mathcal{F}$. □

Proposición 1.38. *Sea* $\{u_i, \ldots, u_n\} \subseteq \mathbf{B}$ *tal que* $u_1 + \ldots + u_n = \mathbf{1}$ *y* $u_i \cdot u_j = \mathbf{0}$ *para* $i \neq j$. *Entonces* $u_1^- = u_2 + \ldots + u_n$

Demostración: Sea $w = u_2 + \ldots + u_n$. Puesto que $\mathbf{0}$ es el elemento neutro de la suma, $u_1^- \cdot w = \mathbf{0} + (u_1^- \cdot w)$ y como $u_1^- \cdot u_1 = u_1 \cdot u_1^- = \mathbf{0}$. Usando la *distribución del producto*, se obtiene que $\mathbf{0} + (u_1^- \cdot w) = (u_1^- \cdot u_1) + (u_1^- \cdot w) = u_1^- \cdot (u_1 + w) = u_1^- \cdot \mathbf{1} = u_1^-$. En consecuencia, $u_1^- = u_1^- \cdot w \ldots (1)$.

Puesto que $w \cdot u_1 = (u_2 + \ldots + u_n) \cdot u_1 = (u_2 \cdot u_1) + \ldots + (u_n \cdot u_1) = \mathbf{0}$ y $u_1 + u_1^- = \mathbf{1}$. Entonces $w = w \cdot \mathbf{1} = w \cdot (u_1 + u_1^-) = (w \cdot u_1) + (w \cdot u_1^-) = \mathbf{0} + (w \cdot u_1^-) = (w \cdot u_1^-) \ldots (2)$. De (1) y (2), podemos concluir que $u_1^- = u_2 + \ldots + u_n$. □

Teorema 1.39. *Sea* $\mathbf{B}$ *álgebra booleana y sea* $\mathcal{U}$ *un ultrafiltro de* $\mathbf{B}$. *Si* $\{u_1, \ldots, u_n\} \subseteq \mathbf{B}$ *es un conjunto tal que* $u_1 + \ldots + u_n = u \in \mathcal{U}$ *y* $u_i \cdot u_j = \mathbf{0}$ *para* $i \neq j$, *entonces existe un único* $m \in \{1, \ldots, n\}$ *tal que* $u_m \in \mathcal{U}$.

Demostración: Probemos su existencia. Para ello supongamos que $u_i \notin \mathcal{U}$ para cada $i \in \{1, \ldots, n\}$. Entonces por ser $\mathcal{U}$ un ultrafiltro, $u_i^- \in \mathcal{U}$ para cada $i \in \{1, \ldots, n\}$. Usando *Leyes de Morgan*, se obtiene que $u^- = (u_1 + \ldots + u_n)^- = u_1^- \cdot \ldots \cdot u_n^- \in \mathcal{U}$. Esto implica que $\mathbf{0} = u \cdot u^- \in \mathcal{U}$, una contradicción. Por lo tanto, existe $m \in \{1, \ldots, n\}$ tal que $u_m \in \mathcal{U}$.

Probemos ahora la unicidad. Para ello, supongamos lo contrario. Sean $m_1, m_2 \in \{1, \ldots, n\}$ tales que $u_{m_1}, u_{m_2} \in \mathcal{U}$ entonces, $\mathbf{0} = u_{m_1} \cdot u_{m_2} \in \mathcal{U}$, lo cual es una contradicción. Por lo tanto, existe un único $m \in \{1, \ldots, n\}$ tal que $u_m \in \mathcal{U}$. □

Nota 1.40. *Sabemos que el conjunto potencia de cualquier conjunto* X, *con las operaciones binarias de unión e intersección, es un álgebra booleana. Por el teorema anterior, si* $\mathcal{S} = \{s_1, \ldots, s_n\} \subseteq \mathcal{P}(X)$ *es una partición y* $\mathcal{U}$ *es un ultrafiltro en* X, *existe un único elemento* $s_m \in \mathcal{S}$ *tal que* $s_m \in \mathcal{U}$.

En el año 1930, el matemático polaco-estadounidense *Alfred Tarski* demostró el *lema del ultrafiltro* que establece que *todo filtro está contenido en un ultrafiltro*. A continuación presentaremos una prueba del *lema del ultrafiltro* usando el *lema de Zorn*.

Lema 1.41. *(Del Ultrafiltro)*
Todo filtro $\mathcal{F}$ en $\mathbf{B}$ está contenido en un ultrafiltro.

Demostración:
Sean $\mathcal{F}$ un filtro sobre $\mathbf{B}$ y $\boldsymbol{Z} = \{\mathcal{F}' \mid \mathcal{F} \subseteq \mathcal{F}' \text{ y } \mathcal{F}' \text{ es un filtro}\}$ un conjunto parcialmente ordenado por $\subseteq$. Puesto que $\mathcal{F} \subseteq \mathcal{F}$, entonces $\mathcal{F} \in \boldsymbol{Z}$. Por lo tanto $\boldsymbol{Z}$ es no vacío.

Ahora probemos que toda cadena está acotada superiormente. Para ello, elíjase $\mathcal{K}$ una cadena sobre el conjunto parcialmente ordenado $(\boldsymbol{Z}, \subseteq)$ y definamos al conjunto $\mathcal{F}^* = \bigcup \mathcal{K}$. Probemos que $\mathcal{F}^*$ es un filtro:

- Es claro que $\mathbf{0} \notin \mathcal{F}^*$. Pues de lo contrario, $\mathbf{0} \in \mathcal{F}^*$, entonces existe un filtro $\mathcal{F}' \in \mathcal{K}$ que contiene a $\mathbf{0}$, lo cual es absurdo. Por otro lado $\mathbf{1} \in \mathcal{F}^*$ pues $\mathbf{1} \in \mathcal{F}'$ para cada $\mathcal{F}' \in \mathcal{K}$.
- Ahora, sean $u, v \in \mathcal{F}^*$. Luego, existen $\mathcal{F}_1, \mathcal{F}_2 \in \mathcal{K}$ tales que $u \in \mathcal{F}_1$ y $v \in \mathcal{F}_2$. Puesto que $\mathcal{K}$ es una cadena, $\mathcal{F}_1 \subseteq \mathcal{F}_2$ ó $\mathcal{F}_2 \subseteq \mathcal{F}_1$. Podemos suponer sin pérdida de la generalidad, que $\mathcal{F}_1 \subseteq \mathcal{F}_2$. Entonces $u, v \in \mathcal{F}_2$ y por lo tanto $u \cdot v \in \mathcal{F}_2 \subseteq \mathcal{K}$.
- Ahora, sean $u \in \mathcal{F}^*$ y $v \in \mathbf{B}$ tales que $u \leq v$. Existe $\mathcal{F}' \in \mathcal{K}$ tal que $u \in \mathcal{F}'$, pero $u \leq v$. Por lo tanto, $v \in \mathcal{F}' \subseteq \mathcal{F}^*$

Hemos verificado así, que $\mathcal{F}^*$ es un filtro. Como $\mathcal{F} \subseteq \mathcal{F}'$ para cada $\mathcal{F}' \in \mathcal{K}$, entonces $\mathcal{F} \subseteq \mathcal{F}^* \in \mathbf{Z}$. Aplicando el *Lema de Zorn*, existe un elemento maximal $\overline{\mathcal{F}} \in \boldsymbol{Z}$ que contiene al filtro $\mathcal{F}$. En consecuencia, $\overline{\mathcal{F}}$ es un ultrafiltro. □

Definición 1.42. *Sea X un conjunto. Decimos que una familia de conjuntos $\mathcal{C} \subseteq \mathcal{P}(X)$ tiene carácter finito si cumple:*

- *Para cada $S \in \mathcal{C}$, todo subconjunto finito de S pertenece a $\mathcal{C}$.*
- *Si $A \subseteq X$ y cada subconjunto finito de A pertenece a $\mathcal{C}$, entonces $A \in \mathcal{C}$.*

Lema 1.43. *(De Cowen-Engeler)*
Sean X, Y conjuntos y sea $\xi = \{f : S \longrightarrow Y \mid f$ es una función y $S \subseteq X\}$ tales que:

(a) $\varphi(x) = \{f(x) \mid f \in \xi$ y $x \in Dom(f)\}$ es un subconjunto finito de Y, para cada $x \in X$.

(b) Para cada conjunto finito $S \subseteq X$, $S = Dom(f)$ para algún $f \in \xi$.

(c) ξ tiene carácter finito. Es decir que $f : S \longrightarrow Y$ pertenece a ξ si y solo sí $f|_{S'} : S' \longrightarrow Y$ pertenece a ξ para cada $S' \subseteq S$ finito.

Entonces existe un elemento $F \in \xi$ tal que $Dom(F) = X$

Demostración: Consideremos el conjunto $Fin(X) = \{S \subseteq X \mid S$ es finito$\}$. Para cada $S \in Fin(X)$, sea $\Gamma_S = \{f \in \xi \mid S \subseteq Dom(f)\}$. Por *(b)*, sabemos que Γ_S es no vacío para cada $S \in Fin(X)$.

Probemos que para cualesquiera $S, T \in Fin(X)$, $\Gamma_S \cap \Gamma_T = \Gamma_{S \cup T}$. Para ello, sea $f \in \Gamma_S \cap \Gamma_T$, lo cual implica que $S \subseteq Dom(f)$ y $T \subseteq Dom(f)$. Por tanto, $S \cup T \subseteq Dom(f)$ y así $f \in \Gamma_{S \cup T}$. Análogamente, si $f \in \Gamma_{S \cup T}$, entonces $f \in \Gamma_S \cap \Gamma_T$. Podemos concluir, que $\gamma = \{\Gamma_S \mid S \in Fin(X)\}$ tiene la propiedad de intersección finita, por la *Proposición 1.31*, existe un filtro $\mathcal{F}$ tal que $\gamma \subseteq \mathcal{F}$ y, por el *Lema del ultrafiltro*, existe un ultrafiltro $\mathcal{U}$ que contiene a $\mathcal{F}$.

Por otro lado, notemos que $\varphi(x) = \{f(x) \mid f \in \Gamma_{\{x\}}\}$. Para cada $y \in \varphi(x)$, sea $K_y = \{f \in \Gamma_{\{x\}} \mid f(x) = y\}$. Por la condición (a), el conjunto $\{K_y \mid y \in \varphi(x)\}$ es finito y no es difícil ver que es una partición de $\Gamma_{\{x\}}$.

Por *Teorema 1.37*, para cada $x \in X$ existe un único $y_x \in \varphi(x)$ tal que $K_{y_x} \in \mathcal{U}$. Denotando a y_x como $F(x)$, tenemos que $\{f \in \Gamma_{\{x\}} \mid f(x) = F(x)\} \in \mathcal{U}$.

Veamos que $F \in \xi$. Para ello, sea $S \subseteq X$ finito y definamos el siguiente conjunto:

$$\Psi = \bigcap_{x \in S} \{f \in \Gamma_{\{x\}} \mid f(x) = F(x)\}$$

Por ser $\mathcal{U}$ un filtro y S un conjunto finito, $\Psi \in \mathcal{U}$ y en consecuencia $\Psi \neq \emptyset$. Luego, para cualquier $f \in \Psi$, $f(x) \in \Gamma_{\{x\}}$ para cada $x \in X$. Entonces $f \in \xi$ y S es un subconjunto finito del dominio de f. Puesto que ξ tiene carácter finito y $f|_S \in \xi$ se cumple que $f|_S \in \xi$ para cada subconjunto finito S de X y por el carácter finito de ξ, $F \in \xi$. □

Ahora que hemos establecido la definición de filtro y algunas de sus propiedades, presentamos una noción que es dual a la definición de filtro.

Definición 1.44. *Sea* $\mathbf{B}$ *un álgebra booleana. Decimos que* $\mathcal{I} \subseteq \mathbf{B}$ *es un ideal si:*

- $\mathbf{0} \in \mathcal{I}$*, pero* $\mathbf{1} \notin \mathcal{I}$
- *Si* $u \in \mathcal{I}$*,* $v \in \mathbf{B}$ *y* $v \leq u$*, entonces* $v \in \mathcal{I}$*.*
- *Si* u*,* $v \in \mathcal{I}$*, entonces* $u + v \in \mathcal{I}$*.*

El siguiente resultados justifica por qué la noción de ideal es dual a la noción de filtro.

Proposición 1.45. *Sean* $\mathbf{B}$ *un álgebra booleana y* $\mathcal{F}$ *un filtro sobre* $\mathbf{B}$*. Entonces,*

$$\mathcal{I}_{\mathcal{F}} = \{u \in \mathbf{B} \mid u^- \in \mathcal{F}\}$$

es un ideal.

Demostración:

Es claro que $\mathbf{0} \in \mathcal{I}_{\mathcal{F}}$ y $\mathbf{1} \notin \mathcal{I}_{\mathcal{F}}$, pues $\mathbf{0}^- = \mathbf{1} \in \mathcal{F}$ y $\mathbf{1}^- = \mathbf{0} \notin \mathcal{F}$.

Si u, $v \in \mathcal{I}_{\mathcal{F}}$, entonces u^-, $v^- \in \mathcal{F}$. Por ser $\mathcal{F}$ un filtro tenemos que $(u+v)^- = u^- \cdot v^- \in \mathcal{F}$. Por lo tanto $u + v \in \mathcal{I}_{\mathcal{F}}$.

Sean $u \in \mathcal{I}_{\mathcal{F}}$ y $v \in \mathbf{B}$ tales que $v \leq u$, entonces $u \cdot v = v$. Por las *Leyes de Morgan*, $u^- + v^- = (u \cdot v)^- = v^-$, es decir que $u^- \leq v^-$. Pero $u^- \in \mathcal{F}$ y $v^- \in \mathbf{B}$, entonces $v^- \in \mathcal{F}$, con lo cual $v \in \mathcal{I}_{\mathcal{F}}$.

Por lo tanto $\mathcal{I}_{\mathcal{F}} = \{u \in \mathbf{B} \mid u^- \in \mathcal{F}\}$ es un ideal. □

Análogamente se obtiene la siguiente proposición

Proposición 1.46. *Sean* $\mathbf{B}$ *un álgebra booleana y* $\mathcal{I}$ *un ideal sobre* $\mathbf{B}$*. Entonces,*

$$\mathcal{F}_{\mathcal{I}} = \{u \in \mathbf{B} \mid u^- \in \mathcal{I}\}$$

es un filtro.

Ejemplo 1.47. *Si* $\mathcal{B}$ *es un álgebra boolena, entonces* $\mathcal{I}_0 = \{\mathbf{0}\}$*, es un ideal en* $\mathcal{B}$*. En efecto:*

- *Se tiene que* $\mathbf{0} \in \mathcal{I}_0$ *y* $\mathbf{1} \notin \mathcal{I}_0$*.*
- *Si* $u, v \in \mathcal{I}_0$*, entonces* $u = \mathbf{0} = v$*, por lo tanto* $u + v = \mathbf{0} \in \mathcal{I}_0$*.*
- *Sean* $u \in \mathcal{I}_0$ *y* $v \in \mathbf{B}$*, tales que* $v \leq u$ *(*$u + v = u$*), pero* $u = \mathbf{0}$*, entonces* $v = v + \mathbf{0} = v + u = u + v = u = \mathbf{0} \in \mathcal{I}_0$*. Por lo tanto,* $v \in \mathcal{I}_0$*.*

Definición 1.48. *Dada un álgebra booleana* $\mathbf{B}$*, diremos que un ideal* $\mathcal{I} \subseteq \mathbf{B}$ *es un ideal maximal si no existe* $\mathcal{I}' \subseteq \mathbf{B}$ *filtro tal que* $\mathcal{I} \subsetneq \mathcal{I}'$*. Por otro lado, diremos que* $\mathcal{I}$ *es un ideal primo, si para cada* $u \in \mathbf{B}$ *se tiene que* $u \in \mathcal{I}$ *o bien* $u^- \in \mathcal{I}$*.*

El siguiente resultado establece que estas dos nociones son equivalentes. Más aún, coinciden con una propiedad adicional, determinada por la multiplicación.

Proposición 1.49. *Dado un ideal $\mathcal{I}$, se tiene que las siguientes propiedades son equivalentes:*

a) $\mathcal{I}$ es un ideal maximal.

b) $\mathcal{I}$ es un ideal primo sobre $\mathbf{B}$.

c) Si $u \cdot v \in \mathcal{I}$, entonces $u \in \mathcal{I}$ ó $v \in \mathcal{I}$.

Demostración: Sea $\mathcal{F}$ un ideal sobre $\mathbf{B}$;

a) $\Rightarrow$ b) Por contrarrecíproca. Supongamos que $u, u^- \notin \mathcal{I}$, entonces $u, u^- \notin \mathcal{F}_\mathcal{I}$ esto pasa si y solo sí $\mathcal{F}_\mathcal{I}$ no es un ultrafiltro. Entonces existe un ultrafiltro $\mathcal{U}$ tal que $\mathcal{F}_\mathcal{I} \subseteq \mathcal{U}$. Podemos suponer sin perdida de la generalidad que $u \in \mathcal{U}$, entonces $u^- \in \mathcal{I}_\mathcal{U}$. Además, para cada $v \in \mathcal{I}$, se tiene que $v^- \in \mathcal{U}$, lo cual implica que $v = (v^-)^- \in \mathcal{I}_\mathcal{U}$. Por lo tanto $\mathcal{I} \subsetneq \mathcal{I}_\mathcal{U}$, es decir $\mathcal{I}$ no es un ideal maximal.

b) $\Rightarrow$ c) Ahora supongamos que $u \cdot v \in \mathcal{I}$. Entonces, $u^- + v^- = (u \cdot v)^- \in \mathcal{F}_\mathcal{I}$. Puesto que $\mathcal{I}$ es un ideal primo, para cada $u \in \mathbf{B}$, $u \in \mathcal{I}$ ó $u^- \in \mathcal{I}$ y en consecuencia $u \in \mathcal{F}_\mathcal{I}$ ó $u^- \in \mathcal{F}_\mathcal{I}$, es decir que $\mathcal{F}_\mathcal{I}$ es un ultrafiltro. Por lo tanto como $u^- + v^- \in \mathcal{F}_\mathcal{I}$, entonces $u^- \in \mathcal{F}_\mathcal{I}$ ó $v^- \in \mathcal{F}_\mathcal{I}$ lo cual implica que $u \in \mathcal{I}$ ó $v \in \mathcal{I}$.

c) $\Rightarrow$ a) Por contrarrecíproca. Supongamos que $\mathcal{I}$ es un ideal que no es maximal, entonces existe $\mathcal{I}'$ que contiene propiamente a $\mathcal{I}$, sea $u \in \mathcal{I}'/\mathcal{I}$ y notemos que $u \cdot u^- = \mathbf{0} \in \mathcal{I}$ ahora bastaría notar que $u^- \notin \mathcal{I}$, pues en caso contrario entonces $u^- \in \mathcal{I}'$ y así se tiene que $\mathbf{1} = u + u^- \notin \mathcal{I}'$, una contradicción. Por lo tanto, existe $u \in \mathbf{B}$ tal que $u, u^- \notin \mathcal{I}$, pero $u \cdot u^- \in \mathcal{I}$. □

Proposición 1.50. *Las siguientes propiedades son equivalentes:*

a) El lema del ultrafiltro

b) El teorema del ideal primo: Todo ideal está contenido en un ideal primo.

Demostración:

a) $\Rightarrow$ b) Sea $\mathcal{I}$ un ideal sobre $\mathbf{B}$. Entonces $\mathcal{F}_\mathcal{I}$ es un filtro y, por el lema del ultrafiltro, $\mathcal{F}_\mathcal{I}$ está contenido en un ultrafiltro digamos $\mathcal{U}$. Luego, para cada $u \in \mathcal{I}$, $u^- \in \mathcal{F}_\mathcal{I} \subseteq \mathcal{U}$ y consecuentemente $u = (u^-)^- \in \mathcal{I}_\mathcal{U}$. Por lo tanto, $\mathcal{I} \subseteq \mathcal{I}_\mathcal{U}$. Notemos por otro lado que $\mathcal{I}_\mathcal{U}$ es un ideal primo. Para ello si $u \in \mathbf{B}$, entonces $u \in \mathcal{U}$ ó bien $u^- \in \mathcal{U}$, entonces $u \in \mathcal{I}_\mathcal{U}$ ó $u^- \in \mathcal{I}_\mathcal{U}$. Por lo tanto $\mathcal{I}_\mathcal{U}$ es un ideal primo, con ello $\mathcal{I}$ está contenido en un ideal primo.

b) $\Rightarrow$ a) Es análogo □

Definición 1.51. *Dada un álgebra booleana $\mathbf{B}$, decimos que $\mathbf{A}$ es una subálgebra booleana de $\mathcal{B}$, si $\mathbf{A}$ es cerrada bajo las operaciones $+, \cdot, -$ y además $\mathbf{1}, \mathbf{0} \in \mathbf{A}$.*

Nuestro siguiente objetivo es probar que toda subálgebra booleana finitamente generada es finita.

Proposición 1.52. *Sea $\mathcal{B}$ un álgebra booleana y sea $\mathcal{C} = \{\mathbf{A}_i : i \in I\}$ una familia de subálgebras booleanas de $\mathcal{B}$. Entonces $\bigcap_{i \in I} \mathbf{A}_i$ es una subálgebra booleana de $\mathcal{B}$.*

Demostración: Se cumple que $\mathbf{1}, \mathbf{0} \in \mathbf{A}_i$ para cada $i \in I$, con lo cual $\mathbf{1}, \mathbf{0} \in \bigcap_{i \in I} \mathbf{A}_i$. Por otro lado, para cada $x, y \in \bigcap_{i \in I} \mathbf{A}_i$, $x, y \in \mathbf{A}_i$ para cada $i \in I$, entonces $x^-, x + y, x \cdot y \in \mathbf{A}_i$ para cada $i \in I$. Por lo tanto, $\bigcap_{i \in I} \mathbf{A}_i$ es una subálgebra de $\mathbf{B}$. □

Definición 1.53. *Definimos a la subálgebra generada por el conjunto X como la mínima subálgebra que contiene a X y la denotaremos como $\langle X\rangle$.*

Notemos que $\langle\emptyset\rangle = \{\mathbf{0},\mathbf{1}\}$, pues para cada subálgebra $\mathbf{A}$ de $\mathbf{B}$, se tiene que $\mathbf{0},\mathbf{1} \in \mathbf{A}$ y no es difícil ver que dicho conjunto es una subálgebra booleana.

También no es difícil probar que $\langle X\rangle = \bigcap\{\mathbf{A} \mid X \subseteq \mathbf{A}$ y $\mathbf{A}$ es una subálgebra de $\mathbf{B}\} = \mathbf{X}$. Pues, $\langle X\rangle \in \mathbf{X}$, entonces $\mathbf{X} \subseteq \langle X\rangle$. Por otro lado, por la minimalidad de $\langle X\rangle$, se tiene que $\langle X\rangle \subseteq \mathbf{X}$. Por lo tanto, $\langle X\rangle = \mathbf{X}$.

Nota 1.54. *Sean $\mathbf{B}$ un álgebra booleana y $X \subseteq \mathbf{B}$. Construimos de manera recursiva los siguientes conjuntos: $A^0 = X \cup \{\mathbf{0},\mathbf{1}\}$, y para cada $n > 0$ sean $A^n = \{x \cdot y \mid x, y \in A_{n-1}\} \cup \{x + y \mid x, y \in A_{n-1}\} \cup \{x^- \mid x \in A_{n-1}\}$. Definimos a $\overline{X} = \bigcup_{n\in\mathbb{N}} A_n$. Entonces:*

- $\mathbf{0},\mathbf{1} \in \overline{X}$ *y* $X \subset \overline{X}$.
- *Para cada $x, y \in \overline{X}$, entonces existen $p, q \in \mathbb{N}$ tales que $x \in A^p$, $y \in A^q$. Sin perdida de la generalidad podemos suponer que $p \leq q$, luego $x, y \in A^q$ con lo cual $x+y$, $x \cdot y$, $x^- \in A^{p+1} \subset \overline{X}$.*

Es decir, $\overline{X}$ es una subálgebra booleana que contiene a X y, dado que $\langle X\rangle$ es la mínima con esa propiedad, se obtiene que $\langle X\rangle \subseteq \overline{X}$.

Veremos por inducción que $A_n \subset \langle X\rangle$ para cada $n \in \mathbb{N}$. En efecto, es claro que $A_0 \subseteq \langle X\rangle$. Supongamos que para $k \in \mathbb{N}$, $A_k \subset \langle X\rangle$ y demostremos que $A_{k+1} \in \langle X\rangle$. Dado que $A_{k+1} = \{x \cdot y \mid x, y \in A_k\} \cup \{x \cdot y \mid x, y \in A_k\} \cup \{x^- \mid x \in A_k\}$, luego por hipótesis inductiva sabemos que $A_k \subseteq \langle X\rangle$ por ende al ser $\langle X\rangle$ una subálgebra, entonces para para cada $x, y \in A_k$ tenemos que $x \cdot y$, $x + y, x^- \in \langle X\rangle$ con lo cual $A_{k+1} \subset \langle X\rangle$. Por lo tanto, $\overline{X} = \langle X\rangle$. Así obtenemos que cada elemento de $\langle X\rangle$ puede escribirse como sumas finitas con productos finitos de elementos y complementos de X.

Lema 1.55. *Para un álgebra booleana $\mathbf{B}$, si $\mathbf{B}'$ es una subálgebra booleana y $r \in \mathbf{B}$. Entonces la subálgebra generada por el conjunto $\mathbf{B}' \cup \{r\}$ consiste de los elementos de $\mathbf{B}$ que se escriben de la forma:*

$$(p \cdot r) + (q \cdot r^-)$$

donde $p, q \in \mathbf{B}'$.

Demostración: Sea $\mathbf{C} = \langle \mathbf{B}' \cup \{r\}\rangle$, sabemos por la nota anterior que $\mathbf{C}$ puede escribirse como sumas finitas con productos finitos de elementos y complementos de $\mathbf{B}'$. Sea $\mathbf{C}' = \{(p \cdot r) + (q \cdot r^-) \mid p, q \in \mathbf{B}'\}$. Entonces $r = (\mathbf{1} \cdot r) + (\mathbf{0} \cdot r^-) \in \mathbf{C}'$, y para cada $p \in \mathbf{B}'$, por *Principio de absorción*, se tiene que $p = p \cdot (p + r^-) = ((p \cdot r) + p) \cdot ((p + r^-) \cdot \mathbf{1}) = ((p \cdot r) + p) \cdot ((p + r^-) \cdot (r + r^-)) = ((p \cdot r) + p) \cdot ((p \cdot r) + r^-) = (p \cdot r) + (p \cdot r^-) \in \mathbf{C}'$, es decir que $\mathbf{B}' \cup \{r\} \subseteq \mathbf{C}'$, por otro lado para cada $(p_1 \cdot r) + (q_1 \cdot r^-)$, $(p_2 \cdot r) + (q_2 \cdot r^-) \in \mathbf{C}'$:

- $((p_1 \cdot r) + (q_1 \cdot r^-)) + ((p_2 \cdot r) + (q_2 \cdot r^-)) = ((p_1 \cdot r) + (p_2 \cdot r)) + ((q_1 \cdot r^-) + (q_2 \cdot r^-)) = ((p_1 + p_2) \cdot r) + ((q_1 + q_2) \cdot r^-) \in \mathbf{C}'$.
- $((p_1 \cdot r) + (q_1 \cdot r^-)) \cdot ((p_2 \cdot r) + (q_2 \cdot r^-)) = ((p_1 \cdot r) + (q_1 \cdot r^-)) \cdot (p_2 \cdot r) + ((p_1 \cdot r) + (q_1 \cdot r^-)) \cdot (q_2 \cdot r^-) = ((p_1 \cdot r) \cdot (p_2 \cdot r)) + ((q_1 \cdot r^-) \cdot (p_2 \cdot r)) + ((p_1 \cdot r) \cdot (q_2 \cdot r^-)) + ((q_1 \cdot r^-) \cdot (q_2 \cdot r^-)) = ((p_1 \cdot p_2) \cdot r) + ((q_1 \cdot q_2) \cdot r^-) \in \mathbf{C}'$.
- Ya que $((p_1 \cdot r) + (q_1 \cdot r^-)) \cdot ((p_1^- \cdot r) + (q_1^- \cdot r^-)) = ((p_1 \cdot p_1^-) \cdot r) + ((q_1 \cdot q_1^-) \cdot r^-) = \mathbf{0}$ y $((p_1 \cdot r) + (q_1 \cdot r^-)) + ((p_1^- \cdot r) + (q_1^- \cdot r^-)) = ((p_1 + p_1^-) \cdot r) + ((q_1 + q_1^-) \cdot r^-) = r + r^- = \mathbf{1}$, entonces por la unicidad del inverso tenemos que $((p_1 \cdot r) + (q_1 \cdot r^-))^- = (p_1^- \cdot r) + (q_1^- \cdot r^-) \in \mathbf{C}'$.

Es decir que $\mathbf{C}'$ es una subálgebra booleana que contiene a $\langle \mathbf{B}' \cup \{r\}\rangle$ y puesto que $\mathbf{C}$ es la mínima con esa propiedad, entonces $\mathbf{C} \subseteq \mathbf{C}'$. No es difícil ver que $\mathbf{C}' \subseteq \mathbf{B}' \cup \{r\}$ y por consiguiente $\mathbf{C}' = \mathbf{C}$. □

Corolario 1.56. *Toda subálgebra booleana finitamente generada es finita.*

Demostración: Sean $\mathbf{B}$ un álgebra booleana y un conjunto $X \subseteq \mathbf{B}$ finito. Probaremos por inducción sobre $n = |X|$ que $|\langle X\rangle| \leq 2^{2^n}$:

- Para $n = 0$, entonces $X = \emptyset$ con lo cuál $|\langle X\rangle| = |\{\mathbf{0}, \mathbf{1}\}| = 2 = 2^{2^0}$.
- Para cada $k \in \mathbb{N}$, por hipótesis inductiva supongamos que $|\langle X\rangle| \leq 2^{2^k}$. Para $|X| = k + 1$, elíjase $x \in X$. Por hipótesis inductiva, si $X' = X\backslash\{x\}$, entonces $|\langle X'\rangle| \leq 2^{2^n}$, y por el *Lema 1.58*, se tiene que $\langle X\rangle = \{(p \cdot r) + (q \cdot r^-) \,|\, p, q \in \langle X'\rangle\}$ y así $|\langle X\rangle| = |\{(p \cdot r) + (q \cdot r^-) \,|\, p, q \in \langle X'\rangle\}| \leq |\{p \cdot r \,|\, p \in \langle X'\rangle\}| + \{q \cdot r^- \,|\, q \in \langle X'\rangle\}| \leq |\{p \cdot r \,|\, p \in \langle X'\rangle\}|\,|\{q \cdot r^- \,|\, p, q \in \langle X'\rangle\}| \leq 2^{2^k} \cdot 2^{2^k} = 2^{2^k+2^k} = 2^{2(2^k)} = 2^{2^{k+1}}$

Por lo tanto toda subálgebra finitamente generada es finita. □

Capítulo 2

Campos algebraicamente cerrados sin elección

En el capitulo anterior mostramos una prueba de la equivalencia del *lema del ultrafiltro* con *teorema del ideal primo* en álgebras booleanas. También probamos el *lema de Cowen-Engeler* el cual usaremos para demostrar que todo campo está contenido en un campo algebraicamente cerrado. El libro *Álgebra* de *Serge Lang*, presenta una prueba de que todo campo K está contenido en un campo algebraicamente cerrado (llamado clausura algebraica del campo K) usando el *teorema de Krull* que establece:

"Todo ideal propio I de un anillo conmutativo R, está contenido en un ideal máximo de R"

Resulta que tal resultado es equivalente al *Axioma de elección*. Para evitar el *Axioma de elección* emplearemos el *lema de Cowen-Engerlen*, para probar que todo ideal propio está contenido en un ideal primo y probaremos que ambos resultados son equivalentes al *lema del ultrafiltro*. Lo cual nos garantizara la existencia de la clausura algebraica del campo K.

De manera similar usando el *lema de Zorn*, se prueba la unicidad de la clausura algebraica del campo K, en este caso optaremos por el *teorema de tychonoff para espacios Hausdorff*. Basta mencionar que el *teorema de Tychonoff* es equivalente al *Axioma de elección* obteniendo el mismo problema, pero al restringir el *teorema de Tychonoff* a espacios Hausdorff obtenemos una propiedad mas débil que elección.

2.1. Algunas definiciones básicas

Nuestro siguiente objetivo es comprender que es un campo y que significa que sea algebraicamente cerrado. Para ello analicemos que son los grupos, los anillos, los polinomios y los ideales junto con algunos resultados relacionados.

Definición 2.1. *Sean S un conjunto distinto del vacío y $*$ operación binaria sobre S. Decimos que $(S, *)$ es un semigrupo si:*

- *La operación $*$ es asociativa sobre S, es decir, que para cualesquiera a, b, $c \in S$, $a * (b * c) = (a * b) * c$.*

Definición 2.2. *Sea $(S, *)$ un semigrupo y $T \subseteq S$. Decimos que $(T, *|_T)$ es un subsemigrupo de $(S, *)$, si $(T, *|_T)$ es un semigrupo. En adelante, si $(T, *|_T)$ es un subsemigrupo escribiremos simplemente $(T, *)$.*

Ejemplo 2.3. *Notemos que un álgebra booleana* **B** *con cualquiera de las dos operaciones $+$, $\cdot$ (ver Definición 1.22) es un semigrupo.*

Definición 2.4. *Sean M un conjunto distinto del vacío y $*$ una operación binaria. Decimos que $(M,*)$ es un monoide si:*

- *$(M,*)$ es un semigrupo.*
- *Existe un elemento $e \in M$ tal que para cada $u \in M$, $u * e = u = e * u$.*

Ejemplo 2.5. *Para cualquier conjunto X, denotamos a S_X como el conjunto de todas las funciones biyectivas sobre el conjunto X. Entonces S_X con la composición como operación forma un monoide cuyo elemento neutro es la función identidad en X.*

Proposición 2.6. *Si $(M,*)$ un monoide, entonces existe un único elemento $e \in M$ tal que para cada $u \in M$, $u * e = u = e * u$.*

Demostración: Sean $e, e' \in M$ tal que para cada $u \in M$, $u * e = u = e * u$ y $u * e' = u = e' * u$, en particular $e * e' = e = e' * e$ y $e * e' = e' = e' * e$, por lo tanto $e = e'$, así concluimos que existe un único elemento $e \in M$ tal que para cada $u \in M$, $u * e = u = e * u$, a dicho elemento lo llamaremos elemento neutro de M □

Proposición 2.7. *Dado un conjunto de índices I. Si $(S_i, *_i)$ es un monoide para cada $i \in I$, entonces $\prod_{i\in I} S_i = S$ es un monoide con la operación $*$. Donde para cada $(a_i)_{i\in I}, (b_i)_{i\in I} \in S$, se tiene que $(a_i) * (b_i) = (a_i *_i b_i)$*

Demostración:

La operación $*$ está bien definida, pues cada $*_i$ es una operación binaria, y con ello para cada $(a_i), (b_i) \in S$, entonces $a_i *_i b_i \in S_i$ y así $(a_i *_i b_i) \in S$.

Sean $(a_i), (b_i), (c_i) \in S$, entonces $((a_i) * (b_i)) * (c_i) = (a_i *_i b_i) * (c_i) = a_i *_i (b_i *_i c_i) = (a_i) * (b_i *_i c_i) = (a_i) * ((b_i) * (c_i))$.

Finalmente, definimos $e \in S$ como $e = (e_i)$, donde e_i es el elemento neutro de S_i. Entonces para cada $(a_i) \in S$ se tiene que $(a_i) * e = (a_i *_i e_i) = (a_i) = (e_i *_i a_i) = e * (a_i)$, Por lo tanto S es un monoide. □

Definición 2.8. *Sean G un conjunto distinto del vacío y $*$ operación binaria. Decimos que $(G,*)$ es un grupo si:*

- *$(G,*)$ es un monoide.*
- *Para cada $g \in G$, existe un elemento $g' \in G$ tal que $g * g' = e = g' * g$.*

Ejemplo 2.9. *Sean X un conjunto y $\mathbb{Z}_p$ con p primo un grupo. Si consideramos a:*

$$\mathbb{Z}_p^X = \{f : X \longrightarrow \mathbb{Z}_p\},$$

$\mathbb{Z}_p^X$ es un grupo con la siguiente operación: Dados $f, g \in \mathbb{Z}_p^X$ y $z \in X$, $(f * g)(z) = [f(z)][g(z)]$.

Proposición 2.10. *Si $(G,*)$ un grupo, entonces para cada $g \in G$ existe un único elemento $g' \in G$ tal que $g * g' = e = g' * g$.*

Demostración: Sean $g', g'' \in M$ tal que para $g \in G$, $g * g' = e = g' * g$ y $g * g'' = e = g'' * g$, entonces $g'' = g'' * e = g'' * (g * g') = (g'' * g) * g' = e * g' = g'$, por lo tanto $g' = g''$, así concluimos que existe un único elemento $g' \in M$ tal que $g' * g = e = g * g'$, a dicho elemento lo llamaremos elemento inverso de g, y lo denotaremos como g^{-1}. □

Proposición 2.11. *Si $(G,*)$ un grupo, entonces para cada $a, b \in G$ tenemos que $(a * b)^{-1} = (b)^{-1} * (a)^{-1}$ y $(a^{-1})^{-1} = a$.*

Demostración: Ya que $(a*b)*(a*b)^{-1} = e$ y $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*a^{-1} = e$, entonces $(a*b)*(a*b)^{-1} = (a*b)*(b^{-1}*a^{-1})$, luego $(a*b)^{-1} = (a*b)^{-1}*((a*b)*(b^{-1}*a^{-1})) = ((a*b)^{-1}*(a*b))*(b^{-1}*a^{-1}) = b^{-1}*a^{-1}$.

Por la proposición anterior se sabe que el elemento inverso de a^{-1} es único, pero a es el inverso de a^{-1} lo cual implica que $(a^{-1})^{-1} = a$ □

Definición 2.12. *Decimos que un grupo G es abeliano si:*

- *Para cada $x, y \in G$, $x*y = y*x$*

Sea $(G', *)$ es un grupo. Si $(G', *)$ es un subsemigrupo de $(G, *)$ tal que $(G', *)$ es un grupo entonces $(G', *)$ es un subgrupo de $(G, *)$, lo cual lo denotaremos por $G' \leq G$.

Proposición 2.13. *Sean G un grupo y J un conjunto de índices. Si $H_j \leq G$ para cada $j \in J$, entonces $H = \bigcap_{j\in J} H_j \leq G$*

Demostración:

Afirmamos que H es un monoide. En efecto, si e es el elemento neutro de G, entonces $e \in H_j$ para cada $j \in J$, luego $e \in H$. Por lo tanto H es distinto del vacío. Sean $a, b, c \in H \subseteq G$, así $a*(b*c) = (a*b)*c$. Por lo tanto $(H, *)$ es un monoide.

Sea $h \in H$, por lo que para cada $i \in J$ se tiene que $h \in H_i$ y como cada H_i es un grupo, existe $h' \in H_i$ tal que $h*h' = e = h'*h$. Por lo tanto $H \leq G$. □

En la proposición anterior, si $(G, *)$ es abeliano, entonces para cada $x, y \in H$ se tiene que $x*y = y*x$. Por lo tanto H es también un grupo abeliano.

Definición 2.14. *Dado un grupo $(G, *)$ y $H \leq G$. Dado un elemento $g \in G$ definimos la clase lateral izquierda (derecha) de g en H como el conjunto $gH = \{g*h \mid h \in H\}$ ($Hg = \{h*g \mid h \in H\}$).*

Proposición 2.15. *Para $H \leq G$ y para cada $g, g_0 \in G$, $gH = g_0H$ si y solo sí $g_0^{-1}*g \in H$*

Demostración: $\Rightarrow$] Como $e \in H$, tenemos que $g = g*e \in gH = g_0H$, entonces existe $h \in H$ tal que $g = g_0*h$, luego $g_0^{-1}*g = g_0^{-1}*g_0*h = h$. Por lo tanto $g_0^{-1}*g = h \in H$.

$\Leftarrow$] Si $g_0^{-1}*g \in H$, luego existe $h \in H$ tal que $g_0^{-1}*g = h$, por lo que $g = g_0*h \in g_0H$, lo cual implica que para cada $h' \in H$ tenemos que $g*h' = (g_0*h)*h' = g_0*(h*h') \in g_0H$. Así $gH \subseteq g_0H$ y análogamente obtenemos que $g_0H \subseteq gH$. Por lo tanto $gH = g_0H$. □

De manera similar para cada $g, g_0 \in G$, tenemos que $Hg = Hg_0$ si y solo sí $g*g_0^{-1} \in H$. Definimos la relación $\sim$ sobre G como sigue:

$$g \sim g_0 \text{ si y solo sí } g_0^{-1}*g \in H$$

Proposición 2.16. *La relación $\sim$ es de equivalencia.*

Demostración: Para cada $a \in G$, $a^{-1}*a = e \in H$, es decir que $a \sim a$. Por lo tanto $\sim$ es reflexiva.

Sean $a, b \in G$ tales que $a \sim b$, luego $a^{-1}*b \in H$, como $H \leq G$, se tiene que $b^{-1}*a = (a^{-1}*b)^{-1} \in H$. Por lo tanto $\sim$ es simétrica.

Ahora sean $a, b, c \in G$ tal que $a \sim b$ y $b \sim c$, por definición $b^{-1}*a \in H$ y $c^{-1}*b \in H$, luego $c^{-1}*a = (c^{-1}*b)*(b^{-1}*a) \in H$. Por lo tanto $\sim$ es transitiva. □

Con lo anterior podemos definir al siguiente conjunto $G/H = \{gH \mid g \in G\}$ que denota el conjunto de clases de equivalencia de G bajo la relación $\sim$, lo cual por el *Teorema 1.13*, sabemos que $\sim$ induce una partición en el conjunto G.

Definición 2.17. *Decimos que un subgrupo H de G es normal, si para cada $g \in G$ tenemos que $gH = Hg$. Para cada $a, b \in G$ definimos el siguiente conjunto $aH \cdot bH = \{x*y \mid x \in aH \text{ y } y \in bH\}$.*

Proposición 2.18. *Sea $(H,*)$ un subgrupo normal de $(G,*)$. Entonces $(G/H,\cdot)$ es un grupo.*

Demostración: Sean $aH, bH \in G/H$, mostremos que $aH \cdot bH = (a*b)H$. Sea $c \in aH \cdot bH$, luego existen $h, h_1 \in H$ tales que $c = (a*h_1)*(b*h)$. Puesto que H un subgrupo normal de G, entonces $h_1 * b \in Hb = bH$, con lo cual existe $h_2 \in H$ tal que $h_1 * b = b * h_2$, entonces $c = (a*h_1)*(b*h) = a*(h_1*b)*h = a*(b*h_2)*h = (a*b)*(h_2*h)$ y en consecuencia $c \in (a*b)H$. Por otro lado sea $d \in (a*b)H$, luego elíjase $h \in H$ tal $d = (a*b)*h$. Como $e \in H$, entonces $(a*b)*h = (a*e)*(b*h) \in aH \cdot bH$. Por tanto $(a*b)H = aH \cdot bH$.

Sean $a, a', b, b' \in H$ tales que $aH = a'H$ y $bH = b'H$, demostremos que $(a*b)H = (a'*b')H$. Para ello sea $c \in (a*b)H$, entonces existe $h \in H$ tal que $c = (a*b)*h$. Puesto que $a \in aH = a'H$ y $b \in bH = b'H$, luego existen $h', h_1 \in H$ tales que $a = a'*h_1$ y $b = b'*h'$, con lo cual $a*b = (a'*h')*(b'*h') = a'*(h_1*b')*h'$...(1). Nuevamente por la normalidad de H, existe $h_2 \in H$ tal que $h_1 * b' = b' * h_2$ y por (1), $a*b = a'*(b'*h_2)*h' = (a'*b')*(h_2*h') \in (a'*b')H$. Por lo que $(a*b)*h \in (a'*b')H$, es decir que $(a*b)H \subseteq (a'*b')H$. Análogamente, $(a'*b')H \subseteq (a*b)H$, de lo anterior se obtiene que $(a*b)H = (a'*b')H$. Por lo tanto $\cdot$ es una operación binaria en G/H.

Ya que $*$ es una operación asociativa. entonces para cada $a, b, c \in G$ se tiene que $(aH \cdot bH) \cdot cH = (a*b)H \cdot cH = ((a*b)*c)H = (a*(b*c))H = aH \cdot (b*c)H = aH \cdot (bH \cdot cH)$. Por tanto la operación $\cdot$ es asociativa.

Ahora proponemos a $eH = H$ como el elemento neutro en $(G/H,\cdot)$, pues para cada $aH \in G/H$ se tiene que $aH \cdot H = (a \cdot e)H = aH$.

Puesto que $(G,*)$ es un grupo, para cada $a \in G$, existe un elemento $a^{-1} \in G$ que es inverso de a. Luego $aH \cdot a^{-1}H = (a * a^{-1})H = eH = H$. Por lo tanto $(G/H,\cdot)$ es un grupo. □

En la proposición anterior, si $(G,*)$ es abeliano, entonces para cada $aH, bH \in G/H$, $aH \cdot bH = (a*b)H = (b*a)H = bH \cdot aH$. Por lo tanto $(G/H,\cdot)$ es abeliano.

Definición 2.19. *Sean R un conjunto y $+, \cdot$ dos operaciones binarias que se les llamara adición y multiplicación respectivamente, decimos que $(R,+,\cdot)$ es un anillo si:*

- *$(R,+)$ es un grupo abeliano, con 0_R como elemento neutro.*
- *$(R,\cdot)$ es un semigrupo.*
- *La multiplicación es distributiva con respecto de la suma, es decir:*
  - *Para cualesquiera a, b, $c \in R$, $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$*
  - *Para cualesquiera a, b, $c \in R$, $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$*

Decimos que un anillo $(R,+,\cdot)$ es un anillo con uno si $(R,+,\cdot)$ es un anillo y $(R,\cdot)$ es un monoide donde 1_R es el elemento neutro.

Decimos que un elemento $r \in R$ es unidad si existe $r' \in R$, tal que $r \cdot r' = r' \cdot r = 1_R$. De manera similar a la *Proposición 2.10*, podemos probar que el inverso multiplicativo para cada unidad en el anillo R es único.

En la definición anterior, si $(R,+,\cdot)$ es un anillo con uno, entonces a los elementos 0_R y 1_R los llamaremos elemento neutro de la adición y elemento neutro de la multiplicación respectivamente.

Decimos que $(R',+,\cdot)$ es un subanillo de $(R,+,\cdot)$, si $R' \subseteq R$ y $(R',+,\cdot)$ es un anillo.

Proposición 2.20. *En un anillo $(R,+,\cdot)$, para cada $a \in R$, $a \cdot 0_R = 0_R$.*

Demostración: Notemos que $0_R + 0_R = 0_R$, entonces $a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R$, luego $0_R = a \cdot 0_R - a \cdot 0_R = (a \cdot 0_R + a \cdot 0_R) - a \cdot 0_R = a \cdot 0_R + (a \cdot 0_R - a \cdot 0_R) = a \cdot 0_R$. □

Definición 2.21. *Sean $(R,+,\cdot)$ un anillo y $(S,*)$ un semigrupo, definimos al conjunto*

$$R[S] = \{f : S \longrightarrow R \,|\, f(s) \neq 0_R \text{ para un subconjunto finito de } S\}.$$

Con las siguientes operaciones sobre el conjunto $R[S]$:

I) $(f+g)(s) = f(s) + g(s)$.

II) $(f \cdot g)(s) = \sum_{j*i=s} f(j) \cdot g(i)$.

Definición 2.22. *Si f es un elemento de $R[S]$, denotaremos*

$$sop(f) = \{x \in S \mid f(x) \neq 0_R\}.$$

Proposición 2.23. *$(R[S], +, \cdot)$ es un anillo.*

Demostración: Veamos que $+, \cdot$ son operaciones binarias. Sean $f, g \in R[S]$, entonces $sop(f)$ y $sop(g)$ son finitos, demostremos que $sop(f) \cup sop(g)$ es finito.

Para ello, supongamos que $sop(f+g) \nsubseteq sop(f) \cup sop(g)$. $+$ $s \in sop(f+g) \backslash (sop(f) \cup sop(g))$, entonces $(f+g)(s) \neq 0_R$, pero $f(s) = 0_R$ y $g(s) = 0_R$, lo cual implica que $(f+g)(s) = 0_R$ una contradicción. En consecuencia $sop(f+g) \subseteq sop(f) \cup sop(g)$.

Por otro lado sea $s \in sop(f \cdot g)$, entonces $(f \cdot g)(s) = \sum_{j*i=s} f(j) \cdot g(i) \neq 0_R$, luego existen $i \in sop(g)$ y $j \in sop(g)$ tales que $j * i = s$. Como $sop(f)$ y $sop(g)$ son finitos, lo cual implica que el conjunto de elementos de la forma $f(j) \cdot g(i) \neq 0_R$ es finito. Por consiguiente $f \cdot g$ es finito.

Sean $f, g, h \in R[S]$, entonces $(f + (g+h))(s) = f(s) + (g+h)(s) = f(s) + (g(s) + h(s)) = (f(s) + g(s)) + h(s) = ((f+g)(s)) + h(s) = ((f+g)+h)(s)$ y $(f \cdot (g \cdot h))(s) = \sum_{i*j=s} f(i) \cdot (g \cdot h)(j) = \sum_{i*j=s} f(i) \cdot (\sum_{k*l=j} g(k) \cdot h(l)) = \sum_{i*(k*l)=s} f(i) \cdot (g(k) \cdot h(l))$, análogamente obtenemos que $((f \cdot g) \cdot h)(s) = \sum_{i*(k*l)=s} (f(i) \cdot g(k)) \cdot h(l)$ por la asociatividad de $\cdot$ obtenemos que $((f \cdot g) \cdot h)(s) = (f \cdot (g \cdot h))(s)$.

Notemos que $f, g \in R[S]$, se tiene que $(f+g)(s) = f(s) + g(s) = g(s) + f(s) = (g+f)(s)$. En particular si $\cdot$ es conmutativa se obtiene que $(f \cdot g)(s) = \sum_{i*j=s} f(i) \cdot g(j) = \sum_{i*j=s} g(j) \cdot f(i) = (g \cdot f)(s)$.

Proponemos a $\overline{0} \in R[S]$ tal que $\overline{0}(s) = 0_R$ para cada $s \in S$ como el elemento neutro con respecto a la operación $+$. Pues $(f + \overline{0})(s) = f(s) + \overline{0}(s) = f(s) = \overline{0}(s) + f(s) = (\overline{0} + f)(s)$.

Para cada $f \in R[S]$, definimos a $f^- : S \longrightarrow R$ tal que $f^-(s) = -f(s)$ (el inverso aditivo de $f(s) \in R$). Luego $(f + f^-)(s) = f(s) + f^-(s) = f(s) - f(s) = \overline{0}(s) = (f^- + f)(s)$.

Veamos que $\cdot$ se distribuye sobre $+$. En efecto, pues $(f \cdot (g+h))(s) = \sum_{i*j=s} f(i) \cdot (g+h)(j) = \sum_{i*j=s} f(i) \cdot (g(j) + h(j)) = \sum_{i*j=s} (f(i) \cdot g(j) + f(i) \cdot h(j)) = \sum_{i*j=s} (f(i) \cdot g(j)) + \sum_{i*j=s} (f(i) \cdot h(j)) = (f \cdot g) + (f \cdot h)$. Análogamente se obtiene que $((g+h) \cdot f)(s) = (g \cdot f) + (h \cdot f)$.

Por lo tanto $(R[S], +, \cdot)$ es un anillo. □

En la proposición anterior, si $(S, *)$ es un monoide cuyo elemento neutro es 1_S, y $(R, +, \cdot)$ es un anillo con uno. Entonces, proponemos a $\overline{1} \in R[S]$ tal que $\overline{1}(s) = 0$ si $s \neq 1_S$ y $\overline{1}(1_S) = 1_R$ como el elemento neutro con respecto a la multiplicación. Pues $(f \cdot \overline{1})(s) = \sum_{i*j=s} f(i)\overline{1}(j)$ pero $\overline{1}(j) = 0$ si $j \neq 1_S$, entonces $(f \cdot \overline{1}) = f$. Análogamente, obtenemos que $f = (\overline{1} \cdot f)$.

Al anillo $(R[S], +, \cdot)$ le llamaremos simplemente *anillo semigrupo*. En caso de que $(M, *)$ sea un monoide y $(R, +, \cdot)$ es un anillo con uno, entonces denominaremos al anillo $(R[M], +, \cdot)$ como *anillo monoide*. A los elementos del anillo semigrupo (monoide) los llamaremos polinomios.

Para $(R[S], +, \cdot)$ un anillo semigrupo (o monoide) y $f \in R[S]$, si $T = sop(f)$ entonces podemos expresar al polinomio f como $f = \sum_{s \in T} f(s) \cdot s$. Lo anteriormente mencionado puede consultarlo en [4].

En particular como $(\mathbb{N}, +)$ es un monoide obtenemos el *anillo de polinomios* $R[\mathbb{N}]$ que denotaremos como $R[X]$, cabe aclarar que la operación en $(\mathbb{N}, +)$ no necesariamente es la misma operación suma que la del anillo $(R, +, \cdot)$. Cada elemento en $f \in R[X]$, sea $n = \text{máx}\{m \in \mathbb{N} \mid f(m) \neq 0\}$ entonces podemos expresar a cada polinomio f como $f(x) = \sum_{i=1}^{n} a_i \cdot x^i$, donde $a_i = f(i)$. Diremos que el polinomio f es de grado n.

Decimos que un polinomio $f(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$ es mónico si $a_n = 1_R$. Además definimos al *grado del polinomio* $f(x)$ como $gr(f) = max\{m \in \mathbb{N} \,|\, f(m) \neq 0\}$. Decimos que un polinomio es lineal si es de la forma $f(x) = a \cdot x + b$, donde $a, b \in R$ (es decir que $gr(f) = 1$).

Sea $+$ una operación sobre el conjunto $\mathbb{N}^n$ tal que $(x_1, \ldots, x_n)+(y_1, \ldots, y_n) = (x_1+x_2, \ldots, x_n+y_n)$. Entonces, $(\mathbb{N}^n, +)$ es un monoide, obtiendo el anillo de polinomios de n-variables $R[\mathbb{N}^n]$ denotado como $R[X_1, \ldots, X_n]$.

Definición 2.24. *Sean $(R, +, \cdot)$ y $(R', \overline{+}, \bar{\cdot})$ anillos. Decimos que una función $\phi : R \longrightarrow R'$ es un morfismo de anillos si para cada $x, y \in R$, $\phi(x + y) = \phi(x)\overline{+}\phi(y)$ y $\phi(x \cdot y) = \phi(x)\bar{\cdot}\phi(y)$.*

Por otro lado ϕ es un monomorfismo de anillos si para cada $f : R'' \longrightarrow R$ y $g : R'' \longrightarrow R$ morfismos de anillos tales que $\phi \circ f = \phi \circ g$ entonces $f = g$.

Ejemplo 2.25. *Dados dos anillos $(R, +, \cdot)$ y $(R', \overline{+}, \bar{\cdot})$, definimos una función $\overline{0} : R \longrightarrow R'$ tal que $\overline{0}(r) = 0_{R'}$ para cada $r \in R$, luego $\overline{0}(r + r') = \overline{0}(r)\overline{+}\overline{0}(r') = 0_{R'}\overline{+}0_{R'} = 0'_R$ y $\overline{0}(r \cdot r') = \overline{0}(r)\bar{\cdot}\overline{0}(r') = 0_{R'}\bar{\cdot}0_{R'} = 0'_R$. Por lo tanto $\overline{0}$ es un morfismo de anillos*

Proposición 2.26. *Dados dos anillos $(R, +, \cdot)$, $(R', \overline{+}, \bar{\cdot})$ y un morfismo de anillos $\phi : R \longrightarrow R'$, entonces $\phi(0_R) = 0_{R'}$ y $-\phi(r) = \phi(-r)$.*

Demostración: Ya que $\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R)\overline{+}\phi(0_R)$, entonces $\phi(0_R) = 0_{R'}$.

Ahora ya que $\phi(0_R) = 0_{R'}$, luego $\phi(r)\overline{+}\phi(-r) = \phi(r - r) = 0_{R'}$. Por lo tanto $\phi(-r) = -\phi(r)$ □

Sea R un anillo. Dado $c \in R$, definimos la función $Ev_c : \mathbb{Z}[X] \longrightarrow R$ tal que para cada $f(x) \in \mathbb{Z}[X]$, $Ev_c(f(x)) = f(c)$. Probemos que Ev_c es un morfismo de anillos. Sean $f(x), g(x) \in \mathbb{Z}[X]$, entonces $Ev_c(f(x) + g(x)) = Ev_c((f + g)(x)) = (f + g)(c) = f(c) + g(c) = Ev_c(f(x)) + Ev_c(g(x))$ y $Ev_c(f(x) \cdot g(x)) = Ev_c((f + g)(x)) = (f + g)(c) = f(c) + g(c) = Ev_c(f(x)) + Ev_c(g(x))$

Proposición 2.27. *Dados dos anillos $(R, +, \cdot)$, $(R', \overline{+}, \bar{\cdot})$ y un morfismo de anillos $\phi : R \longrightarrow R'$, entonces las siguientes propiedades son equivalentes:*

a) ϕ es un monomorfismo.

b) ϕ es inyectivo.

c) $Ker(\phi) = \{0_R\}$ (Donde $ker(\phi) = \{x \in R \,|\, \phi(x) = 0_{R'}\}$).

Demostración: **a) ⇒ b)** Por contradicción. Supongamos que ϕ no es inyectivo, por lo que existen $a, b \in R$ distintos tales que $\phi(a) = \phi(b)$, sean $Ev_a : \mathbb{Z}[X] \longrightarrow R$ y $Ev_b : \mathbb{Z}[X] \longrightarrow R$. Entonces $Ev_a(x) = a$, $Ev_b(x) = b$ y además $\phi(Ev_a(x)) = \phi(a) = \phi(b) = \phi(Ev_b(x))$, pero ϕ al ser monomorfismo, entonces $Ev_a = Ev_b$ y en particular $a = Ev_a(x) = Ev_b(x) = b$, una contradicción. Por lo tanto ϕ es inyectiva.

b) ⇒ c) Puesto que $\phi(0_R) = 0_{R'}$, luego $\{0_R\} \subseteq Ker(\phi)$. Sea $r \in Ker(\phi)$ por consiguiente, $\phi(r) = 0_{R'} = \phi(0_R)$, por ser ϕ inyectiva tenemos que $r = 0_R$ y con ello $Ker(\phi) \subseteq \{0_R\}$. Por lo tanto $Ker(\phi) = \{0_R\}$.

c) ⇒ a) Ahora consideremos $f : R'' \longrightarrow R$ y $g : R'' \longrightarrow R$ morfismos de anillos tales que $\phi(f(x)) = \phi(g(x))$, luego $\phi(f(x) - g(x)) = \phi(f(x)) - \phi(g(x)) = 0_{R'}$ y ya que $Ker(\phi) = 0_R$, entonces $f(x) - g(x) = 0_R$ con lo cual $f(x) = g(x)$ y así $f = g$. Por lo tanto ϕ es monomorfismo. □

Definición 2.28. *Dado un anillo $(R, +, \cdot)$, decimos que un conjunto $I \subseteq R$ es un ideal izquierdo (derecho) si cumple que:*

- *$(I, +)$ es un subgrupo de $(R, +)$.*
- *Para cada $r \in R$ y $a \in I$, entonces $r \cdot a \in I$ $(a \cdot r \in I)$.*

Decimos que I es un ideal (bilateral) si este es un ideal derecho e izquierdo.

Proposición 2.29. *Dados dos anillos $(R,+,\cdot)$, $(R',\overline{+},\dot{-})$ y un morfismo de anillos $f: R \longrightarrow R'$, entonces $Ker(f)$ es un ideal del anillo $(R,+,\cdot)$.*

Demostración: En la demostración de **b) ⇒ c)** de la proposición anterior sabemos que $0_R \in ker(f)$. Ahora sean $a,b \in Ker(f)$, luego $f(a+b) = f(a)\overline{+}f(b) = 0_{R'}\overline{+}0_{R'} = 0_{R'}$, entonces $a+b \in Ker(f)$, Para cada $a \in Ker(f)$, $f(-a) = -f(a) = -0_R = 0_R$, es decir que $-a \in Ker(f)$. Por otro lado ya que $+$ es asociativo, tenemos que $(Ker(f),+)$ es un subgrupo de $(R,+)$.

Para cada $r \in R$ y $a \in Ker(f)$, $f(r\cdot a) = f(r)\dot{-}f(a) = f(r)\dot{-}0_{R'} = 0_{R'}$, es decir que $r\cdot a \in Ker(f)$. Análogamente $a \cdot r \in Ker(f)$. Por lo tanto $Ker(f)$ es un ideal. □

Al conjunto $Ker(f)$ lo llamaremos como el kernel del morfismo f.

Definición 2.30. *Decimos que $\phi: R \longrightarrow R'$ es un epimorfismo de anillos, si para cada $f: R' \longrightarrow R''$ y $g: R' \longrightarrow R''$ morfismos de anillos tales que $f\circ\phi = g\circ\phi$, entonces $f = g$.*

Proposición 2.31. *Sea $\phi: R \longrightarrow R'$ un morfismo de anillos suprayectivo, entonces ϕ es un epimorfismo.*

Demostración: Sean $f: R' \longrightarrow R''$ y $g: R' \longrightarrow R''$ morfismos de anillos tales que para cada $x \in G$, $f(\phi(x)) = g(\phi(x))$ por la suprayectividad de ϕ para cada $r' \in R'$, existe $r \in R$ tal que $\phi(r) = r'$, luego $f(r') = f(\phi(r)) = g(\phi(r)) = g(r')$, luego $f = g$. Por lo tanto ϕ es epimorfismo. □

Nota 2.32. *El recíproco de la proposición anterior no es verdadero. Pues tomando a los anillos $(\mathbb{Z},+,\cdot)$ y $(\mathbb{Q},+,\cdot)$ con sus respectivas operaciones usuales $(+,\cdot)$. Sea $\iota: \mathbb{Z} \longrightarrow \mathbb{Q}$ una función tal que para cada $z \in \mathbb{Z}$, $i(z) = z$. No es difícil probar que ι es un morfismo que no es suprayectivo. Afirmamos que es un epimorfismo, pues para cada $f: \mathbb{Q} \longrightarrow R$ y $g: \mathbb{Q} \longrightarrow R$ morfismos de anillos tales que $f\circ\iota = g\circ\iota$. Entonces, para cada $z \in \mathbb{Z}$, $f(z) = f(\iota(z)) = g(\iota(z)) = g(z)$. Con ello, para cada $\frac{a}{b} \in \mathbb{Q}$, tenemos que $f(\frac{a}{b}) = f(\frac{1}{b}a) = f(\frac{1}{b})\cdot f(a) = f(\frac{1}{b})\cdot g(a) = f(\frac{1}{b})\cdot g(b\frac{a}{b}) = f(\frac{1}{b})\cdot g(b)\cdot g(\frac{a}{b}) = f(\frac{1}{b})\cdot f(b)\cdot g(\frac{a}{b}) = f(\frac{1}{b}b)\cdot g(\frac{a}{b}) = f(1)\cdot g(\frac{a}{b}) = g(1)\cdot g(\frac{a}{b}) = g(1\cdot\frac{a}{b}) = g(\frac{a}{b})$ y con lo cual $f = g$. Por lo tanto ι es un epimorfismo que no es suprayectivo*

Definición 2.33. *Dados dos anillos $(R,+,\cdot)$ y $(R',\overline{+},\dot{-})$, decimos que $\phi: R \longrightarrow R'$ es un isomorfismo de anillos si existe un morfismo de anillos $g: R' \longrightarrow R$ tal que $\phi\circ g = Id_{R'}$ y $g\circ\phi = Id_R$.*

Si esto ocurre decimos que $(R,+,\cdot)$ y $(R',\overline{+},\dot{-})$ son isomorfos y lo denotamos como $R \cong R'$.

Nota 2.34. *Notemos que dicha función g en la definición anterior es única, pues supongamos que existe otro morfismo de anillos $g^*: R' \longrightarrow R$ tal que $\phi\circ g^* = Id_{R'}$ y $g^*\circ\phi = Id_R$, entonces $g = Id_R\circ g = (g^*\circ\phi)\circ g = g^*\circ(\phi\circ g) = g^*\circ Id_{R'} = g^*$. A dicha función la denotaremos simplemente como ϕ^{-1}.*

Además la composición de isomorfismos es también un isomorfismo. Para poder demostrar este hecho, sean $\phi_1: R \longrightarrow R'$ y $\phi_2: R' \longrightarrow R''$ isomorfismos de anillos, entonces $\phi_1\circ\phi_1^{-1} = Id_{R'}$, $\phi_1^{-1}\circ\phi_1 = Id_R$, $\phi_2\circ\phi_2^{-1} = Id_{R''}$ y $\phi_2^{-1}\circ\phi_2 = Id_{R'}$. Por lo tanto, $(\phi_2\circ\phi_1)\circ(\phi_1^{-1}\circ\phi_2^{-1}) = \phi_2\circ(\phi_1\circ\phi_1^{-1})\circ\phi_2^{-1} = \phi_2\circ\phi_2^{-1} = Id_{R''}$ y análogamente $(\phi_1^{-1}\circ\phi_2^{-1})\circ(\phi_2\circ\phi_1) = Id_R$. Es decir que $\phi_2\circ\phi_1$ es un isomorfismo

Proposición 2.35. *Todo isomorfismo de anillos es un monomorfismo y un epimorfismo de anillos.*

Demostración: Sea $\phi: R \longrightarrow R'$ un isomorfismo, entonces existe $\psi: R' \longrightarrow R$ tal que $\phi\circ\psi = Id_{R'}$ y $\psi\circ\phi = Id_R$. Sean $f: R'' \longrightarrow R$ y $g: R'' \longrightarrow R$ morfismos tales que $\phi\circ g = \phi\circ f$, entonces $g = Id_R\circ g = (\psi\circ\phi)\circ g = \psi\circ(\phi\circ g) = \psi\circ(\phi\circ f) = (\psi\circ\phi)\circ f = Id_R\circ f = f$, es decir que ϕ es un monomorfismo. Análogamente obtenemos que ϕ es epimorfismo. □

Proposición 2.36. *Dados dos anillos $(R,+,\cdot)$ y $(R',\overline{+},\dot{-})$. Son equivalentes para un morfismo de anillos $f: R \longrightarrow R'$ lo siguiente:*

a) f es un isomorfismo de anillos.

b) f es biyectiva (es decir que f es una función inyectiva y suprayectiva).

Demostración:

a) ⇒ b) Por la *Proposición 2.27*, f es inyectivo. Para probar que f es una una función suprayectiva, notemos que existe un morfismo de anillos $g : R' \longrightarrow R$ tal que $f \circ g = Id_{R'}$ y $g \circ f = Id_R$. Con ello, para cada $r' \in R'$, $f(g(r')) = (f \circ g)(r') = Id_{R'}(r') = r'$ y puesto que $g(r') \in R$, sea $r \in R$ tal que $r = g(r')$. Con lo cual, para cada $r' \in R$ existe $r \in R$, tal que $f(r) = r'$. Por lo tanto f es suprayectiva. Así, podemos concluir que f es un morfismo biyectivo.

a) ⇒ b) Por la *Proposición 2.27*, desde que f es un morfismo inyectivo, entonces f es un monomorfismo. Por la *Proposición 2.31* f es un epimorfismo. Por lo tanto f es un isomorfismo de anillos. □

Nota 2.37. *Decimos que un anillo $(R, +, \cdot)$ se sumerge en un anillo $(R', \overline{+}, \bar{\cdot})$, si existe un morfismo inyectivo $\phi : R \longrightarrow R'$.*

Por ejemplo, el anillo $(R, +, \cdot)$ se sumerge sobre el anillo de polinomios $(R[X], +, \cdot)$, pues la siguiente función es un morfismo inyectivo $i : R \longrightarrow R[X]$ donde $i(r) = r$ para cada $r \in R$.

Definición 2.38. *Dados dos anillos $(A, +, \cdot)$, $(B, +, \cdot)$ tales que $(A, +, \cdot)$ es subanillo de $(B, +, \cdot)$. Decimos que $\alpha \in B$ es una raíz para un polinomio $f(x) \in A[X]$ si $f(\alpha) = 0_R$.*

Ejemplo 2.39. *Dado un anillo $(R, +, \cdot)$. Sea un conjunto $S \subseteq R$, definimos:*

$$I(S) = \cap\{I \subseteq R \,|\, I \text{ es un ideal izquierdo, tal que } S \subseteq I\}.$$

Entonces $I(S)$ es un ideal izquierdo.
Demostración:

Por la proposición 2.13, $(I(S), +)$ es un subgrupo de $(R, +)$. Sean $r \in R$ y $s \in I(S)$, entonces para cada ideal $I' \in \{I \subseteq R \,|\, I \text{ es un ideal izquierdo}\}$ se tiene que $sr \in I'$ y en consecuencia $sr \in I(S)$. Por lo tanto $I(S)$ es un ideal izquierdo. □

Notemos que $I(S)$ es el menor ideal que contiene a S. Para ello supongamos que J es el minimo ideal que contiene a S, luego $J \subseteq I(S)$. Pero como J es ideal y J contiene a S, entonces por como definimos a $I(S)$, tenemos que $I(S) \subseteq J$. Por lo tanto $I(S) = J$

En particular, dado un elemento $r \in R$, denotamos al ideal principal derecho (izquierdo) generado por el elemento r como el conjunto $Rr = \{a \cdot r \,|\, a \in R\}$ ($rR = \{r \cdot a \,|\, a \in R\}$). Análogamente, también definimos al ideal principal (bilateral) generado por el elemento r como el conjunto $(r) = \{a \cdot r \cdot b \,|\, a, b \in R\}$.

De manera similar dado un anillo R podemos demostrar la existencia de un subanillo generado por un conjunto S, denotado por $R(S)$.

Sabemos que $(R/I, *)$ es un grupo, donde para cada $a + I, b + I \in R/I$ se tiene que $(a + I) * (b + I) = (a + b) + I$. Definiendo otra operación $\bullet$ en R/I tal que $(a + I) \bullet (b + I) = (a \cdot b) + I$ tenemos el siguiente resultado:

Proposición 2.40. *$(R/I, *, \bullet)$ es un anillo.*

Demostración:

Desde que $(I, +)$ es un subgrupo de $(R, +)$ y $(R, +)$ es un grupo abeliano, entonces $(I, +)$ es un subgrupo normal de $(R, +)$ y así $(R/I, *)$ es un grupo abeliano.

Sean $r, r', s, s' \in R$ tales que $r + I = r' + I$ y $s + I = s' + I$, entonces $r - r' \in I$ y $s - s' \in I$, por la definición de ideal $s' \cdot (r - r') \in I$ y $(s - s') \cdot r \in I$, luego como $(I, +)$ es un grupo $s \cdot r - s' \cdot r' = s' \cdot (r - r') - (s - s') \cdot r \in I$. Por lo tanto $(s+I) \bullet (r+I) = (s \cdot r) + I = (s' \cdot r') + I = (s' + I) \bullet (r' + I)$. Por lo tanto $\bullet$ es una operación binaria en R/I.

Ya que la operación $\cdot$ es asociativa en R, tenemos que para cada $a, b, c \in R$, $((a+I)\bullet(b+I))\bullet(c+I) = ((a\cdot b)+I)\bullet(c+I) = ((a\cdot b)\cdot c)+I = (a\cdot(b\cdot c))+I = (a+I)\bullet((b\cdot c)+I) = (a+I)\bullet((b+I)\bullet(c+I))$.

Por la distribución de la suma sobre el producto en R, tenemos que para cada $a, b, c \in I$, $((a+I)\bullet(b+I)) * ((a+I)\bullet(c+I)) = ((a\cdot b)+I) * ((a\cdot c)+I) = ((a\cdot b)+(a\cdot c))+I = (a\cdot(b+c))+I = (a+I)\bullet((b+c)+I) = (a+I)\bullet((b+I)*(c+I))$. □

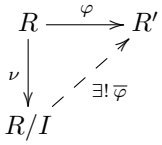
En caso que $(R, +, \cdot)$ sea un anillo con uno, entonces para cualquier $r \in R$, $1_R \cdot r = r \cdot 1_R = r$, Proponemos a $1_R + I$ como elemento neutro de $(R/I, \bullet)$. Pues para cada $r + I \in R/I$, $(r + I) \bullet (1_R + I) = (r \cdot 1_R) + I = r + I$.

Y particular si $(R, +, \cdot)$ es un anillo con división, entonces para cada $r \in R$, existe un elemento $r' \in R$ tal que $r \cdot r' = 1_R$. Notemos que $r' + I$ es el inverso multiplicativo de $r + I$. En efecto, $(r + I) \bullet (r' + I) = (r \cdot r') + I = 1_R + I = (r' + I) \bullet (r + I)$.

Nota 2.41. *Definamos la siguiente función $\nu : R \longrightarrow R/I$ tal que $\nu(r) = r + I$. Notemos que $\nu(r + r') = (r + r') + I = (r + I) * (r' + I) = \nu(r) * \nu(r')$. Análogamente, $\nu(r \cdot r') = \nu(r) \bullet \nu(r')$, Por lo tanto ν es un morfismo de anillos. Para cada $r + I \in R/I$, $\nu(r) = r + I$ es decir que ν es un morfismo suprayectivo, lo cual implica que ν es un epimorfismo.*

Teorema 2.42. *(Primer teorema de isomorfismos)*

Sea $\varphi : R \longrightarrow R'$ un morfismo de anillos con núcleo $Ker(\varphi) = I$. Entonces I es un ideal de R y existe un único monomorfismo $\overline{\varphi} : R/I \longrightarrow R'$ tal que $\varphi = \overline{\varphi} \circ \nu$, donde ν es el morfismo natural. En otras palabras el siguiente diagrama conmuta:



Demostración:

La *Proposición 2.29* nos dice que I es un ideal de R.

Definimos a $\overline{\varphi}$ tal que para cada $r+I \in R/I$, $\overline{\varphi}(r+I) = \varphi(r)$. Probemos que $\overline{\varphi}$ es una función, para ello sean $x+I, y+I \in R/I$ tal que $x+I = y+I$, entonces $x-y \in I$ por lo que existe $z \in I$ tal que $z = x-y$. Así tenemos que $x = z+y$, con lo cual $\varphi(x) = \overline{\varphi}(x+I) = \overline{\varphi}((z+y)+I) = \varphi(z+y) = \varphi(z)+\varphi(y)$ y puesto que $z \in I = Ker(\varphi)$, tenemos que $\varphi(z)+\varphi(y) = 0+\varphi(y) = \overline{\varphi}(y+I)$.

Por otro lado tenemos que $\overline{\varphi}((r_1+I)+(r_2+I)) = \overline{\varphi}((r_1+r_2)+I) = \varphi(r_1+r_2) = \varphi(r_1)+\varphi(r_2) = \overline{\varphi}(r_1+I)+\overline{\varphi}(r_2+I)$ y además $\overline{\varphi}((r_1+I)\cdot(r_2+I)) = \overline{\varphi}((r_1\cdot r_2)+I) = \varphi(r_1\cdot r_2) = \varphi(r_1)\cdot\varphi(r_2) = \overline{\varphi}(r_1+I)\cdot\overline{\varphi}(r_2+I)$. De aquí podemos afirmar que $\overline{\varphi}$ es un morfismo de anillos.

Notemos que $\overline{\varphi}$ hace conmutar el triangulo, pues para cada $r \in R$, $\overline{\varphi} \circ \nu(r) = \overline{\varphi}(\nu(r)) = \overline{\varphi}(r+I) = \varphi(r)$, es decir que $\varphi = \overline{\varphi} \circ \nu$.

Notemos que $\overline{\varphi}$ es monomorfismo, pues sean $x+I, y+I \in R/I$ tales que $\varphi(x) = \overline{\varphi}(x+I) = \overline{\varphi}(y+I) = \varphi(y)$, entonces $\varphi(x-y) = \varphi(x)-\varphi(y) = 0_{R'}$, luego $x-y \in Ker(\varphi) = I$ lo cual sucede si y solo sí $x+I = y+I$.

Veamos la unicidad de $\overline{\varphi}$. Para ello sea $\sigma : R/I \longrightarrow R'$ tal que $\sigma \circ \nu = \varphi$. Luego por ser ν un epimorfismo y ya que $\overline{\varphi} \circ \nu = \varphi = \sigma \circ \nu$, entonces $\overline{\varphi} = \sigma$. Por lo tanto $\overline{\varphi}$ es el único monomorfismo que hace conmutar el triangulo. □

Proposición 2.43. *Sean I, J ideales en un anillo $(R, +, \cdot)$. Entonces $I + J = \{i + j \mid i \in I,\ j \in J\}$ es un ideal.*

Demostración: Por ser I, J ideales, entonces $0_R \in I$ y $0_R \in J$, entonces $0_R = 0_R + 0_R \in I + J$.

Por otro lado, para cada $a = i_1 + j_1 \in I + J$ y $b = i_2 + j_2 \in I + J$ (donde $i_1, i_2 \in I$ y $j_1, j_2 \in J$), por la conmutatividad de la operación suma, $a+b = (i_1+i_2)+(j_1+j_2) \in I+J$. En consecuencia $+$ es una operación binaria, que hereda las propiedades asociativas y conmutativas del anillo. Ahora,

probemos que cada elemento de $I+J$ tiene un inverso aditivo. Para cada $c = i + j \in I + J$ con $i \in I$ y $j \in J$, existen $-i \in I$ y $-j \in J$, con ello $-c = -i - j \in I + J$. Por consiguiente $(I + J, +)$ es un grupo.

Dado $c \in I + J$, como $c = i + j$ con $i \in I$ y $j \in J$, entonces para cada $r \in R$, $r \cdot i \in J$ y $r \cdot j \in J$, luego $r \cdot c = r \cdot i + r \cdot j \in I + J$. Por lo tanto $I + J$ es un ideal. □

Nota 2.44. *Dado un una familia de ideales derechos $\{I_m\}_{m\in M}$ de un anillo $(R, +, \cdot)$, definimos al conjunto:*

$$K = \sum_{m\in M} I_m = \{\sum_{i=1}^{n} r_i \cdot a_i \,|\, r_i \in R,\, a_i \in I_i\}.$$

Usando un razonamiento análogo a la proposición anterior no es difícil ver que dicho conjunto es de hecho un ideal.

Por otro lado, si J es el ideal generado por la unión de $\{I_m\}_{m\in M}$, entonces J es igual que K. Por la minimalidad del ideal J, entonces $J \subseteq K$. Para probar la otra contención, sea $y \in K$ y por como está definido este conjunto, existen $r_i \in R$ y $a_i \in I_i$ tales que $y = \sum_{i=1}^{n} r_i \cdot a_i$, Por lo tanto $y \in J$ y con ello $J \subseteq K$. Esto prueba que:

$$\sum_{m\in M} I_m = I(\bigcup_{m\in M} I_m).$$

Es decir, que cada elemento del conjunto K puede verse como una combinación lineal finita de elementos de J.

2.2. Extensiones de campos

Definición 2.45. *Dado un conjunto K, y dos operaciones binarias $+$ (adición) y $\cdot$ (multiplicación). Decimos que $(K, +, \cdot)$ es un campo si:*

- *$(K, +, \cdot)$ es un anillo con 0_K el elemento neutro de la suma y 1_K es el elemento neutro del producto ($0_K \neq 1_K$).*
- *$(K, \cdot)$ es abeliano.*
- *Para cada elemento $x \in K\backslash\{0_R\}$, existe $y \in K$ tal que $x \cdot y = 1_K$.*

Proposición 2.46. *Los únicos ideales de un campo $(F, +, \cdot)$ son $\{0_F\}, F$.*

Demostración: Claramente $\{0_F\}$ es un ideal de $(F, +, \cdot)$. Ahora sea J un ideal distinto de $\{0_F\}$ entonces existe $r \in J$ tal que $r \neq 0_F$, entonces ya que F es un campo tenemos que $r^{-1} \in F$ y en consecuencia $1_F = r \cdot r^{-1} \in J$. Por lo tanto, para cada $r' \in F$ tenemos que $r' = r' \cdot 1_F \in J$, es decir $F \subseteq J$ y así $J = F$. □

Definición 2.47. *Dado un campo $(K, +, \cdot)$, decimos que un polinomio $p(x) \in K[X]$ es un polinomio irreducible si cumple lo siguiente:*

- *$gr(p) > 0$*
- *Si $p(x) = g(x)h(x)$, entonces $gr(g) = 0$ ó $gr(h) = 0$.*

Decimos que un polinomio es reducible, si este no es irreducible.

Decimos que un polinomio $f \in K[X]$, es mónico si su coeficiente principal es 1. Es decir que si $f(x) = a_n \cdot x^n + \ldots + a_1 \cdot x + a_0$, entonces $a_n = 1$.

El siguiente resultado puede consultarlo en el capitulo IV, Teorema 1.1 en [10], dicha prueba es libre de elección.

Proposición 2.48. *(algoritmo de la división)*
Sean $(R,+,\cdot)$ un anillo conmutativo y $f,g \in R[X]$ distintos de cero. Entonces, existen $q,r \in R[X]$ únicos tales que

$$f(x) = g(x)q(x) + r(x)$$

con $0 \leq gr(r(x)) < gr(m(x))$.

Definición 2.49. *Decimos que un anillo conmutativo $(R,+,\cdot)$ es dominio entero si para cualesquiera $a,b \in R$, tales que $a \cdot b = 0_R$ entonces $a = 0_R$ ó $b = 0_R$.*

Decimos que un dominio entero $(R,+,\cdot)$ es un dominio de ideales principales, si todo ideal I es un ideal principal (es decir que para cada ideal I, existe un elemento $r \in R$ tal que $I = (r)$).

Ejemplo 2.50. *Todo campo es un dominio entero.*
Demostración: Sean $(K,+,\cdot)$ un campo y $a,b \in K$ tales que $a \cdot b = 0_K$. Supongamos que $a \neq 0_K$, entonces a tiene elemento inverso. Con lo cual, $b = 1_K \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_K = 0_K$. Por lo tanto $(K,+,\cdot)$ es un dominio entero. □

Proposición 2.51. *Dado un dominio entero $(R,+,\cdot)$, si $c \cdot a = c \cdot b$ para cada $c \neq 0$, entonces $a = b$.*

Demostración: Puesto que $c \cdot a = c \cdot b$, entonces $c \cdot (a-b) = c \cdot a - c \cdot b = 0$, Pero $c \neq 0$ y $(R,+,\cdot)$ es dominio entero, luego $a - b = 0$. Por lo tanto $a = b$. □

Proposición 2.52. *Sea F un campo, entonces $F[X]$ es un ideal de dominios principales*

Demostración: Descartando los casos triviales en que los ideales son de la forma $\{0_F\} = (0_F)$ y $(1_F) = F[X]$.

Consideremos al ideal J distinto de $F[X]$ y $\{0_F\}$. Puesto que $\mathbb{N}$ es un conjunto bien ordenado, sea $n = min\{gr(f) \mid f(x) \in J\}$ y elíjase a $p(x) \in J$ tal que $gr(p) = n$, entonces $(p(x)) \subseteq J$. Ahora, sea $a(x) \in J$ tal que $p(x) \nmid a(x)$, entonces por el *algoritmo de la división* existen $r(x), q(x) \in F[X]$ tales que $p(x) = a(x)q(x) + r(x)$ y $gr(r) < gr(p)$ con $r \neq 0$. Por lo tanto $r(x) = p(x) - a(x)q(x) \in J$, una contradicción. Así obtenemos que $p(x) | a(x)$ y por lo tanto $J \subseteq (p(x))$. □

Proposición 2.53. *Dado un campo $(K,+,\cdot)$ y $p(x) \in F[X]$. Si $p(x)$ es un polinomio irreducible entonces $(p(x))$ es un ideal máximo.*

Demostración: Por contrarrecíproca supongamos que $(p(x))$ no es un ideal máximo, luego existe $q(x) \in F[X]$ tal que $(p(x)) \subsetneq (q(x)) \subsetneq F[X]$. Esto implica que $q(x), p(x) \notin F$ $(gr(p) \neq 0 \neq gr(q))$, además $p(x) \in (q(x))$, entonces existe $r(x) \in F[X]$ tal que $q(x)r(x) = p(x)$ $(q(x) \mid p(x))$, luego tenemos que $gr(p) = gr(q) + gr(r)$. Supongamos que $gr(r) = 0$, entonces $r(x) \in F$ por lo que r es unidad y consecuentemente $q(x) = p(x)(r(x))^{-1} \in (p(x))$, lo cual contradice que $(p(x)) \subsetneq (q(x))$. Por lo tanto $gr(r) > 0$, esto implica que $p(x)$ es un polinomio reducible. □

Proposición 2.54. *Dado un anillo $(R,+,\cdot)$, si J es un ideal máximo entonces R/J es un campo.*

Demostración: Sea $J + a \in R/J$ (donde $a \notin J$) y consideremos al ideal $K = J + (a)$, por la maximalidad de J y que $J \subseteq K$, entonces tenemos que $K = R$. Esto implica que $1_R \in K$, luego existen $j \in J$ y $r \in R$ tales que $1_R = j + r \cdot a$, con lo cual $J + 1_R = J + (r \cdot a) = (J + r) \cdot (J + a)$. Por lo tanto $J + a$ tiene inverso multiplicativo y con ello R/I es un campo. □

Decimos que $(K',+,\cdot)$ es un subcampo de $(K,+,\cdot)$, si $K' \subseteq K$ y K' es un campo. De esta manera decimos que $(K,+,\cdot)$ es una extensión de campos de $(K',+,\cdot)$ lo cual lo denotaremos como K/K'.

Teorema 2.55. *(Primer teorema de kronecker) Dado un campo $(F,+,\cdot)$ y $f(x) \in F[X]$. Entonces existe una extensión de campos E de F tal que $f(\alpha) = 0$ para $\alpha \in E$.*

Demostración: Como F es un campo entonces $F[X]$ es un *dominio de factorización única*. Sea $p(x)$ un polinomio irreducible tal que $p(x)|f(x)$, luego $(p(x))$ es un ideal máximo en $F[X]$ con lo cual $K = F[X]/(p(x))$ es un campo.

Sea $\Psi : F \longrightarrow K$ tal que $\Psi(a) = a+(p(x))$, luego Ψ es un morfismo, probemos que es inyectivo. Sean $a, b \in F$ tales que $\Psi(a) = \Psi(b)$, entonces $\Psi(a-b) = \Psi(a) - \Psi(b) = 0_K$ y como los únicos ideales de F son 0_F y F, entonces $Ker(\Psi) = F$ ó $Ker(\Psi) = 0_F$, pero Ψ es disntinto al morfismo nulo $\overline{0}$ y así $Ker(\Psi) = \{0_F\}$. Por lo tanto Ψ es inyectivo. Luego $\Psi|^{\Psi(F)} : F \longrightarrow \Psi(F)$ es una función biyectiva y por tanto es un isomorfismo.

Ahora sea $E = K$ y $\alpha \in E$. donde $\alpha = x + (p(x))$ y consideremos a $Ev_{(\alpha)} : F[X] \longrightarrow E$ tal que $Ev_{(\alpha)}(q(x)) = q(\alpha)$, luego si $p(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$, entonces $Ev_{(\alpha)}(p(x)) = p(\alpha) = a_0 + a_1 \cdot \alpha + \ldots + a_n \cdot \alpha^n = (a_0 + p(x)) + a_1 \cdot (x + (p(x))) + \ldots + a_n \cdot (x + (p(x)))^n = (a_0 + p(x)) + (a_1 \cdot x) + (p(x)) + \ldots + (a_n \cdot x^n) + (p(x)) = (a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n) + (p(x)) = p(x) + (p(x)) = 0_K$.

Por lo tanto E es una extensión de campos de F con $\alpha \in E$ tal que $f(\alpha) = 0$ □

Dado un campo $(K, +, \cdot)$, definimos el K-espacio vectorial V como una estructura algebraica $(V, +, \cdot)$ donde $+ : V \times V \to V$ es la suma y $\cdot : R \times V \to V$ es la multiplicación escalar. Donde $(V, +)$ es un grupo abeliano y para cada $r, r' \in K$, $m, m' \in V$ se tiene que:

- (Elemento neutro) $1 \cdot m = m \cdot 1$
- (Asociatividad) $r \cdot (r' \cdot m) = (r \cdot r') \cdot m$
- (Propiedad distributiva) $(r + r') \cdot m = r \cdot m + r' \cdot m$ y $r \cdot (m + m') = r \cdot m + r \cdot m'$

Definición 2.56. *Sea V un K-espacio vectorial V. Decimos que un conjunto $S \subseteq V$ es linealmente independiente si para cada $s_1, \ldots, s_n \in S$ y $k_1, \ldots, k_n \in K$ son tales que $k_1 \cdot s_1 + \ldots + k_n \cdot s_n = 0$, entonces $k_i = 0$ para cada $i \in \{1, \ldots, n\}$.*

Por otro lado decimos que $S \subseteq V$ genera a V, si para cada $v \in V$, existen $s_1, \ldots, s_n \in S$ y $k_1, \ldots, k_n \in K$ son tales que $v = k_1 \cdot s_1 + \ldots + k_n \cdot s_n$.

Decimos $S \subseteq V$ es una base, si S es linealmente independiente y genera a V. Con ello definimos a la dimensión de V como $Dim_K(V) = |\beta|$ donde β es una base.

Ejemplo 2.57. *Notemos que si K es una extensión de campo de E, entonces K es un E- espacio vectorial. A la dimensión de F como K-espacio vectorial la denotaremos por $[F : K] = Dim_K(F)$ la cual se le llamara grado de extensión. Decimos que K/F es una extensión finita si $[F : K] = n \in \mathbb{N}$*

Definición 2.58. *Sea P un ideal propio en un anillo conmutativo $(R, +, \cdot)$, se dice que es primo si para cada $a, b \in R$ tal que $a \cdot b \in P$, entonces $a \in P$ ó $b \in P$.*

Proposición 2.59. *Dado $f(x) \in F[X]$ con $(F, +, \cdot)$ un campo, si $(p(x))$ es primo entonces $p(x)$ es irreducible.*

Demostración: Supongamos por contradicción que $(p(x))$ es reducible, entonces si $gr(p) = 0$ tenemos que $p(x) \in F$ es decir que $p(x)$ tiene inverso y con ello $1 \in (p(x))$ lo cual contradice el hecho de que $(p(x))$ es un ideal propio.

Por otro lado, suponiendo que $gr(p) > 0$. Por ser $p(x)$ irreducible, existen $a(x), b(x) \in F[X]$ tales que $p(x) = a(x) \cdot b(x)$, $gr(a) \neq 0$ y $gr(b) \neq 0$. Entonces $a(x)|p(x)$, entonces por ser $(p(x))$ un ideal primo, $a(x) \in (p(x))$ de lo cual tenemos que $p(x)|a(x)$. Con lo cual, $a(x) = p(x)$ entonces $b(x)$ es una constante, lo cual contradice el hecho de que $gr(b) \neq 0$. Por lo tanto $p(x)$ es irreducible. □

Definición 2.60. *Dada una extensión de campos K/K'. Decimos que $\alpha \in K$ es algebraico sobre K' si existe $f \in K'[X]$ dinto del polinomio 0 tal que $f(\alpha) = 0$.*

Dado $\alpha \in K$, definimos al conjunto $K'(\alpha)$ como el mínimo subcampo que contiene a K' y a α.

Nota 2.61. *Sea* $A_\alpha = \{m \in \mathbb{N} \mid f(x) \in K[X], gr(f) = m, f(x) \neq 0, f(\alpha) = 0 \text{ y } f \text{ es mónico}\}$. *Por el principio del buen orden de los números naturales, existe* $d \in \mathbb{N}$ *tal que* $d = min(A_\alpha)$. *Sea* $m(x) = a_0 + a_1 \cdot x + \ldots + x^d \in K[X]$ *un polinomio mónico distinto de* 0 *y tal que* $m(\alpha) = 0$. *Demostremos que* $m(x)$ *es único con las propiedades antes mencionadas. Para ello supongamos que existe* $q(x) = b_0 + b_1 \cdot x + \ldots + x^d \in K[X]$ *polinomio mónico distinto de* 0, *tal que* $q(\alpha) = 0$ *y* $q(x) \neq m(x)$. *Sea* $h(x) = m(x) - q(x) = a_0 - b_0 + (a_1 - b_1) \cdot x + \ldots + (a_{d-1} - b_{d-1}) \cdot x^{d-1} \neq 0$, *entonces* $h(\alpha) = m(\alpha) - q(\alpha) = 0$ *y* $gr(h) < d$, *considerando el siguiente polinomio* $p(x) = (a_{d-1} - b_{d-1})^{-1}h(x)$, *obtenemos un polinomio mónico distinto de* 0 *y tal que* $p(\alpha) = 0$, *lo cual contradice la minimalidad de* d.

Ahora probemos que $m(x)$ *es irreducible en* $K[X]$. *Para ello, supongamos que no lo es, entonces existen* $f, g \in K[X]$ *tales que* $m(x) = f(x) \cdot g(x)$, $0 < gr(f) < d$ *y* $0 < gr(g) < d$. *Con lo cual,* $0 = m(\alpha) = f(\alpha)g(\alpha)$ *es decir* $f(\alpha) = 0$ *ó* $g(\alpha) = 0$, *una contradicción. Por lo tanto* m *es el único polinomio mónico irreducible no cero y tal que* $m(\alpha) = 0$.

Para cada $t(x) \in K[X]$ *tal que* $t(\alpha) = 0$, *afirmamos que* $gr(t) \geq gr(m)$. *Para ello, sea* $I = \{d(x) \in K[X] \mid d(\alpha) = 0\}$. *Demostremos que* I *es un ideal:*

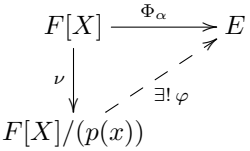
- $0 \in I$; *pues* $0(\alpha) = 0$
- *Para cada* $q_1, q_2 \in K[X]$; *entonces* $(q_1 + q_2)(\alpha) = q_1(\alpha) + q_2(\alpha) = 0 + 0 = 0$, *es decir que* $q_1 + q_2 \in K[X]$.
- *Para cada* $r \in K[X]$, $t \in K[X]$; *entonces* $s(\alpha) = t(\alpha) \cdot r(\alpha) = 0 \cdot r(\alpha) = 0$

Ya que $F[X]$ *es un dominio de ideales principales, existe* $h(x) \in I$ *tal que* $(h(x)) = I$. *Mostremos que* $(m(x)) = I$. *Puesto que* $m \in I$, *luego existe* $r(x) \in I$ *tal que* $m(x) = r(x) \cdot h(x)$, *por ser* $m(x)$ *irreducible se puede implicar que* $gr(r) = 0$, *es decir que* $r(x) = c \in K$, *por lo que* $m(x) = c \cdot h(x)$. *Por tanto* $I = (h(x)) = (c^{-1}m(x)) = (m(x))$. *Por ultimo para cada* $t \in K[X]$ *tal que* $t(\alpha) = 0$, *entonces* $t \in I$, *con lo cual existe* $r(x) \in K[X]$ *tal que* $t(x) = r(x) \cdot m(x)$. *Por lo tanto* $gr(t) \geq gr(m)$

Proposición 2.62. *Sean* E/F *una extensión de campo y* $\alpha \in E$ *algebraico sobre* F. *Entonces* $F(\alpha) \cong F[X]/(p(x))$, *donde* $p(x) \in F[X]$ *es irreducible y* $p(\alpha) = 0$.

Demostración: Sea $\Phi_\alpha : F[X] \longrightarrow E$ tal que $\Phi_\alpha(f(x)) = f(\alpha)$. Entonces, $Ker(\Phi_\alpha) = \{f(x) \in F[X] \mid f(\alpha) = 0\}$ y puesto que α es algebraico sobre F, $Ker(\Phi_\alpha) \neq \{0\}$. Puesto que F es un campo, $F[X]$ es un *dominio de ideales principales*, con ello existe $p(x) \in F[X]$ tal que $(p(x)) = Ker(\Phi_\alpha)$.

Entonces por el *primer teorema de isomorfismos*, existe $\varphi : F[X]/(p(x)) \longrightarrow E$ tal que $\varphi \circ \nu = \Phi_\alpha$ y $F[X]/(p(x)) \cong Rang(\Phi_\alpha) \subseteq E$, así tenemos que el siguiente diagrama conmuta:



Como E es un campo, entonces $Rang(\Phi_\alpha)$ es un dominio entero lo cual sucede si y solo sí $p(x)$ es un ideal primo. Por lo que $p(x)$ es irreducible.

Puesto que $\varphi(f(x) + (p(x))) = f(\alpha)$, entonces $\varphi(x + (p(x))) = \alpha$ y para cada $c \in F$, $\varphi(c + (p(x))) = c$. Luego tenemos que $F \subseteq Rang(\Phi_\alpha)$ y $\alpha \in Rang(\Phi_\alpha)$, entonces $F(\alpha) \subseteq Rang(\Phi_\alpha)$.

Ahora para cada extensión de campos K/F tal que $\alpha \in K$, si $c_i \in F$ entonces $c_0 + c_1 \cdot \alpha + \ldots + c_n \cdot \alpha^n \in K$, para cada $i \in \{1, \ldots, n\}$, Es decir que $Rang(\Phi_\alpha) \subseteq K$. En particular tenemos que $Rang(\Phi_\alpha) \subseteq F(\alpha)$ por lo tanto $F[X]/(p(x)) \cong Rang(\Phi_\alpha) = F(\alpha)$. □

Teorema 2.63. *Sea* $p(x) \in F[X]$ *un polinomio irreducible de grado* d. *Entonces* $E = F[X]/(p(x))$ *es una extensión de campo de* F *de grado* d. *De hecho,* E *contiene una raíz* α *de* $p(x)$ *y una base de* E *como* F*-espacio vectorial.*

Demostración: Supongamos sin perdida de la generalidad que $p(x)$ es un polinomio mónico. Sean $I = (p(x))$ y $\alpha = x + I$. Probemos que $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ es una base de E. Primero, supongamos que S no es linealmente independiente, es decir que existen $a_1, \ldots, a_d \in F$ no todos cero tales que $a_1 \cdot 1 + a_2 \cdot \alpha + a_3 \cdot \alpha^2 + \ldots + a_d \cdot \alpha^{d-1} = 0$. Consecuentemente, si $b_i = a_d^{-1} \cdot a_i$ para cada $i \in \{1, \ldots, n\}$, podemos definir un polinomio mónico de grado menor que d, $f(x) = b_1 + b_2 \cdot x + \ldots + b_d \cdot x^{d-1}$ y tal que $f(\alpha) = 0$, esto contradice lo visto en la *nota 2.61.* Por tanto S es linealmente independiente.

Notemos que cada elemento de E es de la forma $f(x) + I$ con $f(x) \in F[X]$. Por el algoritmo de la división existen $q(x), r(x) \in F[X]$ tales que $f(x) = p(x)q(x) + r(x)$ donde $0 < gr(r) < d = gr(p)$. Dado que $f(x) - r(x) = p(x)q(x) \in I$, entonces $f(x) + I = r(x) + I$. Podemos reescribir a r de la siguiente manera $r(x) = c_0 + c_1 \cdot x + \ldots + c_{d-1} \cdot x^{d-1}$ donde $c_i \in F$ para cada $i \in \{1, \ldots, d-1\}$. Luego $r(\alpha) = r(x+I) = (c_0+I) + c_1 \cdot (x+I) + \ldots + c_{d-1} \cdot (x+I)^{d-1} = c_0 + I + c_1 \cdot x + I + \ldots + c_{d-1} \cdot x^{d-1} + I = (c_0 + c_1 \cdot x + \ldots + c_{d-1} \cdot x^{d-1}) + I = r(x) + I = f(x) + I = f(\alpha)$. Por lo tanto S genera a E y así S es una base para E. □

Teorema 2.64. *(Segundo teorema de Kronecker)*
Sea $f(x) \in F[X]$ donde $(F, +, \cdot)$ es un campo. Entonces existe un campo E que contiene a F como subcampo y tal que $f(x)$ se escribe como producto de polinomios lineales es $E[X]$.

Demostración:
Haremos la prueba por inducción sobre el grado de f. Si $gr(f) = 1$, entonces $f(x)$ es lineal, así que bastaria tomar a $E = F$.

Ahora supongamos que $gr(f) > 1$. Sea $p(x) \in F[X]$ un polinomio irreducible y tal que $f(x) = p(x) \cdot h(x)$, esto se puede ya que cada elemento de $F[X]$ se puede escribir como producto de irreducibles. Por el *primer teorema de Kronecker* existe un campo K tal que $\alpha \in K$ y $p(\alpha) = 0$, con ello $p(x) = (x - \alpha) \cdot g(x)$ y así $f(x) = (x - \alpha) \cdot g(x) \cdot h(x)$. Por hipótesis inductiva existe un campo $F \subseteq E$ en el que $g(x) \cdot h(x)$ se descompone como un producto de factores lineales, es decir que f se escribe como un producto de factores lineales en E. □

Usando el *lema de Zorn*, podemos demostrar la existencia de un campo $\overline{K}$, tal que cualquier polinomio $f \in K[X]$ pueda escribirse como producto de factores lineales, pues la relación de *ser subcampo de* es un orden parcial que cumple las hipótesis del *lema de Zorn.*

Definición 2.65. *Sea F un subcampo de E y sea $f(x) \in F[X]$. Decimos que f se escinde sobre E, si existen $\alpha_1, \ldots, \alpha_n \in E$, tales que $f(x) = a(x - \alpha_1) \cdot (a - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$.*
Sean F un subcampo de E y $f(x) \in F[X]$. Entonces E/F es llamado campo de descomposición de $f(x)$ sobre E, si $f(x)$ se escinde sobre E pero no se escinde sobre ningún subcampo de E.

Teorema 2.66. *Si F es un campo , entonces todo polinomio $f(x) \in F[X]$ tiene un campo de descomposición*

Demostración: Por el *segundo teorema de Kronecker*, existe un campo K/F en el cual $f(x)$ se encinde. Sean $\alpha_1, \ldots, \alpha_n$ todas las raices del polinomio f en K y consideremos a $E = F(\alpha_1, \ldots, \alpha_n) = \cap\{E' \subseteq K \mid E' \text{ es un campo, } F \subseteq E' \text{ y } \alpha_1, \ldots, \alpha_n \in E'\}$ (dicho campo es el mínimo campo que contiene a F y todas las raíces de f). Por lo que E es el campo de descomposición de f. □

Nota 2.67. *Sean $\varphi : F \longrightarrow F'$ un isomorfismo de campos y $\varphi^* : F[X] \longrightarrow F'[X]$ una función definida como $\varphi^*(a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n) = \varphi(a_0) + \varphi(a_0) \cdot x + \ldots + \varphi(a_n)x^n$. Demostremos que $p(x) \in F[X]$ irreducible, si y solo sí $p^*(x) = \varphi^*(p(x)) \in F'[X]$ también lo es. Para ello, probemos que $\varphi^* : F[X] \longrightarrow F'[X]$ es un isomorfismo. Sean $f, g \in F[X]$ tales que $f(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$ y $g(x) = b_0 + b_1 \cdot x + \ldots + b_m \cdot x^m$, sin pérdida de la generalidad podemos suponer que $m > n$ y con ello sea $a_j = 0$ para cada $m \geq j > n$, así tenemos que $\varphi^*((f+g)(x)) = \varphi^*(\sum_{i=1}^{m}(a_i + b_i) \cdot x^i) = \sum_{i=1}^{m}\varphi(a_i + b_i) \cdot x^i = \sum_{i=1}^{m}(\varphi(a_i) + \varphi(b_i)) \cdot x^i = \sum_{i=1}^{m}(\varphi(a_i) \cdot x^i) + \sum_{i=1}^{m}(\varphi(b_i) \cdot x^i) = \varphi^*(f) + \varphi^*(g)$. Por*

otro lado $\varphi^*((f\cdot g)(x)) = \varphi^*(\sum_{i=1}^{n+m} r_i\cdot x^i)$*, donde* $r_i = \sum_{j=0}^{i} a_j\cdot b_{i-j}$*, así se tiene que* $\varphi^*(\sum_{i=1}^{n+m} r_i\cdot x^i) = \sum_{i=1}^{n+m}\varphi(r_i)\cdot x^i = \sum_{i=1}^{n+m}\varphi(\sum_{j=0}^{i} a_j\cdot b_{i-j})\cdot x^i = \sum_{i=1}^{n+m}(\sum_{j=0}^{i}\varphi(a_j)\cdot\varphi(b_{i-j})\cdot x^i) = \varphi(f(x))\cdot\varphi(g(x))$*. Es claro que* φ^* *es suprayectivo. Por otro lado,* $Ker(\varphi^*) = \{t(x)\in F[X]\,|\,\varphi^*(t(x)) = 0\} = \{t(x) = c_0 + c_1\cdot x + \ldots + c_n\cdot x^n = 0\,|\,\varphi(t(x)) = 0\}$*, al ser* φ *un monomorfismo y* $0 = \varphi^*(t(x)) = \varphi(c_0) + \varphi(c_1)\cdot x + \ldots + \varphi(c_n)\cdot x^n$*, entonces* $c_i = 0$ *para cada* $i\in\{1,\ldots,n\}$*. Por lo tanto* $Ker(\varphi^*) = \{0\}$*.*

Luego por contrarrecíproca suponiendo que $p^*(x)$ *es reducible entonces existen* $f^*, g^*\in F'[X]$ *tales que* $\varphi^*(p(x)) = p^*(x) = f^*(x)\cdot g^*(x) = \varphi^*(f(x)\cdot g(x))$*,* $0 < gr(f^*) < gr(p^*)$ *y* $0 < gr(g^*) < gr(p^*)$*. Entonces* $p(x) = f(x)\cdot g(x)$*,* $0 < gr(f) < gr(p)$ *y* $0 < gr(g) < gr(p)$*, es decir que* p *es reducible. De manera similar obtenemos que si* p^* *es irreducible, entonces* $p(x)$ *es irreducible.*

Lema 2.68. *Sea* $\varphi : F\longrightarrow F'$ *un isomorfismo de campos y* $\varphi^* : F[X]\longrightarrow F'[X]$ *definida por* $\varphi^*(a_0 + a_1\cdot x + \ldots + a_n\cdot x^n) = \varphi(a_0) + \varphi(a_0)\cdot x + \ldots + \varphi(a_n)x^n$*. Sean* $p(x)\in F[X]$ *irreducible,* $p^*(x) = \varphi^*(p(x))\in F'[X]$*. Si* β *es una raíz de* $p(x)$ *y* β' *es una raíz de* $p^*(x)$*, entonces existe un único isomorfismo* $\overline{\varphi} : F(\beta)\longrightarrow F'(\beta')$ *que extiende a* φ *con* $\overline{\varphi}(\beta) = \beta'$*. Es decir el siguiente diagrama conmuta:*

$$\begin{array}{ccc} F(\beta) & \overset{\overline{\phi}}{\dashrightarrow} & F'(\beta') \\ \uparrow & & \uparrow \\ F & \xrightarrow[\varphi]{} & F' \end{array}$$

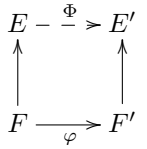
Demostración: Como φ^* es un isomorfismo y p^* es irreducible. Entonces, φ^* induce un isomorfismo $\Psi : F[X]/(p(x))\longrightarrow F'[X]/(p^*(x))$ tal que para cada $c\in F$, $\Psi(c + (p(x))) = c + (p^*(x))$ y $\Psi(x + (p(x))) = x + (p^*(x))$. Como β es algebraico sobre F y β' es algebraico sobre F', por la *proposición 2.62*, existen isomorfismos $\phi_1 : F[X]/(p(x))\longrightarrow F(\beta)$ y $\phi_2 : F'[X]/(p^*(x))\longrightarrow F'(\beta')$ de tal manera que ϕ_1 fija a F y ϕ_2 fija a F', obteniendo el siguiente diagrama:

$$\begin{array}{ccc} F(\beta) & & F'(\beta') \\ {\scriptstyle\phi_1}\uparrow\ \downarrow{\scriptstyle\phi^{-1}} & & {\scriptstyle\phi_2}\uparrow \\ F[X]/(p(x)) & \xrightarrow{\Psi} & F'[X]/(p^*(x)) \\ \uparrow{\scriptstyle\nu_1} & & \uparrow{\scriptstyle\nu_2} \\ F[X] & \xrightarrow{\varphi^*} & F'[X] \\ \uparrow & & \uparrow \\ F & \xrightarrow[\varphi]{} & F' \end{array}$$

Sea $\overline{\varphi} = (\phi_2\circ\Psi)\circ\phi^{-1}$, entonces $\overline{\varphi}$ es un isomorfismo. Para cada $c\in F\subseteq F(\beta)$, $\overline{\varphi}(c) = (\phi_2\circ\Psi)\circ\phi^{-1}(c) = (\phi_2\circ\Psi)(\phi^{-1}(c)) = (\phi_2\circ\Psi)(c + (p(x))) = \phi_2(\Psi(c + (p(x)))) = \phi_2(\varphi(c) + (p^*(x))) = \varphi(c)$. Es decir que $\overline{\varphi}|_F = \varphi$.

Notemos que $\overline{\varphi}$ es único. Suponiendo que existe otro isomorfismo $G : F(\beta)\longrightarrow F'(\beta')$ que extiende a φ y tal que $G(\beta) = \beta'$, entonces $G|_F = \varphi$. Puesto que $Id_F : F\longrightarrow F(\beta)$ es un isomorfismo, en particular un epimorfismo. Como $G\circ Id_F = G|_F = \varphi = \overline{\varphi}|_F = \overline{\varphi}\circ Id_F$, entonces $G = \overline{\varphi}$. Por lo tanto existe un único isomorfismo $\overline{\varphi} : F(\beta)\longrightarrow F'(\beta')$ que extiende a φ, donde $\overline{\varphi}(\beta) = \beta'$. □

Teorema 2.69. *Sea* $f(x)\in F[X]$ *un polinomio cualquiera y* E *su campo de descomposición sobre* F*. Sea* $\varphi : F\longrightarrow F'$ *un isomorfismo de campos y* $\varphi^* : F[X]\longrightarrow F'[X]$ *definida como en el lema anterior. Sea* E' *el campo de descomposición de* f^* *sobre* F'*. Entonces existe un isomorfismo* $\Phi : E\longrightarrow E'$ *que extiende a* φ*, es decir el siguiente diagrama conmuta:*



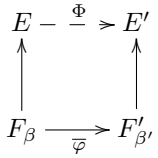
Demostración: La prueba se hará por inducción sobre el numero n de raíces de f sobre E.

Si $n = 1$, entonces f es un polinomio lineal y con ello sea $E = F$. Así no es difícil ver que f se escinde sobre $F[X]$, de modo que f^* se escinde sobre $F'[X]$. Solo basta tomar a $\varphi = \Phi$.

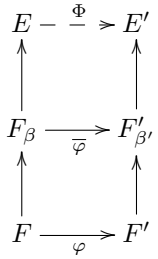
Ahora supongamos que para cada numero natural k existe un isomorfismo $\Phi : E \longrightarrow E'$ que extiende a φ.

Ahora, probemos que tal propiedad se cumple para $n = k + 1$. Sean $p \in F[X]$ un polinomio irreducible que divide al polinomio f y $\beta_1, \ldots, \beta_{k+1} \in E$ raíces de f. Sea β una raíz de p en E y consideremos una raíz β' del polinomio $p^*(x) = \varphi^*(p(x))$ en E'. Por el lema anterior, existe un único isomorfismo $\overline{\varphi} : F(\beta) \longrightarrow F'(\beta')$ tal que $\overline{\varphi}(\beta) = \beta'$ y $\overline{\varphi}|_F = \varphi$.

Puesto que $F \subseteq F(\beta) = F_\beta$, entonces $F[X] \subseteq F_\beta[X]$. Consecuentemente, $F_\beta(\beta_1, \ldots, \beta_{k+1}) = F(\beta, \beta_1, \ldots, \beta_{k+1}) = F(\beta_1, \ldots, \beta_{k+1}) = E$, es decir que E es el campo de descomposición de f sobre F_β. De manera similar E' es el campo de descomposición de f^* sobre $F'_{\beta'} = F'(\beta')$. Por hipótesis inductiva existe un isomorfismo Ψ que extiende a $\overline{\varphi}$, es decir el siguiente diagrama conmuta:



También notemos que Φ extiende a φ:



□

Proposición 2.70. *Sean L/E y E/K extensiones finitas, entonces L/K es finita*

Demostración: Sean $[E : L] = m$ y $[K : E] = n$. Entonces, existen $\beta_1 \subseteq L$ base de L/E y $\beta_2 \subseteq E$ base de E/K, con ello sean $\beta_1 = \{\alpha_1, \ldots, \alpha_m\}$ y $\beta_2 = \{\gamma_1, \ldots, \gamma_n\}$. Afirmamos que $\beta = \{\alpha_i \cdot \gamma_j \,|\, i \in \{1, \ldots, m\},\, j \in \{1, \ldots, n\}\}$ es base de L/K.

Probemos, que β genera a L/K. Para cada $x \in L$, existen $a_1, \ldots, a_m \in E$ tales que $x = a_1 \cdot \alpha_1 + \ldots + a_m \cdot \alpha_m$ (pues β_1 es base de L/E). Análogamente, existen $b_{i_1}, \ldots, b_{i_n} \in K$ tales que $a_i = b_{i_1} \cdot \gamma_1 + \ldots + b_{i_n}\gamma_n$ (pues β_2 es base de E/K). Por lo cual, $x = \sum_{i=1}^{m}(\sum_{j=1}^{n} b_{i_j} \cdot (\alpha_i \cdot \gamma_j))$ es decir que β genera a L/K.

Ahora, demostremos que β es linealmente independiente. Para ello, sean $a_{i_j} \in K$ tales que $\sum_{i=1}^{m}(\sum_{j=1}^{n} a_{i_j} \cdot (\alpha_i \cdot \gamma_j)) = 0$, usando la propiedad distributiva $\sum_{i=1}^{m}(\sum_{j=1}^{n} a_{i_j} \cdot (\alpha_i \cdot \gamma_j)) = \sum_{i=1}^{m} \alpha_i \cdot (\sum_{j=1}^{n} a_{i_j} \cdot \gamma_j)$ y como β_1 es linealmente independiente para cada $i \in \{1, \ldots, m\}$, $\sum_{j=1}^{n} a_{i_j} \cdot \gamma_j = 0$. Análogamente, $a_{i_j} = 0$ para cada $j \in \{1, \ldots, n\}$. Por lo tanto β es base de L/K y $[E : L][K : E] = mn = [E : K]$. □

Las pruebas anteriores nos aseguran que las extensiones de un campo K donde f se escribe como producto de polinomios lineales son isomorfos. Dichas pruebas las usaremos para demostrar que las clausuras algebraicas de un campo K son isomorfas.

Definición 2.71. *Sea E/F una extensión algebraica. Un polinomio irreducible $p(x)$ es llamado separable si no tiene raíces repetidas. Un polinomio $f(x)$ es separable si cada uno de sus factores irreducibles es separable.*

Sea $(E,+,\cdot)$ un campo que tiene a $(F,+,\cdot)$ como subcampo. Un automorfismo de E es un isomorfismo $\sigma : E \longrightarrow E$. Diremos que σ fija a F, si $\sigma(\alpha) = \alpha$ para $\alpha \in F$.

Proposición 2.72. *Sean $(F,+,\cdot)$ un subcampo de $(E,+,\cdot)$, $f(x) = x^n + \ldots + a_1 \cdot x + a_0 \in K[X]$. Tambien sea $(K,+,\cdot)$ el campo de descomposición de f. Si $\sigma : E \longrightarrow E$ es un automorfismo fija a F, entonces σ permuta el conjunto de raíces $Z = \{z_1, \ldots, z_n\}$ de f.*

Demostración: Si $r \in K$, es una raíz de f, entonces $0 = f(r) = r^n + \ldots + a_1 \cdot r + a_0$. Puesto que σ fija a F, $0 = \sigma(r)^n + \ldots + \sigma(a_1)\sigma(r) + \sigma(a_0) = \sigma(r)^n + \ldots + a_1\sigma(r) + a_0 = f(\sigma(r))$ con ello $\sigma(r)$ es una raíz de f. Por lo tanto $\sigma|_Z : Z \longrightarrow Z$ es una función biyectiva (esto se debe porque σ lo es), y como $|Im(\sigma|_Z)| = |Z| = |Dom(\sigma|_Z)|$, entonces $\sigma|_Z$ es biyectiva. □

Lema 2.73. *Sea $E = F(\beta_1, \ldots, \beta_n)$. Si $\sigma : E \longrightarrow E$ es un automorfismo que fija a F. Si para cada $i \in \{1, \ldots, n\}$ $\sigma(\beta_i)$, entonces $\sigma = Id_E$*

Demostración:

Haremos la prueba por inducción sobre n.

Si $n = 1$, entonces $E = F(\beta_1)$. Sea $a_k \cdot \beta_1^k + \ldots + a_1 \cdot \beta_1 + a_0 \in E$. Entonces, $\sigma(a_k \cdot \beta_1^k + \ldots + a_1 \cdot \beta_1 + a_0) = \sigma(a_k) \cdot \sigma(\beta_1^k) + \ldots + \sigma(a_1) \cdot \sigma(\beta_1) + \sigma(a_0) = a_k \cdot \beta_1^k + \ldots + a_1 \cdot \beta_1 + a_0$. Por lo tanto $\sigma = Id_E$

Supongamos que se cumple la hipótesis para $K = F(\beta_1, \ldots, \beta_{n-1})$. Sea $E = K(\beta_n) = F(\beta_1, \ldots, \beta_{n-1})(\beta_n) = F(\beta_1, \ldots, \beta_n)$. Con ello, E es el menor campo que contiene a K y a β_n. Sea σ un automorfismo que fija a F, tal que $\sigma(\beta_i) = \beta_i$ para cada $i \in \{1, \ldots, n\}$. Sea $a_m \cdot \beta_n^m + \ldots + a_1\beta_n + a_0 \in E$ con $a_i \in K$. Entonces, por hipótesis inductiva $\sigma(a_m \cdot \beta_n^m + \ldots + a_1 \cdot \beta_n + a_0) = \sigma(a_m) \cdot \sigma(\beta_n^m) + \ldots + \sigma(a_1) \cdot \sigma(\beta_n) + \sigma(a_0) = a_m \cdot \sigma(\beta_n^m) + \ldots + a_1 \cdot \sigma(\beta_n) + a_0 = a_m \cdot \beta_n^m + \ldots + a_1\beta_n + a_0$. Por lo tanto $\sigma = Id_E$

□

Proposición 2.74. *Sea E/F un campo de descomposición de un polinomio separable $f \in F[X]$ $(f(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n)$. Sean $\varphi : F \longrightarrow F'$ un isomorfismo y $f^*(x) = \varphi(a_0) + \varphi(a_1) \cdot x + \ldots + \varphi(a_n) \cdot x^n$. Entonces existen $[F : E]$ isomorfismos que extienden a φ.*

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow[\varphi]{} & F' \end{array}$$

Demostración: Haremos la prueba por inducción sobre $[F : E]$.

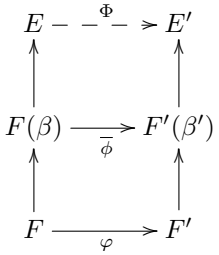
Si $[F : E] = 1$, entonces $E = F$ y bastaría tomar a $\Phi = \varphi$.

Ahora si $[F : E] > 0$, supongamos que $f(x) = p(x)g(x)$ donde p es un polinomio irreducible y $gr(p) = d$.

- Si $d = 1$. Por el *segundo teorema de kronecker*, existen E/K y K/F campos de descomposición de p y g respectivamente. Como $d = 1$, p es lineal y así $[F : K] = [E : K][K : F] = [K : F]$.

- Si $d > 1$, Sean β una raíz de $p(x)$ y $\Psi : E \longrightarrow E'$ un isomorfismo que extiende a φ. Entonces, $\Psi(\beta) = \beta'$ es una raíz de f y puesto f^* es separable, por *Proposición 2.72*, p^* tiene exactamente d raíces $\beta' \in E'$. Por *Lema 2.68* y *Lema 2.73*, hay exactamente d isomorfismos $\overline{\phi} : F(\beta) \longrightarrow F'(\beta)$ que extienden a φ, fijan a F y tales que $\overline{\varphi}(\beta) = \beta'$ para cada $\beta \in E$. Por un lado notemos que E es el campo de descomposición de $f(x)$ sobre $F(\beta)$ y E' es el campo de descomposición de $f^*(x)$ sobre $F'(\beta')$.

  Dado que $[F : E] = [F : F(\beta)][F(\beta) : E] = d[F(\beta) : E]$, entonces $[F(\beta) : E] = \frac{[F:E]}{d} = k$. Entonces por hipótesis inductiva tenemos que los d isomorfismos $\overline{\phi}$ tiene exactamente k isomorfismos los extienden. Por lo tanto φ tiene exactamente $[F : E]$ extensiones Φ.



□

Proposición 2.75. *Dado un anillo $(R, +, \cdot)$ y un ideal I del mismo anillo, entonces las siguientes propiedades son equivalentes:*

a) I es un ideal primo.

b) $(R/I, +, \cdot)$ es un dominio entero.

Demostración:

- ***a)* $\Rightarrow$ *b)*** Sean $a + I, b + I \in R/I$ tales que $(a \cdot b) + I = (a + I) \cdot (b + I) = I = 0_{R/I}$, esto pasa si y solo sí $a \cdot b \in I$. Pero I es un ideal primo, con lo cual $a \in I$ ó $b \in I$, esto implica que $a + I = 0_{R/I}$ ó $b + I = I = 0_{R/I}$. Por lo tanto R/I es dominio entero.
- ***b)* $\Rightarrow$ *a)*** Sean $a, b \in R$ tales que $a \cdot b \in I$, entonces $I = (a \cdot b) + I = (a + I) \cdot (b + I)$. Pero R/I es dominio entero, con ello $a + I = I$ ó bien $b + I = I$, esto implica que $a \in I$ ó $b \in I$. Así, I es un ideal primo. □

Dado dominio entero $(R, +, \cdot)$, definimos al conjunto $R^* = R\backslash\{0\}$ y a la relación $\sim$ sobre el conjunto $R \times R^*$ tal que:

$$(a, b) \sim (x, y) \text{ si y solo sí } a \cdot y = b \cdot x$$

Proposición 2.76. *La relación $\sim$ es de equivalencia.*

Demostración:

Sea $(a, b) \in R \times R^*$, puesto que $\cdot$ es una operación conmutativa, $a \cdot b = b \cdot a$ lo cual sucede si y solo sí $(a, b) \sim (a, b)$. Por lo tanto $\sim$ es reflexiva.

Sean$(a, b), (x, y) \in R \times R^*$ tales que $(a, b) \sim (x, y)$, entonces $a \cdot y = b \cdot x$ y en consecuencia $x \cdot b = y \cdot a$, es decir que $(x, y) \sim (a, b)$. Por lo tanto $\sim$ es simétrica.

Sean $(a, b), (x, y), (m, n) \in R \times R^*$ tales que $(a, b) \sim (x, y)$ y $(x, y) \sim (m, n)$, con lo cual tenemos que $a \cdot y = b \cdot x$ y $x \cdot n = y \cdot m$, luego $(a \cdot n) \cdot y = (a \cdot y) \cdot n = (b \cdot x) \cdot n = b \cdot (x \cdot n) = b \cdot (y \cdot m) = (b \cdot m) \cdot y$, esto implica que $a \cdot n = b \cdot m$, es decir que $(a, b) \sim (m, n)$. Por lo tanto $\sim$ es transitiva.

□

Al cada clase de equivalencia del elemento (a, b) la denotamos por $\frac{a}{b}$ y sea $F = R \times R^*/\sim$. Luego definamos las siguientes operaciones $+ : F \times F \longrightarrow F$ y $\cdot : F \times F \longrightarrow F$:

$$\frac{a}{b} + \frac{x}{y} = \frac{a \cdot y + x \cdot b}{b \cdot y} \text{ y } \frac{a}{b} \cdot \frac{x}{y} = \frac{a \cdot x}{b \cdot y}$$

Probemos que dichas operaciones están bien definidas, para ello sean $(\frac{a}{b}, \frac{c}{d}), (\frac{a'}{b'}, \frac{c'}{d'}) \in F \times F$, tales que $(\frac{a}{b}, \frac{c}{d}) = (\frac{a'}{b'}, \frac{c'}{d'})$. Demostremos que $\frac{a \cdot d + b \cdot c}{b \cdot d} = \frac{a' \cdot d' + b' \cdot c'}{b' \cdot d'}$ y $\frac{a \cdot c}{b \cdot d} = \frac{a' \cdot c'}{b' \cdot d'}$.

Puesto que $(\frac{a}{b}, \frac{c}{d}) = (\frac{a'}{b'}, \frac{c'}{d'})$, entonces $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$, por definición $a \cdot b' = a' \cdot b$ y $c \cdot d' = c' \cdot d$, por consiguiente $(a \cdot b') \cdot d \cdot d' = (a' \cdot b) \cdot d \cdot d'$ y $(c \cdot d') \cdot b \cdot b' = (c' \cdot d) \cdot b \cdot b'$, con ello $(a \cdot b') \cdot d \cdot d' + (c \cdot d') \cdot b \cdot b' = (a' \cdot b) \cdot d \cdot d' + (c' \cdot d) \cdot b \cdot b'$, usando la *ley distributiva* obtenemos que $(a \cdot d + b \cdot c) \cdot (b' \cdot d') = (a' \cdot d' + b' \cdot c') \cdot b \cdot d$ lo cual sucede si y solo sí $\frac{a \cdot d + b \cdot c}{b \cdot d} = \frac{a' \cdot d' + b' \cdot c'}{b' \cdot d'}$.

Puesto que $a \cdot b' = a' \cdot b$ y $c \cdot d' = c' \cdot d$, entonces $(a \cdot c) \cdot b' \cdot d' = (a \cdot b') \cdot c \cdot d' = (a' \cdot b) \cdot c' \cdot d = (a' \cdot c') \cdot b \cdot d$ lo cual sucede si y solo sí $\frac{a \cdot c}{b \cdot d} = \frac{a' \cdot c'}{b' \cdot d'}$.

Proposición 2.77. $(F, +, \cdot)$ *es un campo.*

Demostración:

Probemos que $(F, +)$ es un grupo abeliano. Anteriormente, demostramos que $+$ es una operación cerrada sobre el conjunto F, bastaría ver las otras propiedades. Ahora, probemos que la operación suma es asociativa, para ello sean $\frac{u}{v}, \frac{a}{b}, \frac{c}{d} \in F$, entonces $\frac{u}{v} + (\frac{a}{b} + \frac{c}{d}) = \frac{u}{v} + (\frac{a \cdot d + b \cdot c}{b \cdot d}) = \frac{u \cdot (b \cdot d) + v \cdot (a \cdot d + b \cdot c)}{v \cdot (b \cdot d)} = \frac{(u \cdot (b \cdot d) + v \cdot (a \cdot d)) + (v \cdot b) \cdot c}{(v \cdot b) \cdot d} = \frac{(u \cdot b + v \cdot a) \cdot d + (v \cdot b) \cdot c}{(v \cdot b) \cdot d} = \frac{(u \cdot b + v \cdot a)}{v \cdot b} + \frac{c}{d} = (\frac{u}{v} + \frac{a}{b}) + \frac{c}{d}$. Además, $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} = \frac{c \cdot b + d \cdot a}{d \cdot b} = \frac{c}{d} + \frac{a}{b}$ es decir que la operación suma es conmutativa. Ahora, proponemos a $\frac{0_R}{1_R} \in F$ como el elemento neutro de la operación suma. Pues para cada $\frac{a}{b} \in F$, se tiene que $\frac{a}{b} + \frac{0_R}{1_R} = \frac{a \cdot 1_R + b \cdot 0_R}{b \cdot 1_R} = \frac{a}{b}$. Por otro lado, para cada $\frac{a}{b} \in F$, consideremos $\frac{-a}{b} \in F$, entonces $\frac{a}{b} + \frac{-a}{b} = \frac{a \cdot b + (-a) \cdot b}{b \cdot b} = \frac{0_R}{b^2}$, pero $b^2 \cdot 0_R = 0_R = 1_R \cdot 0_R$. Por lo tanto $\frac{0_R}{1_R} = \frac{0_R}{b^2}$.

Ahora, probemos que $(F \backslash \{0\}, \cdot)$ es un grupo abeliano. Demostremos que la multiplicación es asociativa, pues para cualesquiera $\frac{u}{v}, \frac{a}{b}, \frac{c}{d} \in F$, tenemos que $\frac{u}{v} \cdot (\frac{a}{b} \cdot \frac{c}{d}) = \frac{u}{v} \cdot \frac{a \cdot c}{b \cdot d} = \frac{u \cdot (a \cdot c)}{v \cdot (b \cdot d)} = \frac{(u \cdot a) \cdot c}{(v \cdot b) \cdot d} = (\frac{u \cdot a}{v \cdot b}) \frac{c}{d} = (\frac{u}{v} \cdot \frac{a}{b}) \cdot \frac{c}{d}$, además $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} = \frac{c \cdot a}{d \cdot b} = \frac{c}{d} \cdot \frac{a}{b}$, es decir que la operación $\cdot$ es conmutativa. Consideremos a $\frac{1_R}{1_R} \in F$ como elemento neutro de la multiplicación, pues para cada $\frac{a}{b} \in F$, $\frac{a}{b} \cdot \frac{1_R}{1_R} = \frac{a \cdot 1_R}{b \cdot 1_R} = \frac{a}{b}$. Como $(a \cdot b) \cdot 1_R = 1_R \cdot (b \cdot a)$ $(\frac{1_R}{1_R} = \frac{a \cdot b}{b \cdot a})$, entonces $\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{1_R}{1_R}$. Por lo tanto $\frac{b}{a} \in F$ es el inverso multiplicativo de $\frac{a}{b} \in F$.

Ahora, demostraremos la distribución del producto sobre la suma. Para cada $\frac{a}{b}, \frac{u}{v}, \frac{c}{d} \in F$, $\frac{a}{b} \cdot (\frac{u}{v} + \frac{c}{d}) = \frac{a}{b} \cdot (\frac{u \cdot d + c \cdot v}{v \cdot d}) = \frac{a \cdot (u \cdot d + c \cdot v)}{b \cdot (v \cdot d)} = \frac{a \cdot (u \cdot d) + a \cdot (c \cdot v)}{b \cdot (v \cdot d)} = \frac{a \cdot (u \cdot d)}{b \cdot (v \cdot d)} + \frac{a \cdot (c \cdot v)}{b \cdot (v \cdot d)} = \frac{a \cdot u}{b \cdot v} + \frac{a \cdot c}{b \cdot d} = \frac{a}{b} \cdot \frac{u}{v} + \frac{a}{b} \cdot \frac{c}{d}$. Por lo tanto $(F, +, \cdot)$ es un campo al cual llamaremos *campo de cocientes del dominio entero R.*

□

Definimos la función $\varphi : R \longrightarrow F$ tal que $\varphi(r) = \frac{r}{1_R}$. Entonces para cada $x, y \in R$, $\varphi(x + y) = \frac{x + y}{1_R} = \frac{x \cdot 1_R + y \cdot 1_R}{1_R} = \frac{x}{1_R} + \frac{y}{1_R} = \varphi(x) + \varphi(y)$, además $\varphi(x \cdot y) = \frac{x \cdot y}{1_R} = \frac{x \cdot y}{1_R \cdot 1_R} = \frac{x}{1_R} \cdot \frac{x}{1_R} = \varphi(x) \cdot \varphi(y)$. Esto prueba que φ es un morfismo de anillos. Probemos que φ es un monomorfismo. Para ello, sean $x, y \in R$ tales que $\frac{x}{1_R} = \varphi(x) = \varphi(y) = \frac{y}{1_R}$, entonces $x = x \cdot 1_R = 1_R \cdot y = y$. Por lo tanto φ es morfismo inyectivo, es decir un monomorfismo y en consecuencia $(R, +, \cdot)$ se sumerge en $(F, +, \cdot)$.

Definición 2.78. *Decimos que un campo es algebraicamente cerrado si para cualquier polinomio $f \in F[X]$, entonces F contiene todas las raíces de f.*

En el libro *Algebra* del autor *Serge Lang* [10], se demuestra que todo campo está contenido en un campo algebraicamente cerrado. Dicha prueba usa un resultado que establece que *todo ideal*

propio de un anillo conmutativo $(R,+,\cdot)$ *está contenido en un ideal maximal*, dicho resultado es equivalente al *Axioma de elección*.

Para probar que todo campo está contenido en un campo algebraicamente cerrado sin usar el *Axioma de elección* ó alguna de sus equivalencias. Usaremos el *lema de Cowen-Engeler* para probar que *todo ideal propio de un anillo conmutativo* $(R,+,\cdot)$ *está contenido en un ideal primo*. Posteriormente, la prueba expuesta en el libro de *Serge Lang* se modificará por lo antes mencionado.

Para demostrar el siguiente resultado, es necesario definir el concepto de subsemigrupo parcial, esta definición puede consultarla en [8].

Definición 2.79. *Decimos que una relación* p *de* A *a* B *es una función parcial si para cada* $(a,b),(a,c)\in p$, *entonces* $b=c$. *Es decir que hay como máximo un elemento* $b\in B$ *tal que* afb.

Decimos que una relación binaria $*$ de $X\times X$ a X es una operación parcial si $*$ es una función parcial.

Ejemplo 2.80. *Consideremos el conjunto de los números impares* $2\mathbb{Z}+1$ *y la* $+$ *suma usual de los números naturales, entonces* $+$ *es una operación parcial sobre* $2\mathbb{Z}+1$.

Definición 2.81. *Dado un conjunto* S *y* $\cdot$ *una operación binaria parcial sobre* S. *Entonces decimos que* $(S,\cdot)$ *es un semigrupo parcial si para cualesquiera* $x,y,z\in S$ *tales que* $x\cdot y, y\cdot z\in S$, *se cumple:*

- $(x\cdot y)\cdot z\in S$ *si y solo sí* $x\cdot(y\cdot z)\in S$.
- $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ *si* $x\cdot(y\cdot z)\in S$

Naturalmente, si $(G,*)$ es un grupo y $S\subseteq G$, entonces $(S,*|_S)$ es un semigrupo parcial

Definición 2.82. *Sea* $(R,+,\cdot)$ *un anillo. Decimos que* $(I,+)$ *es un ideal parcial izquierdo, si* $\cdot$ *es una operación parcial de* $R\times I$ *a* I *y* $(I,+)$ *es un semigrupo parcial tal que:*

- *Para cualesquiera* $x,y\in I$, *si* $x+y\in S$ *entonces* $y+x=x+y$.

Análogamente, definimos de manera similar a los ideales parciales derechos y los ideales parciales (bilaterales).

Teorema 2.83. *Dado un anillo* $(R,+,\cdot)$ *conmutativo con uno y un ideal propio* I. *Existe un ideal primo* P *tal que* $I\subseteq P$.

Demostración: Podemos suponer, sin perdida de generalidad que $1_R\notin I$. Por otro lado, sea $S=\{1_R\}$, entonces $(S,\cdot)$ es un subsemigrupo de $(R,\cdot)$ tal que $S\cap I=\emptyset$. Nuestro siguiente objetivo es extender al ideal I a un ideal primo P. Para ello, construiremos una familia de funciones ξ tal que para cada $\varphi\in\xi$, $Dom(\varphi)\subseteq R$, $Rang(\varphi)=\{0,1\}$ y:

a) Para cada $a\in I$, si $a\in Dom(\varphi)$, entonces $\varphi(a)=0$.

b) Si $a,b,a-b\in Dom(\varphi)$ y $\varphi(a)=0=\varphi(b)$, entonces $\varphi(a-b)=0$.

c) Si $a,ar\in Dom(\varphi)$ y $\varphi(a)=0$, entonces $\varphi(ar)=0$

d) Si $1_R\in Dom(\varphi)$, entonces $\varphi(1_R)=1$.

e) Si $x,y,xy\in Dom(\varphi)$ y $\varphi(x)=1=\varphi(y)$, entonces $\varphi(xy)=1$

Para cada subconjunto finito F de R, definimos a $\varphi_F\in\xi$ tal que $Dom(\varphi_F)=F$. Entonces podemos suponer que F es de la forma:

$$F=\{x_1,\ldots,x_q\}$$

Si $x_i\cdot x_j\notin I$ para cada $i,j\in\{1,\ldots,q\}$, sea φ_F tal que $\varphi_F(x_i)=1$ para cada $x_i\in F$, en consecuencia φ_F cumple las condiciones $a)-e)$. Ahora, si $I_F=F\cap I$ y $F=I_F\cup S$, sea φ_F tal que para cada $x_i\in I_F$, $\varphi_F(x_i)=0$, entonces φ_F cumple las condiciones $a)-e)$. Por otro lado, si existen i,j tales que $x_i\cdot x_j\in I$, consideremos los siguientes conjuntos:

- R_F el subanillo de R generado por el conjunto F y
- $\mathcal{I}_F$ el ideal generado por el conjunto I_F del anillo R_F.

Puesto que $\mathcal{I}_F$ es el menor ideal del anillo R_F que contiene al conjunto $I_F \subseteq I$, entonces $\mathcal{I}_F \subseteq I$ y $\mathcal{I}_F \cap S = \emptyset$. Consideremos el conjunto $\Psi_F = \{J \text{ ideal de } R_F \,|\, \mathcal{I}_F \subseteq J \text{ y } J \cap S = \emptyset\}$. Sean $J_F \in \Psi_F$ el ideal que contiene la cantidad máxima de elementos del conjunto $F = \{x_1, \ldots, x_q\}$ y $P_F = J_F \cap F$. Entonces, $F \backslash P_F = (R_F \backslash J_F) \cap F$ y como J_F es un ideal, $(P_F, +)$ es un ideal parcial. Ahora, suponiendo que $F \backslash P_F = \emptyset$, definimos a $\varphi_F(x) = 0$ para cada $x \in F$ y entonces φ_F cumple las condiciones $a) - e)$. Por otro lado sí $F \backslash P_F \neq \emptyset$, demostremos que $(F \backslash P_F, \cdot)$ es un semigrupo parcial. Supongamos que no es un semigrupo parcial, entonces existen $y_1, y_2 \in F \backslash P_F$ tales que $y_1 \cdot y_2 \in F$ y $y_1 \cdot y_2 \notin F \backslash P_F$. Esto implica que $y_1 \cdot y_2 \in J_F$. Por la maximalidad de J_F puesto que $y_1, y_2 \notin J_F$, se sigue que $1_R \in I(J_F \cup \{y_1\})$. Con lo cual, existen $j_1, \ldots, j_m \in J_F$ y $b_1, \ldots, b_m, b \in R$ tales que $1_R = b_1 \cdot j_1 + \ldots + b_m \cdot j_m + b \cdot y_1$. Consecuentemente $1_R - b \cdot y_1 = b_1 \cdot j_1 + \ldots + b_m \cdot j_m \in J_F$, pero J_F es un ideal, con ello $y_2 - b \cdot y_1 \cdot y_2 = (1_R - b \cdot y_1) \cdot y_2 \in J_F$ y $b \cdot y_1 \cdot y_2 \in J_F$. Obteniendo una contradicción, pues $y_2 \notin J_F$. Por lo tanto $y_1 \cdot y_2 \in F \backslash P_F$ y con ello $(F \backslash P_F, \cdot)$ es un semigrupo parcial. Con el argumento anterior, definimos a $\varphi_F(x) = 0$ si $x \in P_F$ y $\varphi_F(x) = 1$ si $x \in F \backslash P_F$, en consecuencia φ_F cumple las condiciones $a) - e)$. Ahora, si F' es un conjunto finito $\varphi_{F'} \in \xi$ sí es alguna de las funciones definidas anteriormente ó bien $\varphi_{F'} = \varphi_F|_{F'}$, donde $\varphi_F \in \xi$.

Para cada $T \subseteq R$, sea $\mathcal{F} = \{F \subseteq T \,|\, F \text{ es finito}\}$. Análogamente siguiendo la misma idea del párrafo anterior, para cada $F \in \mathcal{F}$ obtenemos los siguientes conjuntos:

- R_F el subanillo de R generado por el conjunto F,
- $\mathcal{I}_F$ el ideal generado por el conjunto $I_F = F \cap I$ del anillo R_F,
- $\Psi_F = \{J \text{ ideal de } R_F \,|\, \mathcal{I}_F \subseteq J \text{ y } J \cap S = \emptyset\}$ y
- $J_F \in \Psi_F$ el ideal que contiene la cantidad máxima de elementos del conjunto F.

Consideremos $J_T = I(\bigcup\{J_F \,|\, F \in \mathcal{F}\})$ un ideal del anillo $(R, +, \cdot)$. Ahora, demostremos que $J_T \cap S = \emptyset$. Para ello, supongamos lo contrario es decir $1_R \in J_T$, luego existen $x_1, \ldots, x_n \in J_T$ y $r_1, \ldots, r_n \in R$ tales que $1_R = r_1 \cdot x_1 + \ldots + r_n \cdot x_n$. En consecuencia para cada $i \in \{1, \ldots, n\}$, $x_i \in J_{F_{x_i}}$ para algún $F_{x_i} \in \mathcal{F}$. Con lo anterior definamos los siguientes conjuntos:

- $Q = \{x_1, \ldots, x_n, r_1 \cdot x_1, -r_2 \cdot x_2, \ldots, -r_n \cdot x_n\} \cup \{\sum_{i=1}^{m} r_i \cdot x_i \,|\, m \in \{1, \ldots, n\}\}$ y
- $A = \bigcup_{i=1}^{n} F_{x_i} \cup Q$

Entonces, A es finito y $x_i \in J_{F_{x_i}} \subseteq J_A$. Con lo cual, $\varphi_A(x_i) = 0$, $\varphi_A(r_i \cdot x_i) = 0$ y $1 = \varphi_A(1_R) = \varphi_A(r_1 \cdot x_1 + \ldots + r_n \cdot x_n) = 0$ una contradicción. Esto prueba que $J_T \cap S = \emptyset$. Ahora, podemos definir una función $\varphi_T : T \longrightarrow \{0, 1\}$ tal que $\varphi_T(x) = 0$ si $x \in T \cap J_T$ y $\varphi_T(x) = 1$ si $x \in T \backslash J_T$. En consecuencia, φ_T cumple las condiciones $a) - e)$. Entonces cada $T \subseteq R$ decimos que $\varphi_T \in \xi$ si es alguna de las funciones que hemos definido anteriormente y en consecuencia ξ cumple las condiciones del *lema (De Cowen-Engeler)*. Por lo tanto, existe una función $\varphi \in \xi$ tal que $Dom(\varphi) = R$.

Ahora, probemos que $\varphi^{-1}(0) = P$ es un ideal primo que contiene a I. Claramente $I \subseteq P$, ahora supongamos que P no es un ideal primo, entonces existen $x, y \in R$ tales que $x \cdot y \in P$, pero $x, y \notin R \backslash P$. Con lo cual, $0 = \varphi(x \cdot y) = 1$ una contradicción. Análogamente, se prueba que $(R - P, \cdot)$ es un semigrupo de $(R, \cdot)$ que contiene al conjunto S. □

Corolario 2.84. *Las siguientes propiedades son equivalentes:*

a) El lema del ultrafiltro

b) El lema de Cowen-Engeler

c) En un anillo $(R,+,\cdot)$ todo ideal propio está contenido en un ideal primo.

d) El teorema del ideal primo

Demostración: Ya probamos **a) ⇒ b)**, **b) ⇒ c)** y **d) ⇒ a)** solo bastaría probar que **c) ⇒ d)** lo cual es sencillo por el hecho de que un álgebra booleana es un anillo con identidad. □

El siguiente resultado fue probado por Bernhard Banaschewski [6] modificando la demostración de Artin (Ver *Teorema 2.5* pagina 231 de [10]).

Teorema 2.85. *Todo campo $(F,+,\cdot)$ está contenido en un campo algebraicamente cerrado.*

Demostración: Sea $S \subseteq F[X]$ un conjunto tal que $S = \{p(x) \mid gr(p(x)) \geq 1\} \cup \{1\}$. Entonces, cada elemento $f \in S$ lo representamos por x_f. Además, es claro que $(S,\cdot)$ es un monoide y consecuentemente, $(F[S],+,\cdot)$ forma un *anillo monoide*.

Sea $J = I(\{f(x_f) \mid gr(f) \geq 1\})$ el ideal generado por los polinomios $f(x_f) \in F[S]$. Afirmamos que J es un ideal propio de $F[S]$. Pues suponiendo lo contrario, existen $g_1, \ldots, g_n \in F[S]$ tales que:

$$1 = g_1 \cdot f_i(x_{f_1}) + \ldots + g_n \cdot f_n(x_{f_n}) ...(1)$$

Por definición de *anillo monoide* cada g_i tiene una cantidad finita de variables digamos $x_{f_1}, \ldots, x_{f_m}$. Reescribamos a cada variable x_{f_i} como x_i, así tenemos que:

$$\sum_{i=1}^{n} g_i(x_1, \ldots, x_n, x_{n+1}, \ldots, x_m) f_i(x_i) = 1$$

Luego aplicando el *segundo teorema de kronecker* existe una extensión de campos E donde $f_1(x_1) \cdot \ldots \cdot f_n(x_n)$ se divide, así existen $\alpha_1, \ldots, \alpha_n \in E$ tal que α_i es raíz de $f_i(x_i)$. Luego al ser $x_{n+1} = \ldots = x_m = 0$ y $x_i = \alpha_i$ para cada $i \in \{1, \ldots, n\}$ en la ecuación (1) obtenemos que $0 = 1$, una contradicción y en consecuencia J es un ideal propio de $F[S]$. Entonces existe un ideal primo P del anillo $F[S]$ tal que $J \subseteq P$ esto pasa si y solo sí $F[S]/P$ es un dominio entero. Por *Proposición 2.77* existe el *campo de cocientes* K_1 de $F[S]/P$. Notemos que $x_f + P$ es una raíz de $f(x)$. Pues $f(x_f + P) = f(x_f) + P = P$. Entonces cada polinomio en $F[X]$ tiene una raíz en K_1, repitiendo el mismo proceso construimos una sucesión $K_1, K_2, \ldots, K_n, \ldots$ tal que K_{i+1} es una extensión de campo de K_i. Entonces, sea $K = \bigcup_{i \in \mathbb{N}} K_i$. Demostremos que $(K,+,\cdot)$ es un campo que es algebraicamente cerrado.

Es claro que $1, 0 \in K_1 \subseteq K$. Ahora, para cualesquiera $x, y \in K$, existen $n, m \in \mathbb{N}$ tales que $x \in K_n$ y $y \in K_m$, asumiendo que $m \leq n$, entonces $x, y \in K_n$ y así $x + y, x \cdot y \in K_n \subseteq K$. Por lo que $+$ y $\cdot$ son dos operaciones cerradas sobre K, la propiedad asociativa, conmutativa tanto de la suma y como del producto se heredan al igual que la propiedad distributiva. Por lo que K es un campo.

Ahora, probemos que K es algebraicamente cerrado. Para ello, sea $f(x) \in K[X]$, entonces existe $n \in \mathbb{N}$ tal que $f(x) \in K_n[X]$, por construcción tenemos que $f(x)$ tiene una raíz en $K_{n+1} \subseteq K$. Por lo tanto K es algebraicamente cerrado y $F \subseteq K$. □

Si $(F,+,\cdot)$ es un campo, decimos $(K,+,\cdot)$ es una *clausura algebraica de F*, si este es un campo algebraicamente cerrado que contiene a F.

2.3. Unicidad de la clausura algebraica

Ahora probaremos que para cualquier campo $(F, +, \cdot)$, las *clausuras algebraicas de* F son únicas salvo isomorfismo. Para este fin necesitamos probar *teorema de Tychonoff para espacios de Hausdorff* para ello definamos los siguientes conceptos y probemos algunos de sus resultados.

Definición 2.86. *Sean X un conjunto y $\tau \subseteq \mathcal{P}(X)$. Decimos que (X, τ) es un espacio topológico si:*

- $\emptyset, X \in \tau$.
- *Para cada $A, B \in \tau$, $A \cap B \in \tau$.*
- *Si $\mathcal{A} \subseteq \tau$, entonces $\bigcup \mathcal{A} \in \tau$*

Al conjunto τ la llamamos simplemente topología de X, cada elemento de τ lo llamaremos conjunto abierto o simplemente abierto.

Ejemplo 2.87. *Para cualquier conjunto X, su conjunto potencia $\mathcal{P}(X)$ es una topología. Al espacio topológico $(X, \mathcal{P}(X))$ le llamaremos topología discreta.*

Definición 2.88. *Sea (X, τ) un espacio topológico, entonces:*

- *Un conjunto $E \subseteq X$ es cerrado en τ, si $X \backslash E \in \tau$.*
- *Sea x un elemento del conjunto X. Un subconjunto V de X es una vecindad de x en el espacio (X, τ) si podemos encontrar un $A \in \tau$ que satisfaga $x \in A \subseteq V$.*

Proposición 2.89. *Dado un espacio topológico (X, τ), entonces:*

1. *$\emptyset, X$ son cerrados.*
2. *Si E, F son conjuntos cerrados, entonces $E \cup F$ es un conjunto cerrado.*
3. *Si $\mathcal{E}$ es una familia de conjuntos cerrados, entonces $\bigcap E$ es cerrado.*

Demostración:

1. Puesto que $X \backslash \emptyset = X \in \tau$ y $X \backslash X = \emptyset \in \tau$, entonces $\emptyset, X$ son cerrados.
2. Sean E, F cerrados, luego $X \backslash E, X \backslash F \in \tau$ con lo cual $X \backslash (E \cup F) = (X \backslash E) \cup (X \backslash F) \in \tau$. Entonces $E \cup F$ es cerrado.
3. Si $\mathcal{E}$ es una familia de conjuntos cerrados, entonces $X \backslash E \in \tau$ para cada $E \in \mathcal{E}$, entonces $X \backslash (\bigcap \mathcal{E}) = \bigcup_{E \in \mathcal{E}} (X \backslash E) \in \tau$. Entonces $\bigcap \mathcal{E}$ es cerrado. □

Nota 2.90. *Dado un conjunto $E \subseteq X$, definimos al conjunto $E' = \bigcap \{F \subseteq X \mid F$ es cerrado en $\tau\}$ por la proposición anterior sabemos que es cerrado y además si C es el conjunto cerrado mas pequeño que contiene a E, entonces $C \subseteq E'$. Por otro lado, $C \in \{F \subseteq X \mid F$ es cerrado en $\tau\}$ y consecuentemente $E' \subseteq C$. Por lo tanto, $C = E'$, Al conjunto $cl_X E = \bigcap \{F \subseteq X \mid F$ es cerrado en $\tau\}$ le llamamos clausura del conjunto E en el espacio topológico (X, τ). Por otro lado si E es cerrado, entonces no es difícil notar que $E = cl_X(E)$.*

Definición 2.91. *Dado un espacio topológico (X, τ), decimos que:*

- *Una colección $\mathcal{U}$ de subconjuntos de X es una cubierta de X, si $X = \bigcup \mathcal{U}$. Además, si cada elemento de $\mathcal{U}$ es un abierto en τ, decimos que $\mathcal{U}$ es una cubierta abierta de X.*

- *Sea $\mathcal{U}$ una cubierta de X, diremos que $\mathcal{V}$ es una subcubierta de $\mathcal{U}$, si $\mathcal{V}$ está contenido en $\mathcal{U}$ y además $\bigcup \mathcal{V} = X$.*
- *X compacto si toda cubierta abierta de X tiene una subcubierta finita*

Nota 2.92. *Sean X un conjunto finito y (X, τ) un espacio topológico. Probemos que (X, τ) es compacto. Sea $\mathcal{U}$ es una cubierta abierta de X, entonces $\bigcup \mathcal{U} = X$. Para cada $x \in X$, elíjase $U_x \in \mathcal{U}$ tal que $x \in U_x$, con ello $X \subseteq \bigcup_{x \in X} U_x$ y puesto que X es finito, entonces $\{U_x\}_{x \in X}$ es una subcubierta finita de $\mathcal{U}$.*

Definición 2.93. *Sea $\mathcal{F}$ un filtro sobre $(\mathcal{P}(X), \cup, \cap)$, entonces:*

- *$\mathcal{F}$ es libre si $\bigcap \mathcal{F} = \emptyset$.*
- *$\mathcal{F}$ converge a un punto $x \in X$, si toda vecindad de x pertenece al filtro $\mathcal{F}$. Para denotar este hecho, escribimos $\mathcal{F} \longrightarrow x$.*

Proposición 2.94. *Sea (X, τ) un espacio topológico. Entonces las siguientes condiciones son equivalentes:*

a) X es compacto.

b) Todo filtro en X no es libre.

c) Todo ultrafiltro en X no es libre.

d) Todo ultrafiltro en X converge.

Demostración: **a) ⇒ b)** Supongamos por contradicción, que hay un filtro $\mathcal{F}$ que es libre. Por otro lado, si $F \in \mathcal{F}$ entonces $F \subseteq cl(F)$, con lo cual $cl(F) \in \mathcal{F}$. Esto implica, $\bigcap_{F \in \mathcal{F}} cl(F) \subseteq \bigcap \mathcal{F} = \emptyset$ y como $cl(F)$ es un conjunto cerrado para cada $F \in \mathcal{F}$, entonces $X \backslash cl(F) \in \tau$, con ello:

$$X = X \backslash \emptyset = X \backslash (\bigcap_{F \in \mathcal{F}} cl(F)) = \bigcup_{F \in \mathcal{F}} (X \backslash cl(F))$$

Es decir $\{X \backslash cl(F)\}_{F \in \mathcal{F}}$ es una cubierta del conjunto X. Pero (X, τ) es compacto y por consiguiente existen $F_1, \ldots, F_n \in \mathcal{F}$ tales que:

$$X = \bigcup_{i=1}^{n} X \backslash cl(F_i) = X \backslash \bigcap_{i=1}^{n} cl(F_i)$$

Por lo tanto, $\emptyset = \bigcap_{i=1}^{n} cl(F_i)$. Esto contradice el hecho de que $\mathcal{F}$ sea un filtro y por lo tanto $\mathcal{F}$ no es libre.

b) ⇒ c) Como todo ultrafiltro es un filtro terminamos.

c) ⇒ d) Por **c)** se tiene que $\bigcap \mathcal{U} \neq \emptyset$. Sea $x \in \bigcap \mathcal{U}$, probemos que $\mathcal{U} \longrightarrow x$. Suponiendo lo contrario, existe una vecindad V_x que no pertenece a $\mathcal{U}$, por ser $\mathcal{U}$ un ultrafiltro $X / V_x \in \mathcal{U}$, en consecuencia $x \notin \bigcap \mathcal{U}$ una contradicción. Por lo tanto $\mathcal{U} \longrightarrow x$.

d) ⇒ a) Supongamos por contradicción, que (X, τ) no es compacto. Entonces, existe una cubierta abierta $\mathcal{U}$ que no tiene subcubiertas finitas. Por lo tanto, para cada $U_1, \ldots, U_n \in \mathcal{U}$:

$$\bigcup_{i=1}^{n} U_i \neq X, \text{ entonces } \bigcap_{i=1}^{n} (X \backslash U_i) = X \backslash (\bigcup_{i=1}^{n} U_i) \neq \emptyset$$

Es decir que $\{X \backslash U\}_{U \in \mathcal{U}}$ cumple la propiedad de intersección finita. Por *Proposición 1.35*, existe un filtro $\mathcal{F}$ que contiene a $\mathcal{U}$, y por el *lema del ultrafiltro*, $\mathcal{F}$ está contenido en un ultrafiltro $\mathcal{U}'$.

Ahora, demostremos que $x \in U'$ para cada $U' \in \mathcal{U}'$. Suponiendo lo contrario, existe $U'_0 \in \mathcal{U}'$ tal que $x \notin U'_0$. Con ello, sea $U_0 \subseteq X$ tal que $U'_0 = X/U_0$ y así U_0 es una vecindad de x. Por ***d)***, $\mathcal{U}' \longrightarrow x$, con lo cual $U_0 \in \mathcal{U}'$ y $\emptyset = U'_0 \cap U_0 \in \mathcal{U}'$, una contradicción. Por lo tanto $x \in U'$ para cada $U' \in \mathcal{U}'$, por consiguiente $x \notin U$ para cada $U \in \mathcal{U}$, esto contradice el hecho de que $\mathcal{U}$ sea una cubierta abierta. Por lo tanto (X, τ) es compacto. □

Definición 2.95. *Decimos que un espacio topológico (X, τ) es Hausdorff. si para cualesquiera $x, y \in X$ distintos, existen abiertos U, V tales que $x \in U$, $y \in V$ y $U \cap V = \emptyset$.*

Un claro ejemplo de un espacio topológico que es un espacio de Hausdorff, es el espacio discreto.

Teorema 2.96. *Sea (X, τ) un espacio topológico, si (X, τ) es Hausdorff, entonces todo ultrafiltro $\mathcal{U}$ tiene exactamente un punto limite.*

Demostración: Por contradicción, sean $x, y \in X$ puntos limite distintos de un ultrafiltro $\mathcal{U}$. Puesto que (X, τ) es Hausdorff, existen abiertos U, V tales que $x \in U$, $y \in V$ y $U \cap V = \emptyset$. Pero $\mathcal{U} \longrightarrow x$ y $\mathcal{U} \longrightarrow y$, luego $U, V \in \mathcal{U}$. Pero $\emptyset = U \cap V \in \mathcal{U}$, una contradicción. Por lo tanto, $\mathcal{U}$ tiene exactamente un punto limite. □

Definición 2.97. *Sea (X, τ) un espacio topológico. Decimos, que una subcolección $\mathcal{B}$ de τ es una base para τ, si para cada elemento $A \in \tau$, existe $\mathcal{A} \subseteq \mathcal{B}$ tal que $A = \bigcup \mathcal{A}$.*

Proposición 2.98. *Sea $\mathcal{B}$ una familia de subconjuntos de un conjunto X tal que:*

- $X = \bigcup \mathcal{B}$,
- *Si B_1 y B_2 son elementos de $\mathcal{B}$, y $x \in B_1 \cap B_2$, entonces existe $B \in \mathcal{B}$ tal que $x \in B \subseteq B_1 \cap B_2$.*

Entonces, la colección $\tau_{\mathcal{B}} = \{A \subseteq X \mid \text{existe } \mathcal{A} \subseteq \mathcal{B} \text{ con } A = \bigcup \mathcal{A}\}$ es una topología en X que contiene a $\mathcal{B}$ como base.

Demostración: Por el primer inciso se tiene que $X \in \tau_{\mathcal{B}}$. Ya que $\emptyset \subseteq \mathcal{B}$, entonces $\bigcup \emptyset = \emptyset \in \tau_{\mathcal{B}}$. Naturalmente para cada familia $\mathcal{A} \subseteq \mathcal{B}$ se tiene que $\bigcup \mathcal{A} \in \tau_{\mathcal{B}}$.

Tomemos ahora $A_1, A_2 \in \tau_{\mathcal{B}}$. Para cada $x \in A_1 \cap A_2$, existe un elemento B_x de $\mathcal{B}$ tal que $x \in B_x \subseteq B_1 \cap B_2$. Entonces, $A_1 \cap A_2 = \bigcup \{B_x \mid x \in A_1 \cap A_2\}$. Con lo cual, $A_1 \cap A_2$ pertenece a $\tau_{\mathcal{B}}$. □

Definición 2.99. *Dados dos espacios topológicos (X, τ_X) y (Y, τ_Y), decimos que una función $f : X \longrightarrow Y$ es continua si para cualquier abierto U de τ_Y, $f^{-1}[U]$ es abierto en X.*

Si consideramos un espacio topológico (Y, τ) y una función $f : X \longrightarrow Y$, definimos un conjunto $\tau^f = \{f^{-1}[U] \mid U \in \tau\}$. Entonces:

- $\emptyset = f^{-1}[\emptyset] \in \tau^f$ y $X = f^{-1}[Y] \in \tau^f$.
- Para cualquier conjunto de índices J, $\bigcup_{j \in J} f^{-1}[U_j] = f^{-1}[\bigcup_{j \in J} U_j] \in \tau^f$.
- Para cualquier conjunto finito de índices J, $\bigcap_{j \in J} f^{-1}[U_j] = f^{-1}[\bigcap_{j \in J} U_j] \in \tau^f$.

Por lo tanto, τ^f es una topología en X. Esta topología es la inducida por la función f.

Proposición 2.100. *Sean (X, τ_X), (Y, τ_Y) dos espacios topológicos y $f : X \longrightarrow Y$ una función continua, entonces:*

a) Si X es compacto, entonces $f[X]$ es compacto.

b) Si $\mathcal{F}$ es un ultrafiltro, entonces $\mathcal{F}' = \{f[F]\}_{F \in \mathcal{F}}$ es un ultrafiltro.

Demostración:

a) Sea $\mathcal{U}$ una cubierta abierta de $f[X]$, entonces por la continuidad de f, $\{f^{-1}[U]\}_{U\in\mathcal{U}}$ es una cubierta abierta de X. Ya que X es compacto existen $U_1,\ldots,U_n$ tales que $X=\bigcup_{i=1}^{n} f^{-1}[U_i]$. Por lo tanto $f[X]=\bigcup_{i=1}^{n} U_i$. Por consiguiente, $f[X]$ es compacto.

b) Afirmamos que $\{f[F]\}_{F\in\mathcal{F}}$ es un filtro. Pues $\emptyset=F^{-1}[\emptyset]$ y $X=f^{-1}[Y]$, entonces $Y\in\mathcal{F}'$, pero $\emptyset\notin\mathcal{F}'$.

Por otro lado sean $U,V\in\mathcal{F}'$, entonces $f^{-1}[U],f^{-1}[V]\in\mathcal{F}$ y puesto que $f^{-1}[U\cap V]=f^{-1}[U]\cap f^{-1}[V]\in\mathcal{F}$. En consecuencia, $U\cap V\in\mathcal{F}'$.

Ahora sea $A\in\mathcal{F}$ y $C\subseteq Y$ tales que $A\subseteq C$, entonces $f^{-1}[A]\subseteq f^{-1}[C]$ y $f^{-1}[A]\in\mathcal{F}$. En consecuencia, $f^{-1}[C]\in\mathcal{F}$. Con lo cual, $C\in\mathcal{F}'$.

Ahora supongamos que existe $U\subseteq Y$ tal que $U\notin\mathcal{F}'$, entonces $f^{-1}[U]\notin\mathcal{F}$. Por ser $\mathcal{F}$ un ultrafiltro, $V=X\backslash f^{-1}[U]\in\mathcal{F}$ y con ello $f[V]\in\mathcal{F}'$. Pero $f[V]=f[X\backslash f^{-1}[U]]=Y\backslash F[U]$. Por lo tanto $\mathcal{F}'$ es un ultrafiltro. □

Definición 2.101. *Dada una familia de espacios topológicos $\{(X_\alpha,\tau_\alpha)\}_{\alpha\in I}$, consideremos el conjunto producto:*

$$X=\prod_{\alpha\in J}X_\alpha=\{f:J\longrightarrow\bigcup_{\alpha\in J}X_\alpha\mid \text{ para cada } j\in J, f(j)\in X_j\}.$$

Sea τ, es la topología de X generada por el conjunto $\beta=\{\prod_{\alpha\in J}U_\alpha\,|\,U_\alpha\in\tau_\alpha$, para cada $\alpha\in J\}$.

Definimos la función proyección $\pi_j:X\longrightarrow X_j$, tal que para cada $(a_i)_{i\in I}\in X$, $\pi_j((a_i)_{i\in I})=a_j$.

Corolario 2.102. *Sea $\{(X_i,\tau_i)\}_{i\in I}$ una familia de espacios topológicos. Con ello sea el producto $X=\prod_{i\in I}X_i$ y τ la topología de Tychonoff. Entonces la función proyección $\pi_j:\prod_{i\in I}A_i\longrightarrow A_j$ es continua para cada $j\in I$.*

Demostración: Por definición de proyección y a la naturaleza de la topología de Tychonoff, para cada $i\in I$ y cada abierto U_i de X_i, $\pi_j^{-1}[U_i]$ es abierto de X. Por lo tanto, la proyección $\pi_i:X\longrightarrow X_i$ es continua □

Teorema 2.103. *(Teorema de Tychonoff para espacios de Hausdorff)*

Dada una familia $\{(X_\alpha,\tau_\alpha)\}_{\alpha\in I}$ de espacios topológicos no vacíos que son Hausdorff, Entonces (X,τ) es compacto si y solo sí para cada $i\in I$ se tiene que $\{(X_\alpha,\tau_\alpha)\}_{\alpha\in I}$ también lo es. (Donde $X=\prod_{\alpha\in I}X_\alpha$ y τ es la topología de Tychonoff)

Demostración: $\Rightarrow$] Sea (X,τ) es compacto. Puesto que la proyección de espacios topológicos es continua, entonces $\pi_i:X\longrightarrow X_i$ es continua y como la imagen de compactos es compacta, entonces tenemos que X_i es tambien compacto.

$\Leftarrow$] Sea $\{(X_i,\tau_i)\}_{i\in I}$ una familia de espacios Hausdorff compactos y sea $\mathcal{U}$ un ultrafiltro en X. Entonces, para cada $i\in I$ se tiene que $\mathcal{U}_i=\{A\subseteq X_i\,|\,\pi_i^{-1}[A]\in\mathcal{U}\}$ es un ultrafiltro en X_i (donde π_i denota la i–esima proyección). Puesto que X_i es compacto y Hausdorff, entonces $\mathcal{U}_i$ converge a un único punto x_i. Por lo tanto $\mathcal{U}$ converge a $x=(x_i)_{i\in I}$. □

Teorema 2.104. *Dado un campo $(F,+,\cdot)$, entonces su clausura algebraica es única salvo isomorfismo.*

Demostración: Sean $(K,+,\cdot)$, $(E,+,\cdot)$ clausuras algebraicas del campo $(F,+,\cdot)$. Para cada $f\in F[X]$, sea $(K_f,+,\cdot)$ el mínimo subcampo de $(K,+,\cdot)$ que contiene a F y a todas las raíces de f. Análogamente, también definimos al subcampo $(E_f,+,\cdot)$. Notemos que si f divide a g, entonces $K_f\subseteq K_g$ y $E_f\subseteq K_g$. Además, $K=\bigcup_{f\in F[X]}K_f$ y $E=\bigcup_{f\in F[X]}E_f$.

Sea $H_f = \{\varphi : K_f \longrightarrow E_f \,|\, \varphi \text{ es un isomorfismo}\}$, entonces por *Proposición 2.69*, H_f es distinto del vacío. Por otro lado, notemos que H_f es finito y en consecuencia, para cada $f \in F[X]$, $(H_f, \mathcal{P}(H_f))$ es un espacio topológico compacto que es Hausdorff.

Ahora, consideremos al conjunto $H = \prod_{f\in F[X]} H_f$ y para $p|q$, sea:

$$H_{pq} = \{(h_f) \in H \,|\, h_p = h_q|_{E_p}\}$$

- Por el *teorema de Tychonoff para espacios Hausdorff* se sabe que H es compacto sobre la topología producto.
- Por otro lado, probemos que $\mathcal{H} = \{H_{pq} \,|\, p, q \in F[X]\}$ tiene la propiedad de intersección finita. Tomando un elemento $\varphi \in H_g$, restringiendo su dominio a K_f obtenemos que la imagen de dicha función es E_p, es decir, H_{pq} es no vacío. Ahora, sean $H_{pq}, H_{p'q'} \in \mathcal{H}$, entonces $H_{pq} \cap H_{p'q'} = \{(h_f) \in H \,|\, h_p = h_q|_{E_p}\} \cap \{(h_f) \in H \,|\, h_{p'} = h_{q'}|_{E_{p'}}\} = \{(h_f) \in H \,|\, h_p = h_q|_{E_p} \text{ y } h_{p'} = h_{q'}|_{E_{p'}}\}$. Sean g mínimo común divisor de p, p' y g' el mínimo común divisor de q, q', entonces $\{(h_f) \in H \,|\, h_p = h_q|_{E_p} \text{ y } h_{p'} = h_{q'}|_{E_{p'}}\} = \{(h_f) \in H \,|\, h_g = h_{g'}|_{E_g}\} = H_{gg'} \in \mathcal{H}$. Por lo tanto $\mathcal{H}$ tiene la propiedad de intersección finita, por el *lema del ultrafiltro* y *Proposición 1.34*, existe un ultrafiltro $\mathcal{U}$ que contiene a dicho conjunto.

Por los dos incisos anteriores y el *Teorema 2.96*, existe exactamente un $h \in H$ tal que $\mathcal{U} \longrightarrow h$, entonces $(h) \in \bigcap \mathcal{U} \subseteq \bigcap \mathcal{H}$, determina un único isomorfismo de campos $h : \bigcup_{f\in F[X]} K_f \longrightarrow \bigcup_{f\in F[X]} E_f$, es decir, $K \cong E$. □

Capítulo 3

Lenguajes, estructuras y teorías

3.1. Preliminares

El objetivo de esta sección es probar la equivalencia del *lema del ultrafiltro* con el *teorema de compacidad* de la lógica de primer orden. Consecuentemente, usando el *teorema de compacidad*, se demostrarán algunos resultados de la teoría de modelos.

El *Teorema de compacidad* es uno de los resultados de la teoría de modelos. El caso numerable del teorema de compacidad fue probado por *Kurt Gödel* en el año 1930 y el caso no numerable por *Anatoly Maltsev* en 1936.

Definición 3.1. *El lenguaje $\mathcal{L}$ del cálculo predicativo clásico consiste de:*

- *Un conjunto de variables $\{x_n : n \in \omega\}$*
- *Un conjunto $\{c_\alpha : \alpha \in \omega\}$ de constantes.*
- *Un conjunto $f_1, , \ldots, f_n$ de símbolos funcionales, donde f_i es de aridad a_i.*
- *Un conjunto $A_1, \ldots, A_m$ de símbolos relacionales, donde A_j es de aridad r_j.*
- *Una colección $\{\vee, \wedge, \rightarrow, \leftrightarrow, \neg\}$ de símbolos denominados conectivos lógicos.*
- *Un conjunto $\{\forall, \exists\}$ de cuantificadores.*
- *Dos símbolos llamados símbolos de agrupación "(,)" (También podemos ocupar como símbolos de agrupación a "[,]" para evitar inconvenientes)*

Para referirnos al lenguaje $\mathcal{L}$, escribiremos $\mathcal{L} = \{\{A_1, \ldots, A_m\}, \{f_1, , \ldots, f_n\}, \{c_\alpha\}_{\alpha \in \omega}\}$

Definición 3.2. *El conjunto $TERM$ de términos es el menor conjunto X que cumple:*

- *Para cada $n \in \omega$, $x_n \in X$ (las variables son términos).*
- *Si c_α es una constante para algún $\alpha \in \omega$, entonces $c_\alpha \in X$.*
- *Si f_k es un símbolo funcional y $t_1, \ldots, t_{a_k} \in X$, entonces $f_k(t_1, \ldots, t_{a_k}) \in X$.*

Definición 3.3. *El conjunto $FORM$ de fórmulas bien formadas es el menor conjunto Y que cumple:*

- *Si A_j es un símbolo relacional y $t_1, \ldots, t_{r_j} \in TERM$, entonces $A_j(t_1, \ldots, t_{r_j}) \in Y$.*
- *Si $t, s \in TERM$, entonces $t = s \in Y$.*

- *Si $\varphi, \psi \in Y$ y $\square \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, entonces $(\varphi \square \psi) \in Y$*
- *Si $\varphi \in Y$, entonces $\neg\varphi \in Y$*
- *Si $\varphi \in Y$, x_m es una variable y $\bigtriangledown \in \{\forall, \exists\}$, entonces $(\bigtriangledown x_m)\varphi \in Y$*

Diremos que una fórmula φ es atómica si esta no contiene conectivos, ni cuantificadores; es decir, si φ se escribe de alguna de las siguientes maneras: $\varphi := t_1 = t_n$ ó $\varphi := R(t_1, \ldots, t_n)$. El conjunto de fórmulas atómicas se denota por $ATOM$.

Teorema 3.4. *(Principio de Inducción)*
Sea A una propiedad. Entonces, $A(t)$ se cumple para todo término $t \in TERM$, si:

1. *Para cada variable x_i $(i \in \omega)$, se cumple que $A(x_i)$.*
2. *Para cada constante c_i $(i \in \omega)$, se cumple que $A(c_i)$.*
3. *Si $t_1, \ldots, t_{a_k}$ son términos, tales que $A(t_i)$ para cada $i \in \{1, \ldots, a_k\}$, y f_k es un símbolo funcional, entonces se cumple $A(f_k(t_1, \ldots, t_{a_k}))$.*

Demostración:
Sea $X = \{t \in TERM : A(t)\}$. Entonces:

a) Toda variable x_i $(i \in \omega)$, cumple que $x_i \in X$.

b) Toda constante c_i $(i \in \omega)$, cumple que $c_i \in X$.

c) Si $t_1, \ldots, t_{a_k} \in X$, entonces se cumple $f_k(t_1, \ldots, t_{a_k}) \in X$

Lo anterior garantiza que $TERM \subseteq X \subseteq TERM$. □

Teorema 3.5. *Sea B una propiedad, $B(\varphi)$ se cumple para toda fórmula $\varphi \in FORM$ si ocurre:*

1. *$B(\varphi)$ para cada formula atómica φ.*
2. *Para cualesquiera $\varphi, \psi \in FORM$ y $\square \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, si $B(\varphi)$, $B(\psi)$, entonces $B(\varphi \square \psi)$.*
3. *Para cada $\varphi \in FORM$, si $B(\varphi)$ entonces $B(\neg\varphi)$.*
4. *Para cada $\varphi \in FORM$, x_m una variable y $\bigtriangledown \in \{\forall, \exists\}$, si $B(\varphi)$ entonces $B((\bigtriangledown x_m)\varphi)$.*

Demostración: Sea $Y = \{\varphi \in FORM : B(\varphi)\}$. Entonces:

a) Para cualesquiera fórmulas atómicas $A_j(t_1, \ldots, t_{r_j})$ y $t = s$, entonces $A_j(x_1, \ldots, x_{r_j}) \in Y$ y $t = s \in Y$.

b) Si $\varphi, \psi \in FORM$, $B(\varphi)$, $B(\psi)$ y $\square \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, entonces $\varphi \square \psi \in Y$.

c) Si $\varphi \in FORM$ y $B(\varphi)$, entonces $\neg\varphi \in Y$.

d) Sean $\varphi \in FORM$ y x_m una variable. Si $B(\varphi)$ y $\bigtriangledown \in \{\forall, \exists\}$, entonces $(\bigtriangledown x_m)\varphi \in Y$.

Lo anterior garantiza que $FORM \subseteq Y \subseteq FORM$. □

Denotaremos al conjunto de todas las constantes del lenguaje $\mathcal{L}$ como $Cons$, al conjunto de al conjunto de todas las variables del lenguaje $\mathcal{L}$ como Var.
La demostración de los siguientes resultados los puede consultar en [13]

Teorema 3.6. *(Definición por Recursión sobre los términos)*
Sean $B \neq \emptyset$,

- $H_0 : Var \cup Cons \longrightarrow B$,
- *Para cada* $k \in \{1, \ldots, n\}$, $H_k : B^{a_k} \longrightarrow B$.

Entonces existe una única función $H : TERM \longrightarrow B$ *tal que:*

- *Para cada término* $t \in Var \cup Cons$, $H(t) = H_0(t)$.
- *Para cada símbolo funcional* f_k *y* $t_1, \ldots, t_{a_k}$ *términos,* $H(f_k(t_1, \ldots, t_{a_k})) = H_k(H(t_1), \ldots, H(t_{a_k}))$.

Teorema 3.7. *(Definición por Recursión sobre las fórmulas)*
Sean

- $G_{ATOM} : ATOM \longrightarrow A$,
- *Para cada conectivo* $\square \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, $G_\square : A^2 \longrightarrow A$,
- $G_\neg : A \longrightarrow A$,
- $G_\forall : A \times \omega \longrightarrow A$.

Entonces existe una única función $G : FORM \rightarrow A$ *tal que:*

- *Para cada* $\varphi \in ATOM$, *donde* $t_1, t_2 \in TERM$ $G(\varphi) = G_{ATOM}(\varphi)$.
- *Para cada* $\psi, \gamma \in FORM$ *y* $\square \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, $G(\psi \square \gamma) = G_\square(G(\psi), G(\gamma))$.
- *Para cada* $\psi \in FORM$, $G(\neg\psi) = G_\neg(G(\psi))$.
- *Para cada* $\psi \in FORM$, $G((\forall x_n)\psi) = G_\forall(G(\psi), n)$.

Definición 3.8. *Sea* $\mathcal{L}'$ *el conjunto de todos los símbolos constantes, funcionales y relacionales del lenguaje* $\mathcal{L}$. *Un modelo o estructura* $\mathfrak{A}$ *para un lenguaje* $\mathcal{L}$ *es un par ordenado* $(A, (\cdot)^{\mathfrak{A}})$, *donde* A *es un conjunto distinto del vacio y* $(\cdot)^{\mathfrak{A}} : \mathcal{L}' \rightarrow A$ *es una función de interpretación tal que:*

- *Si* c *símbolo constante, entonces* $(c)^{\mathfrak{A}} \in A$,
- *Si* F *símbolo funcional de aridad* n *y* $t_1, \ldots, t_n \in \mathcal{L}'$ *términos, entonces* $(F(t_1, \ldots, t_n))^{\mathfrak{A}} = F^{\mathfrak{A}}(t_1^{\mathfrak{A}}, \ldots, t_n^{\mathfrak{A}})$ *es una función* $n-$*aria en* A.
- *Si* R *es un símbolo funcional de aridad* n *y* $t_1, \ldots, t_n \in \mathcal{L}'$ *términos, entonces* $(R(t_1, \ldots, t_n))^{\mathfrak{A}} = R^{\mathfrak{A}}(t_1^{\mathfrak{A}}, \ldots, t_n^{\mathfrak{A}})$

A es llamado el universo de el modelo $\mathfrak{A}$.

Los modelos (o estructuras) son denotados por letras góticas $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, ...$ y los universos (o dominios) son denotados por letras latinas $A, B, C, D, ...$,

Ahora deseamos mostrar cómo usar fórmulas para expresar enunciados matemáticos sobre los elementos de un modelo. Primero necesitamos ver cómo interpretar un término en un modelo.

Definición 3.9. *Dada una interpretación* $\mathfrak{A}$ *del modelo* A, *definimos una valuación* $v : TERM \rightarrow A$ *como sigue:*

1. *si* $t = x$ *es una variable, entonces* $v(t) = v(x)$ *(Para ser mas prácticos denotemos la interpretación de una variable* x *en un modelo* $\mathfrak{A}$ *como* $v(t) = x^{\mathfrak{A}}$*).*
2. *si* $t = c$ *es un símbolo constante, entonces* $v(t) = c^{\mathfrak{A}}$.

3. si $t = f(t_1, ..., t_n)$ es un símbolo funcional de aridad n, entonces $v(t) = f^{\mathfrak{A}}(v(t_1), ..., v(t_n))$.

Definición 3.10. *Dado un modelo $\mathfrak{A}$ para el lenguaje $\mathcal{L}$ y una valuación $v : TERM \to A$, definimos la relación $\mathfrak{A} \vDash \varphi$ para cada sentencia φ en $\mathcal{L}$, como sigue:*

- *Si $\varphi := t = s$, entonces $\mathfrak{A} \vDash (t = s)$ sii $v(t) = v(s)$;*
- *Si $\varphi := R(t_1, ..., t_n)$, entonces $\mathfrak{A} \vDash R(t_1, ..., t_n)$ sii $(v(t_1), ..., v(t_n)) \in R^{\mathfrak{A}}$;*
- *Si $\varphi := \gamma \wedge \psi$, entonces $\mathfrak{A} \vDash (\gamma \wedge \psi)$ sii $\mathfrak{A} \vDash \gamma$ y $\mathfrak{A} \vDash \psi$;*
- *Si $\varphi := \gamma \vee \psi$, entonces $\mathfrak{A} \vDash (\gamma \vee \psi)$ sii $\mathfrak{A} \vDash \gamma$ ó $\mathfrak{A} \vDash \psi$;*
- *Si $\varphi := \gamma \to \psi$, entonces $\mathfrak{A} \vDash (\gamma \to \psi)$ sii $\mathfrak{A} \vDash \gamma$ implica que $\mathfrak{A} \vDash \psi$;*
- *Si $\varphi := \gamma \leftrightarrow \psi$, entonces $\mathfrak{A} \vDash (\gamma \leftrightarrow \psi)$ sii $\mathfrak{A} \vDash \gamma$ sii $\mathfrak{A} \vDash \psi$;*
- *Si $\varphi := \neg\psi$, entonces $\mathfrak{A} \vDash \neg\psi$ sii $\mathfrak{A} \nvDash \psi$;*
- *Si $\varphi := (\exists x)\psi$, entonces $\mathfrak{A} \vDash (\exists x)\psi(x)$ sii para algún $a \in A$, $\mathfrak{A} \vDash \psi(a)$;*
- *Si $\varphi(x) := (\forall x)\psi(x)$, entonces $\mathfrak{A} \vDash (\forall x)\psi(x)$ sii para cada $a \in A$, $\mathfrak{A} \vDash \psi(a)$;*

Una teoría $\mathcal{T}$ para el lenguaje $\mathcal{L}$ es un conjunto tal que $\mathcal{T} \subseteq FORM$.
$\mathfrak{A}$ es un modelo de la teoría $\mathcal{T}$ si $\mathfrak{A} \vDash \varphi$ para cada $\varphi \in \mathcal{T}$. La relación $\mathfrak{A} \vDash \varphi$ lee como: $\mathfrak{A}$ satisface φ, φ es verdadera en $\mathfrak{A}$ ó φ se cumple en $\mathfrak{A}$, En el caso de que $\mathfrak{A}$ sea un modelo de la teoría $\mathcal{T}$ lo denotamos como $\mathfrak{A} \vDash \mathcal{T}$. en algunas ocasiones si $x_1, \ldots, x_n \in FV(\varphi)$ escribiremos que $\mathfrak{A} \vDash \varphi[x_1, \ldots, x_n]$ en lugar de $\mathfrak{A} \vDash \varphi$.

Decimos que $\mathfrak{A} = (A, (\cdot)^{\mathfrak{A}})$ es un submodelo de $\mathfrak{B} = (B, (\cdot)^{\mathfrak{B}})$ si $A \subseteq B$ y $(\cdot)^{\mathfrak{B}}|_A = (\cdot)^{\mathfrak{A}}$. A la situación antes descrita la escribimos como $\mathfrak{A} \subseteq \mathfrak{B}$.

Con lo anterior, dada una teoría $\mathcal{T}$ podemos definir una valuación $v : TERM \longrightarrow \{0, 1\}$ tal que $v(\varphi) = 1$ si para cada modelo $\mathfrak{A}$ se tiene que $\mathfrak{A} \vDash \varphi$. A dicha función la llamaremos $\mathcal{T}$*-esquema*

Teorema 3.11. *Sean $\mathfrak{A} = (A, (\cdot)^{\mathfrak{A}})$ y $\mathfrak{B} = (B, (\cdot)^{\mathfrak{B}})$ modelos para un lenguaje $\mathcal{L}$, tales que $\mathfrak{A} \subseteq \mathfrak{B}$. Sea φ una fórmula libre de cuantificadores y $\overline{a} \in A^n$. Entonces:*

$$\mathfrak{A} \vDash \varphi(\overline{a}) \text{ si y solo sí } \mathfrak{B} \vDash \varphi(\overline{a})$$

Demostración: La prueba se hará por inducción sobre la complejidad de la fórmula:

- Si $\varphi := t = t'$, donde $t, t' \in TERM$, entonces:

$$\begin{aligned} \mathfrak{A} \vDash (t = t') &\text{ si y solo sí } (t)^{\mathfrak{A}} = (t')^{\mathfrak{A}} \\ \text{Ya que } \mathfrak{A} \text{ es un submodelo de } \mathfrak{B} \text{ esto pasa} &\text{ si y solo sí } (t)^{\mathfrak{B}} = (t')^{\mathfrak{B}} \\ &\text{si y solo sí } \mathfrak{B} \vDash (t = t') \end{aligned}$$

- Si $\varphi := R(t_1, ..., t_n)$, donde R es un símbolo relacional de aridad n y donde $t_1, ..., t_n \in TERM$ el resultado es claro.
- Si $\varphi := \psi \wedge \gamma$, donde $\psi, \gamma \in FORM$, entonces:

$$\begin{aligned} \mathfrak{A} \vDash (\psi \wedge \gamma) &\text{ si y solo sí } \mathfrak{A} \vDash \psi \text{ y } \mathfrak{A} \vDash \gamma \\ \text{Por h.i. esto pasa} &\text{ si y solo sí } \mathfrak{B} \vDash \psi \text{ y } \mathfrak{B} \vDash \gamma \\ &\text{si y solo sí } \mathfrak{B} \vDash \psi \wedge \gamma \end{aligned}$$

- Si $\varphi := \neg\psi$, donde $\psi \in FORM$, entonces:

$$\begin{aligned} \mathfrak{A} \vDash (\neg\psi) &\text{ si y solo sí } \mathfrak{A} \nvDash \psi \\ \text{Por h.i. si y solo sí } &\mathfrak{B} \nvDash \psi \\ \text{si y solo sí } &\mathfrak{B} \vDash \neg\psi \end{aligned}$$

□

Definición 3.12. *Si $\mathcal{T}$ es una teoría y σ es una fórmula, decimos que $\mathcal{T} \vDash \sigma$ si para cada $\mathfrak{A}$ tal que $\mathfrak{A} \vDash \sigma$, entonces $\mathfrak{A} \vDash \sigma$. Si sucede lo anterior decimos que σ es consecuencia de $\mathcal{T}$.*

Proposición 3.13. *Sean Γ un conjunto de fórmulas y $\varphi \in FORM$. Entonces $\Gamma \cup \{\neg\varphi\}$ es satisfacible si y solo sí $\Gamma \nvDash \varphi$.*

Demostración: $\Rightarrow$] Supongamos que $\mathcal{T} = \Gamma \cup \{\neg\varphi\}$ es satisfacible. Para el $\mathcal{T}$-esquema $v : FORM \longrightarrow \{0,1\}$ se tiene que $v(\psi) = 1$ para cada $\psi \in \Gamma$ y no puede suceder que $v(\varphi) = 1$, en consecuencia $v(\varphi) = 0$. Por tanto para cada modelo $\mathfrak{A}$ tal que $\mathfrak{A} \vDash \mathcal{T}$, entonces $\mathfrak{A} \nvDash \varphi$ es decir que $\mathcal{T} \nvDash \varphi$.

$\Leftarrow$] Supongamos ahora que $\Gamma \nvDash \varphi$. Entonces del $\mathcal{T}$-esquema tenemos que $v(\psi) = 1$ para cada $\psi \in \Gamma$ y $v(\varphi) = 0$. Lo anterior permite concluir que $\Gamma \cup \{\neg\varphi\}$ es satisfacible. □

Definición 3.14. *Se dice que dos modelos $\mathfrak{A}$ y $\mathfrak{B}$ para un lenguaje $\mathcal{L}$, son elementalmente equivalentes, si para cada sentencia $\varphi \in FORM$:*

$$\mathfrak{A} \vDash \varphi \text{ si y solo sí } \mathfrak{B} \vDash \varphi$$

Lo anterior se representa por $\mathfrak{A} \equiv \mathfrak{B}$.

Definición 3.15. *Un conjunto de axiomas para $\mathcal{T}$ es una teoría $\mathcal{T}'$, que tiene los mismos modelos de $\mathcal{T}$ (es decir, $\mathcal{T}'$ es lógicamente equivalente a $\mathcal{T}$)*

Omitiendo la mención explícita de los símbolos lógicos (incluyendo la infinidad de variables) que están en $\mathcal{L}$. podemos denotar a un modelo $\mathfrak{A}$ para $\mathcal{L}$ como:

$$\mathfrak{A} = \langle A, \{H_1, \ldots, H_m\}, \{S_1, \ldots, S_n\}, \{a_k\}_{k\in\omega}\rangle$$

donde la interpretación de los símbolos en el lenguaje $\mathcal{L}$ está dada por $(R_i)^{\mathfrak{A}} = H_i$, $(F_j)^{\mathfrak{A}} = S_j$ y $(a_k)^{\mathfrak{A}} = a_k$

Ejemplo 3.16. *Dado un lenguaje $\mathcal{L} = \{\{+, \cdot\}, \{\mathbf{0}, \mathbf{1}\}\}$, donde $+, \cdot$ son símbolos funcionales de aridad 2 y $\{\mathbf{0}, \mathbf{1}\}$ son símbolos constantes, entonces podemos definir las siguientes teorías:*

- *La teoría de grupos $\mathcal{T}_G$, con los siguientes axiomas:*

  (G1) (Asociatividad en la adición) $(\forall x, y, z)((x + (y + z)) = ((x + y) + z))$

  (G2) (Elemento neutro en la adición) $(\forall x)((x+\mathbf{0}) = x) \wedge ((\mathbf{0}+x) = x))$, también podemos escribirlo de la siguiente manera si no hay confusión $(\forall x)((x+\mathbf{0}) = (\mathbf{0}+x) = x))$.

  (G3) (Elemento inverso en la adición) $(\forall x)(\exists y)((x + y = \mathbf{0}) \wedge (y + x = \mathbf{0}))$, también podemos escribirlo de la siguiente manera si no hay confusión $(\forall x)(\exists y)(x+y = y+x = \mathbf{0})$.

  Decimos que la teoría formal $\mathcal{T}_{AG}$ es la teoría de los grupos abelianos (o conmutativos), si $\mathcal{T}_G \subseteq \mathcal{T}_{AG}$ y además anexamos el siguiente axioma:

  (G4) (Conmutatividad en la adición) $(\forall x, y)((x + y = y + x)$

- *Una teoría formal $\mathcal{T}_R$ que denota la teoría de anillos (con unidad), donde $\mathcal{T}_{AG} \subseteq \mathcal{T}_R$ y anexando los siguientes axiomas:*

(R1) ***(Asociatividad del producto)*** $(\forall x, y, z)((x \cdot (y \cdot z)) = ((x \cdot y) \cdot z))$

(R2) ***(Elemento neutro del producto)*** $(\forall x)((x \cdot \mathbf{1}) = x) \wedge ((\mathbf{1} \cdot x) = x))$, también podemos escribirlo de la siguiente manera si no hay confusión $(\forall x)((x \cdot \mathbf{1}) = (\mathbf{1} \cdot x) = x))$.

(R3) ***(Propiedad distributiva del producto sobre la adición)*** $(\forall x)(\forall y)(\forall z)((x \cdot (y + z) = (x \cdot y) + (x \cdot z))$.

El axioma **R2** *se puede omitir, obteniendo la teoría de los anillos sin uno, convenientemente diremos que $\mathcal{T}_R$ describe la teoría de anillos incluyendo el axioma* **R2**.

Nota 3.17. *Notemos que en los anillos con uno, no es necesario el axioma* **G4** *pues $a+(a+b)+b) = (a+a)+(b+b) = (1+1)a+(1+1)b = (1+1)(a+b) = (a+b)+(a+b) = a+(b+a)+b$ cancelando se obtiene que $a + b = b + a$*

Decimos que la teoría formal $\mathcal{T}_{CR}$ es la teoría de los anillos conmutativos si $\mathcal{T}_R \subseteq \mathcal{T}_{CR}$ y anexando el siguiente axioma:

(R4) ***(Conmutatividad del producto)*** $(\forall x)(\forall y)(x \cdot y = y \cdot x)$

- *Definimos la teoría formal $\mathcal{T}_F$ que denota la teoría de campos (ó cuerpos), donde $\mathcal{T}_{CR} \subseteq \mathcal{T}_F$ y anexando los siguientes axiomas:*

(K1) ***(Elemento inverso del producto)*** $(\forall x)(\exists y)((x = \mathbf{0}) \vee (\neg(x = 0) \wedge (x \cdot y = \mathbf{1}) \wedge (y \cdot x = \mathbf{1})))$, también podemos escribirlo de la siguiente manera si no hay confusión $(\forall x)(\exists y)((x = \mathbf{0}) \vee ((x \neq \mathbf{0}) \wedge x \cdot y = y \cdot x = \mathbf{1})$.

(K2) $\neg(\mathbf{0} = \mathbf{1})$

Definición 3.18. *Sean S un conjunto y $\mathbf{B}$ una familia de funciones tales que $f \in \mathbf{B}$ si $f : D \longrightarrow \{0, 1\}$ para cada $D \subseteq S$ finito. Decimos que $\mathcal{B}$ es un desorden binario sobre S, si $\mathbf{B}$ satisface lo siguiente:*

- *Para cada $P \subseteq S$ finito, existe $g \in \mathbf{B}$ tal que $Dom(g) = P$*
- *Para cada $g \in \mathbf{B}$ y cada subconjunto finito $D \subseteq S$, entonces $g|_D \in \mathbf{B}$*

Dada una función $f : S \longrightarrow \{0, 1\}$, entonces f es consistente con $\mathbf{B}$ si para cada $D \subseteq S$, se tiene que $f_D \in \mathbf{B}$

Analicemos algunos resultados equivalentes al *lema del ultrafiltro*:

Proposición 3.19. *Las siguientes propiedades son equivalentes:*

a) Lema del ultrafiltro

b) Para cada desorden binario $\mathbf{B}$ sobre un conjunto S, existe una función $f : S \longrightarrow \{0, 1\}$ que es consistente con $\mathbf{B}$.

c) Una teoría $\mathcal{T}$ es satisfacible si y solo si cada subconjunto $\Sigma \subseteq \mathcal{T}$ finito es satisfacible

d) Teorema del ideal primo

Demostración: ***a) ⇒ b)*** Sea $\mathbf{B}$ un desorden binario sobre un conjunto S. Sea $Fin(S) = \{D \subseteq S \,|\, D \text{ es finito}\}$. Para cada $D \in Fin(S)$ sea:

$$A_D = \{g : S \longrightarrow \{0,1\} \,|\, g|_D \in \mathbf{B}\}$$

Desde que $\mathbf{B}$ es un desorden binario, para cualesquiera $C, D \in Fin(S)$, $A_{C\cup D} = \{g : S \longrightarrow \{0,1\} \,|\, g|_{C\cup D} \in \mathbf{B}\}$. Dado que $f = g|_{C\cup D} \in \mathbf{B}$, entonces $g|_C = f|_C$ y $g|_D = f|_D$, con ello $g|_C, g|_D \in \mathbf{B}$ y así $g \in A_C \cap A_D$, lo cual nos dice que $\mathcal{C} = \{A_P \,|\, P \in Fin(S)\}$ tiene la propiedad de intersección finita y en consecuencia existe un filtro $\mathcal{F}$ tal que $\mathcal{C} \subseteq \mathcal{F}$. Por el *lema del ultrafiltro*, existe un ultrafiltro $\mathcal{U}$ que contiene a dicho filtro y entonces para cada $s \in S$, $\{g : S \longrightarrow \{0,1\} \,|\, g(s) = 0\} \in \mathcal{U}$ ó bien $\{g : S \longrightarrow \{0,1\} \,|\, g(s) = 1\} \in \mathcal{U}$, luego para cada $s \in S$ podemos definir una función f tal que $A_s = \{g : S \longrightarrow \{0,1\} \,|\, g(s) = f(s)\} \in \mathcal{U}$. Dado un conjunto finito $P = \{s_1, \ldots, s_n\}$, entonces $\bigcap_{i=1}^{n} A_{s_i} \in \mathcal{U}$, pero $\bigcap_{i=1}^{n} A_{s_i} = \bigcap_{i=1}^{n} \{g : S \longrightarrow \{0,1\} \,|\, g(s_i) = f(s_i)\} = \{g : S \longrightarrow \{0,1\} \,|\, g(s_i) = f(s_i) \text{ para cada } i \in \{1, \ldots, n\}\} = f|_P$. Por lo tanto f es consistente con $\mathbf{B}$.

b) ⇒ c) ⇒] Supongamos que $\mathcal{T}$ es satisfacible, entonces existe $\mathfrak{A}$, tal que $\mathfrak{A} \vDash \varphi$ para cada $\varphi \in \mathcal{T}$, entonces para cada $\Sigma \subseteq \mathcal{T}$, se tiene que $\mathfrak{A} \vDash \sigma$ para cada $\sigma \in \Sigma \subseteq \mathcal{T}$, particularmente si Σ es finito. Por lo tanto, Σ es satisfacible.

⇐] Sea $\mathcal{T}$ una teoría y $S \subseteq \mathcal{L}$ el conjunto de todas las variables que aparecen en $\mathcal{T}$. Asumiendo que todo subconjunto finito Σ de $\mathcal{T}$ es satisfacible, hay un modelo $\mathfrak{A}$ tal que $\mathfrak{A} \vDash \sigma$, sin perdida de la generalidad podemos definir la interpretación de dicho modelo como la función $g_\Sigma : S_\Sigma \longrightarrow \{0,1\}$ de tal manera que Σ es satisfacible y donde S_Σ denota al conjunto de todas las variables que aparecen en Σ. Sea:

$$\mathbf{B}_\mathcal{T} = \{g_\Sigma|_P \,|\, \Sigma \in Fin(\mathcal{T}) \text{ y } P \subseteq S_\Sigma\}$$

Luego $\mathbf{B}_\mathcal{T}$ es un desorden binario en S y por *principio de consistencia* existe una función $f : S \longrightarrow \{0,1\}$ consistente con $\mathbf{B}$, la cual es una interpretación de $\mathcal{T}$. Por lo tanto $\mathcal{T}$ es satisfacible

c) ⇒ d) Sea $\mathbf{B}$ un álgebra booleana y definimos un lenguaje $\mathcal{L}$ tal que $\{p_u \,|\, u \in \mathbf{B}\} \subseteq \mathcal{L}$. Además, sea $\Sigma_\mathbf{B}$ un conjunto de fórmulas, que tiene como a elementos a:

- $p_\mathbf{0}, \neg p_\mathbf{1}$;
- $p_u \vee \neg p_{-u}$ para cada $u \in \mathbf{B}$;
- $(p_{u_1} \wedge \ldots \wedge p_{u_n}) \to p_{u_1+\ldots+u_n}$ para cada $u_1, \ldots, u_n \in \mathbf{B}$;
- $(p_{u_1} \vee \ldots \vee p_{u_n}) \to p_{u_1 \cdot \ldots \cdot u_n}$ para cada $u_1, \ldots, u_n \in \mathbf{B}$;

Para probar que cada subconjunto finito de $\Sigma_\mathbf{B}$ es satisfacible, sea $\Sigma \subseteq \Sigma_\mathbf{B}$ y $S = \{p_u \,|\, p_u \in \Sigma\}$. Puesto que $\langle S \rangle = \mathbf{S}$ es un conjunto finito (ver *Corolario 1.56*), por la finitud del conjunto $\mathbf{S}$, podemos elegir un elemento $u \in \mathbf{S}\backslash\{\mathbf{1}\}$, tal que para cada $v \in \mathbf{S}$ no puede suceder $u < v < \mathbf{1}$. Probemos que $\mathfrak{I}_u = \{v \in \mathbf{B} \,|\, v \leq u\}$ es un ideal primo. Sabemos por la *Proposición 1.45*, que $\mathfrak{I}_u$ es un ideal. Ahora, supongamos que $\mathfrak{I}_u$ no es un ideal primo, entonces existe un ideal $\mathfrak{I}$ tal que $\mathfrak{I}_u \subsetneq \mathfrak{I}$. Elíjase $x \in \mathfrak{I}\backslash\mathfrak{I}_u$, entonces $x \not\leq u$ y con ello $u < u + x$, lo cual es una contradicción. Por lo tanto $\mathfrak{I}_u$ es un ideal primo.

Por el inciso *c)*, $\Sigma_\mathbf{B}$ es una teoría satisfacible y por tanto la teoría tiene un modelo $\mathfrak{A}$. Sea $f : FORM_\mathcal{L} \longrightarrow \{0,1\}$ tal que $f(\varphi) = 1$ si y solo sí $\mathfrak{A} \vDash \varphi$ con ello definamos al conjunto $I = \{u \in \mathbf{B} \,|\, f(p_u) = 1\}$, entonces:

- $f(p_0) = 1$ y $f(p_1) = 0$; luego $1 \notin I$, pero $0 \in I$.
- $f(p_u) = 1 - f(\neg p_{u^-})$; esto nos dice que para cada $u \in \mathbf{B}$, $u \in I$ ó $u^- \in I$.
- Si $f(p_{u_1}) = f(p_{u_2}) = 1$, entonces $f(p_{u_1} \wedge p_{u_2}) = 1$; esto nos dice que si $u_1, u_2 \in I$, entonces $u_1 + u_2 \in I$

- Si $f(p_{u_1}) = 1$, entonces $f(p_{u_1} \vee p_{u_2}) = 1$; esto nos dice que si $u_1 \in I$ y $u_2 \in \mathbf{B}$, entonces $u_1 \cdot u_2 \in I$

Por lo tanto el conjunto I es un ideal primo de $\mathbf{B}$.

c) ⇒ d) Es un resultado que ya vimos anteriormente. □

Al inciso *b*) de la proposición anterior, se le conoce como *principio de consistencia* y por otro lado, al inciso *a*) se le conoce como el *teorema de compacidad.*

3.2. Ultraproductos

Definición 3.20. *Sea I un conjunto de índices. Para cada $i \in I$, sea $\mathfrak{A}_i$ un modelo con universo A_i. Definimos el producto cartesiano de estructuras $\mathfrak{A} = \prod_{i\in I} \mathfrak{A}_i$ como sigue:*

- $\prod_{i\in I} A_i = \{f : I \to \bigcup_{i\in I} A_i \,|\, f(i) \in A_i\}$ *para mayor comodidad, podemos escribir* $\prod_{i\in I} A_i = A$
- *Para cualquier símbolo relacional de aridad n se tiene que $R^{\mathfrak{A}}(f_1, \ldots, f_n)$ si y solo si $R^{\mathfrak{A}_i}(f_1(i), \ldots, f_n(i))$ para cada $i \in I$.*
- *Para cualquier símbolo funcional de aridad n se tiene que $F^{\mathfrak{A}}(f_1, \ldots, f_n) = (F^{\mathfrak{A}_i}(f_1, \ldots, f_n))_{i\in I}$*
- *Para cualquier símbolo constante se tiene que $c^{\mathfrak{A}} = (c^{\mathfrak{A}_i})_{i\in I}$.*
- $\mathfrak{A} = \langle A, \{R_j^{\mathfrak{A}}\}_{j\in\omega}, \{F_j^{\mathfrak{A}}\}_{j\in\omega}, \{c_j^{\mathfrak{A}}\}_{j\in\omega}\rangle$.

Notemos de la definición anterior, que I puede tener cualquier cardinalidad.

Nota 3.21. *Sean I un conjunto no vacío y $\mathcal{F} \subseteq \mathcal{P}(I)$. Se define la relación $\sim_{\mathcal{F}}$ en $\mathcal{F}$ como sigue:*

$$f \sim_{\mathcal{F}} g \text{ sii } \{i \in I | f(i) = g(i)\} \in \mathcal{F}$$

Proposición 3.22. *Si $\mathcal{F}$ es un filtro sobre I, entonces $\sim_{\mathcal{F}}$ es una relación de equivalencia sobre $\mathfrak{A}$.*

Demostración: Puesto que $\mathcal{F}$ es un filtro, se tiene que $I \in \mathcal{F}$. Entonces, para cada $f \in A$, $f \sim_{\mathcal{F}} f$ sii $I = \{i \in I \,|\, f(i) = f(i)\} \in \mathcal{F}$. De aquí $\sim_{\mathcal{F}}$ es reflexiva.

Por otro lado, notemos que para cualesquiera $f, g \in A$ se cumple que $f \sim_{\mathcal{F}} g$ sii $X = \{i \in I \,|\, f(i) = g(i)\} \in \mathcal{F}$ sii $X = \{i \in I \,|\, g(i) = f(i)\} \in \mathcal{F}$ sii $g \sim_{\mathcal{F}} f$. Con ello, $\sim_{\mathcal{F}}$ es simétrica.

Por último, veamos que $\sim_{\mathcal{F}}$ es transitiva. Sean $f, g, h \in A$ tales que $f \sim_{\mathcal{F}} g$ y $g \sim_{\mathcal{F}} h$. Lo anterior ocurre si y sólo si $X = \{i \in I \,|\, f(i) = g(i)\} \in \mathcal{F}$ y $Y = \{i \in I \,|\, g(i) = h(i)\} \in \mathcal{F}$ sii $X \cap Y \subseteq Z = \{i \in I \,|\, f(i) = h(i)\} \in \mathcal{F}$ sii $f \sim_{\mathcal{F}} h$, por lo que $\sim_{\mathcal{F}}$ es transitiva y por lo anterior es una relación de equivalencia □

Es bien sabido que toda relación de equivalencia induce una partición. Luego, para cada elemento $f \in A$ definimos $f/\mathcal{F}$, la clase de equivalencia de f bajo la relación $\sim_{\mathcal{F}}$.

Lema 3.23. *Sea $\mathcal{F}$ un filtro sobre el conjunto I y sea $\sim_{\mathcal{F}}$ la relación antes mencionada. Entonces:*

a) Si $f_1 \sim_{\mathcal{F}} g_1, \ldots, f_n \sim_{\mathcal{F}} g_n$, entonces $\{i \in I \,|\, R^{\mathfrak{A}_i}(f_1(i), \ldots, f_n(i))\} \in \mathcal{F}$ si y solo si $\{i \in I \,|\, R^{\mathfrak{A}_i}(g_1(i), \ldots, g_n(i))\} \in \mathcal{F}$

b) Si $f_1 \sim_{\mathcal{F}} g_1, \ldots, f_n \sim_{\mathcal{F}} g_n$, entonces $F^{\mathfrak{A}}(f_1(i), \ldots, f_n(i)) \sim_{\mathcal{F}} F^{\mathfrak{A}}(g_1(i), \ldots, g_n(i))$

Demostración:

a) $\Rightarrow$] Sean $A_1 = \{i \in I \,|\, f_1(i) = g_1(i))\}, \ldots, A_n = \{i \in I \,|\, f_n(i) = g_n(i))\}$ tales que $A_1, \ldots, A_n \in \mathcal{F}$ y sea $B = \{i \in I \,|\, R^{\mathfrak{A}_i}(f_1(i), \ldots, f_n(i))\} \in \mathcal{F}$, sea $i \in D = A_1 \cap \ldots \cap A_n \cap B$ así $f_1(i) = g_1(i), \ldots, f_n(i) = g_n(i)$ y $R^{\mathfrak{A}_i}(f_1(i), \ldots, f_n(i))$. Por tanto, $R^{\mathfrak{A}_i}(g_1(i), \ldots, g_n(i))$. Entonces, puesto que $\mathcal{F}$ es un filtro se tiene que $D \in \mathcal{F}$, además $D \subseteq \{i \in I \,|\, R^{\mathfrak{A}_i}(g(i), \ldots, g_n(i))\} \in \mathcal{F}$.
$\Leftarrow$] es análogo.

b) Tomemos los mismos conjuntos $A_1, \ldots A_n$ de la demostración anterior, entonces $E = A_1 \cap \ldots \cap A_n \in \mathcal{F}$. Consideremos el siguiente conjunto $C = \{i \in I \,|\, F^{\mathfrak{A}_i}(f_1(i), \ldots, f_n(i)) = F^{\mathfrak{A}_i}(g_1(i), \ldots, g_n(i))\}$. Si $i \in E$, entonces $f_1(i) = g_1(i), \ldots, f_n(i) = g_n(i)$ y por lo tanto $F^{\mathfrak{A}_i}(f_1(i), \ldots, f_n(i)) = F^{\mathfrak{A}_i}(g_1(i), \ldots, g_n(i))$. De aquí se sigue que $E \subseteq C$, pero como $E \in \mathcal{F}$ y ya que $\mathcal{F}$ es un filtro, entonces $C \in \mathcal{F}$ □

Definición 3.24. *Sea $\mathcal{F}$ un filtro sobre un conjunto I, se definimos el modelo $\mathfrak{A}/\mathcal{F}$ de la siguiente forma:*

$$\mathfrak{A}/\mathcal{F} = \prod_{i\in I}\mathfrak{A}_i/\mathcal{F} = \langle \prod_{i\in I} A_i/\mathcal{F}, \{\overline{R}_j\}_{j\in\omega}, \{\overline{F}_j\}_{j\in\omega}, \{\overline{c}_j\}_{j\in\omega}\rangle,$$

donde:

- $\prod_{i\in I} A_i/\mathcal{F} = \{f/\mathcal{F} \,|\, f \in \prod_{i\in I} A_i\}$
- $R_j^{\mathfrak{A}/\mathcal{F}}(f_1/\mathcal{F}, \ldots, f_n/\mathcal{F}) = \{i \in I \,|\, R_j^{\mathfrak{A}_i}(f_1(i), \ldots, f_n(i))\} \in \mathcal{F}$
- $F_j^{\mathfrak{A}/\mathcal{F}}(f_1/\mathcal{F}, \ldots, f_n/\mathcal{F}) = F_j^{\mathfrak{A}}(f_1(i), \ldots, f_n(i))/\mathcal{F}$
- $c_j^{\mathfrak{A}/\mathcal{F}} = c_j^{\mathfrak{A}}/\mathcal{F}$

Al modelo anterior se le denomina *producto reducido*. En caso de que $\mathcal{F}$ es un ultrafiltro, se dice que $\prod_{i\in I}\mathfrak{A}_i/\mathcal{F}$ es un *ultraproducto*. Finalmente, si $\mathfrak{A}_i = \mathfrak{A}$, entonces $\prod_{i\in I}\mathfrak{A}/\mathcal{F}$ se denomina una *ultrapotencia*.

Lema 3.25. *Para cada $t \in TERM$ se tiene que $t^{\mathfrak{A}/\mathcal{F}}(f_1, \ldots, f_n) = t^{\mathfrak{A}}(f_1(i), \ldots, f_n(i))/\mathcal{F}$*

Demostración: La demostración se hará por inducción sobre la complejidad del término:

- Si $t = c$ un símbolo constante, entonces;

$$t^{\mathfrak{A}/\mathcal{F}}(f_1, \ldots, f_n) = c^{\mathfrak{A}/\mathcal{F}} = c^{\mathfrak{A}}/\mathcal{F} = t^{\mathfrak{A}}(f_1, \ldots, f_n)/\mathcal{F}$$

- Si $t = x$ una variable, entonces:

$$t^{\mathfrak{A}/\mathcal{F}}(f_1, \ldots, f_n) = x^{\mathfrak{A}/\mathcal{F}} = x^{\mathfrak{A}}/\mathcal{F} = t^{\mathfrak{A}}(f_1, \ldots, f_n)/\mathcal{F}$$

- Si $t = F(t_1, \ldots, t_n)$ es un símbolo funcional de aridad n, entonces:

$$t^{\mathfrak{A}/\mathcal{F}}(f_1, \ldots, f_n) = F^{\mathfrak{A}/\mathcal{F}}(t_1(f_1, \ldots, f_n), \ldots, t_n(f_1, \ldots, f_n)) =$$

$$\text{Por definición } F^{\mathfrak{A}/\mathcal{F}}(t_1^{\mathfrak{A}/\mathcal{F}}(f_1, \ldots, f_n), \ldots, t_n^{\mathfrak{A}/\mathcal{F}}(f_1, \ldots, f_n)) =$$

$$\text{por H.I. } F^{\mathfrak{A}/\mathcal{F}}(t_1^{\mathfrak{A}}(f_1, \ldots, f_n)/\mathcal{F}, \ldots, t_n^{\mathfrak{A}}(f_1, \ldots, f_n)/\mathcal{F}) =$$

$$F^{\mathfrak{A}}(t_1^{\mathfrak{A}}(f_1, \ldots, f_n), \ldots, t_n^{\mathfrak{A}}(f_1, \ldots, f_n))/\mathcal{F}$$

□

Teorema 3.26. *(De Łos: Fundamental de los Ultraproductos) Sean $\{\mathfrak{A}_i : i \in I\}$ una familia de modelos y $\mathcal{U}$ un ultrafiltro en I. Entonces, para cada fórmula $\varphi \in \mathcal{L}$:*

$$\prod_{i\in I} \mathfrak{A}_i/\mathcal{U} \vDash \varphi \text{ si y solo si } \{i \in I \,|\, \mathfrak{A}_i \vDash \varphi\} \in \mathcal{U}$$

Demostración: Para términos mas prácticos, denotemos a $\prod_{i\in I} \mathfrak{A}_i/\mathcal{U}$ simplemente por $\mathfrak{A}/\mathcal{F}$. La prueba se hará sobre inducción sobre la complejidad de la fórmula.

- Si $\varphi := t = t'$, donde $t, t' \in TERM$, entonces:

$$\begin{aligned} \mathfrak{A}/\mathcal{F} \vDash (t = t') &\text{ si y solo sí } (t)^{\mathfrak{A}/\mathcal{F}} = (t')^{\mathfrak{A}/\mathcal{F}}. \\ &\text{si y solo sí } (t)^{\mathfrak{A}}/\mathcal{F} = (t')^{\mathfrak{A}}/\mathcal{F} \\ &\text{si y solo sí } (t)^{\mathfrak{A}} \sim_{\mathcal{F}} (t')^{\mathfrak{A}} \\ &\text{si y solo sí } \{i \in I \,|\, (t)^{\mathfrak{A}_i} = (t')^{\mathfrak{A}_i}\} \in \mathcal{U} \\ &\text{si y solo sí } \{i \in I \,|\, \mathfrak{A}_i \vDash (t = t')\} \in \mathcal{U} \end{aligned}$$

- Si $\varphi := R(t_1, ..., t_n)$, donde R es un símbolo relacional de aridad n y donde $t_1, ..., t_n \in TERM$ el resultado es claro.

- Si $\varphi := \psi \wedge \gamma$, donde $\psi, \gamma \in FORM$, entonces:

$$\begin{aligned} \mathfrak{A} \vDash (\psi \wedge \gamma) &\text{ si y solo sí } \mathfrak{A} \vDash \psi \text{ y } \mathfrak{A} \vDash \gamma \\ &\text{si y solo sí } I_\psi = \{i \in I \,|\, \mathfrak{A}_i \vDash \psi\} \in \mathcal{U} \text{ y } I_\gamma = \{i \in I \,|\, \mathfrak{A}_i \vDash \gamma\} \in \mathcal{U} \\ I_\psi \cap I_\gamma \in \mathcal{U} &\text{ si y solo sí } I_\psi \cap I_\gamma = \{i \in I \,|\, \mathfrak{A}_i \vDash \psi \text{ y } \mathfrak{A}_i \vDash \gamma\} \in \mathcal{U} \\ &\text{si y solo sí } \{i \in I \,|\, \mathfrak{A}_i \vDash \psi \wedge \gamma\} \in \mathcal{U} \end{aligned}$$

- Si $\varphi := \neg\psi$, donde $\psi \in FORM$, entonces:

$$\begin{aligned} \mathfrak{A} \vDash (\neg\psi) &\text{ si y solo sí } \mathfrak{A} \nvDash \psi \\ &\text{si y solo sí } I_\psi = \{i \in I \,|\, \mathfrak{A}_i \vDash \psi\} \notin \mathcal{U} \\ I - I_\psi \in \mathcal{U} &\text{ si y solo sí } I - \{i \in I \,|\, \mathfrak{A}_i \vDash \psi\} \in \mathcal{U} \\ &\text{si y solo sí } \{i \in I \,|\, \mathfrak{A}_i \nvDash \psi\} \in \mathcal{U} \\ &\text{si y solo sí } \{i \in I \,|\, \mathfrak{A}_i \vDash \neg\psi\} \in \mathcal{U} \end{aligned}$$

- Si $\varphi := (\exists x)\psi(x)$, donde $\psi \in FORM$, entonces:

$$\begin{aligned} \mathfrak{A} \vDash (\exists x)\psi(x) &\text{ si y solo sí existe } a = (a_1/\mathcal{U}, \ldots, a_n/\mathcal{U}, \ldots) \in \mathfrak{A} \text{ tal que } \mathfrak{A} \vDash \psi(a) \\ &\text{si y solo sí existe } a_i/\mathcal{U} \in \mathfrak{A}_i \text{ tal que } I_\psi = \{i \in I \,|\, \mathfrak{A}_i \vDash \psi(a_i/\mathcal{U})\} \in \mathcal{U} ...(1). \end{aligned}$$

  Por lo anterior, se cumple que $I_\psi = \{i \in I \,|\, \mathfrak{A}_i \vDash \psi(a_i/\mathcal{U})\} \subseteq \{i \in I \,|\, \mathfrak{A}_i \vDash (\exists x)\psi(x)\}$. Ahora, dado que $\mathcal{U}$ es un filtro, tenemos que $\{i \in I \,|\, \mathfrak{A}_i \vDash (\exists x)\psi(x)\} \in \mathcal{U}$. Por otro lado, si $\{i \in I \,|\, \mathfrak{A}_i \vDash (\exists x)\psi(x)\} \in \mathcal{U}$, existe $a_i/\mathcal{U} \in \mathfrak{A}_i$ para cada $i \in I$, de forma que $\{i \in I \,|\, \mathfrak{A}_i \vDash \psi(a_i/\mathcal{U})\} \in \mathcal{U}$. Luego, por hipótesis inductiva existe $a = (a_1/\mathcal{U}, ..., a_n/\mathcal{U})$ tal que $\mathfrak{A} \vDash \psi(a)$ y por lo tanto $\mathfrak{A} \vDash (\exists x)\psi(x)$. □

Teorema 3.27. *(De compacidad)*
Una teoría $\mathcal{T}$ es satisfacible si y solo si cada subconjunto $\Sigma \subseteq \mathcal{T}$ finito es satisfacible.

Demostración:

$\Rightarrow$] Supongamos que $\mathcal{T}$ es satisfacible, entonces existe $\mathfrak{A}$, tal que $\mathfrak{A} \vDash \varphi$ para cada $\varphi \in \mathcal{T}$. Entonces, si $\Sigma \subseteq \mathcal{T}$ es un subconjunto finito, se tiene que $\mathfrak{A} \vDash \sigma$ para cada $\sigma \in \Sigma \subseteq \mathcal{T}$.

$\Leftarrow$] Enumeremos por $\{\Sigma_i : i \in I\}$ a la colección de subconjuntos finitos de $\mathcal{T}$. Supongamos que para cada $i \in I$ se cumple que $\mathfrak{A}_i$ es un modelo para Σ_i. Para cada $\sigma \in \mathcal{T}$, defínase $\Gamma_\sigma = \{i \in I \,|\, \sigma \in i\}$, la colección de los subconjuntos finitos de Σ que contienen a σ. Ahora, sea $\Gamma = \{\Gamma_\sigma \,|\, \sigma \in \mathcal{T}\}$. Afirmamos que Γ cumple la propiedad de intersección finita. En efecto, sean $\sigma_1, \ldots, \sigma_n \in \mathcal{T}$, entonces $\Gamma_{\sigma_1}, \ldots, \Gamma_{\sigma_n} \in \Gamma$, lo cual implica que $\{\sigma_1, \ldots, \sigma_n\} \in \bigcap_{i=1}^{n} \Gamma_{\sigma_i} \neq \emptyset$.

Ahora, ya que Γ es una familia que cumple la propiedad de intersección finita, existe $\mathcal{F} \subseteq \mathcal{P}(I)$ filtro en I, tal que $\Gamma \subseteq \mathcal{F}$. Más aún, existe un ultrafiltro $\mathcal{U}$ tal que $\mathcal{F} \subseteq \mathcal{U}$. Ahora, si $\Sigma \in \Gamma_\sigma$, se tiene que $\sigma \in \Sigma$ y entonces existe por hipótesis un modelo $\mathfrak{A}_\Sigma$ tal que $\mathfrak{A}_\Sigma \vDash \sigma$, entonces $\Gamma_\sigma \subseteq \{\Sigma \,|\, \mathfrak{A}_\Sigma \vDash \sigma\}$, entonces ya que $\mathcal{U}$ es un filtro $\{\Sigma \,|\, \mathfrak{A}_\Sigma \vDash \sigma\} \in \mathcal{U}$. Ahora por el *teorema (De Łos)* se tiene que $\{\Sigma \,|\, \mathfrak{A}_\Sigma \vDash \sigma\} \in \mathcal{U}$ si y solo si $\prod_{i \in I} \mathfrak{A}_i/\mathcal{U} \vDash \sigma$, de aquí que $\prod_{i \in I} \mathfrak{A}_i/\mathcal{U} \vDash \mathcal{T}$ □

Notemos que en ningún momento hemos usado el *axioma de elección* o alguna de sus equivalencias salvo para demostrar el *lema del ultrafiltro*. Miroslav Repický demostro [17] en 2015 que existe un modelo donde el *teorema del ideal primo* se cumple, pero el *axioma de elección* falla.

Uno pensaría que el *Teorema 3.28* bastaría para probar la equivalencia del Lema del ultrafiltro con el axioma de elección, pero resulta que el *teorema de Łos* con el *lema del ultrafiltro* implican el axioma de elección, lo cual no nos permitiría demostrar dicha equivalencia. Ahora, mostremos dicho resultado que puede consultar en [2].

Proposición 3.28. *El teorema de Łos y el lema del ultrafiltro implican el axioma de elección.*

Demostración: Sea X un conjunto no vacío. Supongamos que X no tiene una función de elección, luego consideremos al conjunto $\mathcal{I} = \{Y \subseteq X \,|\, Y \text{ tiene una función de elección }\} \cup \{\emptyset\}$. Veamos que $\mathcal{I}$ es un ideal sobre $\mathcal{P}(X)$. En efecto:

$\emptyset \in \mathcal{I}$ y por suponer que X no tiene una función de elección, entonces $X \notin \mathcal{I}$.

Por otro lado, sean $A \in \mathcal{I}$ y $B \in \mathcal{P}(X)$ tales que $B \subseteq A$, luego A tiene una función de elección $f : \mathcal{P}(A)\backslash\{\emptyset\} \longrightarrow A$, y ya que $\mathcal{P}(B) \subseteq \mathcal{P}(A)$, existe una función de elección $g : \mathcal{P}(B)\backslash\{\emptyset\} \longrightarrow B$ para B tal que para cada $C \subseteq B$, $g(C) = f(C) \in C$, entonces $B \in \mathcal{I}$.

Ahora, consideremos $A, B \in \mathcal{I}$. Entonces, existen $f : \mathcal{P}(A)\backslash\{\emptyset\} \longrightarrow A$ y $g : \mathcal{P}(B)\backslash\{\emptyset\} \longrightarrow B$ funciones de elección. Defínase la función $h : \mathcal{P}(A \cup B)\backslash\{\emptyset\} \longrightarrow A \cup B$ tal que:

$$h(C) = \begin{cases} f(C \cap A) & si \quad C \cap A \neq \emptyset \\ \\ g(C) & si \quad C \cap A = \emptyset \end{cases}$$

Entonces, h es una función de elección de $A \cup B$, pues dado $S \in \mathcal{P}(A \cup B)\backslash\{\emptyset\}$, si $S \cap A \neq \emptyset$, entonces $h(S) = f(S \cap A) \in S \cap A \subseteq S$. Por otro lado al suponer que $S \cap A = \emptyset$, entonces $h(S) = g(S) \in S \subseteq B$. Por lo tanto $\mathcal{I}$ es un ideal. Por el teorema del ideal primo existe un filtro $\mathcal{I}'$ que contiene a dicho ideal. Lo anterior ocurre si y solo si $\mathcal{U} = \{A \in \mathcal{P}(X) \,|\, X\backslash A \in \mathcal{I}'\}$ es un ultrafiltro.

Ahora, consideremos al conjunto $A = \mathcal{P}(X) \cup X$ y con ello definimos la siguiente relación $\mathcal{R}$ en A:

$$t\mathcal{R}y \text{ si y solo sí } (y \in \mathcal{P}(X) \text{ y } t \in y) \text{ o bien } (y = t \text{ y } t \in X).$$

Así obtenemos los modelos $\mathfrak{M}_x = \mathfrak{M} = \langle A, \mathcal{R}\rangle$, luego notemos que para cada $y \in A$, existe $t \in X$ tal que $t \in y$, es decir que $\mathfrak{M}_x \vDash (\forall y)(\exists t)(t\mathcal{R}y)$, entonces $\{x \in \mathcal{P}(X) \,|\, \mathfrak{M}_x \vDash (\forall y)(\exists t)(t\mathcal{R}y)\} = \mathcal{P}(X) \in \mathcal{U}$, luego por el teorema *de Łos ó Fundamental de los ultraproductos* esto pasa si y solo sí $\prod_{i \in I} \mathfrak{M}_i/\mathcal{U} \vDash (\forall y)(\exists t)(t\mathcal{R}y)$, en particular sea $Id_A \in \prod_{i \in I} \mathfrak{M}_i$, luego existe $f \in \prod_{i \in I} \mathfrak{M}_i$ tal que

$\mathcal{R}^{\mathfrak{M}/\mathcal{U}}(Id_A/\mathcal{U}, f/\mathcal{U})$ se satisface en $\prod_{i\in I}\mathfrak{M}_i/\mathcal{U}$, entonces cuando $y \in \mathcal{U}$ tenemos que $\{y \mid f(y) \in y\} = \{y \mid f(y)\mathcal{R}y\} = \{y \mid f(y)\mathcal{R}\,Id(y)\} \in \mathcal{U}$, pero $\{y \mid f(y) \in y\} \in \mathcal{I}'$ una contradicción. Por lo tanto X tiene una función de elección. □

3.3. Algunas consecuencias del lema del ultrafiltro en teoría de modelos

Definición 3.29. *Sean $\mathfrak{A}$ y $\mathfrak{B}$ modelos. Definimos un morfismo entre $\mathcal{L}$-estructuras como una función $\alpha : \mathfrak{A} \longrightarrow \mathfrak{B}$ que cumple:*

- *Para cualquier símbolo constante $c \in \mathcal{L}$ se tiene que $\alpha(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$.*
- *Para cualquier símbolo funcional f de aridad n y $\overline{a} = (a_1, \ldots, a_n) \in \mathfrak{A}$, se tiene que $\alpha(f^{\mathfrak{A}}(\overline{a})) = f^{\mathfrak{B}}(\alpha(\overline{a}))$.*
- *Para cualquier símbolo relacional R de aridad n de $\mathcal{L}$ y $\overline{a} = (a_1, \ldots, a_n) \in \mathfrak{A}$, tenemos que si $R^{\mathfrak{M}}(\overline{a})$ se satisface, entonces $R^{\mathfrak{N}}(\alpha(\overline{a}))$ también se satisface,*

donde $\overline{a} = (a_1, \ldots, a_n)$ y $\alpha(\overline{a})$ denota a $(\alpha(a_1), \ldots, \alpha(a_n))$.

Decimos que α es una incrustación si es un morfismo inyectivo. Finalmente, decimos que un morfismo entre $\mathcal{L}$-estructuras $g : \mathfrak{A} \longrightarrow \mathfrak{B}$ es un isomorfismo si existe otro morfismo $f : \mathfrak{B} \longrightarrow \mathfrak{A}$ que es el inverso de g. Escribiremos $\mathfrak{A} \cong \mathfrak{B}$ si existe un isomorfismo entre los modelos $\mathfrak{A}$ y $\mathfrak{B}$

Proposición 3.30. *Si dos modelos son isomorfos, entonces son elementalmente equivalentes.*

Demostración: Haremos la prueba por inducción sobre la complejidad de la fórmula. Sean $\mathfrak{A}$ y $\mathfrak{B}$ modelos isomorfos, entonces existe un isomorfismo $g : \mathfrak{A} \longrightarrow \mathfrak{B}$ y con ello tenemos lo siguiente:

1. Si $\varphi := (t_1 = t_2)$, entonces:

$$\begin{aligned} \mathfrak{A} \vDash (t_1 = t_2) &\text{ si y solo sí } t_1^{\mathfrak{A}} = t_2^{\mathfrak{A}} \\ \mathfrak{A} \cong \mathfrak{B} &\text{ si y solo sí } t_1^{\mathfrak{B}} = g(t_1^{\mathfrak{A}}) = g(t_2^{\mathfrak{A}}) = t_2^{\mathfrak{B}} \\ &\text{si y solo sí } \mathfrak{B} \vDash (t_1 = t_2) \end{aligned}$$

2. Si $\varphi := R(t_1, ..., t_n)$:

$$\begin{aligned} \mathfrak{A} \vDash R(t_1, ..., t_n) &\text{ si y solo sí } (t_1^{\mathfrak{A}}, ..., t_n^{\mathfrak{A}}) \in R^{\mathfrak{A}} \\ \mathfrak{A} \cong \mathfrak{B} &\text{ si y solo sí } (t_1^{\mathfrak{A}}, ..., t_n^{\mathfrak{A}}) = (g(t_1^{\mathfrak{A}}), ..., g(t_n^{\mathfrak{A}})) \in R^{\mathfrak{B}} \\ &\text{si y solo sí } \mathfrak{B} \vDash R(t_1, ..., t_n) \end{aligned}$$

3. Si $\varphi := (\neg\theta)$, donde $\theta \in FORM$:

$$\begin{aligned} \mathfrak{A} \vDash (\neg\theta) &\text{ si y solo sí } \mathfrak{A} \nvDash \theta \\ \text{Por h.i.} \quad &\text{si y solo sí } \mathfrak{B} \nvDash \theta \\ &\text{si y solo sí } \mathfrak{B} \vDash (\neg\theta) \end{aligned}$$

4. Si $\varphi := (\theta \wedge \gamma)$, donde $\theta, \gamma \in FORM$:

$$\begin{aligned} \mathfrak{A} \vDash (\theta \wedge \gamma) &\text{ si y solo sí } \mathfrak{A} \vDash \theta \text{ y } \mathfrak{A} \vDash \gamma \\ \text{Por h.i.} \quad &\text{si y solo sí } \mathfrak{B} \vDash \theta \text{ y } \mathfrak{B} \vDash \gamma \\ &\text{si y solo sí } \mathfrak{B} \vDash (\theta \wedge \gamma) \end{aligned}$$

5. Si $\varphi := (\exists x)\theta$, donde $\theta \in FORM$:

$$\begin{aligned} \mathfrak{A} \vDash (\exists x)\theta(x) &\text{ si y solo sí para algun } a \in A,\ \mathfrak{A} \vDash \theta(a) \\ \text{Por h.i.} &\text{ si y solo sí para algún } b \in B,\ \mathfrak{B} \vDash \theta(b) \\ &\text{si y solo sí } \mathfrak{B} \vDash (\exists x)\theta(x) \end{aligned}$$

Por lo tanto si dos modelos son isomorfos, entonces son equivalentes. □

Ejemplo 3.31. *Sean $\mathfrak{G}_1 = (G_1, +)$ y $\mathfrak{G}_2 = (G_2, \oplus)$ grupos. Entonces $\alpha : \mathfrak{G}_1 \longrightarrow \mathfrak{G}_2$ definida por:*

- *Para $\mathbf{0}, \mathbf{1} \in \mathcal{L}$ se tiene que $\alpha(\mathbf{0}^{\mathfrak{G}_1}) = \mathbf{0}^{\mathfrak{G}_2}$ y $\alpha(\mathbf{1}^{\mathfrak{G}_1}) = \mathbf{1}^{\mathfrak{G}_2}$.*
- *Para el símbolo funcional $+ \in \mathcal{L}$ y $(g_1, g_2) \in \mathfrak{G}_1$, se tiene que $\alpha(g_1 + g_2) = \alpha(g_1 +^{\mathfrak{G}_1} g_2) = \alpha(g_1) +^{\mathfrak{G}_2} \alpha(g_2) = \alpha(g_1) \oplus \alpha(g_2)$*

  es un morfismo entre $\mathcal{L}$-estructuras.

Notemos que α se comporta de manera similar a los morfismos que definimos en la sección anterior. Similar a lo estudiado anteriormente, es posible verificar que dicho morfismo hereda algunas propiedades.

Sea un conjunto $X \subseteq A$, expandimos al lenguaje $\mathcal{L}$ añadiendo nuevas constantes teniendo el siguiente conjunto $\mathcal{L}_X = \mathcal{L} \cup \{c_x \,|\, x \in X\}$. Luego expandamos al modelo $\mathfrak{A}$ a un modelo $\mathfrak{A}_X = \langle A, (\cdot)^{\mathfrak{A}_X} \rangle$ donde $(\cdot)^{\mathfrak{A}_X}$ es tal que $c_x^{\mathfrak{A}_X} = x$ para cada $x \in X$. En particular en el caso de que $A = X$, entonces obtenemos al modelo $\mathfrak{A}_A$ del lenguaje $\mathcal{L}_A$.

Definición 3.32. *Sean $\mathfrak{A}$ un modelo para $\mathcal{L}$ y $X \subseteq A$, definimos:*

- *La teoría de $\mathfrak{A}$, como el conjunto $Th(\mathfrak{A}) = \{\varphi \in FORM \,|\, \mathfrak{A} \vDash \varphi\}$*
- *Diagrama elemental de $\mathfrak{A}$ en X el conjunto $Th(\mathfrak{A}_X) = \{\varphi \in FORM \,|\, \mathfrak{A}_X \vDash \varphi\}$.*
- *Diagrama atómico de $\mathfrak{A}$ en X el conjunto $\Delta^{\mathfrak{A}} = \{\varphi \in FORM \,|\, \varphi$ es una $\mathcal{L}_X$-fórmula y φ es una fórmula atómica o la negación de una fórmula atómica$\}$*
- *Diagrama de $\mathfrak{A}$ en X el conjunto $\Delta_{\mathfrak{A}} = \{\varphi \in FORM \,|\, \varphi$ es una $\mathcal{L}_X$-fórmula y φ no tiene cuantificadores$\}$.*

Definición 3.33. *Sean $\mathfrak{A} = \langle A, (\cdot)^{\mathfrak{A}} \rangle$ y $\mathfrak{B} = \langle B, (\cdot)^{\mathfrak{B}} \rangle$ modelos para un lenguaje $\mathcal{L}$, decimos que $\mathfrak{A}$ es un submodelo elemental de $\mathfrak{B}$ y $\mathfrak{B}$ es una extensión elemental de $\mathfrak{A}$ sí:*

- *$A \subseteq B$;*
- *Para cada fórmula $\varphi[v_0, \ldots, v_n]$ de $\mathcal{L}$ y para cada $a_0, \ldots, a_n \in A$:*

$$\mathfrak{A} \vDash \varphi[a_0, \ldots, a_n] \text{ si y solo sí } \mathfrak{B} \vDash \varphi[a_0, \ldots, a_n]$$

Definición 3.34. *Decimos que una incrustación $f : \mathfrak{A} \longrightarrow \mathfrak{B}$ de $\mathcal{L}$-estructuras es elemental si para toda fórmula $\varphi[x_0, \ldots, x_n]$ en $\mathcal{L}$ y cada $(a_0, \ldots, a_n) \in A^n$, se tiene que:*

$$\mathfrak{A} \vDash \varphi[a_0, \ldots, a_n] \text{ si y solo sí } \mathfrak{B} \vDash \varphi[f(a_0), \ldots, f(a_n)]$$

Es decir que $\mathfrak{A}$ es un submodelo elemental de $\mathfrak{B}$ si; $\mathfrak{A}$ es un submodelo de $\mathfrak{B}$ y hay una incrustación elemental entre ambos modelos. Lo anterior lo denotamos como $\mathfrak{A} \prec \mathfrak{B}$.

Definición 3.35. *Sea $\mathcal{T}$ una teoría para un lenguaje $\mathcal{L}$, decimos que $\mathcal{T}$ es una teoría completa, si para cada $\varphi \in FORM$, $\mathcal{T} \vDash \varphi$ ó $\mathcal{T} \vDash \neg\varphi$.*

Proposición 3.36. *Sea $\mathfrak{A} = (A, (\cdot)^{\mathfrak{A}})$ un modelo para un lenguaje $\mathcal{L}$ y $X \subseteq A$. Entonces la teoría $Th(\mathfrak{A}_X)$ es completa.*

Demostración: Sea φ una $\mathcal{L}$-fórmula. Suponiendo que $Th(\mathfrak{A}_X) \nvdash \varphi$, entonces $\varphi \notin Th(\mathfrak{A}_X)$. Por definición de $Th(\mathfrak{A}_X)$, $\mathfrak{A}_X \nvdash \varphi$, con lo cual $\mathfrak{A}_X \vDash \neg\varphi$. Por lo tanto, $\neg\varphi \in Th(\mathfrak{A}_X)$. □

Proposición 3.37. *Una teoría $\mathcal{T}$ es completa si y solo sí todos sus modelos son elementalmente equivalentes.*

Demostración: $\Rightarrow$] En particular, sea $\mathfrak{A} = (A, (\cdot)^{\mathfrak{A}})$ un modelo para un lenguaje $\mathcal{L}$ y $\mathcal{T}$ es una $\mathcal{L}$-teoría completa. Afirmamos que $\mathcal{T} = Th(\mathfrak{A})$. Sea $\varphi \in \mathcal{T}$, al ser $\mathfrak{A}$ un modelo de la teoría se tiene que $\mathfrak{A} \vDash \varphi$. Consecuentemente, $Th(\mathfrak{A}) \vDash \varphi$, con lo cual $\varphi \in Th(\mathfrak{A})$. Ahora, supongamos que $\varphi \notin \mathcal{T}$, entonces al ser $\mathcal{T}$ una teoría completa $\neg\varphi \in \mathcal{T}$ y así $\mathfrak{A} \vDash \neg\varphi$, con ello $Th(\mathfrak{A}) \vDash \neg\varphi$, $\mathfrak{A} \nvdash \varphi$, es decir $\varphi \notin Th(\mathfrak{A}_A)$. Por lo tanto, $Th(\mathfrak{A}) = \mathcal{T}$.

Luego, sean $\mathfrak{A}$ y $\mathfrak{B}$ modelos de $\mathcal{T}$, entonces $Th(\mathfrak{A}) = \mathcal{T} = Th(\mathfrak{B})$. Por tanto $\mathfrak{A} \equiv \mathfrak{B}$.

$\Leftarrow$] Supongamos que existe $\varphi \in FORM$ tal que $\mathcal{T} \nvdash \varphi$. Entonces, $\mathcal{T}' = \mathcal{T} \cup \{\neg\varphi\}$ ($\mathcal{T} \vDash \neg\varphi$) es satisfacible y en consecuencia hay un modelo $\mathfrak{A}$ de $\mathcal{T}'$. Luego, para cada $\mathfrak{M}$ modelo de $\mathcal{T}$ por hipótesis se tiene que $\mathfrak{M}$ es equivalente a $\mathfrak{A}$. Esto implica que, $\mathfrak{M} \vDash \neg\varphi$ y en consecuencia $\mathcal{T} \vDash \neg\varphi$. Por lo tanto $\mathcal{T}$ es una teoría completa. □

Lema 3.38. *(Condición de Tarski-Vaught) Sea $\mathfrak{A}$ y $\mathfrak{B}$ para $\mathcal{L}$ tales que $\mathfrak{A} \subseteq \mathfrak{B}$. Entonces las siguientes condiciones son equivalentes:*

a) $\mathfrak{A} \prec \mathfrak{B}$

b) Para cualquier fórmula $\psi(v_0, ..., v_q)$, para cualquier $i \leq q$ y cuales quiera $a_0, ..., a_q \in A$:

Si hay algun $b \in B$ tal que $\mathfrak{B} \vDash \psi[a_0, ..., a_{i-1}, b, a_{i+1}, ..., a_q]$
Entonces hay algun $a \in A$ tal que $\mathfrak{B} \vDash \psi[a_0, ..., a_{i-1}, a, a_{i+1}, ..., a_q]$

Demostración: En el caso de que **a**) $\Rightarrow$ **b**), la demostración es directa por definición.

por otro lado bastaría probar que **b**) $\Rightarrow$ **a**), para ello demostremos que para cada $\varphi(v_0, ..., v_r)$ y para cualquier $a_0, ..., a_r \in A$, se tiene que:

$$\mathfrak{A} \vDash \varphi[a_0, ..., a_r] \text{ si y solo si } \mathfrak{B} \vDash \varphi[a_0, ..., a_r]$$

Usando inducción sobre la complejidad de la fórmula, y por *Lema 3.12* obtenemos si φ es una fórmula libre de cuantificadores y para cada $\overline{a} \in A^n$:

$$\mathfrak{A} \vDash \varphi(\overline{a}) \text{ si y solo sí } \mathfrak{B} \vDash \varphi(\overline{a})$$

Bastaría ver el caso en que $\varphi = (\exists v_i)\psi$:

$\mathfrak{A} \vDash (\exists v_i)\psi[a_0, ..., a_q]$ sii Existe algún $a \in A$ tal que $\mathfrak{A} \vDash \psi[a_0, ..., a_{i-1}, a, a_{i+1}, ..., a_q]$
Por h.i. sobre $\psi, \mathfrak{B} \vDash \psi[a_0, ..., a_{i-1}, a, a_{i+1}, ..., a_q]$
Por **b**) Existe algún $b \in B$, tal que $\mathfrak{A} \vDash \psi[a_0, ..., a_{i-1}, b, a_{i+1}, ..., a_q]$
Entonces $\mathfrak{B} \vDash (\exists v_i)\psi[a_0, ..., a_q]$

De lo anterior, deducimos que $\mathfrak{A} \vDash (\exists v_i)\psi[a_0, ..., a_q]$ implica que $\mathfrak{B} \vDash (\exists v_i)\psi[a_0, ..., a_q]$. De manera análoga obtenemos que $\mathfrak{B} \vDash (\exists v_i)\psi[a_0, ..., a_q]$ implica que $\mathfrak{A} \vDash (\exists v_i)\psi[a_0, ..., a_q]$. Por lo tanto **a**) y **b**) son equivalentes.

□

Teorema 3.39. *Si una teoría $\mathcal{T}$ tiene modelos finitos arbitrariamente grandes, entonces tiene un modelo infinito.*

Demostración: Consideremos, nuevos símbolos constantes c_i para cada $i \in \omega$ y expandimos al lenguaje $\mathcal{L}$ de $\mathcal{T}$ a $\mathcal{L}' = \mathcal{L} \cup \{c_i : i \in \omega\}$ y sea:

$$\Sigma = \mathcal{T} \cup \{\neg(c_i = c_j) : i \neq j, \text{ donde } i, j \in \omega\}$$

Sea $\mathcal{S} \subseteq \Sigma$ finito, notemos que tiene un modelo:

- Si $\varphi \in \mathcal{T} \cap \mathcal{S}$, terminamos pues como $\mathcal{T}$ tiene modelos finitos arbitrariamente grandes, entonces existe un modelo $\mathfrak{U}$ tal que $\mathfrak{U} \vDash \varphi$.
- Si $\varphi \in \mathcal{S} \backslash \mathcal{T}$, luego $\varphi = \neg(c_i = c_j)$, (con $i, j \in \omega$), entonces sea $\mathfrak{U}'$ tal que $(c_i)^{\mathfrak{U}'} \neq (c_j)^{\mathfrak{U}'}$, en consecuencia $\mathfrak{U}' \nvDash c_i = c_j$ si y solo si $\mathfrak{U}' \vDash \neg(c_i = c_j)$.

Sea $\mathfrak{K}$ tal que para cada $\varphi \in \mathcal{S}$, entonces $\mathfrak{K} \vDash \varphi$ si y solo si $\mathfrak{U} \vDash \varphi$ (si $\varphi \in \mathcal{T} \cap \mathcal{S}$) ó $\mathfrak{U}' \vDash \varphi$ (si $\varphi \in \mathcal{S} \backslash \mathcal{T}$), entonces por teorema (De compacidad) Σ es consistente y admite un modelo $\mathfrak{U}^*$ que es infinito (Donde $\mathfrak{U}^* \vDash \neg(c_i = c_j)$, con $i, j \in \omega$ distintos), entonces $\mathfrak{U}^* \vDash \Sigma$ y ya que $\mathcal{T} \subseteq \Sigma$. Por lo tanto $\mathfrak{U}^* \vDash \mathcal{T}$ □

Teorema 3.40. *(Ascendente de Löwenheim-Skolem-Tarski) Todo modelo infinito tiene extensiones elementales arbitrariamente grandes.*

Demostración: Sea $\mathfrak{A}$ un modelo infinito (es decir su conjunto universo A es infinito).

Dado X un conjunto, y para cada $x \in X$ definimos una nueva constante c_x que no este en $\mathcal{L}_{\mathfrak{A}}$. Sea $\mathcal{L}' = \mathcal{L}_{\mathfrak{A}} \cup \{c_x \,|\, x \in X\}$. Consideremos la teoría Γ para $\mathcal{L}'$:

$$Th(\mathfrak{A}) \cup \{\neg(c_x = c_y) \,|\, x, y \in X,\, x \neq y\}$$

Siguiendo la misma idea que la demostración del teorema anterior, se tiene por *teorema (De Compacidad)*, que Γ tiene un modelo, entonces existe $\mathfrak{B}$ modelo para Γ y así $\mathfrak{B}$ es un modelo para $Th(\mathfrak{A})$ de aquí que existe una incrustación elemental $f : \mathfrak{A} \to \mathfrak{B}$, entonces podemos identificar a $\mathfrak{A}$ con un submodelo elemental de $\mathfrak{B}$ y la asignación $x \to (c_x)^{\mathfrak{B}}$ es una función inyectiva de X a B. □

Teorema 3.41. *(Descendente de Löwenheim-Skolem-Tarski) Sea $\mathfrak{B}$ un modelo para $\mathcal{L}$ y sea κ un cardinal tal que $|\mathcal{L}| \leq \kappa \leq |B|$. Entonces $\mathfrak{B}$ tiene un submodelo elemental $\mathfrak{A}$ de cardinalidad κ.*

Además si $X \subseteq B$ y $|X| \leq \kappa$, entonces también se puede tener que $X \subseteq A$.

Demostración: Sin perdida de la generalidad, supongamos que $|X| = \kappa$ y definamos conjuntos X_n para $n \in \omega$, tales que $X = X_0 \subseteq X_1 \subseteq ... \subseteq X_n \subseteq \ldots$ y tales que para cada fórmula $\varphi(v_0, ..., v_q)$ de $\mathcal{L}$, cada $i \leq q$ y cada $a_0, ..., a_q \in X_n$ tal que:

$$\mathfrak{B} \vDash (\exists v_i)\varphi[a_0, ..., a_q]$$

Elegimos $x \in X_{n+1}$ tal que:

$$\mathfrak{B} \vDash \varphi[a_0, ..., a_{i-1}, x, a_{i+1}, ..., a_q]$$

Ya que $\mathcal{L} \leq \kappa$ y cada fórmula de $\mathcal{L}$ es una cadena finita de símbolos en $\mathcal{L}$, hay al menos κ fórmulas de $\mathcal{L}$. Por lo tanto, hay como máximo κ elementos de B que deben agregarse a cada X_n y así sin perdida de la generalidad cada $|X_n| = \kappa$. Sea $A = \cup\{X_n \,|\, n \in \omega\}$, entonces $|A| = \kappa$, Desde

que A es cerrado bajo funciones en $\mathfrak{B}$ y contiene todas las constantes de $\mathfrak{B}$, entonces A da lugar a un submodelo $\mathfrak{A} \subseteq \mathfrak{B}$. Dada una fórmula $\psi(v_0, ..., v_q)$ de $\mathcal{L}$, y $a_0, ..., a_q \in A$, si:

$$\text{Si hay algun } b \in B \text{ tal que } \mathfrak{B} \vDash \psi[a_0, ..., a_{i-1}, b, a_{i+1}, ..., a_q]$$
$$\text{sii } \mathfrak{B} \vDash (\exists v_i)\psi[a_0, ..., a_q]$$

Pero $a_0, ..., a_q \in A$, entonces $a_0, ..., a_q \subseteq X_j$, para algún $j \in \omega$, y por la construccion anterior existe $x \in X_{j+1}$ tal que:

$$\mathfrak{B} \vDash \psi[a_0, ..., a_{i-1}, x, a_{i+1}, ..., a_q]$$

Por el lema de la *Condición de Tarski-Vaught* se tiene que $\mathfrak{A} \prec \mathfrak{B}$ □

Definición 3.42. *Una teoría $\mathcal{T}$ es α-categórica para algún numero cardinal α, si para cada par de modelos de la teoría, $\mathfrak{A} = (A, (\cdot)^{\mathfrak{A}})$ y $\mathfrak{B} = (B, (\cdot)^{\mathfrak{B}})$ tales que $|A| = |B| = \alpha$ entonces $\mathfrak{A} \cong \mathfrak{B}$*

Teorema 3.43. *(Condición de Łos-Vaught) Sea $\mathcal{T}$ es una $\mathcal{L}$-teoría que tiene solamente modelos infinitos y $\mathcal{T}$ es α-categórica para un cardinal $\alpha \geq |\mathcal{L}|$. Entonces $\mathcal{T}$ es una teoría completa.*

Demostración: Sean $\mathfrak{A} = (A, (\cdot)^{\mathfrak{A}})$ y $\mathfrak{B} = (B, (\cdot)^{\mathfrak{B}})$ modelos de $\mathcal{T}$, luego por hipótesis A y B son infinitos. Sea $\beta = max\{|A|, |B|, \alpha\}$ y por el *teorema ascendente de Löwenheim-Skolem-Tarski*, existen extensiones elementales $\mathfrak{A}' = (A', (\cdot)^{\mathfrak{A}'})$ y $\mathfrak{B}' = (B', (\cdot)^{\mathfrak{B}'})$ tales que $|A'| = |B'| = \beta$. Por consiguiente, por el *teorema descendente de Löwenheim-Skolem-Tarski*, existen submodelos elementales $\mathfrak{A}'' = (A'', (\cdot)^{\mathfrak{A}''})$ y $\mathfrak{B}'' = (B'', (\cdot)^{\mathfrak{B}''})$ tales que $|A''| = |B''| = \alpha$.Puesto que $\mathcal{T}$ es α-categórica, entonces:

$$\mathfrak{A} \equiv \mathfrak{A}' \equiv \mathfrak{A}'' \cong \mathfrak{B}'' \equiv \mathfrak{B}' \equiv \mathfrak{B}$$

Entonces, por la *Proposición 3.31*, $\mathfrak{A}' = (A', (\cdot)^{\mathfrak{A}'})$ y $\mathfrak{B}' = (B', (\cdot)^{\mathfrak{B}'})$ son elementalmente equivalentes, y en consecuencia, por la *Proposición 3.38*, $\mathcal{T}$ es una teoría completa. □

Nota 3.44. *Demostraremos, usando el teorema (De compacidad), que todo campo está contenido en un campo algebraicamente cerrado. Para ello consideremos la teoría $\mathcal{T}_{ACF} = \mathcal{T}_F \cup \{\varphi_n \mid n \in \omega\}$, donde $\varphi_n = (\forall a_n)(\forall a_{n-1}) \ldots (\forall a_0)(\exists x_0)(a_n \cdot x_0^n + a_{n-1} \cdot x_0^{n-1} + \ldots + a_1 \cdot x_0 + a_0 = \mathbf{0})$, por el primer teorema de Kronecker, dicha teoría es finitamente satisfacible y por teorema de compacidad, $\mathcal{T}_{ACF}$ es satisfacible.*

Ahora, probemos que $\mathcal{T}_{ACF}$ es una teoría que no admite modelos finitos. Supongamos que tiene un modelo finito $\mathfrak{F} = \langle A, \{+, \cdot\}, \{\mathbf{0}, \mathbf{1}\}\rangle$. Podemos suponer sin perdida de la generalidad que, $A = \{\alpha_1, \ldots, \alpha_n\}$ y sea $f \in A[X]$ tal que $f(x) = (x - \alpha_n) \cdot \ldots \cdot (x - \alpha_1) + 1$. Pero, $f(\alpha_i) \neq 0$, para cada $i \in \{1, \ldots, n\}$, una contradicción. Por lo tanto A es infinito.

Como $\mathcal{T}_{ACF}$ es una teoría que no admite modelos finitos. y por teorema 2.103, también es α-categórica para cada $\alpha > \omega$ y por la Condición de Łos-Vaught, $\mathcal{T}_{ACF}$ es una teoría completa.

Bibliografía

[1] Zermelo, E. Beweis,*daß jede Menge wohlgeordnet werden kann (Aus einem an Herrn Hilbert gerichteten Briefe)*. Mathematische Annalen, Volumen 59, 514-516. (1904).

[2] Howard, P. E. *Łos' Theorem and the Boolean Prime Ideal Theorem Imply the Axiom of Choice*. Proceedings of the American Mathematical Society, 49(2), 426. (1975).

[3] Rav, Y. *Variants of RADO'S Selection Lemma and their Applications*. Math. Nachr. Vol. 79. 145-165. (1977).

[4] Gilmer, R. *Commutative semigroup rings*. Chicago: University of Chicago Press. (1984).

[5] Lewin, J. *A simple proof of Zorn's lemma*. The American Mathematical Monthly, Vol. 98. No. 4, 353-354. (1991).

[6] Banaschewski, B. *ALGEBRAIC CLOSURE WITHOUT CHOICE*. Mathematical Logic Quarterly, Vol. 38. No. 1, 383–385. (1992).

[7] Schechter, E. *Handbook of Analysis and Its Foundations (1st ed.)*. Academic Press. 152-153. (1996).

[8] Ljapin, E. S., & Evseev, A. E. *The Theory of Partial Algebraic Operations (1st ed.)*. Springer Netherlands. (1997).

[9] Weiss W. & D'Mello C. *Fundamentals of Model Theory.* (1997).

[10] Lang, S. *Algebra (Third Edition)*. Springer-Verlag New York. (2002).

[11] Rotman, J. J. *Advanced Modern Algebra*. Pearson. (2002).

[12] Hernández F. *Teoría de Conjuntos (una introducción)*. (2003).

[13] Dalen, D. *Logic and Structure (Fourth Edition)*. Springer London (2003).

[14] Jech T. *Set Theory (The Third Millennium Edition)*. Springer-Verlag Berlin Heidelberg. 73-89. (2006).

[15] Tamariz A. & Casarrubias F. *Elementos de Topología de Conjuntos*. (2011).

[16] Halbeisen, L. J. *Combinatorial Set Theory: With a Gentle Introduction to Forcing (1st ed.)*. Springer-Verlag London. (2012).

[17] Repický, M. *A proof of the independence of the Axiom of Choice from the Boolean Prime Ideal Theorem*. Commentationes Mathematicae Universitatis Carolinae, Vol. 56. No. 4, 543–546.(2015)

[18] Schardijn, Amy, *AN INTRODUCTION TO BOOLEAN ALGEBRAS*. Electronic Theses, Projects, and Dissertations. (2016).