Universidad de Valladolid

Facultad de Ciencias

# Trabajo Fin de Grado

Grado en Matemáticas

# Introducción a la lógica y teoría axiomática de conjuntos. Construcción del conjunto de los números naturales.

***Autor:***

***Rubén Martín Valmaseda***

***Tutor/es:***

***José María Cano Torres***

# Agradecimientos

Deseo expresar mi sincero agradecimiento al profesor José María Cano Torres, tutor de este trabajo, por su ayuda, dedicación y paciencia. Agradezco también a mis padres, hermanos y familiares, el apoyo recibido durante esta etapa.

# Índice general

# Introducción

Este trabajo es una pequeña recopilación de diferentes libros y notas sobre lógica y teoría de conjuntos con el objeto de conocer la base sólida en la que se apoyan todas las matemáticas.
Observando que todas las ramas de la matemática parten de unos axiomas y se demuestran enunciados a partir de ellos se intuía que podía haber una relación entre la matemática y la lógica y por eso matemáticos como Zermello y Hilbert redujeron las matemáticas a la lógica y a la teoría de conjuntos.
Este trabajo comienza con lógica proposicional y de primer orden viendo sus sintaxis y algunos resultados porque saber razonar en lógica es saber razonar en matemáticas y en la vida en general.
El trabajo acaba con los axiomas de Zermello-Fraenkel y la construcción de los números naturales.

# Capítulo 1

# Lógica Proposicional

La lógica y las matemáticas son las dos únicas ciencias deductivas. La lógica es un sistema que permite verificar si un razonamiento es correcto o incorrecto cuya finalidad es el estudio de la razón en el conocimiento. En este primer capítulo trataremos un poco la lógica proposicional, también llamada lógica simbólica o matemática, esta lógica se basa en la aplicación de símbolos por medio de tablas que nos permite ver lo verdadero o falso de las proposiciones.

## 1.1. Sistemas Formales

**Definición 1.1.** *Un sistema formal está compuesto de:*

1. *Un alfabeto A. Es el conjunto de todos los símbolos que podremos utilizar.*

2. *Un conjunto de fórmulas.*
   *Una fórmula es una secuencia finita de símbolos del alfabeto. El sistema formal proporcionará un algoritmo que determine si una secuencia finita de símbolos es una fórmula del sistema o no, ya que no toda secuencia finita de símbolos es una fórmula.*

3. *Un conjunto de axiomas. El cual es un subconjunto del conjunto de fórmulas. Al igual que para el conjunto de fórmulas también habrá un algoritmo que determine si una fórmula es un axioma.*

4. *Un conjunto de reglas de inferencia.*
   *Las reglas de inferencia son funciones en las que dadas unas fórmulas(premisas) nos devolverá otra fórmula.*

**Definición 1.2.** *Sean $\Sigma$ un conjunto de fórmulas de un sistema formal $S$ y $F$ una fórmula de $S$. Una demostración en el sistema formal $S$ o una derivación de $F$ en $S$ a partir de $\Sigma$ es una sucesión de fórmulas $F_1, F_2, F_3, ..., F_j$ tal que $F_j = F$ y todo elemento $F_i$ de la sucesión es, bien un axioma, bien ha sido obtenido mediante las reglas de inferencia de fórmulas $F_h$ anteriores a $F_i (h < i)$, bien $F_i \in \Sigma$, escribiremos $\Sigma \vdash_S F_j$ y diremos que $F_j$ es consecuencia sintáctica de $\Sigma$.*
*Podemos tratar al sistema formal como un objeto matemático y razonar sobre él. A las conclusiones a las que lleguemos lo llamaremos metateoremas.*

**Definición 1.3.** *Una fórmula $F$ es un teorema de un sistema formal si y solo si $\emptyset \vdash F$.*

**Observación.** *Hemos hablado de consecuencia sintáctica y más adelante hablaremos de consecuencia semántica, en ambos casos se puede hablar de consecuencia lógica, pero veremos que no es lo mismo.*
*Si no hay ambigüedad escribiremos $\Sigma \vdash F$ en lugar de $\Sigma \vdash_S F$.*

**Ejemplo 1.1.** *El alfabeto del sistema formal $M$ es el conjunto $\{a, b, c\}$. Definimos las fórmulas de la siguiente manera:*

1. *a, b y c son fórmulas.*

2. *Si A es una fórmula entonces aAa, bAb y cAc son fórmulas.*

*Observemos que las fórmulas de $M$ son solamente los palíndromos de longitud impar. Pondremos un único axioma llamado aaa y unas reglas de inferencia:*

1. *Para cualquier cadena que acabe y empiece en a podemos añadir una a al comienzo y otra final.*

2. *Para cualquier cadena que acabe y empiece en a podemos añadir una b al comienzo y otra final.*

3. *Para cualquier cadena que acabe y empiece en b podemos añadir una b al comienzo y otra final.*

4. *Para cualquier cadena que acabe y empiece en b podemos añadir una c al comienzo y otra final.*

*Un ejemplo de demostración en el sistema M sería: aaa, baaab, bbaaabb, bbbaaabbb, cbbbaaabbba. En el sistema formal cualquier teorema tiene una cantidad impar de a's.*
*Para probarlo haremos inducción sobre la cantidad de términos de la sucesión que prueban los teoremas.*
*Si la sucesión solo tiene un término entonces el teorema es el axioma aaa el cual tiene una cantidad impar de a's. Suponemos que para cualquier sucesión* $B_1, B_2, B_3, ..., B_n$ *el teorema* $B_n$ *tendrá una cantidad impar de a's.*
*Sea* $B_{n+1}$ *el teorema de la sucesión* $B_1, B_2, B_3, ..., B_{n+1}$*. Por hipótesis sabemos que* $B_n$ *tiene una cantidad impar de a's y por las reglas de inferencia del sistema formal sabemos que* $B_{n+1}$ *tendrá, o bien la misma cantidad de a's que* $B_n$*, o bien dos más, luego en cualquier caso tiene una cantidad impar de a's.*

## 1.2. Sistema Formal de la Lógica proposicional

A partir ahora vamos a estudiar el sistema formal de la lógica proposicional.

**Definición 1.4.** *El alfabeto del sistema formal de la lógica proposicional es el conjunto* $\{'(','), \wedge, \vee, \neg, \rightarrow, p_0, p_1, p_2, ...\}$*. Llamaremos variables proposicionales a los símbolos* $p_0, p_1, p_2, ....$ *Los símbolos* $\wedge, \vee$ *y* $\rightarrow$ *son conectores binarios y* $\neg$ *un conector unario. Definimos una fórmula de la siguiente manera:*

1. *Una variable proposicional es una fórmula.*
2. *Si* $p$ *y* $q$ *son fórmulas entonces* $(\neg p), (p \wedge q), (p \vee q)$ *y* $(p \rightarrow q)$ *son fórmulas.*

**Definición 1.5.** *Se construye el conjunto de fórmulas sobre* $P_0 = \{p_0, p_1, p_2, ...\}$ *de forma inductiva sobre k.*
$P_0 = \{p_0, p_1, p_2, ...\}$
$P_{k+1} := P_k \cup \{(F \# G), (\neg H) : F, G, H \in P_k, \# \in \{\wedge, \vee, \rightarrow\}\}$

*Llamamos $\mathcal{P}$ al conjunto de fórmulas proposicionales sobre $P_0$, es decir $\mathcal{P} := \bigcup P_k, k \in \mathbb{N}$.*

**Definición 1.6.** *Un conjunto de fórmulas $\Sigma$ es inconsistente si existe una fórmula $F$ tal que $\Sigma \vdash F$ y $\Sigma \vdash (\neg F)$. Un conjunto de fórmulas $\Sigma$ es consistente si no es inconsiste.*

**Lema 1.1.** *Sea $F = a_1a_2a_3...a_n$ una fórmula constituida de $n$ símbolos $a_1, a_2, a_3, ....a_n$ del alfabeto. Entonces:*

1. *La fórmula es una variable proposicional si y solo si $n = 1$.*
2. *Si $n \geq 2$ entonces la fórmula tendrá la misma cantidad de los dos tipos de paréntesis.*
3. *Cualquier segmento inicial $a_1a_2a_3...a_m$ con $m < n$ tendrá más paréntesis del tipo "(" que del tipo ")".*

**Demostración.** *1. Cualquier fórmula que es una variable proposicional tiene un único símbolo, por tanto $n = 1$.*
*Tomamos una fórmula $F = a_1$ de un sólo símbolo. Esta fórmula será una variable proposicional si $F \in P_0$.*
*Por ser $F$ una fórmula existirá $j \in \mathbb{N}$ tal que $F \in P_j$. Si $j = 0$ ya está probado. Supongamos que $j > 0$. Por construcción sabemos que $P_j := P_{j-1} \cup \{(H\#G), (\neg J) : H, G, J \in P_{j-1}, \# \in \{\wedge, \vee, \rightarrow\}\}$. Por ser $F$ una fórmula de un único símbolo tenemos $F \notin \{(H\#G) : H, G \in P_{j-1}, \# \in \{\wedge \vee \rightarrow\}\} \cup \{(\neg H) : H \in P_k\}$ luego $F \in P_{j-1}$. Repitiendo el mismo razonamiento $j$ veces obtenemos que $F \in P_0$, por tanto $F$ es una variable proposicional.*

2. *Si $n \geq 2$ significa que $F \in P_k$ con $k \geq 1$ y $F \notin P_0$.*
*Para $F \in P_1 \backslash P_0$. Entonces $F$ es de la forma $(\neg p), (p \wedge q), (p \vee q)$ o $(p \rightarrow q)$ con $p$ y $q$ variables proposicionales. En los cuatro casos podemos contar que hay el mismo número de paréntesis del tipo "(" que del tipo ")". Suponemos que para toda fórmula del conjunto $P_{k-1}$ tiene la misma cantidad de ambos tipos paréntesis. Tomamos $G \in P_k; P_k = (P_{k-1} \backslash P_{k-1}) \cup P_{k-1}$.*
*Si $G \in P_{k-1}$ por hipótesis tiene la misma cantidad de ambos tipos de paréntesis.*
*Si $G \in P_k \backslash P_{k-1}$ entonces $G$ es de la forma $(\neg H)$ o $(H\#J)$ con $H$ y $J$*

*fórmulas de $P_{k-1}$ y # un conector binario.*
*Supongamos que G es una fórmula de la forma $(\neg H)$ con $H \in P_{k-1}$. LLamaremos $G_A, H_A$ y $J_A$ a la cantidad de paréntesis abiertos que tienen las fórmulas G,H y J respectivamente y $G_C, H_C$ y $J_C$ a la cantidad de paréntesis cerrados que tienen las fórmulas G,H y J respectivamente. Observemos que $G_A = 1 + H_A$ y $G_C = 1 + H_C$ y por hipótesis $H_A = H_C$, luego $G_A = G_C$.*
*Si G es una fórmula de la forma $(H\#J)$ entonces $G_A = 1 + H_A + J_A$ y $G_C = 1 + H_C + J_C$, por hipótesis $H_A = H_C$ y $J_A = J_C$ por tanto $G_A = G_C$.*

3. *Por ser $n \geq 2$ volvemos a estar en el caso $F \in P_k \backslash P_0$ con $k \geq 1$.*
*Si $F \in P_1 \backslash P_0$ es de la forma $(\neg p), (p \wedge q), (p \vee q)$ o $(p \rightarrow q)$ con p y q variables proposicionales. Cualquier segmento inicial que tomemos tendrá un paréntesis del "(" y ningno del tipo ")". Suponemos que para toda fórmula del conjunto $P_{k-1}$ cualquier segmento inicial que tomamos tendrá más paréntesis abiertos que cerrados. Tomamos $G \in P_k$ con $P_k = P_k \backslash P_{k-1} \cup P_{k-1}$. Si $G \in P_{k-1}$ entonces cualquier segmento inicial tendrá más paréntesis abiertos que cerrados por hipótesis.*
*Si $G \in P_k \backslash P_{k-1}$ entonces G es de la forma $(\neg H)$ o $(H\#J)$ con H y J fórmulas de $P_{k-1}$ y # un conector binario.*
*Si G es una fórmula de la forma $(\neg H)$ con s símbolos entonces podemos tomar un segmento inicial de r símbolos con $r < s$. En los casos $r = 1$ o $r = 2$ hay un paréntesis del tipo "(" y cero del tipo ")". Si $2 < r < s - 1$ habremos abarcado un segmento inicial de H con unas cantidades l y k de paréntesis de los tipos "(" y ")" respectivamente, con $l > k$ por hipótesis. El segmento inicial que hemos tomado tiene $l + 1$ paréntesis del tipo "(" y k paréntesis del tipo ")". Puesto que $l + 1 > l > k$ habrá más paréntesis del tipo "(" que del tipo ")". En el caso $r = s - 1$ hay un paréntesis más del tipo "(" que del tipo ")", esto es debido a que la fórmula H tiene la misma cantidad de paréntesis de ambos tipos. Un razonamiento similar prueba el caso $G = (H\#J)$.*

**Teorema 1.1.** *Dada cualquier fórmula F en $\mathcal{P}$, solamente una de las siguientes afirmaciones es válida:*

1. *F es una variable proposicional.*

2. *Existen fórmulas únicas, $G, H \in \mathcal{P}$, y un único conector binario, $\#$, tal que $F$ es de la forma $(G\#H)$.*

3. *Existe una única fórmula $G \in \mathcal{P}$ tal que $F$ es de la forma $(\neg G)$.*

**Demostración.** *Sea $F$ una fórmula. Por la definición 1.5 existe un $k$ mínimo tal que $F \in P_k$. Si $k = 0$ entonces $F$ es una variable proposicional.*
*Si $k > 0$, o bien $F$ es del tipo $(G\#H)$ o bien del tipo $(\neg G)$, pues $F \notin P_{k-1}$. Si $F$ es una variable proposicional entonces solo tiene un símbolo y si $F$ es una fórmula de tipo $(G\#H)$ o $(\neg G)$ tendrá más de tres símbolos. Es decir, si $F$ es una variable proposicional no será ni de tipo $(G\#H)$ ni de tipo $(\neg G)$. Si $F$ es de la forma $(\neg G)$ entonces el segundo símbolo de $F$ es '$\neg$'. En cambio si es de tipo $(G\#H)$ el segundo símbolo es "(" o una variable proposicional. Por tanto, si $F \in \mathcal{P}$ es de un único tipo de los enunciados .*
*Falta ver que cada $F \in \mathcal{P}$ solo puede ser leída de una única manera.*
*Si $F$ es una variable proposicional entonces solo puede ser leída de una única manera.*
*Si $F$ es de tipo $(G\#H)$ suponemos que puede ser leída como $(G\#\ H)$ y $(\hat{G}\hat{\#}\hat{H})$ con $G, H, \hat{G}$ y $\hat{H}$ fórmulas y $\#$ y $\hat{\#}$ conectores binarios. Como $(G\#\ H)$ y $(\hat{G}\hat{\#}\hat{H})$ son las misma fórmula tenemos dos posibles casos:*
*$G = \hat{G}$ o una de las dos es el comienzo de otra. Suponemos $G$ es el comienzo de $\hat{G}$. Por 1.1 sabemos que $G$ por ser una fórmula tiene la misma cantidad de paréntesis de cada tipo.*
*También por el 1.1 sabemos que $G$, por ser segmento inicial de $\hat{G}$, tiene más paréntesis del tipo "(" que del tipo ")".Por tanto*
*$G = \hat{G}$ y por consiguiente $\# = \hat{\#}$ y $H = \hat{H}$. Si $F$ es de la forma $(\neg G)$ el razonamiento es igual que en el caso anterior.*

**Observación 1.1.** *Cada fórmula puede ser representada por un único diagrama árbol. De forma recursiva lo haríamos de la siguiente manera.*
*Si $F$ una fórmula tal que $F \in P_0$ entonces $F$ es una variable proposicional. El diagrama árbol con el que representaríamos a $F$ sería con un árbol cuya raíz es al mismo tiempo su única hoja.*
*Si $F$ es de la forma $(\neg G)$ para construir un nuevo árbol partimos de un nuevo nodo que será '$\neg$' y establecemos una relación padre-hijo entre un nodo en el que escribiremos '$\neg$' y otro en el que escribiremos la raíz del árbol que representa a $G$.*
*Si $F$ es de la forma $(G\#H)$ para construir un nuevo árbol partimos de un nuevo nodo en el que escribiremos $\#$ y establecemos una relación padre-hijo*

*entre este y otro par de nodos en los que escribiremos las raíces $r_G$ y $r_H$ de los árboles que representan a las fórmulas G y H respectivamente. Es decir, los nodos $r_G$ y $r_H$ son los hijos del nodo #. Nótese que el orden es importante.*

**Definición 1.7.** *Sea $F \in \mathcal{P}$ una fórmula el conector principal de F es:*

1. *# si $F = (G\#H)$ con G y H fórmulas y # conector binario.*
2. *$\neg$ si $F = (\neg G)$ con G fórmula.*

El siguiente teorema proporcionará un algoritmo que determia el conector principal de una fórmula. A partir de este teorema podremos determinar un algoritmo que compruebe si una sucesión de símbolos es una fórmula y otro algoritmo para determinar si una sucesión de símbolos es, a parte de una fórmula, un axioma.

**Teorema 1.2.** *Sea F una fórmula tal que $F \notin P_0$ y $F = a_1a_2a_3...a_n$ con $a_1, a_2, a_3, ..., a_n$ símbolos. Definimos la aplicación $p : \{1, 2, 3, ..., n\} \to \mathbb{N}$ tal que $p(i)$ es el número de paréntesis abiertos menos el número de paréntesis cerrados que hay en el segmento inicial $a_1a_2a_3...a_{i-1}$. Entonces el conector principal es el único símbolo $a_i$ tal que $a_i$ es un conector y $p(i) = 1$.*

**Demostración.** *Sea F una fórmula de la forma $(\neg G)$, por definición el conector principal es '$\neg$'. Escribiendo F de la forma $A = a_1a_2a_3...a_n$ tenemos:*

| | $i = 1$ | $i = 2$ |
|---|---|---|
| $a_i$ | $'('$ | $\neg$ |
| $p(i)$ | 0 | 1 |

*Veamos que si $a_s$ es un conector distinto al principal entonces $p(s) > 1$. Si $G = b_1b_2b_3...b_r$ donde $b_i = a_{i+2}$ para todo $i \in \{1, 2, 3, ..., r\}$ entonces $a_s = b_{s-2}$. Por ser G una fórmula debe cumplir el lema de los paréntesis, luego en el segmento inicial $b_1b_2b_3...b_{s-2}$ hay más paréntesis abiertos que cerrados, además $a_1$ es un paréntesis abierto, por tanto $p(s) > 1$. Vemos que se verifica el teorema.*

*Haremos una demostración similar para ver que se cumple el teorema en el caso de que la fórmula F sea de la forma $(G\#H)$. Si la fórmula F es de la forma $(G\#H)$ con $G = b_1b_2b_3...b_r$ y $H = c_1c_2c_3...c_t$ entonces sustituyendo $a_2a_3a_4...a_{r+1}$ por $b_1b_2b_3...b_r$ y $a_{r+3}a_{r+4}a_{r+5}...a_{n-1}$ por $c_1c_2c_3...c_t$ tenemos*

*$F = (b_1b_2b_3...b_r\#c_1c_2c_3...c_t)$. Observemos que el conector # está en la posición $r+2$. Podemos comprobar que $p(r+2) = 1$ debido a que en la cadena $b_1b_2b_3...b_r$ hay el mismo número de paréntesis de ambos tipos por el lema de los paréntesis(recordemos que G es una fórmula) y además $a_1 =' ('$.*

*Veamos ahora que si $a_s$ es un conector pero no es el conector principal entonces $p(s) > 1$. Primero observemos que el conector principal es $a_{r+2}$, entonces, o bien $s < r+2$, o bien $s > r+2$.*

*Si $s < r+2$ entonces $a_s = b_{s-1}$ es un símbolo de la fórmula G. Por ser G una fórmula en el segmento inicial $b_1b_2b_3...b_{s-1}$ debe haber más paréntesis abiertos que cerrados y $a_1$ es un paréntesis abierto, luego $p > 1$.*
*Si $s > r+2$ entonces $a_s = c_{s-r-2}$ es un símbolo de la fórmula H. Por ser G una fórmula hay la misma cantidad de paréntesis abiertos que cerrados en el segmento $b_1b_2b_3...b_r$ y por ser H una fórmula hay más paréntesis abiertos que cerrados en el segmento $c_1c_2c_3...c_{s-r-2}$, además $a_1$ es un paréntesis abierto y $a_{r+2}$ es un conector, luego $p(s) > 1$.*

El algoritmo que determina si una sucesión de símbolos es una fórmula o no es el siguiente:

Sea F una sucesión de n símbolos. Si $n = 1$ entonces F fórmula si y solo si F es una variable proposicional.

Si $n > 1$ primeros debemos verificar que se cumple el lema de los paréntesis, es decir hay que comprobar que $p(i) > 1$ para $i \in \{2, 3, 4, ..., n-1\}$, $a_1 = '('$ y $a_n = ')'$.
Después comprobamos que se cumple el 1.2, es decir, tenemos que ver que existe un único conector en la j-ésima posición tal que $p(j) = 1$. Si $a_j = '\neg'$ $j = 2$ y tomamos la sucesión $G = a_3a_4a_5...a_{n-1}$, la cual renombraremos $G = b_1b_2b_3...b_r$.

Si $a_j = \#$ $n > -1j > 2$ y tomamos las sucesiones $H = a_3a_4a_5...a_{j-1}$ y $J = a_{j+1}a_{j+2}a_{j+3}...a_{n-1}$, las cuales renombraremos $H = c_1c_2c_3...c_s$ y
$J = d_1d_2d_3...d_t$.

Repetimos el proceso con la sucesión G o con las sucesiones H y J según el caso en el que nos encontremos. Finalmente las sucesiones de un único símbolo deben ser variables proposicionales.

**Ejemplo 1.2.** *Haciendo uso del algoritmo anterior verificaremos si las sucesiones $(())$, $(\neg)$ y $(p \to (\neg(\neg p)))$ son fórmulas o no.*
*Para la sucesión $(())$ vemos que $a_1 = '('$ y $a_4 =')'$ y*

| | $i=2$ | $i=3$ |
|---|---|---|
| $p(i)$ | 1 | 2 |

*Aquí no encontramos ningún conector, luego no es fórmula.*
*Para la sucesión* $(\neg)$ *vemos que se verifica el lema de los paréntesis y* $a_2$ *es el conector* $\text{`}\neg'$*. La siguiente sucesión que tendríamos que estudiar ahora es una sucesión sin símbolos. Por tanto* $(\neg)$ *no es una fórmula.*
*La sucesión* $(p \to (\neg(\neg p)))$ *verifica el lema de los paréntesis, pues tenemos:*

| | $i=1$ | $i=2$ | $i=3$ | $i=4$ | $i=5$ | $i=6$ | $i=7$ | $i=8$ | $i=9$ | $i=10$ | $i=11$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_i$ | $\text{`}('$ | $p$ | $\to$ | $\text{`}('$ | $\text{`}\neg'$ | $\text{`}('$ | $\text{`}\neg'$ | $p$ | $\text{`})'$ | $\text{`})'$ | $\text{`})'$ |
| $p(i)$ | 0 | 1 | 1 | 1 | 2 | 2 | 3 | 3 | 3 | 2 | 1 |

*Vemos que el símbolo* $a_3 = \text{` }\to'$ *es conector y* $p(3) = 1$*. Además es el único símbolo que cumple estas dos propiedades simultáneamente. Ahora tenemos que estudiar las sucesiones* $p$ *y* $(\neg(\neg p))$*.*
*La sucesión* $p$ *tiene un único símbolo y es una variable proposicional. Para la sucesión* $(\neg(\neg p)) = b_1b_2b_3...b_7$ *vemos que*

| | $i=1$ | $i=2$ | $i=3$ | $i=4$ | $i=5$ | $i=6$ | $i=7$ |
|---|---|---|---|---|---|---|---|
| $b_i$ | $\text{`}('$ | $\text{`}\neg'$ | $\text{`}('$ | $\text{`}\neg'$ | $p$ | $\text{`})'$ | $\text{`})'$ |
| $p(i)$ | 0 | 1 | 1 | 2 | 2 | 2 | 1 |

*Vemos que el símbolo* $b_2 = \text{`}\neg'$ *es un conector y* $p(2) = 1$ *ningún otro símbolo de la sucesión cumple simultáneamente estas dos propiedades.*
*Estudiamos la sucesión* $(\neg p) = c_1c_2c_3c_4$*.*

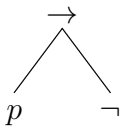
| | $i=1$ | $i=2$ | $i=3$ | $i=4$ |
|---|---|---|---|---|
| $c_i$ | $\text{`}('$ | $\text{`}\neg'$ | $p$ | $\text{`})'$ |
| $p(i)$ | 0 | 1 | 1 | 1 |

*Vemos que el símbolo* $c_2 = \text{`}\neg'$ *es un conector y* $p(2) = 1$ *ningún otro símbolo de la sucesión cumple simultáneamente estas dos propiedades.*

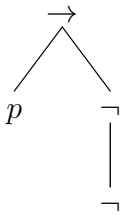
*Estudiamos la sucesión p, la cual tiene un único símbolo y es una variable proposicional. Por tanto* $(p \to (\neg(\neg p)))$ *es una fórmula.*

**Observación 1.2.** *Sea F una fórmula podemos obtener el árbol que la representa utilizando un algoritmo análogo al algoritmo que nos permite determinar si F es una fórmula.*
*El conector principal de la primera sucesión lo escribiremos en la raíz del árbol que construiremos.*
*Si F es de la forma* $(\neg G)$ *establecemos una relación padre-hijo entre dos nodos en los que escribiremos los conectores principales de F y de G.*
*Si F es de la forma* $(G\#H)$ *establecemos relaciones padre-hijo entre un nodo en el que escribiremos el conector principal de F y dos nodos en los que escribiremos los conectores principales de G y H.*
*Si una de las sucesiones es una variable proposicional sería una hoja.*

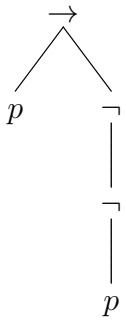
**Ejemplo 1.3.** *Tomemos la fórmula* $F = (p \to (\neg(\neg p)))$*. Como hemos visto antes el conector principal es* $\to$*. Es decir la raíz del árbol es el nodo en el que escribiremos* $\to$ *y las dos siguientes fórmulas con las que tenemos que trabajar son p y* $(\neg(\neg p))$*, la primera es una variable proposicional que en el árbol la representaríamos con una hoja y el conector principal de la segunda fórmula es* $\neg$*. Hasta el momento la representación en árbol sería:*




*Ahora tenemos que trabajar con la fórmula* $(\neg p)$ *cuyo conector principal es* $\neg$*. Si añadimos este nuevo nodo el árbol quedaría:*




*Finalmente nos queda la fórmula p, la cual es una fórmula proposicional, por tanto, el nodo con el que lo representaríamos sería una hoja. El árbol final es:*

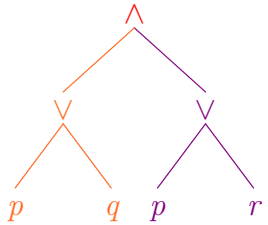



**Ejemplo 1.4.** *Sea $F$ la fórmula* $(((p \vee q) \wedge (p \vee r)) \rightarrow ((\neg(\neg r)) \vee ((\neg p) \rightarrow (\neg r))))$. *Vemos que $F$ es de la forma $G \rightarrow H$ con* $G = ((p \vee q) \wedge (p \vee r))$ *y* $H = ((\neg(\neg r)) \vee ((\neg p) \rightarrow (\neg r)))$. *Para la fórmula* $G = ((p \vee q) \wedge (p \vee r))$ *tenemos:*

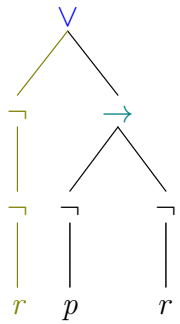
| | $i=1$ | $i=2$ | $i=3$ | $i=4$ | $i=5$ | $i=6$ | $i=7$ |
|---|---|---|---|---|---|---|---|
| $b_i$ | '(' | '(' | $p$ | '$\vee$' | $q$ | ')' | '$\wedge$' |
| $p(i)$ | 0 | 1 | 2 | 2 | 2 | 2 | 1 |

| | $i=8$ | $i=9$ | $i=10$ | $i=11$ | $i=12$ | $i=13$ |
|---|---|---|---|---|---|---|
| $b_i$ | '(' | $p$ | '$\vee$' | $r$ | ')' | ')' |
| $p(i)$ | 1 | 2 | 2 | 2 | 2 | 1 |

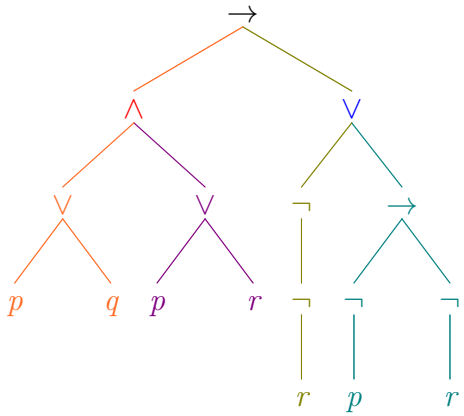
*El conector principal de la fórmula $G$ es '$\wedge$' y $G$ es de la forma $(J \wedge K)$ con* $J = (p \vee q)$ *y* $K = (p \vee r)$. *Siguiendo el algoritmo obtendremos el árbol que representa a la fórmula* $G = ((p \vee q) \wedge (p \vee r))$.




*Hacemos lo propio con la fórmula* $H = ((\neg(\neg r)) \vee ((\neg p) \rightarrow (\neg r)))$.




*El árbol que representa la fórmula $F$ sería:*




**Definición 1.8.** *Llamaremos valoración a una aplicación $\upsilon : \mathcal{P} \longrightarrow \{0,1\}$ que verifica para cualquier $F, G \in \mathcal{P}$:*

$$\upsilon((F \wedge G)) = 1 \text{ si y solo si } \upsilon(F) = 1 \text{ y } \upsilon(G) = 1,$$
$$\upsilon((F \vee G)) = 1 \text{ si y solo si } \upsilon(F) = 1 \text{ o } \upsilon(G) = 1,$$
$$\upsilon((F \to G)) = 1 \text{ si y solo si } \upsilon(F) = 0 \text{ o } \upsilon(G) = 1,$$
$$\upsilon((\neg F)) = 1 \text{ si y solo si } \upsilon(G) = 0.$$

**Lema 1.2.** *Una valoración queda determinada por su restricción al conjunto $P_0$.*

**Demostración.** *Si $F \in P_0$ entonces es trivial que $\upsilon(F)$ queda determinada por su restricción al conjunto $P_0$.*
*Suponemos que se cumple para todo $l \leq k$ con $k \geq 1$. Tomamos $G \in P_{k+1} \backslash P_k$, entonces $G$ es de la forma $(\neg H)$ o $(H \# J)$ con $H$ y $J$ fórmulas de $P_{n-1}$ y $\#$ un conector binario. Por el teorema 1.1 sabemos que $H$ y $J$ son únicas. Usando la hipótesis de inducción y la definición de $\upsilon$ queda demostrado.*

Dada una fórmula cualquiera podemos resumir en una tabla los valores que toma $\upsilon$ según los valores que tomen las variables proposicionales. A estas tablas las llamaremos tablas de la verdad.

| $p$ | $q$ | $(p \wedge q)$ | $(p \vee q)$ | $(p \rightarrow q)$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 |

| $p$ | $(\neg p)$ |
|---|---|
| 1 | 0 |
| 0 | 1 |

**Definición 1.9.** *Sea $\Sigma$ un conjunto de fórmulas de la lógica proposicional y $\upsilon$ una valoración diremos que $\Sigma$ es consistente testado por $\upsilon$ si $\upsilon(F) = 1$ para todo $F \in \Sigma$(escribimos $\upsilon|\Sigma \equiv 1$).*

**Definición 1.10.** *Un conjunto de fórmulas $\Sigma$ es satisfacible si existe una valoración $\upsilon$ tal que $\upsilon|\Sigma \equiv 1$.*

**Definición 1.11.** *Sea $F \in \mathcal{P}$. Diremos que $F$ es una tautología si $\upsilon(F) = 1$ para cualquier valoración $\upsilon$. Diremos que $F$ es una contradicción si $\upsilon(F) = 0$ para cualquier valoración $\upsilon$. Una fórmula $F$ es una contingencia si no es ni tautología ni contradicción.*

**Definición 1.12.** *Una fórmula $F$ es válida si es una tautología y lo representaremos de la siguiente manera $\models F$.*

**Definición 1.13.** *Sea $\Sigma$ un conjunto de fórmulas y $F$ una fórmula. Diremos que $\Sigma$ implica $F$ tautológicamente si para cada valoración $\upsilon$ con $\upsilon|\Sigma \equiv 1$ se cumple $\upsilon(F) = 1$ y escribiremos $\Sigma \models F$. También diremos que $F$ es una consecuencia lógica de $\Sigma$.*

**Observación 1.3.** *En el caso $\Sigma \models F$ la consecuencia lógica es una consecuencia semántica y no sintáctica. Siempre que no haya ambigüedad diremos simplemente consecuencia.*

**Definición 1.14.** *Dos fórmulas $F, G \in \mathcal{P}$ son equivalentes si $\upsilon(F) = \upsilon(G)$ para cualquier valoración. Escribimos $F \approx G$ para representar que las fórmulas $F$ y $G$ son equivalentes.*

**Ejemplo 1.5.** *Veamos que $(F \wedge G) \approx (\neg(F \to (\neg G)))$.*

| $F$ | $G$ | $(F \wedge G)$ | $(\neg G)$ | $(F \to (\neg G))$ | $(\neg(F \to (\neg G)))$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 | 1 | 0 |

*Las columnas 3 y 6 prueban $(F \wedge G) \approx (\neg(F \to (\neg G)))$.*

**Ejemplo 1.6.** *Veamos que $(F \vee G) \approx (\neg(F) \to G)$.*

| $F$ | $G$ | $(F \vee G)$ | $(\neg F)$ | $((\neg F) \to G))$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 |

*Las columnas 3 y 5 prueban $(F \vee G) \approx (\neg(F) \to G)$.*

**Definición 1.15.** *Sea $F, G, H \in \mathcal{P}$ fórmulas denotamos por $Sb(F)$ al conjunto de subfórmulas de $F$ y lo definimos de la siguiente manera:*

1. *$Sb(F) = \{p\}$ si $p = F$ es una variable proposicional.*
2. *$Sb((\neg F)) = Sb(F) \cup \{(\neg F)\}$.*
3. *$Sb(F) = Sb((G \# H)) = Sb(G) \cup Sb(H) \cup \{F\}$ si $F = G \# H$ y $\#$ un conector binario.*

**Teorema 1.3.** *(Teorema de sustitución) Si se sustituyen subfórmulas de una fórmula F por otras que les son respectivamente equivalentes el resultado es una fórmula equivalente a F.*

**Demostración.** *La afirmación es equivalente para fórmulas en $P_0$, pues las variables proposicionales solamente son equivalentes a ellas mismas. Suponemos que se cumple para fórmulas en $P_j$ con $j < n$ y consideremos una fórmula $G \in P_n$, entonces G es de la forma $(\neg H)$ o $(H \# J)$ con H y J fórmulas de $P_{n-1}$ y $\#$ un conector binario. Por la definición de subfórmula una subfórmula de G distinta de G es también subfórmula de H o J. Sin pérdida de generalidad suponemos que sustuimos en H una subórmula por otra que le es equivalente. Por hipótesis de inducción $H' \approx H$. Las siguientes tablas de verdad concluyen $(H' \# J) \approx (H \# J)$ y $(\neg H) \approx (\neg H')$.*

| $H$ | $H'$ | $J$ | $(H \vee J)$ | $(H' \vee J)$ | $(H \wedge J)$ | $(H' \wedge J)$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| $H$ | $H'$ | $J$ | $(H \to J)$ | $(H' \to J)$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 |

| $H$ | $H'$ | $(\neg J)$ | $(\neg J')$ |
|---|---|---|---|
| 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 |

**Definición 1.16.** *Un sistema axiomático para una lógica de primer orden viene dado por un conjunto de axiomas y unas reglas de inferencia.*

**Definición 1.17.** *Vamos a definir dos sistemas axiomáticos para la lógica proposicional. Aunque solamente vamos a trabajar con uno de ellos también demostraremos que cualquier teorema de la lógica proposicional puede ser demostrado desde el otro sistema axiomático.*
*La única regla con la que trabajaremos en ambos sistemas axiomáticos será la regla de inferencia denominada modus ponens, mp. Dadas dos fórmulas del tipo $F \to G$ y $F$ entonces tenemos $G$.*
*El primer conjunto de axiomas lo constituyen los siguientes axiomas:*

1. *axioma 1* $(F \to (G \to F))$.
2. *axioma 2* $((F \to (G \to H)) \to ((F \to G) \to (F \to H)))$.
3. *axioma 3* $(((\neg F) \to (\neg G)) \to (G \to F))$.

*El segundo conjunto de axiomas lo constituyen los siguientes axiomas:*

1. *axioma 1* $(F \to (G \to F))$.
2. *axioma 2* $((F \to (G \to H)) \to ((F \to G) \to (F \to H)))$.
3. *axioma 3* $(((\neg G) \to (\neg F)) \to (((\neg G) \to F) \to G))$.

*Vamos a trabajar con el primer sistema axiomático, es decir, el sistema axiomático formado por la regla de inferencia modus ponens y por los tres primeros axiomas.*

**Observación 1.4.** ***(Esta observación es importante).*** *En los dos sistemas axiomáticos que hemos definido los únicos conectores que hemos utilizado son $\neg$ y $\to$. Por los ejemplos 1.5 y 1.6 y por el teorema de sustitución cualquier fórmula es equivalente a otra fórmula que solo utilice $\neg$ y $\to$ como símbolos conectores . Esto resulta útil para ganar claridad.*

**Observación 1.5.** *Los axiomas son equivalentes a otras fórmulas. Por ejemplo:*
$((\neg F) \to (\neg G)) \to (G \to F) \approx (((F \wedge G) \vee (F \to G)) \to (G \to F))$.
$(F \to (G \to F)) \approx (F \to ((\neg G)) \vee F)$.

Existen algoritmos que determinan si una fórmula es alguno de los axiomas anteriores. Estos algoritmos están basados en el algoritmo que determina si una secuencia es o no una fórmula. Veamos de modo breve un algoritmo

para determinar si una fórmula es un axioma del primer tipo:
Sea F una fórmula de la lógica proposicional. La fórmula F debe ser de la forma $(G \to H)$, es decir, el conector principal de F debe ser $\to$.
La fórmula H debe ser de la forma $(J \to K)$, es decir, el conector principal de H debe ser $\to$.
Finalmente para que F sea un axioma del tipo 1 debe verificarse que $G = K$, es decir, si $G = b_1 b_2 b_3 ... b_n$ y $K = e_1 e_2 e_3 ... e_n$ entonces $G = K$ si y solo si $b_i = e_i$ para todo $i \in \{1, 2, 3, ..., n\}$.

**Lema 1.3.** *Para cualquier fórmula $F \in \mathcal{P}$, $(F \to F)$ es un teorema de la lógica proposicional, es decir $\emptyset \vdash (F \to F)$.*

**Demostración.** *1.* $((F \to ((F \to F) \to F)) \to ((F \to (F \to F)) \to (A \to A)))$ *axioma 2 (sustituyendo G por $(F \to F)$).*

*2.* $(F \to ((F \to F) \to F))$ *axioma 1 (sustituyendo G por $(F \to F)$).*

*3.* $((F \to (F \to F)) \to (F \to F))$ *mp 1,2.*

*4.* $(F \to (F \to F))$ *axioma 1 (sustituyendo G por F).*

*5.* $(F \to F)$ *mp 3,4.*

**Teorema 1.4.** *(Teorema de la deducción) Si $\Sigma \cup \{F\} \vdash G$ entonces $\Sigma \vdash (F \to G)$.*

**Demostración.** *Por hipótesis sabemos que existe una demostración $B_1, B_2 B_3, ... B_n = G$ que prueba $\Sigma \cup \{F\} \vdash G$. Demostraremos el resultado por inducción en n.*
*Para el caso $n = 1$ tenemos que $B_1$ es un axioma, una fórmula de $\Sigma$ o es F. Si $B_1 = G$ es una fórmula de $\Sigma$:*

*1.* $\Sigma \vdash (B \to (F \to G))$ *axioma 1.*

*2.* $\Sigma \vdash B$ *ya que $G \in \Sigma$.*

*3.* $\Sigma \vdash (F \to G)$ *mp 1,2.*

*Si G es un axioma:*

*1.* $\Sigma \vdash (G \to (F \to G))$ *axioma 1.*

*2.* $\Sigma \vdash G$ *por ser G un axioma.*

3. $\Sigma \vdash (F \to G)$ *mp 1,2.*

*Para el caso* $G = F$ *basta aplicar el teorema 1.3.*
*Para el caso* $B_1, B_2B_3, ...B_n = G$ *con* $n > 1$ *si* $G$ *es un axioma o una fórmula de* $\Sigma$ *hacemos lo mismo que en el caso* $n = 1$. *Si no es así,* $B_n = G$ *habrá sido deducido mediante modus ponens de* $B_r$ *y* $B_s$ *con* $r, s < n$*( sin pérdida de generalidad suponemos r<s) siendo* $B_r = (B_s \to G)$. *Por hipótesis de inducción sabemos* $\Sigma \vdash (A \to (B_s))$ *y* $\Sigma \vdash (F \to (B_r))$ *es decir,*
$\Sigma \vdash (F \to (B_s \to G))$ *y* $\Sigma \vdash (F \to (B_s))$. *Entonces*

1. $\Sigma \vdash (F \to (B_s \to G)$ *por hipótesis de inducción.*

2. $\Sigma \vdash (F \to (B_s))$ *por hipótesis de inducción.*

3. $\Sigma \vdash ((F \to (B_s \to G)) \to ((F \to (B_s)) \to (A \to G)))$ *axioma 2 (sustituyendo G por* $B_s$ *y H por F por G).*

4. $\Sigma \vdash (F \to (B_s)) \to (F \to B)$ *mp 3,1.*

5. $\Sigma \vdash (F \to G)$ *mp 4,2.*

**Observación 1.6.** *El teorema de la deducción es un metateorema.*

**Corolario 1.1.** ***(Transitividad)****Sean F, G y H fórmulas de la lógica proposicional entonces* $\{(F \to G), (G \to H)\} \vdash (F \to H)$.

**Demostración.** *Por el teorema de la deducción el corolario quedará demostrado si* $\{(F \to G), (G \to H), F\} \vdash H$ *Sea* $\Sigma = \{(F \to G), (G \to H), F\}$.

1. $\Sigma \vdash F$ *ya que* $F \in \Sigma$.

2. $\Sigma \vdash (F \to G)$ *ya que* $G \in \Sigma$.

3. $\Sigma \vdash G$ *mp 2,1.*

4. $\Sigma \vdash (G \to H)$ *ya que* $(G \to H) \in \Sigma$.

5. $H$ *mp 4,3.*

**Lema 1.4.** *Sean F, G y H fórmulas de la lógica proposicional entonces* $\{(F \to (G \to H)), G\} \vdash (F \to H)$.

**Demostración.** *Sea* $\Sigma = \{(F \to (G \to H)), G\}$ *entonces:*

1. $\Sigma \vdash (F \to (G \to H))$ *ya que* $(F \to (G \to H)) \in \Sigma$.

2. $\Sigma \vdash G$ *ya que* $G \in \Sigma$.

3. $\Sigma \vdash ((F \to (G \to H)) \to ((F \to G) \to (F \to H)))$ *axioma 2.*

4. $\Sigma \vdash ((F \to G) \to (F \to H))$ *mp 3,1.*

5. $\Sigma \vdash (G \to (F \to G))$ *axioma 1.*

6. $\Sigma \vdash (F \to G)$ *mp 5,2.*

7. $\Sigma \vdash (F \to H)$ *mp 4,6.*

**Teorema 1.5.** *Sean* $\Sigma$ *un sistema inconsistente y* $F$ *una fórmula cualquiera entonces* $\Sigma \vdash F$.

**Demostración.** *Por ser* $\Sigma$ *un sistema inconsiste entonces existirá* $G$ *tal que* $\Sigma \vdash (\neg G)$ *y* $\Sigma \vdash G$. *Entonces:*

1. $\Sigma \vdash G$ *por ser hipótesis.*

2. $\Sigma \vdash (\neg G)$ *por hipótesis.*

3. $\Sigma \vdash ((\neg G) \to ((\neg F) \to (\neg G)))$ *axioma 1 (sustituendo* $F$ *por* $(\neg G)$ *y* $G$ *por* $(\neg F)$*).*

4. $\Sigma \vdash ((\neg F) \to (\neg G))$ *mp 3,1.*

5. $\Sigma \vdash (((\neg F) \to (\neg G)) \to (G \to F))$ *axioma 3.*

6. $\Sigma \vdash (G \to F)$ *mp 5,4.*

7. $\Sigma \vdash F$ *mp 6,1.*

*Por tanto* $\Sigma \vdash F$ *siendo* $F$ *una fórmula cualquiera.*

Demostraremos algunos teoremas de la lógica proposicional que nos resultarán útiles:

**Lema 1.5.** *La fórmula* $(((\neg F) \to G) \to ((\neg F) \to (\neg G)) \to F)$ *es un teorema de la lógica proposicional.*

**Demostración.** *Por el teorema de la deducción demostrar*
$\emptyset \vdash (((\neg F) \to G) \to (((\neg A) \to (\neg G)) \to F))$ *es equivalente a demostrar* $((\neg F) \to G) \vdash (((\neg F) \to (\neg G)) \to F)$ *y otra vez por el teorema de la deducción esto último quedará demostrado si probamos*
$\{((\neg F) \to G), ((\neg F) \to (\neg G))\} \vdash F$.
*Por lo tanto, para probar que la fórmula*
$(((\neg F) \to G) \to (((\neg F) \to (\neg G)) \to F))$ *es un teorema de la lógica proposicional vamos a probar*
$\{((\neg F) \to G), ((\neg F) \to (\neg G))\} \vdash F$.
*Antes de probar el teorema probaremos que si*
$\Sigma \cup \{(\neg F)\} \vdash (\neg G)$ *y* $\Sigma \cup \{(\neg F)\} \vdash G$ *entonces* $\Sigma \vdash F$.
*El conjunto* $\Sigma \cup \{(\neg F)\}$ *es un sistema inconsiste.*
*Sea* $G$ *un axioma cualquiera, por el teorema 1.5 tenemos* $\Sigma \cup \{(\neg F)\} \vdash (\neg G)$ *y* $\Sigma \cup \{(\neg F)\} \vdash G$ *siendo* $G$ *un axioma cualquiera. Por el teorema de la deducción tenemos* $\Sigma \vdash ((\neg F) \to (\neg G))$ *y* $\Sigma \vdash ((\neg F) \to G)$.

1. $\Sigma \vdash ((\neg F) \to (\neg G))$ *(ya explicado).*
2. $\Sigma \vdash ((\neg F) \to (\neg G)) \to (G \to F)$ *axioma 3.*
3. $\Sigma \vdash (G \to F)$ *mp 2,1.*
4. $\Sigma \vdash G$ *por ser* $G$ *un axioma.*
5. $\Sigma \vdash F$ *mp3,4.*

*Hemos probado que si* $\Sigma \cup \{(\neg F)\} \vdash (\neg G)$ *y* $\Sigma \cup \{(\neg F)\} \vdash G$ *entonces* $\Sigma \vdash F$.
*Por lo tanto, si demostramos*
$\{((\neg F) \to G), ((\neg F) \to (\neg G))\} \cup \{(\neg F)\} \vdash H$ *y*
$\{((\neg F) \to G), ((\neg F) \to (\neg G))\} \cup \{(\neg F)\} \vdash (\neg H)$ *habremos probado*
$\{((\neg F) \to G), ((\neg F) \to (\neg G))\} \vdash F$ *y por consiguiente todo el teorema. Sea* $\Sigma = \{((\neg F) \to G), ((\neg F) \to (\neg G))\} \cup \{(\neg F)\}$ *entonces:*

1. $\Sigma \vdash ((\neg F) \to G)$ *ya que* $((\neg F) \to G) \in \Sigma$.
2. $\Sigma \vdash ((\neg F) \to (\neg G))$ *ya que* $((\neg F) \to (\neg G)) \in \Sigma$.
3. $\Sigma \vdash (\neg F)$ *ya que* $(\neg F) \in \Sigma$.
4. $\Sigma \vdash (((\neg F) \to (\neg G)) \to (G \to F))$ *axioma 3.*
5. $\Sigma \vdash (G \to F)$ *mp 4,2.*

6. $\Sigma \vdash G$ *mp 3,1.*

7. $\Sigma \vdash (((\neg H) \to (\neg F)) \to (F \to H))$ *axioma 3.*

8. $\Sigma \vdash ((\neg F) \to ((\neg H) \to (\neg F)))$ *axioma 1 (sustituyendo $F$ por $(\neg F)$ y $G$ por $(\neg H)$).*

9. $\Sigma \vdash ((\neg H) \to (\neg F))$ *mp 8,3.*

10. $\Sigma \vdash (F \to H)$ *mp 7,9.*

11. $\Sigma \vdash F$ *mp 5,6.*

12. $\Sigma \vdash H$ *mp 10,11.*

13. $\Sigma \vdash ((\neg F) \to ((\neg(\neg H)) \to (\neg F)))$ *axioma 1 (sustituyendo $F$ por $(\neg F)$ y $G$ por $(\neg(\neg H))$).*

14. $\Sigma \vdash ((\neg(\neg H)) \to (\neg F))$ *mp 13,3.*

15. $\Sigma \vdash (((\neg(\neg H)) \to (\neg F)) \to (F \to (\neg H)))$ *axioma 3 (sustituyendo $F$ por $(\neg H)$ y $G$ por $F$).*

16. $\Sigma \vdash (F \to (\neg H))$ *mp 15,14.*

17. $\Sigma \vdash (\neg H)$ *mp 16,11.*

*Esto prueba* $\{((\neg F) \to G), ((\neg F) \to (\neg G))\} \cup \{(\neg F)\} \vdash H$ *y*
$\{((\neg F) \to G), ((\neg F) \to (\neg G))\} \cup \{(\neg F)\} \vdash (\neg H)$*, por lo que el lema queda demostrado.*

**Lema 1.6.** *La fórmula* $(((\neg G) \to (\neg F)) \to (((\neg G) \to F) \to G))$ *es un teorema de la lógica proposicional.*

**Demostración.** *Demostraremos* $\{((\neg G) \to (\neg F)), ((\neg G) \to F)\} \vdash G$ *y aplicaremos dos veces el teorema de la deducción.*
*Sea* $\Sigma = \{((\neg G) \to (\neg F)), ((\neg G) \to F)\}$ *entonces:*

1. $\Sigma \vdash ((\neg G) \to (\neg F))$ *ya que* $((\neg G) \to (\neg F)) \in \Sigma$.

2. $\Sigma \vdash ((\neg G) \to F)$ *ya que* $((\neg G) \to F) \in \Sigma$.

3. $\Sigma \vdash (((\neg G) \to F) \to ((\neg G) \to (\neg F)) \to G)$ *lema 1.5.*

4. $\Sigma \vdash (((\neg G) \to (\neg F)) \to G)$ *mp 2,3.*

5. $\Sigma \vdash G$ *mp 1,4.*

**Lema 1.7.** *La fórmula* $((\neg(\neg F)) \to F)$ *es un teorema de la lógica proposicional.*

**Demostración.** 1. $(((\neg F) \to (\neg F)) \to (((\neg F) \to (\neg(\neg F))) \to F))$ *lema 1.5 (sustituendo* $G$ *por* $(\neg F)$*).*

2. $((\neg F) \to (\neg F))$ *lema 1.3.*

3. $(((\neg F) \to (\neg(\neg F))) \to F)$ *mp 1,2.*

4. $((\neg(\neg F)) \to ((\neg F) \to (\neg(\neg F))))$ *axioma 1 (sustituendo* $F$ *por* $(\neg(\neg F))$ *y* $G$ *por* $(\neg F)$*).*

5. $((\neg(\neg F)) \to F)$ *corolario 1.1 4,3.*

**Lema 1.8.** *La fórmula* $(F \to (\neg(\neg F)))$ *es un teorema de la lógica proposicional.*

**Demostración.** 1. $(F \to ((\neg(\neg(\neg F))) \to F))$ *axioma 1 (sustituyendo* $G$ *por* $(\neg(\neg F))$*).*

2. $(((\neg(\neg(\neg F))) \to F) \to (((\neg(\neg(\neg F))) \to (\neg F)) \to (\neg(\neg F))))$ *lema1.5 (sustituyendo* $F$ *por* $(\neg(\neg F))$ *y* $G$ *por* $F$*).*

3. $(F \to (((\neg(\neg(\neg F))) \to (\neg F)) \to (\neg(\neg F))))$ *corolario 1.1 1,2.*

4. $((\neg(\neg(\neg F))) \to (\neg F))$ *lema 1.7 (sustityendo* $F$ *por* $(\neg F)$*).*

5. $(F \to (\neg(\neg F)))$ *lema 1.4 3,4.*

**Lema 1.9.** *La fórmula* $((F \to G) \to ((\neg G) \to (\neg F)))$ *es un teorema de la lógica proposicional.*

**Demostración.** *Probando* $\{(F \to G)\} \vdash ((\neg G) \to (\neg F))$ *y aplicando el teorema de la deducción quedará demostrado el lema. Veamos que* $\{(F \to G)\} \vdash ((\neg G) \to (\neg F))$*:*

1. $\{(F \to G)\} \vdash (F \to G)$ *ya que* $(F \to G) \in \{(F \to G)\}$.

2. $\{(F \to G)\} \vdash ((\neg(\neg F)) \to F)$ *lema 1.7.*

3. $\{(F \to G)\} \vdash ((\neg(\neg F)) \to G)$ *corolario 1.1 2,1.*

4. $\{(F \to G)\} \vdash (G \to (\neg(\neg G)))$ *lema 1.8.*

5. $\{(F \to G)\} \vdash ((\neg(\neg F)) \to (\neg(\neg G)))$ *corolario 1.1 3,4.*

6. $\{(F \to G)\} \vdash (((\neg(\neg F)) \to (\neg(\neg G))) \to ((\neg G) \to (\neg F)))$ *axioma 3 (sustituyendo F por* $(\neg F)$ *y G por* $(\neg G)$*).*

7. $\{(F \to G)\} \vdash ((\neg G) \to (\neg F))$ *mp 6,5.*

**Lema 1.10.** *La fórmula* $(F \to ((F \to G) \to G))$ *es un teorema de la lógica proposicional.*

**Demostración.** *Por el teorema de la deducción la fórmula* $(F \to ((F \to G) \to G))$ *es un teorema si* $\{F, (F \to G)\} \vdash G$*. Veamos que* $\{F, (F \to G)\} \vdash G$*. Sea* $\Sigma = \{F, (F \to G)\}$ *entonces:*

1. $\Sigma \vdash F$ *ya que* $F \in \Sigma$*.*

2. $\Sigma \vdash (F \to G)$ *ya que* $(F \to G) \in \Sigma$*.*

3. $\Sigma \vdash G$ *mp,2,1.*

*Aplicando dos veces el teorema de la deducción queda demostrado el lema.*

**Lema 1.11.** *La fórmula* $(F \to ((\neg G) \to (\neg(F \to G))))$ *es un teorema de la lógica proposicional.*

**Demostración.** 1. $(((F \to G) \to G) \to ((\neg G) \to (\neg(F \to G))))$ *lema 1.9 (sustituyendo F por* $(G \to G)$*).*

2. $(F \to ((F \to G) \to G))$ *lema 1.10.*

3. $(F \to ((\neg G) \to (\neg(F \to G))))$ *por transitividad.*

**Lema 1.12.** *La fórmula* $((\neg F) \to (F \to G))$ *es un teorema de la lógica proposicional.*

**Demostración.** *Basta probar* $\{(\neg F), F\} \vdash G$ *y aplicar dos veces el teorema de la deducción para demostrar el lema. Por ser* $\Sigma = \{(\neg F), F\}$ *un conjunto inconsistente entonces deducimos de él cualquier fórmula. Veamos otra demostración:*

1. $\Sigma \vdash (\neg F)$ *ya que* $(\neg F) \in \Sigma$.

2. $\Sigma \vdash F$ *ya que* $F \in \Sigma$.

3. $\Sigma \vdash (F \to ((\neg G) \to F))$ *axioma 1 (sustituyendo* $G$ *por* $(\neg G)$*).*

4. $\Sigma \vdash ((\neg F) \to ((\neg G) \to (\neg F)))$ *axioma 1 (sustituyendo* $F$ *por* $(\neg F)$ *y* $G$ *por* $(\neg G)$*).*

5. $\Sigma \vdash ((\neg G) \to F)$ *mp 3,2.*

6. $\Sigma \vdash ((\neg G) \to (\neg F))$ *mp 4,1.*

7. $\Sigma \vdash (((\neg G) \to F) \to (((\neg G) \to (\neg F)) \to G))$ *lema 1.5.*

8. $\Sigma \vdash (((\neg G) \to (\neg F)) \to G)$ *mp 7,5.*

9. $\Sigma \vdash G$ *mp 8,6.*

**Lema 1.13.** *La fórmula* $((F \to G) \to (((\neg F) \to G) \to G))$ *es un teorema de la lógica proposicional.*

**Demostración.** *Probaremos* $\{(F \to G), ((\neg F) \to G)\} \vdash G$ *y aplicaremos dos veces el teorema de la deducción para demostrar el lema. Sea* $\Sigma = \{(F \to G), ((\neg F) \to G)\}$ *entonces:*

1. $\Sigma \vdash (F \to G)$ *ya que* $(F \to G) \in \Sigma$.

2. $\Sigma \vdash ((\neg F) \to G)$ *ya que* $((\neg F) \to G) \in \Sigma$.

3. $\Sigma \vdash ((F \to G) \to ((\neg G) \to (\neg F)))$ *lema 1.9.*

4. $\Sigma \vdash ((\neg G) \to (\neg F))$ *mp 3,1.*

5. $\Sigma \vdash (((\neg F) \to G) \to ((\neg G) \to (\neg(\neg F))))$ *lema 1.9 (sustituyendo* $F$ *por* $(\neg F)$*).*

6. $\Sigma \vdash ((\neg G) \to (\neg(\neg F)))$ *mp 5,2.*

7. $\Sigma \vdash (((\neg G) \to (\neg F)) \to (((\neg G) \to ((\neg(\neg F)) \to G))$ *lema 1.5 (sustituyendo* $F$ *por* $G$ *y* $G$ *por* $(\neg F)$*).*

8. $\Sigma \vdash (((\neg G) \to (\neg F)) \to G)$ *por transitividad 7,6.*

*9.* $\Sigma \vdash G$ *mp 8,4.*

Cualquier teorema de la lógica proposicional puede ser demostrado tomando el segundo sistema axiomático, es decir, tomaríamos como axioma la fórmula $(((\neg G) \to (\neg F)) \to (((\neg G) \to F) \to G))$ en vez de
$(((\neg G) \to (\neg F)) \to (F \to G))$. Esto se debe a que
$(((\neg G) \to (\neg F)) \to (F \to G))$ es un teorema de la lógica proposicional que se puede demostrar desde el segundo sistema axiomático.

**Lema 1.14.** *La fórmula* $(((\neg F) \to (\neg G)) \to (G \to F))$ *es un teorema de la lógica proposicional demostrable desde el segundo sistema axiomático definido.*

**Demostración.** *Probaremos* $\{((\neg G) \to (\neg F))\} \vdash (G \to F)$ *y aplicaremos el teorema de la deducción.*

1. $\{((\neg G) \to (\neg F))\} \vdash ((\neg G) \to (\neg F))$ *ya que*
   $((\neg G) \to (\neg F)) \in \{((\neg G) \to (\neg F))\}$.
2. $(((\neg G) \to F) \to (((\neg G) \to (\neg F)) \to G))$ *axioma 3.*
3. $(((\neg G) \to F) \to G)$ *lema 1.4 3,1.*
4. $(F \to ((\neg G) \to F))$ *axioma 1 (sustituyendo B por* $(\neg G)$*).*
5. $(F \to G)$ *por transitividad 4,3.*

**Observación 1.7.** *Notemos que para demostrar el corolario 1.1 y el lema 1.4 no hemos usado el tercer axioma de nuestro sistema axiomático(tampoco lo hemos usado para ningún resultado previo necesario para poder demostrar el corolario 1.1 y el lema 1.4). El hecho de que* $(((\neg G) \to (\neg F)) \to (F \to G))$ *sea un teorema de la lógica proposicional demostrado desde el segundo sistema axiomático demuestra que cualquier teorema de la lógica proposicional demostrado desde el primer sistema axiomático también puede ser demostrado desde el segundo sistema axiomático.*
*También hemos demostrado que la fórmula*
$(((\neg G) \to (\neg F)) \to (((\neg G) \to F) \to G))$ *es un teorema de la lógica proposicional demostrable si trabajamos con el primer sistema axiomático, es decir, cualquier teorema de la lógica proposicional demostrable desde el segundo sistema axiomático es demostrable desde el primer sistema axiomático.*
*Finalmente concluimos que no varían los teoremas si trabajamos con el primer sistema axiomático o con el segundo.*

Dada una valoración cualquiera y una fórmula F definimos la fórmula $\hat{F}$ de la siguiente manera:

$$\hat{F} = \begin{cases} (\neg F) & \text{si } \upsilon(F) = 0 \\ F & \text{caso contrario} \end{cases} \tag{1.1}$$

**Lema 1.15.** *Sea $F \in \mathcal{P}$ sobre $P_0 = \{p_1, p_2, p_3, ..., p_k\}$ y $\upsilon$ una valoración entonces $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{F}$.*

**Demostración.** *Haremos inducción sobre el número de conectores en F. Si $n = 0$ entonces $F$ es una variable proposicional, es decir $F = p_i$ con $i \in \{1, 2, 3, ..., k\}$ y por tanto $\hat{F} = \hat{p_i}$. Para probar $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{p_i}$ basta hacer:*

1. *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{p_i}$ ya que $\hat{p_i} \in \{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\}$.*

*Suponemos que el lema es válido para una cualquier fórmula con una cantidad de conectores menor que n. Sea G una fórmula con n conectores. La fórmula G es de la forma $(\neg H)$ o $(H \to J)$ con H y J fórmulas con una cantidad de conectores menor que n.*

- *Caso $G = (\neg H)$ y $\upsilon(H) = 1$.*
  *Por ser $\upsilon(H) = 1$ entonces $\hat{H} = H$ y $\upsilon(G) = \upsilon(\neg H) = 0$ entonces $\hat{G} = (\neg G)$. Por hipótesis $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{H}$;*
  *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash H$. Probaremos $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{G}$.*

  1. *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{H}$ ya explicado.*
  2. *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (H \to (\neg(\neg H)))$ por el lema 1.8.*
  3. *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (\neg(\neg H))$ mp 2,1.*

  $(\neg(\neg H)) = (\neg G) = \hat{G}$.

- *Caso $G = (\neg H)$ con $\upsilon(H) = 0$.*
  *Por ser $\upsilon(H) = 0$ tenemos $\hat{H} = (\neg H)$ y $\upsilon(G) = \upsilon(\neg H) = 1$ y por consiguiente $\hat{G} = G$. Por hipótesis $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{H}$;*
  *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (\neg H)$;*
  *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash G$.*

- *$(G = (H \to J))$ con $\upsilon(H) = 0$.*
  *En este caso $\hat{H} = (\neg H)$ y $\upsilon(G) = \upsilon(C \to J) = 1$ entonces $\hat{G} = G$. Por hipótesis $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{H}$;*
  *$\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (\neg H)$. Probaremos $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{G}$.*

1. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (\neg H)$ *ya explicado.*
2. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash ((\neg H) \to (H \to J))$ *lema 1.12.*
3. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (C \to J)$ *mp 2,1.*

$\hat{G} = G = (H \to J)$

- *Caso* $(G = (H \to J))$ *con* $\upsilon(J) = 1$.
  *En este caso* $\hat{J} = J$ *y* $\upsilon(G) = \upsilon(H \to J) = 1$ *entonces* $\hat{G} = G$. *Por hipótesis* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{J}$; $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash J$. *Probaremos* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{G}$.

  1. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash J$ *ya explicado.*
  2. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (J \to (H \to J))$ *axioma 1.*
  3. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (H \to J)$ *mp 2,1.*

  $\hat{G} = G = (H \to J)$

- *Caso* $(G = (H \to J))$ *con* $\upsilon(H) = 1$ *y* $\upsilon(J) = 0$
  $\upsilon(G) = \upsilon(G = (H \to J)) = 0$ *entonces* $\hat{G} = (\neg G) = (\neg(H \to J))$. *En este caso* $\hat{H} = H$ *y* $\hat{J} = (\neg J)$, *por tanto* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash H$ *y* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (\neg J)$. *Probaremos* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{G}$

  1. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash H$ *ya explicado.*
  2. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (\neg H)$ *ya explicado.*
  3. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (H \to ((\neg J) \to (\neg(H \to J))))$ *lema 1.11.*
  4. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash ((\neg D) \to (\neg(C \to J)))$ *mp 3,1.*
  5. $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash (\neg(H \to J))$ *mp 4,2.*

**Teorema 1.6.** *1. Una fórmula es un teorema si y solo si es una tautología.*

*2. Un conjunto* $\Sigma$ *es consistente si y solo si existe una valoración tal que* $\upsilon(x) = 1$ *para todo* $x \in \Sigma$.

*3. Una fórmula* $F$ *es una consecuencia sintáctica del conjunto* $\Sigma$ *si y solo si* $F$ *es una consecuencia semántica del conjunto* $\Sigma$, *es decir* $\Sigma \vdash F$ *si y solo si* $\Sigma \models F$.

**Demostración.** *1. Veremos que si F un teorema entonces F es una tautología.*
*Cualquier teorema es el último término de una sucesión formada por axiomas o que han sido obtenidos por modus ponens, en ambos casos ya hemos comprobado que los axiomas y cualquier fórmula obtenida mediante modus ponens son tautologías.*
*Veamos que si F es una tautología entonces es un teorema.*
*Por ser tautología* $\upsilon(F) = 1$ *para cualquier valoración, entonces* $\hat{F} = F$ *para cualquier valoración. Por el lema 1.15 tenemos* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash \hat{F}$; $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_k}\} \vdash F$. *Usando dos valoraciones diferentes* $\upsilon$ *y tal que* $\upsilon(p_k) = 1$, $(p_k) = 0$ *y* $\upsilon(p_i) = (p_i)$ *para todo i menor que k tenemos* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., p_k\} \vdash F$ *y* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., (\neg p_k)\} \vdash F$, *aplicando el teorema de la deducción tenemos* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p_{k-1}}\} \vdash (\hat{p_k} \to F)$ *y* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., (\hat{p_{k-1}})\} \vdash ((\neg p_k) \to F)$.
*Veamos que* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p}_{k-1}\} \vdash F$ *de la siguiente manera:*

a) $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p}_{k-1}\} \vdash ((p_k \to F) \to (((\neg p_k) \to F) \to F))$ *por el lema 1.13.*

b) $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p}_{k-1}\} \vdash (p_k \to F)$ *ya explicado.*

c) $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p}_{k-1}\} \vdash (((\neg p_k) \to F) \to F)$ *mp a,b.*

d) $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., (\hat{p}_{k-1})\} \vdash ((\neg p_k) \to F)$ *ya explicado.*

e) $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p}_{k-1}\} \vdash F$ *mp c,d.*

*De la misma forma se demuestra* $\{\hat{p_1}, \hat{p_2}, \hat{p_3}, ..., \hat{p}_{k-2}\} \vdash F$. *Si repetimos el proceso* $k - 1$ *veces demostramos* $\emptyset \vdash F$.

*2. Primero veamos el siguiente lema: Si un conjunto* $\Sigma$ *es consistente entonces para cualquier fórmula G, bien* $\Sigma \cup \{G\}$ *es consistente, bien* $\Sigma \cup \{(\neg G)\}$ *es consistente.*
*Ya hemos probado que al menos uno de los dos conjuntos es inconsistente, ahora probaremos por reducción al absurdo que uno de ellos es consistente. Para probarlo supondremos que existe una fórmula G tal que ni* $\Sigma \cup \{G\}$ *ni* $\Sigma \cup \{(\neg G)\}$ *son consistentes. Sea k una contradicción entonces por el teorema de la deducción tenemos* $\Sigma \vdash ((\neg G) \to k)$ *y* $\Sigma \vdash (G \to k)$. *Veamos que* $\Sigma \vdash k$*:*

a) $\Sigma \vdash ((\neg G) \to k)$ *ya probado.*

b) $\Sigma \vdash (G \to k)$ *ya probado.*

c) $\Sigma \vdash ((G \to k) \to (((\neg G) \to k) \to k))$ *lema 1.13.*

d) $\Sigma \vdash (((\neg G) \to k) \to k)$ *mp c,b.*

e) $\Sigma \vdash k$ *mp d,a.*

*Esto es absurdo, pues* $\Sigma$ *es consistente, luego o* $\Sigma \cup \{G\}$ *o* $\Sigma \cup \{(\neg G)\}$ *es consistente.*

*Definimos el conjunto de fórmulas* $\Sigma^+$ *de la siguiente manera:*

$$\Sigma^+ = \begin{cases} \Sigma \cup \{G\} & \text{si } \Sigma \cup \{G\}\text{si es consistente} \\ \Sigma \cup \{(\neg G)\} & \text{caso contrario} \end{cases} \tag{1.2}$$

*Observemos que* $\Sigma \subset \Sigma^+$ *y si* $G \in \Sigma^+$ *entonces* $(\neg G) \notin \Sigma^+$.
*Definimos* $\upsilon(p) = 1$ *si* $p \in \Sigma^+$ *y* $\upsilon(p) = 0$ *caso contrario y extendemos* $\upsilon$ *a una valoración.*
*Probaremos* $\upsilon(G) = 1$ *si y solo si* $G \in \Sigma^+$. *Haremos inducción sobre el número de símbolos de G.*
*Caso* $n = 1$. *En este caso G es una variable proposicional. Por la definición dada se cumple el teorema.*
*Suponemos que se cumple para cualquier fórmula con una cantidad de símbolos menor que n. Tenemos dos casos:*

- *Si G una fórmula del tipo* $(\neg H)$ *entonces* $\upsilon(G) = 1$ *si y solo si* $\upsilon(\neg H) = 1$ *si y solo si* $\upsilon(H) = 0$. *Por hipótesis de inducción* $\upsilon(H) = 0$ *si y solo si* $H \notin \Sigma^+$ *si y solo si* $(\neg H) \in \Sigma^+$ *si y solo si* $G \in \Sigma^+$.
- *Si G es una fórmula del tipo* $(H \to J)$ *entonces* $\upsilon(G) = 1$ *si y solo si* $\upsilon(H \to J) = 1$ *si y solo si* $\upsilon(H) = 0$ *o* $\upsilon(J) = 1$. *Por hipótesis de inducción* $\upsilon(H) = 0$ *o* $\upsilon(J) = 1$ *si y solo si* $H \notin \Sigma^+$ *o* $J \in \Sigma^+$ *si y solo si* $(\neg H) \in \Sigma^+$ *o* $J \in \Sigma^+$. *Veremos que en ambos casos* $\Sigma^+ \vdash G$.
  *Si* $(\neg H) \in \Sigma^+$ *entonces:*
  a) $\Sigma^+ \vdash ((\neg H) \to (H \to J))$ *lema 1.12.*
  b) $\Sigma^+ \vdash (\neg H)$ *ya que* $(\neg H) \in \Sigma^+$.
  c) $\Sigma^+ \vdash (H \to J)$ *mp a,b.*
  *Como* $G = (H \to J)$ *entonces* $\Sigma^+ \vdash G$.
  *Si* $J \in \Sigma^+$ *entonces:*

a) $\Sigma^+ \vdash (J \to (H \to J))$ *axioma 1.*

b) $\Sigma^+ \vdash J$ *ya que* $J \in \Sigma^+$.

c) $\Sigma^+ \vdash (H \to J)$ *mp a,b.*

*Por lo tanto* $\Sigma^+ \vdash G$.

*El conjunto* $\Sigma^+$ *es consiste, por lo tanto* $(\neg G) \notin \Sigma^+$ *y por consiguiente* $G \in \Sigma^+$.
*Suponemos* $\upsilon(G) = 0$.
$\upsilon(G) = 0$ *si y solo si* $\upsilon(H \to J) = 0$ *si y solo si* $\upsilon(H) = 1$ *y* $\upsilon(J) = 0$ *si y solo si* $H \in \Sigma^+$ *y* $J \notin \Sigma^+$ *si y solo si* $H \in \Sigma^+$ *y* $(\neg J) \in \Sigma^+$. *Veamos que* $\Sigma^+ \vdash (\neg G)$*:*

a) $\Sigma^+ \vdash H$ *ya que* $H \in \Sigma^+$.

b) $\Sigma^+ \vdash (\neg J)$ *ya que* $(\neg J) \in \Sigma^+$.

c) $\Sigma^+ \vdash (H \to ((\neg J) \to (\neg(H \to J))))$ *teorema 1.11.*

d) $\Sigma^+ \vdash ((\neg J) \to (\neg(H \to J)))$ *mp c,a.*

e) $\Sigma^+ \vdash (\neg(H \to J))$ *mp d,b.*

*Por lo tanto* $\Sigma^+(\neg G)$ *como* $\Sigma^+$ *es consistente* $G \notin \Sigma^+$.
*Concluimos que* $\upsilon(G) = 1$ *si y solo si* $G \in \Sigma^+$ *si y solo si* $G \in \Sigma$.

*Veamos ahora que si existe una valoración* $\upsilon$ *tal que* $\upsilon(x) = 1$ *para todo* $x \in \Sigma$ *entonces* $\Sigma$ *es consistente.*
*Para demostrar esto probaremos que si* $\Sigma$ *es inconsistente entonces no existe ninguna valoración* $\upsilon$ *tal que* $\upsilon(x) = 1$ *para todo* $x \in \Sigma$.
*En el siguiente párrafo demostraremos que si existe una valoración* $\upsilon$ *tal que* $\upsilon(x) = 1$ *para todo* $x \in \Sigma$ *entonces* $\upsilon(F) = 1$ *si* $\Sigma \vdash F$. *Por ser* $\Sigma$ *inconsistente existe una fórmula* $F$ *tal que* $\Sigma \vdash F$ *y* $\Sigma \vdash (\neg F)$, *por lo tanto* $\upsilon(F) = \upsilon(\neg F) = 1$, *lo cual es absurdo. Por lo tanto, si el conjunto* $\Sigma$ *es inconsistente no existe ninguna valoración* $\upsilon$ *tal que* $\upsilon(x) = 1$ *para todo* $x \in \Sigma$.

3. *Veamos que si* $\Sigma \vdash F$ *entonces* $\Sigma \models F$.

   *Si* $\Sigma \vdash F$ *entonces existe una sucesión de fórmulas*
   $A_1, A_2, A_3, ..., A_n = F$ *tal que para todo* $i \in \{1, 2, 3, ..., n\}$ $A_i$ *es, bien un*

*axioma, bien una fórmula de* $\Sigma$*, bien ha sido obtenido mediante modus ponens de* $A_n$ *y* $A_m$ *con* $m, n < i$*. Sea* $\upsilon$ *una valoración cualquiera tal que para todo* $x \in \Sigma$ $\upsilon(x) = 1$*. Veamos por inducción sobre el número de términos de la sucesión* $A_1, A_2, A_3, ..., A_n = F$ *que* $\upsilon(F) = 1$*.*

*Para* $n = 1$ *si* $A_1 \in \Sigma$ *entonces* $\upsilon(A_1) = 1$ *por hipótesis.*
*Si* $A_1$ *es un axioma entonces* $\upsilon(A_1) = 1$ *para cualquier valoración, si* $A_1$ *ha sido obtenido mediante la regla de inferencia modus ponens entonces existen dos fórmulas* $(G \to A_1)$ *y* $G$ *que son axiomas o pertenecen* $\Sigma$*, es decir, en ambos casos por hipótesis* $\upsilon((G \to A_1)) = 1$ *y* $\upsilon(G) = 1$*.*
*Sabemos que* $\upsilon((G \to A_1)) = 1$ *si y solo si* $\upsilon(G) = 0$ *o* $\upsilon(A_1) = 1$*, como* $\upsilon(G) \neq 0$ *entonces* $\upsilon(A_1) = 1$*.*

*Suponemos que para todo* $i < n$ *se cumple* $\upsilon(A_i) = 1$*, veamos que* $\upsilon(A_n) = 1$*. Si* $A_n$ *es un axioma o una fórmula de* $\Sigma$ *entonces, por los mismos razonamientos del párrafo anterior,* $\upsilon(A_1) = 1$*.*
*Si* $A_n$ *ha sido obtenido mediante la regla de inferencia modus ponens entonces existen dos fórmulas* $(G \to A_n)$ *y* $G$ *que son axiomas o pertenecen* $\Sigma$ *o son términos de la sucesión anteriores a* $A_n$*. Si las fórmulas* $(G \to A_n)$ *y* $G$ *son axiomas o pertenecen a* $\Sigma$ *entonces*
$\upsilon((G \to A_n)) = 1$ *y* $\upsilon(G) = 1$ *si son términos anteriores* $A_n$ *entonces, por hipótesis de inducción,* $\upsilon((G \to A_n)) = 1$ *y* $\upsilon(G) = 1$*. Al igual que en el párrafo anterior* $\upsilon((G \to A_1)) = 1$ *si y solo si* $\upsilon(G) = 0$ *o* $\upsilon(A_1) = 1$*, como* $\upsilon(G) \neq 0$ *entonces* $\upsilon(A_1) = 1$*.*

*Veamos ahora que si* $\Sigma \models F$ *entonces* $\Sigma \vdash F$*.*

*Atendiendo a la definición de consecuencia semántica no descartaremos el caso en el que no exista ninguna valoración tal que para todo* $x \in \Sigma$ $\upsilon(x) = 1$*. Si estamos en este caso, hemos visto que un conjunto* $\Sigma$ *es consistente si y solo existe una valoración tal que para* $x \in \Sigma$ $\upsilon(x) = 1$*, es decir,* $\Sigma$ *es inconsistente. Por otra parte hemos probado que cualquier fórmula es una consecuencia sintáctica de un conjunto inconsistente, por tanto* $\Sigma \vdash F$*.*

*Suponemos ahora que existe al menos una valoración* $\upsilon$ *tal que para todo* $x \in \Sigma$ $\upsilon(x) = 1$*. Como* $\Sigma \models F$ *entonces* $\upsilon(F) = 1$*. Por el apartado 2 de este teorema tanto* $\Sigma$ *como* $\Sigma \cup \{F\}$ *son consistentes y* $\Sigma \cup \{(\neg F)\}$ *es inconsistente. En la demostración del lema 1.5 vimos que si* $\Sigma \cup \{(\neg F)\}$ *es inconsistente entonces* $\Sigma \vdash F$*.*

**Teorema 1.7.** *Sea $\Sigma$ un conjunto de fórmulas proposicionales entonces $\Sigma$ es consistente si y solo si cada subconjunto finito de $\Sigma$ es consistente.*

**Demostración.** *1. Veamos que si $\Sigma$ es consistente entonces cada subconjunto finito de $\Sigma$ es consistente.*
*Probar esta implicación es equivalente a probar que si existe un subconjuto finito de $\Sigma$ inconsiste entonces $\Sigma$ es inconsistente. Sea $\Gamma \subset \Sigma$ inconsistente. Por el teorema anterior $\Gamma \vdash k$ con $k$ contradicción. La contradicción ha sido obtenida mediante axiomas, modus ponens y fórmulas en $\Gamma \subset \Sigma$, es decir, desde $\Sigma$ podemos obtener la misma contradicción, por tanto, $\Sigma$ es inconsistente.*

*2. Veamos que si cada subconjunto finito de $\Sigma$ es consistente entonces $\Sigma$ es consistente.*
*Para probar esto veamos que si $\Sigma$ es inconsiste entonces existe algún subconjunto $\Gamma \subset \Sigma$ inconsistente.*
*Por ser $\Sigma$ un conjunto inconsistente podemos obtener con una sucesión finita una contradicción, es decir, existe una sucesión $A_1, A_2, A_3, ..., A_n$ tal que $A_n = k$ siendo $k$ una contradicción y cada $A_i$ con $i \in \mathbb{N}$ es, bien un axioma, bien una fórmula de $\Sigma$, bien ha sido obtenido mediante modus ponens. Entonces el conjunto $\Gamma = \bigcup\{A_j\}$ tal que $A_j \in \Sigma$ es un conjunto finito contenido en $\Sigma$ y del cual deriva una contradicción, por tanto inconsistente.*

# Capítulo 2

# Lógica de Primer Orden

*La lógica de primer orden toma la lógica proposicional y la amplia con el fin de ser más expresiva y reducir el número de sentencias que tenemos en la lógica proposicional.*
*La lógica de primer orden es un sistema formal muy útil para analizar argumentos y para las matemáticas. Estudiaremos la lógica de primer orden por las limitaciones de la lógica proposicional. Por ejemplo:*
*Si un gato juega con un segundo gato entonces el segundo gato juega con el primero. El gato Félix juega con el gato Isidoro, por lo tanto Isidoro juega con Félix.*
*Es imposible de representar en la lógica proposicional, en cambio en la lógica de primer orden escribiríamos:*
$\{(\forall x)(\forall y)(juega(x,y) \rightarrow juega(y,x)), juega(Félix, Isidoro)\} \models juega(Isidoro, Félix)$.

## 2.1. Sintaxis y semántica de la lógica de primer orden.

**Definición 2.1.** *Definimos un alfabeto $\mathcal{A}$ del sistema formal de la lógica de primer orden:*

- *Un conjunto de variables $\{u, v, w, ...\}$.*
- *Un conjunto de conectores $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$.*
- *Cuantificadores '$\forall$' (para todo) y '$\exists$' (existe).*

- *Paréntisis y comas.*
- *El símbolo de igualdad ' =' (igual).*
- *Símbolos para constantes, normalmente serán a,b,c,... .*
- *Símbolos para funciones, normalmente serán f,g,h... .*
- *Símbolos para relaciones que también llamaremos predicados. Normalmente estos símbolos son p,q,r,... .*

**Definición 2.2.** *Un lenguaje formal es un sistema formal en el que hemos especificado los símbolos de funciones de constantes, funciones y predicados. Habitualmente escribiremos lenguaje para referirnos a un lenguaje formal.*

**Definición 2.3.** *La aridad de una función o de una relación es el número de argumentos necesarios para que dicha función o relación se puedan calcular.*

**Definición 2.4.** *Una cadena de símbolos del alfabeto $\mathcal{A}$ es una palabra.*

**Definición 2.5.** *Definiremos el conjunto de los términos de manera recursiva:*

1. *Los símbolos de constantes son términos.*
2. *Las variables son términos.*
3. *Si $f$ es una función de aridad $n$ y $t_1, t_2, t_3, ..., t_n$ son términos entonces $f(t_1, t_2, t_3, ..., t_n)$ es un término.*

*Denotaremos $Término(L)$ al conjunto formado por los términos del lenguaje $L$.*

**Ejemplo 2.1.** *Sean $x$ una variable, $4$ una constante, $+$ y $*$ funciones de aridad $2$ entonces:*

- *$x$ y $4$ son términos.*
- *$+(x, x)$ y $*(4, x)$ son términos.*
- *$*(+(x, x), *(4, x))$ es un término.*

*Véase que $*(+(x, x), *(4, x))$ es escrito habitualmente por $(x + x)4x$.*

**Definición 2.6.** *Sea $L$ el sistema formal de la lógica proposicional de primer orden llamaremos $At(L)$ al conjunto fórmulas atómicas. Las fórmulas atómicas son las palabras de las siguientes formas:*

- $(t_1 = t_2)$ *con* $t_1$ *y* $t_2$ *términos.*
- $p(t_1, t_2, t_3, ..., t_n)$ *con* $p$ *símbolo de relación y* $t_1, t_2, t_3, ..., t_n$ *términos.*

**Ejemplo 2.2.** *En el dominio de los números enteros definimos el predicado binario $|(x, y)$ que se lee $x$ divide a $y$ y la función binaria $f(x, y) = x + y$. Tenemos como ejemplos $|(+(+(1, 2), 3), 12), |(3, 30)$ y $f(2, y) = f(y, 2)$. Observamos que en la teoría de los números enteros escribimos $4|40$ o $2 + y = y + 2$.*

**Definición 2.7.** *El conjunto de las fórmulas del sistema formal de la lógica de primer orden $F(L)$ viene dado por:*

1. *Las fórmulas atómicas son fórmulas.*
2. *Si $F$ y $G$ son fórmulas entonces $(\neg F)$, $(F \wedge G)$, $(F \vee G)$ y $(F \leftrightarrow G)$ son fórmulas.*
3. *Si $F$ es una fórmula y $x$ es una variable entonces $(\exists x)F$ y $(\forall x)F$ son fórmulas.*

**Observación 2.1.** *Al igual que en la lógica proposicional construiremos el conjunto de fórmulas del sistema formal de la lógica de primer orden sobre el conjunto de fórmulas atómicas de manera inductiva sobre k, siendo $P_0$ el conjunto de fórmulas átomicas.*
*$P_0 = At(L)$.*
*Sean $F$ y $G$ fórmulas tal que $F, G \in P_k$ y $x$ una variable definimos el conjunto $P_{k+1}$ de la siguiente forma:*
*$P_{k+1} := P_k \cup \{(F \# G), (\neg F), (\forall x)F, (\exists x)F : \# \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}\}$.*
*Llamamos $\mathcal{P}$ al conjunto de fórmulas sobre $P_0$, es decir $\mathcal{P} := \bigcup P_k, k \in \mathbb{N}$.*

**Ejemplo 2.3.** *Sean $+$ y $*$ símbolos de funciones binarias y $\geq$ y $<$ símbolos de predicados binarios entonces algunos ejemplos de fórmulas son los siguientes:*

- $\geq (*(3, x), +(y, z))$ *es una fórmula por ser una fórmula atómica.*
- $< (*(3, x), +(y, z))$ *es una fórmula por ser una fórmula atómica.*

- $(\geq (*(3,x),+(y,z))) \vee (< (*(3,x),+(y,z)))$.
- $(\exists x)(2 = +(x,1))$.

**Observación 2.2.** *(**Importante**) Toda fórmula tiene la misma cantidad de paréntesis de ambos tipos. Se demuestra utilizando el mismo razonamiento usado para demostrar que una fórmula del sistema formal de la lógica proposicional tiene la misma cantidad de paréntesis de ambos tipos.*

**Observación 2.3.** *Aunque cualquier fórmula del sistema formal de la lógica de primer orden tiene la misma cantidad de paréntesis de ambos tipos el lema de los paréntesis demostrado para la lógica proposicional no se cumple para todas las fórmulas del sistema formal de la lógica de primer orden. Basta tomar una fórmula del tipo $(\forall x)F$ y ver que en el segmento inicial $(\forall x)$ hay la misma cantidad de paréntesis abiertos que cerrados, luego no hay más paréntesis abiertos que cerrados.*

**Observación 2.4.** *(**Importante**)A pesar de la observación anterior si el último símbolo del segmento inicial es un conector o un cuantificador entonces en ese segmento inicial hay más paréntesis abiertos que cerrados.*

**Observación 2.5.** *Si en una fórmula $F = a_1a_2a_3...a_n$ de $n$ símbolos hay cuantificador en la posición $i$-ésima, usando la definicón de fórmula, entonces el símbolo siguiente es un cuantificador.*

**Definición 2.8.** *Sea $F \in F(L)$ definimos el conjunto de subfórmulas de $F$ $Sb(F)$ como:*

- $Sb(F) = \{F\}$ *si* $F \in At(L)$.
- $Sb((\neg F)) = Sb(F) \cup \{(\neg F)\}$.
- $Sb(F) = Sb((G\#H)) = Sb(G) \cup Sb(H) \cup \{(G\#H)\}$ *si* $F = (G\#H)$ *con* $G$ *y* $H$ *fórmulas y* $'\#'$ *un conector binario.*
- $Sb((\forall x)F) = Sb(F) \cup \{(\forall x)F\}$
- $Sb((\exists x)F) = Sb(F) \cup \{(\exists x)F\}$

**Observación 2.6.** *Una subfórmula es una fórmula.*

**Ejemplo 2.4.** *Sea F la fórmula* $((\geq (*(3,x),+(y,z)))\vee < (*(3,x),+(y,z)))$.
*Entonces* $Sb(F) = \{F\} \cup Sb(\geq (*(3,x),+(y,z))) \cup Sb(< (*(3,x),+(y,z))$.
$Sb((\geq (*(3,x),+(y,z)))) = ((\geq (*(3,x),+(y,z)))$ *por ser una fórmula atómica.*
$Sb(< (*(3,x),+(y,z))) =< (*(3,x),+(y,z))$ *por ser una fórmula atómica.*
$Sb(F) = \{F, \geq (*(3,x),+(y,z)), < (*(3,x),+(y,z))\}$

**Ejemplo 2.5.** *Formalizaremos algunas oraciones cotidianas:*

- *Todo número natural es real:* $(\forall x)(natural(x) \rightarrow real(y))$.
- *Todo número natural es, o bien par, o bien impar:* $(\forall x)(natural(x) \rightarrow (par(x) \vee impar(x)))$.
- *En el dominio de los números naturales(o reales, o irracionales, o enteros). Para todo número natural existe otro número natural mayor que el primero:* $(\forall x)(\exists y) < (x,y)$.

*Observemos que en el último apartado no hemos utilizaco ningún predicado para especificar que los números deben ser naturales ya que nuestro dominio era el conjunto de los números naturales y esto se cumple para cualquier elemento de tal dominio.*

**Definición 2.9.** *Si F es una fórmula de la forma* $(G\#H)$ *con* $\#$ *conector binario diremos que el conector* $\#$ *es el conector principal de la fórmula F. Si F es de forma* $(\neg G)$ *entonces el conector principal de F es el conector* $\neg$. *Si F es de la forma* $(\forall x)G$*(o* $(\exists x)G$*) entonces el cuantificador principal de F es* $\forall$*(o* $\exists$*).*

**Teorema 2.1.** *Sea F una fórmula tal que* $F \notin P_0$ *y* $F = a_1a_2a_3...a_n$ *con* $a_1, a_2, a_3, ..., a_n$ *símbolos. Definimos la aplicación* $p : \{1,2,3,...,n\} \longrightarrow \mathbb{N}$ *tal que* $p(i)$ *es el número de paréntesis abiertos menos el número de paréntesis cerrados que hay en el segmento inicial* $a_1a_2a_3...a_{i-1}$. *Entonces el conector o cuantificador principal es el primer símbolo* $a_i$ *tal que* $a_i$ *es un conector o un cuantificador y* $p(i) = 1$.

**Demostración.** *Puesto que la demostración es muy parecida al teorema de la lógica proposicional que nos permitía identificar el conector principal solo lo demostraremos para fórmulas del tipo* $(F\#G)$ *y* $(\forall x)F$.
*Si tenemos una fórmula del tipo* $(\forall x)F$, *según la definicón el cuantificador principal es el símbolo* $\forall$ *y vemos que se cumple el teorema:*

| | $i=1$ | $i=2$ |
|---|---|---|
| $a_i$ | $'('$ | $\forall$ |
| $p(i)$ | 0 | 1 |

*Si $F$ es una fórmula de la forma $(G\#H)$. Observemos que $H$ es una fórmula, luego tiene el mismo número de paréntesis abiertos que cerrados y el primero símbolo de la fórmula $F$ es un paréntesis abierto que no está en $H$, por tanto si el conector principal está en la $i$-ésima vemos que $p(i)=1$. Veamos que si $j<i$ y en la posición $j$-ésima hay un conector o cuantificador entonces $p(j)>1$. Esto último se debe a que $H=c_1c_2c_3...c_{j-1}$ es una fórmula y en el segmento inicial $c_1c_2c_3...c_{j-1}$ hay más paréntesis abiertos que cerrados si $c_{j-1}$ es un conector o cuantificador, además el primer símbolo de la fórmula $F$ es un paréntesis abierto, luego $p(j)>1$.*

**Definición 2.10.** *Sea $F$ una fórmula con un cuantificador llamaremos alcance del cuantificador a la única subfórmula $G$ de $F$ tal que el cuantificador principal de $G$ es dicho cuantificador.*

*Al igual que en la lógica proposicional podemos representar cualquier fórmula de la lógica de primer orden con un único diagrama árbol. Antes de empezar a representar una fórmula vamos a representar una función.*

*Sea $f(t_1,t_2,t_3,...,t_n)$ una función. En la raíz del árbol escribiremos el símbolo de la función, en este caso f, y establecemos n relaciones padre-hijo, en cada nodo escribiremos de forma ordenada $t_1,t_2,t_3,...,t_n$. Si $t_i$ es una constante o una variable en ese nodo no haremos más, en cambio si $t_i$ con $i\in\{1,2,3,...,n\}$ es una función ese nodo será sustituido por el diagrama árbol de esa función. Repetimos el proceso hasta que no podamos continuar, esto es, cuando todas en todas las hojas haya, bien una constante, bien una variable.*

*Sea $F$ una fórmula átomica de la forma $(t_1=t_2)$. En la raíz del árbol escribiremos el símbolo de igualdad y establecemos dos relaciones padre-hijo entre la raíz y dos nodos. En el primer nodo escribiremos $t_1$ y en el segundo nodo $t_2$. Si $t_i$ con $i\in\{1,2\}$ es una constante o una variable lo dejamos como está, en cambio si es un símbolo de función sustituimos ese nodo por el árbol correspondiente a esa función.*

*Sea $F$ una fórmula átomica de la forma $p(t_1,t_2,t_3,...,t_n)$ con p predicado. En la raíz del árbol escribiremos el símbolo del predicado, en este caso p,*

*y establecemos n relaciones padre-hijo, en cada nodo escribiremos de forma ordenada $t_1, t_2, t_3, ..., t_n$. Si $t_i$ es una constante o una variable en ese nodo no haremos más, en cambio si $t_i$ con $i \in \{1, 2, 3, ..., n\}$ es una función ese nodo será sustituido por el diagrama árbol de esa función.*

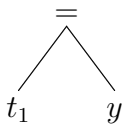
*Si F es una fórmula de la forma $(\neg G)$, $(\forall x)G$ o $(\exists x)G$ entonces en la raíz del árbol escribiremos $\neg$, $(\forall x)$ o $(\exists x)$ según el caso y establecemos una relación padre hijo con un nodo en el que escribiremos G. Sustituimos el nodo G por el diagrama árbol que representa a la fórmula G(es decir, habría una relación padre-hijo entre la raíz del árbol F y la raíz del árbol G).*

*Si F es una fórmula de la forma $(H\#J)$ con $\#$ conector binario entonces en la raíz del árbol escribiremos $\#$ y establecemos dos relaciones padre-hijo con dos nodos en los que escribiremos H y J. Sustituimos los nodos H y J por los diagramas en árbol de las fórmulas H y J(es decir, habría una relación padre-hijo entre la raíz del árbol F y las raíces de los árboles H y J).*

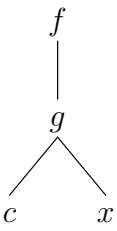
**Ejemplo 2.6.** *Representaremos mediante un árbol algunas fórmulas:*

1. *La fórmula $(\forall y)(f(g(c, x)) = y)$ es una fórmula de la fórmula $(\forall y)G$ siendo G la fórmula atómica $(f(g(c, x)) = y)$. En el primer paso del algoritmo tenemos:*

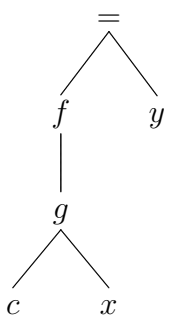

*Ahora necesitamos conocer el árbol de la fórmula $G = (f(g(c, x)) = y)$. Es una fórmula atómica con $t_1 = f(g(c, x))$ y $t_2 = y$. En este segundo paso tenemos:*



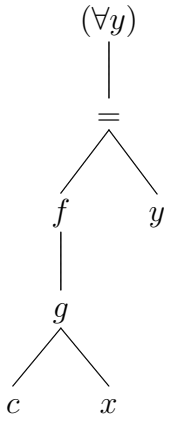

*El árbol de la función f es, según la definición:*



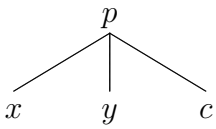
*El árbol que representa a la fórmula G es:*



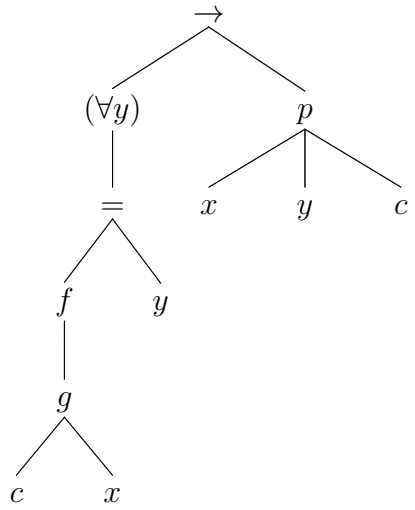

*Y finalmente el árbol que representa a la fórmula* $(\forall y)(f(g(c,x)) = y)$ *es:*




2. *La fórmula atómica* $p(x, y, c)$ *queda representada por el árbol:*




3. *La fórmula* $((\forall y)(f(g(c,x)) = y) \rightarrow p(x,y,c))$ *es una fórmula de la forma* $(F \rightarrow G)$*. Conocemos los árboles que representan a* $(\forall y)(f(g(c,x)) = y)$ *y* $p(x,y,c)$*. Según la definición y los árboles de las fórmulas F y G el árbol que representa a la fórmula* $((\forall y)(f(g(c,x)) = y) \rightarrow p(x,y,c))$ *es:*




**Definición 2.11.** *Sea $t$ un término denotaremos al conjunto de las variables de $t$ de la forma $V(t)$ y los definimos de la siguiente manera:*

1. *Si $t = c$ con $c$ constante entonces $V(t) = \emptyset$.*
2. *Si $t = x$ con $x$ variable entonces $V(t) = \{x\}$.*
3. *Si $t = f(t_1, t_2, t_3, ..., t_n)$ con $f$ una función entonces $V(t) = \bigcup V(t_i)$ con $i \in \{1, 2, 3, ..., n\}$.*

**Definición 2.12.** *Si $F$ es una fórmula denotaremos al conjunto de las variables de $F$ de la forma $V(F)$ y lo definimos de la siguiente manera:*

1. *Si $F = (t_1 = t_2)$ con $t_1$ y $t_2$ términos entonces $V(F) = V(t_1) \cup V(t_2)$.*
2. *Si $F = p(t_1, t_2, t_3, ..., t_n)$ con $p$ predicado entonces $V(F) = \bigcup V(t_i)$ con $i \in \{1, 2, 3, ..., n\}$.*
3. *Si $F = (\neg G)$ entonces $V(F) = V(G)$.*
4. *Si $F = (G \# H)$ con $\#$ conector binario entonces $V(F) = V(G) \cup V(H)$.*
5. *Si $F = (\forall x)G$ o $F = (\exists x)G$ entonces $V(F) = \{x\} \cup V(G)$.*

**Ejemplo 2.7.** *Sea $F = (\exists x)((\forall y)p(x, y) \wedge (0 = f(z)))$ con $p$ predicado, $f$ función y $x$,$y$,$z$ variables veamos que $V(F) = \{x, y, z\}$.*
$V(F) = \{x\} \cup V(((\forall y)p(x, y) \wedge (0 = f(z))))$.

$V(((\forall y)p(x,y) \wedge (0 = f(z)))) = V((\forall y)p(x,y)) \cup V((0 = f(z)))$.
$V((\forall y)p(x,y)) = \{y\} \cup V(x) \cup V(y) = \{y\} \cup \{x\} \cup \{y\}$.
$V((0 = f(z))) = V(0) \cup V(f(z)) = \emptyset \cup V(z) = \emptyset \cup \{z\} = \{z\}$.
*Finalmente vemos que* $V(F) = \{x, y, z\}$.

**Definición 2.13.** *Sea $F$ una fórmula diremos que una aparición u ocurrencia de una variable $x$ en la fórmula $F$ es ligada(a un cuantificador) si es una aparición en una subfórmula del tipo $(\forall x)G$ o $(\exists x)G$.*

*Sea $F$ una fórmula diremos que una aparición u ocurrencia es libre si no es ligada.*

**Ejemplo 2.8.** *Sean $p$ y $q$ predicados vemos que en la fórmula $F = ((\exists x)p(x) \to q(x))$ la variable $x$ tiene dos apariciones ligadas y una libre. El alcance del único cuantificador que hay en la fórmula $F$ es la subfórmula $(\exists x)p(x)$, por lo tanto las dos primeras apariciones son ligadas y la tercera aparición es libre.*

**Definición 2.14.** *Una variable $x$ en una fórmula $F$ es una variable ligada si tiene alguna aparición ligada en $F$. Una variable $x$ en una fórmula $F$ es una variable libre si tiene alguna aparición libre en $F$.*

**Observación 2.7.** *Una aparición de una variable en una fórmula es, o bien libre, o bien ligada, pero una variable puede ser libre y ligada al mismo tiempo, como muestra la fórmula $((\exists x)p(x) \to q(x))$.*

**Teorema 2.2.** *Si $F$ es una fórmula el conjunto $VL(F)$ de variables libres de $F$ es:*

1. *Si $F$ es una fórmula atómica $VL(F) = V(F)$.*
2. *Si $F = (\neg G)$ entonces $VL(F) = VL(G)$.*
3. *Si $F = (G \# H)$ con $\#$ conector binario entonces $VL(F) = VL(G) \cup VL(H)$.*
4. *Si $F = (\forall x)G$ o $F = (\exists x)G$ entonces $VL(F) = VL(G) \backslash \{x\}$.*

**Demostración.** *Sea $F$ una fórmula atómica.*
*Usando la definición de fórmula atómica vemos que $F$ no puede tener cuantificadores, luego cualquier variable que haya en $F$ debe ser libre, esto es $VL(F) = V(F)$.*

*Sea $F$ una fórmula de la forma $(\neg G)$.*
*Usando la definición de subfórmula sabemos que el conjunto de subfórmulas de $F$ es $\{(\neg G)\} \cup Sb(G)$. Usando esta definición podemos deducir que si una variable está ligada a un cuantificador este cuantificador debe ser un símbolo de una subfórmula de $G$.*
*Si $F = (G \# H)$ utilizamos un razonamiento similar al anterior.*
*Sea $F$ una fórmula de la forma $(\forall x)G$ o $(\exists x)G$.*
*La variable $x$ no tiene ninguna aparición libre en $F$ ya que el alcance del cuantificador es la subfórmula $G$, luego la variable $x$ no es una variable libre. Las subfórmulas de $G$ son subfórmulas de $F$, luego si una variable distinta de $x$ tiene una aparición libre o ligada en $G$ también es libre o ligada en $F$.*

**Definición 2.15.** *Llamaremos fórmula cerrada o sentencia a una fórmula sin variables libres.*

**Ejemplo 2.9.** *Unos ejemplos de sentencias son:* $(\forall x)(p(x) \to p(x))$ *y* $(p(3,4) \wedge (\exists y)(\exists x)(f(x,y) = f(y,x)))$.

**Definición 2.16.** *Llamaremos fórmula básica a una fórmula sin variables.*

**Ejemplo 2.10.** *Una fórmula básica es* $(0 = 0)$ *o* $> (8,4)$.

**Definición 2.17.** *Una sustutición $\sigma$ en un lenguaje $L$ es una aplicación $\sigma : Var \longrightarrow Term(L)$ siendo Var el conjunto de las variables de $L$. Escribiremos $[t_1/x_1, t_2/x_2, t_3/x_3, ..., t_n/x_3]$ para denotar a la aplicación $\sigma$ tal que*

$$\sigma(x) = \begin{cases} t_i & \text{si} \quad x_i = t_i \\ x & \text{si} \quad x \notin \{x_1, x_2, x_3, ..., x_n\} \end{cases} \tag{2.1}$$

**Ejemplo 2.11.** *Sea $c$ una constante y $f$ una función escribimos $[f(c)/x, c/y]$ para denotar la sustitución $\sigma$ en $L$ tal que $\sigma(x) = f(c)$ y $\sigma(y) = c$ y las demás variables las envía a ellas mismas.*

**Definición 2.18.** *Sea $t$ un término escribiremos $t[t_1/x_1, t_2/x_2, t_3/x_3, ..., t_n/x_n]$ para denotar al término obtenido tras sustituir las apariciones $x_i$ por $t_i$ en el término $t$.*
*Si $\sigma = [t_1/x_1, t_2/x_2, t_3/x_3, ..., t_n/x_n]$ podemos escribir $t\sigma$.*

**Definición 2.19.** *La extensión de $\sigma$ en términos es la aplicación $\sigma : Term(L) \longrightarrow Term(L)$ definida de la siguiente manera:*

$$t\sigma = \begin{cases} c & \text{si t es la constante c} \\ \sigma(x) & \text{si t es la variable x} \\ f(t_1\sigma, t_2\sigma, t_3\sigma, ..., t_n\sigma) & \text{si t es la función f} \end{cases} \tag{2.2}$$

**Ejemplo 2.12.** *Sea $\sigma = [f(g(a,z),z)/x, g(a,z)/y, a/z]$ con a símbolo de constante. Según la definición el término $f(g(a,z),z)\sigma$ es $f(g(a,z)\sigma, z\sigma) = f(g(a\sigma, z\sigma), \sigma(z)) = f(g(a, \sigma(z)), a) = f(g(a,a),a)$. Por tanto $f(g(a,z),z)\sigma = f(g(a,a),a)$.*

**Observación 2.8.** *Sean $\sigma_1 = [f(y,a)/x]$, $\sigma_2 = [a/y]$ y $\sigma = [f(y,a)/x, a/y]$ con a constante veamos que $f(x,y)\sigma_1\sigma_2 \neq f(x,y)\sigma$.*
*$f(x,y)\sigma_1 = f(x\sigma_1, y\sigma_1) = f(\sigma_1(x), \sigma_1(y)) = f(f(y,a),y)$;*
*$f(f(y,a),y)\sigma_2 = f(f(y,a)\sigma_2, a\sigma_2) = f(f(y\sigma_2, a\sigma_2), a) = f(f(\sigma_2(y),a),a) = f(f(a,a),a)$.*
*$f(x,y)\sigma_1\sigma_2 = f(f(a,a),a)$ $f(x,y)\sigma = f(x\sigma, y\sigma) = f(\sigma(x), \sigma(y)) = f(f(y,a),a)$.*
*Esto se debe a que $\sigma_1\sigma_2$ y $\sigma$ son sustituciones diferentes, ya que $\sigma_1\sigma_2 = [f(a,a)/x, a/y]$ y $\sigma[f(y,a)/x, a/y]$, por lo que $\sigma_1\sigma_2(x) \neq \sigma(x)$.*

**Observación 2.9.** *Las sustituciones se pueden componer, sean $\sigma_1$ y $\sigma_2$ las sustituciones del ejemplo anterior, entonces la composición $\sigma_1\sigma_2$ es $[f(a,a)/x, a/y]$.*

**Definición 2.20.** *Sea $\sigma$ una sustitución y x una variable definimos la sustitución $\sigma_x$ de la siguiente forma:*

$$\sigma_x(y) = \begin{cases} x & \text{si } x{=}y \\ \sigma(y) & \text{si } x \neq y \end{cases} \tag{2.3}$$

**Definición 2.21.** *La extensión de $\sigma$ en la fórmula F es la aplicación $\sigma : F(L) \longrightarrow F(L)$ definida de la siguiente manera:*

$$F\sigma = \begin{cases} (t_1\sigma = t_2\sigma) & \text{si F es de forma } (t_1 = t_2) \\ (G\sigma \# H\sigma) & \text{si F es de la forma } G\#H\text{con \# conector binario.} \\ (\neg(G\sigma)) & \text{si F es de forma } (\neg G) \\ (\forall x)G\sigma_x & \text{si F es de forma } (\forall x)G \\ (\exists x)G\sigma_x & \text{si F es de forma } (\exists x)G \end{cases} \tag{2.4}$$

**Definición 2.22.** *Escribimos $F[t_1/x_1, t_2/x_2, t_3/x_3, ..., t_n/x_n]$ para denotar al término obtenido tras sustituir las apariciones libres $x_i$ por $t_i$ en la fórmula $F$.*
*Si $\sigma = [t_1/x_1, t_2/x_2, t_3/x_3, ..., t_n/x_n]$ podemos escribir $t\sigma$.*

**Definición 2.23.** *Sea $F$ una fórmula y $\sigma$ una sustitución diremos que $\sigma$ es libre para $F$ si todas las apariciones de variables introducidas por la sustitución son libres.*

*Al escribir $F\sigma$ la sustitución $\sigma$ es libre en $F$ a no ser que indiquemos lo contrario.*

**Ejemplo 2.13.**

*Para la fórmula $F$ con $F = (x = y)$ cualquier sustitución es libre(cualquier sustitución en una fórmula sin cuantificadores es una sustitución libre).*
*Sea $\sigma = [y/x]$ vemos que $\sigma$ es libre para $(\forall x)f(x)$ pero no es libre para $(\exists y)f(x)$.*

**Observación 2.10.** *Cuando sustituimos en una fórmula lo hacemos como máximo una vez por variable, es decir $(f(x) = 0)[f(x)/x]$ es $(f(f(x)) = 0)$ y no repetiríamos infinitas veces una sustitución.*

**Definición 2.24.** *Sea $L$ un lenguaje. Una $L$-estructura es un par*
*$\mathcal{M} = (M, I)$ donde $M$ es un conjunto no vacío denominado dominio e $I$ es una función. El dominio de $I$ es el conjunto de símbolos de $L$. La función $I$ debe cumplir:*

- *$I(c) \in M$ si $c \in L$ es un símbolo de constante.*
- *$I(f) : M^n \longrightarrow M$ si $f \in L$ es una función de aridad $n$.*
- *$I(p) \subseteq M^n$ si $p \in L$ es una relación de aridad $n$.*

*Habitualmente diremos que $\mathcal{M}$ es una estructura si no hay lugar a confusión.*

**Definición 2.25.** *Una asignación $A$ en una estructura $\mathcal{M} = (M, I)$ es una función $A : Var \longrightarrow M$ donde $Var$ es el conjunto de las variables del alfabeto.*

**Definición 2.26.** *Una interpretación(o valoración según algunos autores) de $L$ es un par formado por una*
*$L$-estructura $\mathcal{M}$ y una asignación $A$ en $\mathcal{M}$.*

**Ejemplo 2.14.** *Sean $a$ y $b$ constantes y $f_a$ y $f_b$ funciones crearemos para el lenguaje $L = \{a, b, f_a, f_b\}$ una estructura. El dominio $M$ es el conjuto de las palabras que empiezan por $a$ y tienen al menos dos símbolos, escribiremos $M = a\{a, b\}^+$.*

- $I(a) = aa$.
- $I(b) = ab$.
- $I(f_a) : M \longrightarrow M$ *con* $I(f_a)(w) = wa$.
- $I(f_b) : M \longrightarrow M$ *con* $I(f_b)(w) = wb$.

*Veamos otro ejemplo para el mismo lenguaje siendo el dominio $M$ puede ser los palíndromos pares:*

- $I(a) = aa$.
- $I(b) = bb$.
- $I(f_a) : M \longrightarrow M$ *con* $I(f_a)(w) = awa$.
- $I(f_b) : M \longrightarrow M$ *con* $I(f_b)(w) = bwb$.

**Definición 2.27.** *Sean $\mathcal{M} = (M, I)$ una L-estructura y $A$ una asignación en $\mathcal{M}$ llamaremos evaluación de términos a la función $\mathcal{M}_A : Término(L) \longrightarrow M$ definida de la siguiente manera:*

- $\mathcal{M}_A(t) = I(c)$ *si $t$ es el símbolo de constante $c$.*
- $\mathcal{M}_A(t) = A(x)$ *si $t$ es la variable $x$.*
- $\mathcal{M}_A(t) = I(f(\mathcal{M}_A(t_1), \mathcal{M}_A(t_2), \mathcal{M}_A(t_3), ..., \mathcal{M}_A(t_n)))$ *si $t$ es la función $f(t_1, t_2, t_3, ..., t_n)$.*

*$\mathcal{M}_A(t)$ se lee "el valor de $t$ en $\mathcal{M}$ respecto de $A$".*

**Ejemplo 2.15.** *Sean $t = f_a(f_b(a))$ y $t = f_a(f_b(x))$ términos, $a$ una constante, $f_a$ y $f_b$ las funciones del ejemplo anterior y $A(x) = b$ una asignación. Veamos el valor de estos términos en $\mathcal{M}$ con respecto de $A$.*
$\mathcal{M}_A(f_a(f_b(a))) = I(f_a(\mathcal{M}_A(f_b(a)))) = I(f_a(I(f_b(\mathcal{M}_A(a))))) = I(f_a(I(f_b)(I(a))))$;
$\mathcal{M}_A(f_a(f_b(a))) = I(f_a(I(f_b)(aa)) = I(f_a(aab)) = aaba$.
$\mathcal{M}_A(f_a(f_b(x))) = I(f_a(\mathcal{M}_A(f_b(x)))) = I(f_a(I(f_b(\mathcal{M}_A(x))))) = I(f_a(I(f_b)(I(x))))$;
$\mathcal{M}_A(f_a(f_b(x))) = I(f_a(I(f_b)(A(x))) = I(f_a(I(f_b)(b)) = I(f_a(bb)) = abb$.

**Definición 2.28.** *Sean $\mathcal{M} = (M, I)$ una L-estructura, $A$ una asignación en $\mathcal{M}$, $x$ e $y$ variables y $m \in M$ definimos la asignación $A[x/m](y)$ de la siguiente manera:*

$$A[x/m](y) = \begin{cases} m & \text{si } y = x \\ A(y) & \text{si } y \neq x \end{cases} \tag{2.5}$$

**Definición 2.29.** *La función de verdad de la igualdad en un dominio $M$ es la función $V_= : M^2 \longrightarrow \{0, 1\}$ definida de la siguiente manera:*

$$V_=(t_1, t_2) = \begin{cases} 1 & \text{si } t_1 = t_2 \\ 0 & \text{caso contrario} \end{cases} \tag{2.6}$$

*La función de verdad para una relación $p$ en un dominio $M$ es la función $V_p : M^n \longrightarrow \{0, 1\}$ definida de la siguiente manera:*

$$V_p(t_1, t_2, t_3, ..., t_n) = \begin{cases} 1 & \text{si } (t_1, t_2, t_3, ..., t_n) \in p \\ 0 & \text{caso contrario} \end{cases} \tag{2.7}$$

**Definición 2.30.** *Sean $\mathcal{M} = (M, I)$ una estructura y $A$ una asignación sobre $\mathcal{M}$, la función evaluación de fórmulas es la función*
*$\mathcal{M}_A : Fórm(L) \longrightarrow \{0, 1\}$ definida de la siguiente manera:*

- $\mathcal{M}_A((t_1 = t_2)) = V_=(\mathcal{M}_A(t_1), \mathcal{M}_A(t_2))$.
- $\mathcal{M}_A(p(t_1, t_2, t_3, ..., t_n)) = V_{I(p)}(\mathcal{M}_A(t_1), \mathcal{M}_A(t_2), \mathcal{M}_A(t_3), ..., \mathcal{M}_A(t_n))$.
- $$\mathcal{M}_A(\neg F) = V_\neg(F) = \begin{cases} 1 & \text{si} \mathcal{M}_A(F) = 0 \\ 0 & \text{caso contrario} \end{cases} \tag{2.8}$$
- *Sea $F = (G \wedge H)$ entonces*

$$\mathcal{M}_A(G \wedge H) = V_\wedge(F) = \begin{cases} 1 & \text{si } \mathcal{M}_A(G) = 1 \text{y } \mathcal{M}_A(H) = 1 \\ 0 & \text{caso contrario} \end{cases} \tag{2.9}$$

- *Sea $F = (G \vee H)$*

$$\mathcal{M}_A(G \vee H) = V_\vee(F) = \begin{cases} 0 & \text{si } \mathcal{M}_A(G) = 0 \text{y } \mathcal{M}_A(H) = 0 \\ 1 & \text{caso } \textit{contrario} \end{cases} \tag{2.10}$$

- *Sea* $F = (G \to H)$

$$\mathcal{M}_A(G \to H) = V_{\to}(F) = \begin{cases} 0 & \text{si } \mathcal{M}_A(G) = 1 \text{y } \mathcal{M}_A(H) = 0 \\ 1 & \text{caso contrario} \end{cases} \tag{2.11}$$

- *Sea* $(\exists x)G = F$

$$\mathcal{M}_A((\exists x)G) = V_{\exists}(F) = \begin{cases} 1 & \text{si existe al menos un } m \in M \text{tal que } \mathcal{M}_{A[x/m]}(G) = 1 \\ 0 & \text{caso contrario} \end{cases} \tag{2.12}$$

- *Sea* $(\forall x)G = F$

$$\mathcal{M}_A((\forall x)G) = V_{\forall}(F) \begin{cases} 1 & \text{si para todo } m \in M \text{tenemos } \mathcal{M}_{A[x/m]}(G) = 1 \\ 0 & \text{caso contrario} \end{cases} \tag{2.13}$$

*(Cuando escribamos $\mathcal{M}_A(F)$ leeremos "el valor de $F$ en $\mathcal{M}$ respecto de $A$").*
*Si $\mathcal{M}_A(F) = 1$ escribiremos $\mathcal{M}_A \models F$, en el caso contrario escribiremos $\mathcal{M}_A \not\models F$.*

**Observación 2.11.** *Un forma más resumida de la definición anterior es: dado una estructura $\mathcal{M} = (M, I)$ y una asignación $A$ en $\mathcal{M}$ entonces:*

1. $\mathcal{M}_A \models (t_1 = t_2)$ *si y solo si* $\mathcal{M}_A(t_1) = \mathcal{M}_A(t_2)$.
2. $\mathcal{M}_A \models p(t_1, t_2, t_3, ..., t_n)$ *si y solo si* $(\mathcal{M}_A(t_1), \mathcal{M}_A(t_2), \mathcal{M}_A(t_3), ..., \mathcal{M}_A(t_n)) \in I(p)$.
3. $\mathcal{M}_A \models (\neg F)$ *si y solo si* $\mathcal{M}_A \not\models (F)$.
4. $\mathcal{M}_A \models (F \wedge G)$ *si y solo si* $\mathcal{M}_A \models F$ *y* $\mathcal{M}_A \models G$.
5. $\mathcal{M}_A \models (F \vee G)$ *si y solo si* $\mathcal{M}_A \models F$ *o* $\mathcal{M}_A \models G$.
6. $\mathcal{M}_A \models (F \to G)$ *si y solo si* $\mathcal{M}_A \not\models F$ *o* $\mathcal{M}_A \models G$.
7. $\mathcal{M}_A \models (\exists x)F$ *si y solo si existe al menos un* $a \in M$ *tal que* $\mathcal{M}_{A[x/a]} \models F$.
8. $\mathcal{M}_A \models (\forall x)F$ *si y solo si para todo* $a \in M$ *tenemos* $\mathcal{M}_{A[x/a]} \models F$.

**Definición 2.31.** *Sean $\mathcal{M}$ una estructura y $A$ una asignación en $\mathcal{M}$ diremos que el par $(\mathcal{M}, A)$ es una realización de la fórmula $F$ si $\mathcal{M}_A(F) = 1$ y lo representaremos por $\mathcal{M}_A \models F$ (diremos que $F$ se verifica en $\mathcal{M}$ respecto de $A$).*
*Diremos que el par $(\mathcal{M}, A)$ es una realización del conjunto de fórmulas $\Sigma$ si para todo $F \in \Sigma$ tenemos $\mathcal{M}_A \models F$ y denotaremos $\mathcal{M}_A \models \Sigma$.*
*El par $(\mathcal{M}, A)$ no es una realización de la fórmula $F$ si $\mathcal{M}_A(F) = 0$ y lo representaremos por $\mathcal{M}_A \not\models F$ (diremos que $F$ no se verifica en $\mathcal{M}$ respecto de $A$).*
*El par $(\mathcal{M}, A)$ no es una realización del conjunto de fórmulas $\Sigma$ si existe $F \in \Sigma$ tal que $\mathcal{M}_A(F) = 0$ y lo representaremos por $\mathcal{M}_A \not\models \Sigma$.*

**Definición 2.32.** *Sean $F$ una fórmula y $\mathcal{M} = (M, I)$ una L-estructura diremos que $F$ es satisfacible en $\mathcal{M}$ si existe una asignación $A$ en $\mathcal{M}$ tal que $\mathcal{M}_A \models F$. Si $F$ no es satisfacible diremos que es insatisfacible.*

**Ejemplo 2.16.** *Sean $\mathcal{M} = (M, I)$ una L-estructura, $+$ y $*$ símbolos de funciones binarias y $\geq$ y $<$ símbolos de predicados binarios.*
*La fórmula $F = (*(0, x) = 0)$ es satisfacible, ya que para cualquier asignación $A$ tenemos $\mathcal{M}_A \models (*(0, x) = 0)$.*
*La fórmula $F = (*(1, 1) = 0)$ es insatisfible, no existe ninguna asignación $A$ tal que $\mathcal{M}_A \models (*(1, 1) = 0)$.*
*Nos podemos preguntar si la fórmula $F = (\exists y)p(3, y)$ es satisfacible en $\mathcal{M} = (\mathbb{N}, I)$ con $I(p) = |(x, y)$. Si tomamos la asignación $A(x) = 12$ vemos que $\mathcal{M}_A \models F$, luego $F$ es satisfacible.*

**Definición 2.33.** *Una estructura $\mathcal{M} = (M, I)$ es un modelo para una fórmula $F$ si para toda asignación $A$ en $\mathcal{M}$ tenemos $\mathcal{M}_A \models F$ y denotaremos $\mathcal{M} \models F$.*
*Una estructura $\mathcal{M}$ es un modelo para un conjunto de fórmulas $\Sigma$ si para todo $F \in \Sigma$ tenemos $\mathcal{M} \models F$.*

**Ejemplo 2.17.** *La estructura $\mathcal{M} = (\mathbb{N}, I)$ es un modelo para la fórmula $(0 = 0)$ ya que para cualquier asignación $A$ tenemos $\mathcal{M}_A((0 = 0)) = V_=(\mathcal{M}_A(0), \mathcal{M}_A(0)) = 1$, por lo tanto $\models (0 = 0)$.*
*Veamos que la estructura $\mathcal{M} = (\mathbb{N}, I)$ con $I(c) = c$ para cualquier constante es un modelo para la fórmula $(\forall x) \geq (x, 0)$.*
*Sea $A$ una asignación cualquiera. Por definición $\mathcal{M}_A((\forall x) \geq (x, 0)) = 1$ si y solo si para todo $n \in \mathbb{N}$ $\mathcal{M}_{A[x/n]}(\geq (x, 0)) = 1$.*

*Por definición* $\mathcal{M}_{A[x/n]}(\geq (x,0)) = 1$ *si y solo si* $V_{I(\geq)}(\mathcal{M}_{A[x/n]}(x), \mathcal{M}_{A[x/n]}(0))$ *si y solo si* $(\mathcal{M}_{A[x/n]}(x), \mathcal{M}_{A[x/n]}(0)) \in I(\geq)$. *Observemos que* $A[x/n](y) \in \mathbb{N}$ *y* $\mathcal{M}_{A[x/n]}(0) = 0$. *Finalmente vemos que cualquier número natural es mayor o igual que cero.*

**Lema 2.1.** *Sean* $L$ *un lenguaje,* $t \in Término(L)$, $F$ *una fórmula de* $L$ *y* $\mathcal{M} = (M, I)$ *una estrucutra de* $L$. *Entonces:*

1. $\mathcal{M}_A(t) = \mathcal{M}_B(t)$ *si las asignaciones* $A$ *y* $B$ *coinciden sobre las variables de* $t$.

2. $\mathcal{M}_A(F) = \mathcal{M}_B(F)$ *si las asignaciones* $A$ *y* $B$ *coinciden sobre las variables libres de* $F$.

3. *Si* $t$ *no tiene variables entonces* $\mathcal{M}_A(t) = \mathcal{M}_B(t)$ *para cualesquieras asignaciones* $A$ *y* $B$ *en* $\mathcal{M}$.

4. *Si* $F$ *es una fórmula cerrada(es decir, sin variables libres) entonces* $\mathcal{M}_A(F) = \mathcal{M}_B(F)$ *para cualesquieras asignaciones* $A$ *y* $B$ *en* $\mathcal{M}$.

5. *Sean* $x_1, x_2, x_3, ..., x_n$ *variables libres de* $F$. *Entonces* $\mathcal{M}_A(F) = 1$ *para toda asignación* $A$ *en* $\mathcal{M}$ *si y solo si* $\mathcal{M}_B((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)F) = 1$ *para toda asignación* $B$ *en* $\mathcal{M}$.

**Demostración.** *1. Sean* $L$ *un lenguaje,* $F$ *una fórmula de* $L$, $\mathcal{M} = (M, I)$ *una estructura de* $L$ *y* $A$ *y* $B$ *asignaciones en* $\mathcal{M}$.
*Si* $t$ *es un término es, o bien una constante, o bien una variable o bien una función.*
*Si* $t = c$ *con* $c$ *símbolo de constante entonces tenemos por una parte* $\mathcal{M}_A(t) = I(t)$. *Por otra parte tenemos* $\mathcal{M}_B(t) = I(t)$ *con esto se concluye que* $\mathcal{M}_A(t) = \mathcal{M}_B(t)$ *si* $t$ *es un símbolo de constante.*
*Si* $t = x$ *siendo* $x$ *una variable entonces tenemos* $\mathcal{M}_A(t) = A(t)$ *y* $\mathcal{M}_B(t) = B(t)$. *Por hipótesis* $A(t) = B(t)$.
*Si* $t = f(t_1, t_2, t_3, ..., t_n)$ *es una función entonces*
$\mathcal{M}_A(t) = I(f(\mathcal{M}_A(t_1), \mathcal{M}_A(t_2), \mathcal{M}_A(t_3), ..., \mathcal{M}_A(t_n)))$ *y*
$\mathcal{M}_B(t) = I(f(\mathcal{M}_B(t_1), \mathcal{M}_B(t_2), \mathcal{M}_B(t_3), ..., \mathcal{M}_B(t_n)))$ *son iguales si para todo* $i \in \{1, 2, 3, ..., n\}$ *tenemos* $\mathcal{M}_A(t_i) = \mathcal{M}_B(t_i)$ *si* $t_i$ *es una variable o una constante ya ha sido demostrado y si es una función acabará dependiendo en símbolos de constantes y variables. Por lo tanto* $\mathcal{M}_A(t) = \mathcal{M}_B(t)$.

2. *Veamos por inducción sobre $k$ que para toda fórmula $F \in P_k \subset \mathcal{P}$ tenemos $\mathcal{M}_A(F) = \mathcal{M}_B(F)$ si y $A$ y $B$ son asignaciones que coinciden sobre las variables libres de FF.*
*Sea $F \in P_0$. El conjunto $P_0$ es el conjunto de fórmulas atómicas, es decir, no hay ningún cuantificador y por tanto cualquier variable de la fórmula $F$ es una variable libre, por consiguiente las asignaciones $A$ y $B$ coinciden en todas las variables de $F$. Supongamos que la fórmula $F$ es de la forma $(t_1 = t_2)$. Sean $x$ una variable cualquiera de $t_1$ o $t_2$ y $A$ y $B$ asignaciones que coinciden sobre las variables libres de $F$ vemos que $A(x) = B(x)$ ya que $x$ es una variable libre de $F$, por lo tanto las asignaciones $A$ y $B$ coinciden en las variables de $t_1$ y $t_2$. Aplicando el apartado anterior vemos que $\mathcal{M}_A(t_i) = \mathcal{M}_B(t_i)$ con $i \in 1, 2$.*
*Ahora veamos que $\mathcal{M}_A(F) = \mathcal{M}_B(F)$.*
*Por el lema 2.11 vemos que $\mathcal{M}_A(F) = 1$ si y solo si $\mathcal{M}_A(t_1) = \mathcal{M}_A(t_2)$ si y solo si $\mathcal{M}_B(t_1) = \mathcal{M}_B(t_2)$ si y solo si $\mathcal{M}_B(F) = 1$.*

*Veamos con un razonamiento similar que si la fórmula $F$ es de la forma $p(t_1, t_2, t_3, ..., t_n)$ con $p$ predicado entonces $\mathcal{M}_A(F) = \mathcal{M}_B(F)$ si y $A$ y $B$ son asignaciones que coinciden sobre las variables libres de $F$.*
*Al igual que antes $F$ es una fórmula sin cuantificadores y por tanto sin variables libres, es decir, para toda variable $x$ en $F$ tenemos $A(x) = B(x)$. Si $x$ una variable en $t_i$ con $i \in \{1, 2, 3, ..., n\}$ entonces también es una varible en $F$, por tanto las asignaciones $A$ y $B$ coinciden sobre las variables de $t_i$ por el apartado anterior tenemos $\mathcal{M}_A(t_i) = \mathcal{M}_B(t_i)$ con $i \in \{1, 2, 3, ..., n\}$.*
*Por definición $\mathcal{M}_A(F) = 1$ si y solo si*
*$(\mathcal{M}_A(t_1), \mathcal{M}_A(t_2), \mathcal{M}_A(t_3), ..., \mathcal{M}_A(t_n)) \in I(p)$ si y solo si*
*$(\mathcal{M}_A(t_1), \mathcal{M}_A(t_2), \mathcal{M}_A(t_3), ..., \mathcal{M}_A(t_n)) \in I(p)$ si y solo si $\mathcal{M}_A(f) = 1$.*
*Suponemos que para todo $n < k$ tenemos $\mathcal{M}_A(F) = \mathcal{M}_B(F)$ con $A$ y $B$ asignaciones que coinciden en las variables libres de $F$ y $F \in P_n$. Veamos que si $F \in P_k$ entonces $\mathcal{M}_A(F) = \mathcal{M}_B(F)$ con $A$ y $B$ asignaciones que coinciden en las variables libres de $F$.*
*La fórmula $F$ puede ser de la forma $(G \wedge H)$, $(G \vee H)$, $(G \to H)$, $(G \leftrightarrow H)$, $(\neg G)$, $(\forall x)G$ o $(\exists x)G$, todos los casos se razonan de forma similar; usaremos la definición 2.30 , el hecho de que las asignaciones $A$ y $B$ coinciden sobre las variables libres de $F$ y la hipótesis de inducción. Solamente lo vamos a ver cuando $F$ es una fórmula del tipo $(\neg G)$ y $(\forall x)G$. Si $F$ es de la forma $(\neg G)$ entonces $\mathcal{M}_A(F) = 1$ si y*

*solo si* $\mathcal{M}_A(G) = 0$. *Por hipótesis de inducción* $\mathcal{M}_A(G) = 0$ *si y solo* $\mathcal{M}_B(G) = 0$ *si y solo si* $\mathcal{M}_B(F) = 1$. *Por tanto* $\mathcal{M}_A(F) = 1$ *si y solo si* $\mathcal{M}_B(F) = 0$. *Si* $F$ *es de la forma* $(\forall x)G$ *entonces la variable* $x$ *es una variable ligada.*
*Por definición* $\mathcal{M}_A(F) = 1$ *si y solo si para todo* $a \in M$
$\mathcal{M}_{A[x/a]}(G) = 1$, *por otra parte tenemos también por la definición 2.30* $\mathcal{M}_B(F) = 1$ *si y solo si para todo* $a \in M$ $\mathcal{M}_{B[x/a]}(G) = 1$. *Veamos que* $A[x/a]$ *y* $B[x/a]$ *coinciden en las variables libres de* $G$. *Sea* $y$ *una variable libre de* $G$ *distinta de* $x$ *entonces* $A[x/a](y) = A(y)$ *y* $B[x/a](y) = B(y)$, *la variable* $y$ *también es una variable libre de* $F$ *entonces* $A[x/a](y) = B[x/a](y)$. *Si la variable* $y$ *es igual a la variable* $x$, *sea una variable libre o no en* $G$, *tenemos* $A[x/a](y) = a$ *y* $B[x/a](y) = a$ *por tanto* $A[x/a](y) = B[x/a](y)$, *es decir las asignaciones* $A[x/a]$ *y* $B[x/a]$ *coinciden sobre las variables libres de* $G$. *Por hipótesis de inducción* $\mathcal{M}_{A[x/a]}(G) = 1$ *si y solo si* $\mathcal{M}_{C[x/a]}(G) = 1$, *por lo tanto* $\mathcal{M}_A(F) = 1$ *si y solo si* $\mathcal{M}_B(F) = 1$.

3. *Si* $t$ *es un término sin variables libres entonces dos asignaciones* $A$ *y* $B$ *cualquiera coinciden en las variables libres de* $t$. *Ahora aplicamos la propiedad 1 de este teorema.*

4. *Si* $F$ *es una sentencia no tiene variables libres, por lo tanto dos asignaciones* $A$ *y* $B$ *cualquiera coinciden en las variables libres de* $F$. *Ahora aplicamos la propiedad 2 de este teorema.*

5. *Sea* $\{x_1, x_2, x_3, ..., x_n\}$ *el conjunto de variables libres de una fórmula* $F$. *Veamos por inducción sobre el número de variables libres de* $F$ *que si para toda asignación* $A$ *en* $\mathcal{M}$ *tenemos* $\mathcal{M}_A \models F$ *entonces para toda asignación* $B$ *en* $\mathcal{M}$ *tenemos* $\mathcal{M}_B((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)F) = 1$.
*Sean* $\{x_1\}$ *el conjunto de variables libres de* $F$ *y* $A$ *una asignación en* $\mathcal{M}$ *cualquiera. Veamos que si para toda asignación* $B$ *en* $\mathcal{M}$ *tenemos* $\mathcal{M}_B(F) = 1$ *entonces* $\mathcal{M}_A((\forall x_1)F) = 1$.
*Según la definición 2.30* $\mathcal{M}_B((\forall x_1)A) = 1$ *si y solo si para todo* $a \in M$ $\mathcal{M}_{A[x_1/a]}(F) = 1$ *y esto último se cumple por hipótesis.*
*Suponemos que para toda fórmula* $F$ *con menos de* $n$ *variables libres* $x_1, x_2, x_3, ..., x_m$ $\mathcal{M}_B((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_m)F) = 1$.
*Sea* $A$ *una asignación cualquiera veamos que*
$\mathcal{M}_A((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)F) = 1$.
*Por la definición 2.30* $\mathcal{M}_A((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)F) = 1$ *si y solo si*

*para todo* $a \in M$ $\mathcal{M}_{A[x_1/a]}((\forall x_2)(\forall x_3)(\forall x_4)...(\forall x_n)F) = 1$ *y esto último se cumple por hipótesis de inducción.*

*Veamos ahora que si* $\mathcal{M}_B((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)F) = 1$ *para toda asignación* $B$ *entonces* $\mathcal{M}_A(F) = 1$ *para toda asignación* $A$.
*Suponemos ahora que* $F$ *es una fórmula con* $n$ *variables libres* $x_1, x_2, x_3, ..., x_n$ *y que* $\mathcal{M}_B((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)F) = 1$ *para cualquier asignación* $C$.
*Sea* $A$ *una asignación cualquiera con* $A(x_i) = b_i$ *para todo* $i \in \{1, 2, 3, ..., n\}$.
*Por hipótesis* $\mathcal{M}_A((\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)F) = 1$, *usando la definición 2.30 n veces tenemos* $\mathcal{M}_{A[x_1/a_1][x_2/a_2][x_3/a_3]...[x_n/a_n]}(F) = 1$ *para todo* $a_1, a_2, a_3, ..., a_n \in M$, *en particular tenemos* $\mathcal{M}_{A[x_1/b_1][x_2/b_2][x_3/b_3]...[x_n/b_n]}(F) = 1$. *Las asignaciones* $A$ *y* $A[x_1/b_1][x_2/b_2][x_3/b_3]...[x_n/b_n]$ *coinciden sobre las variables libres* $F$, *luego* $\mathcal{M}_A(F) = 1$.

**Definición 2.34.** *Una fórmula* $F$ *es válida en* $\mathcal{M}$ *si para toda asignación* $A$ *en* $\mathcal{M}$ *tenemos* $\mathcal{M}_A \models F$. *Si* $F$ *es válida en* $\mathcal{M}$ *escribiremos* $\mathcal{M} \models F$, *si no es válida escribiremos* $\mathcal{M} \not\models F$.

**Lema 2.2.** *Una fórmula* $F$ *es válida si y solo si* $(\neg F)$ *es insatisfacible.*

**Demostración.** *Una fórmula* $F$ *es válidad si y solo si* $\mathcal{M}_A(F) = 1$ *para toda estructura* $\mathcal{M}$ *y toda asignación* $A$ *en* $\mathcal{M}$. *Por definición* $\mathcal{M}_A(F) = 1$ *si y solo si* $\mathcal{M}_A((\neg F)) = 0$, *por lo tanto no existe ningún par* $(\mathcal{M}, A)$ *tal que* $\mathcal{M}_A((\neg F)) = 1$, *luego* $(\neg F)$ *es insatisfacible.*

**Lema 2.3.** *Si una fórmula* $F$ *es válida entonces es satisfacible.*

**Demostración.** *Sea* $\mathcal{M}$ *una estructura y* $A$ *una asignación en* $\mathcal{M}$. *Como* $F$ *es válida entonces* $\mathcal{M}_A(F) = 1$, *luego* $F$ *es satisfacible.*

**Lema 2.4.** *Sean* $F$ *una sentencia(es decir, sin variables libres) y* $\mathcal{M} = (M, I)$ *una* $L$*-estructura entonces la fórmula* $F$ *es válida en* $\mathcal{M}$ *si y solo si* $F$ *es satisfacible en* $\mathcal{M}$.

**Demostración.** *Probaremos que si una fórmula* $F$ *es válida en* $\mathcal{M}$ *entonces* $F$ *es satisfacible en* $\mathcal{M}$.
*Por definición* $F$ *es satisfacible en* $\mathcal{M}$ *si existe una asignación* $A$ *tal que* $\mathcal{M}_A \models F$. *La fórmula* $F$ *es válida, entonces para cualquier asignación* $B$ *tenemos* $\mathcal{M}_B \models F$, *por tanto, para una asignación* $A$ *se cumple* $\mathcal{M}_B \models F$, *luego* $F$ *es satisfacible. Hemos visto que se cumple para cualquier fórmula,*

*por tanto podemos deducir que se cumple también para una sentencia.*
*Veamos que si una sentencia $F$ es válida en $\mathcal{M}$ entonces es satisfacible en $\mathcal{M}$.*
*Por ser $F$ una fórmula válida en $\mathcal{M}$ existe una asignación $A$ tal que $\mathcal{M}_A(F) = 1$. Sea $B$ una asignación cualquiera. Por ser $F$ una sentencia y por el lema 2.1 entonces $\mathcal{M}_A(F) = \mathcal{M}_B(F)$, por lo tanto $\mathcal{M}_B(F) = 1$ para toda asignación $B$, luego $F$ es satisfacible en $\mathcal{M}$.*

## 2.2. Sistema formal de la lógica de primer orden.

Muchas definiciones vistas en la lógica proposicional servirán para esta parte. Al igual que en la lógica proposicional tendremos los conceptos de teorema, demostración y consecuencia lógica sintáctica entre otros. Si algún concepto varía la definición y fuera necesario lo definiremos.

**Definición 2.35.** *Dos fórmulas $F$ y $G$ en un lenguaje $L$ son equivalentes si para toda estructura $\mathcal{M}$ en $L$ y toda asignación $A$ en $\mathcal{M}$ tenemos $\mathcal{M}_A(F) = \mathcal{M}_A(G)$.*
*Si $F$ y $G$ son fórmulas equivalentes se representa por $F \approx G$ o $F \equiv G$.*

**Ejemplo 2.18.** *Veamos que $(F \leftrightarrow G) \approx (\neg((F \rightarrow G) \rightarrow (\neg(G \rightarrow F))))$ mediante una tabla de verdad. Esto lo podemos hacer porque una vez asignados valores a las fórmulas $F$ y $G$ el valor de las fórmulas $(F \leftrightarrow G)$ y $(\neg((F \rightarrow G) \rightarrow (\neg(G \rightarrow F))))$ tomarían el mismo valor que si fuesen fórmulas de la lógica proposicional.*

| $F$ | $G$ | $(F \leftrightarrow G)$ | $(F \rightarrow G)$ | $(\neg(G \rightarrow F))$ | $(\neg((F \rightarrow G) \rightarrow (\neg(G \rightarrow F))))$ |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 |

*Las columnas 3 y 6 prueban $(F \leftrightarrow G) \approx (\neg((F \rightarrow G) \rightarrow (\neg(G \rightarrow F))))$.*

**Ejemplo 2.19.** *Sea $F$ una fórmula probemos que $(\exists x)F \approx (\neg(\forall x)(\neg F))$.*
*Sean $\mathcal{M}$ una estructura y $A$ una asignación en $\mathcal{M}$ probaremos que*

$\mathcal{M}_A((\neg(\forall x)(\neg F))) = 1$ *si y solo si* $\mathcal{M}_A((\exists x)F) = 1$.
$\mathcal{M}_A((\neg(\forall x)(\neg F))) = 1$ *si y solo si* $\mathcal{M}_A((\forall x)(\neg F)) = 0$ *si y solo si existe al menos un* $a \in M$ *tal que* $\mathcal{M}_{A[x/a]}((\neg F)) = 0$ *si y solo si existe al menos un* $a \in M$ *tal que* $\mathcal{M}_{A[x/a]}(F) = 1$ *si y solo si* $\mathcal{M}_A((\exists x)F)$.

Al igual que en la lógica proposicional utilizaremos axiomas que que solo usen los conectores ' $\rightarrow$' y '$\neg$' y el cuantificador '$\forall$', esto es debido a los ejemplos 2.18 y 2.19 y a lo visto en lógica proposicional.

**Definición 2.36.** *Un sistema axiomático de la lógica proposicional viene dado por los siguientes axiomas y reglas de inferencia.*
*Sean F, G, H fórmulas y t, u, v términos las siguientes fórmulas son axiomas para este sistema axiomático:*

1. *axioma 1* $(F \rightarrow (G \rightarrow F))$.
2. *axioma 2* $((F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H)))$.
3. *axioma 3* $((\neg F) \rightarrow (\neg G)) \rightarrow (G \rightarrow F)$.
4. *axioma 4* $((\forall x)F \rightarrow F[t/x])$*(recordemos que* $[t/x]$ *es libre en F).*
5. *axioma 5* $((\forall x)(F \rightarrow G) \rightarrow (F \rightarrow (\forall x)G))$ *(siempre que x no sea una variable libre de F).*
6. *axioma 6* $(t = t)$.
7. *axioma 7* $((t = u) \rightarrow (u = t))$.
8. *axioma 8* $((t = u) \rightarrow ((u = v) \rightarrow (t = v)))$.
9. *axioma 9* $((t = u) \rightarrow (F[t/x, t/y] \rightarrow F[u/x, u/y]))$*(recordemos que* $[t/x, t/y]$ *y* $[u/x, u/y]$ *son libres en F).*

*Y las dos reglas de inferencia son:*

1. *Modus Ponens.*
2. *(Generalización) Sea x una variable cualquiera entonces F infiere* $(\forall x)F$.

Cuando usemos la regla de inferencia generalización para deducir una consecuencia lógica sintáctica de un conjunto $\Sigma$ debemos hacerlo con variables que no tengan ninguna aparición libre en ninguna fórmula de $\Sigma$. Veámoslo con un ejemplo:
Sea $\Sigma = \{(\exists y)(y = z)\}$ siendo y una variable entonces:

1. $\Sigma \vdash (\exists y)(y = z)$ ya que $(\exists y)(y = z) \in \Sigma$.

2. $\Sigma \vdash (\forall y)(\exists y)(y = z)$ por generalización(y no tiene ninguna aparación libre en la única fórmula de $\Sigma$, no podríamos usar la regla de generalización para inferir $(\forall z)(\exists y)(y = z)$ ya que la variable z si tiene una aparición libre en una fórmula de $\Sigma$).

**Observación 2.12.** *Todos los teoremas probados para la lógica proposicional son válidos para la lógica de primer orden. Esto se debe a que en la lógica proposicional se razona con axiomas y reglas de inferencia que también pertenecen al sistema formal de la lógica de primer orden.*

**Observación 2.13.** *Si F es un axioma entonces* $\mathcal{M}_A(F) = 1$ *para cualquier estructura* $\mathcal{M}$ *y cualquier asignación A en* $\mathcal{M}$*. Vamos a verlo con alguno de ellos:*
*Tomemos el axioma* $(F \to (G \to F))$*. Por reducción al absurdo veamos que* $\mathcal{M}_A(F \to (G \to F)) = 1$.
*Si* $\mathcal{M}_A((F \to (G \to F))) = 0$ *entonces* $\mathcal{M}_A(F) = 1$ *y* $\mathcal{M}_A((G \to F)) = 0$.
*Como* $\mathcal{M}_A((G \to F)) = 0$ *entonces* $\mathcal{M}_A(F) = 0$*, por tanto absurdo.*
*Tomemos el axioma* $((\forall x)(F \to G) \to (F \to (\forall x)G))$ *donde la variable x no tiene apariciones libres en la fórmula F.*
*Por reducción al absurdo veamos que*
$\mathcal{M}_A(((\forall x)(F \to G) \to (A \to (\forall x)G))) = 1$.
*Si* $\mathcal{M}_A(((\forall x)(F \to G) \to (F \to (\forall x)G))) = 0$ *entonces*
$\mathcal{M}_A((\forall x)(F \to G)) = 1$ *y* $\mathcal{M}_A((F \to (\forall x)G)) = 0$.
*Por definición* $\mathcal{M}_A((\forall x)(F \to G)) = 1$ *si para todo* $a \in M$
$\mathcal{M}_{A[x/a]}(F \to G) = 1$ *y esto último se da siempre que no se cumplan de forma simultáneas* $\mathcal{M}_{A[x/a]}(F) = 1$ *y* $\mathcal{M}_{A[x/a]}(G) = 0$.
*Por otra parte si* $\mathcal{M}_A((F \to (\forall x)G)) = 0$ *entonces* $\mathcal{M}_A(F) = 1$ *y*
$\mathcal{M}_A((\forall x)G) = 0$*. La variable x no tiene aparaiciones libres en la fórmula F, luego x es una variable ligada en F y por tanto las asignaciones A y* $A[x/a]$ *coinciden sobre las variables libres de F, por lo tanto*
$\mathcal{M}_A(F) = \mathcal{M}_{A[x/a]}(F) = 1$*. Como* $\mathcal{M}_{A[x/a]}(F) = 1$ *entonces* $\mathcal{M}_{A[x/a]}(G) = 1$

*para todo $a \in M$. Por otra parte tenemos $\mathcal{M}_A((\forall x)G) = 0$, luego existe $a \in M$ tal que $\mathcal{M}_{A[x/a]}(G) = 0$, por tanto absurdo.*

**Teorema 2.3.** ***(De la Deducción)****Si $\Sigma \cup \{F\} \vdash G$ entonces $\Sigma \vdash (F \to G)$.*

**Demostración.** *Como $\Sigma \cup \{F\} \vdash G$ entonces existe una demostración $G_1, G_2, G_3, ..., G_n = G$ donde $G_i$ es un axioma, una fórmula de $\Sigma \cup \{F\}$ o ha sido obtenida mediante una regla de inferencia(modus pones o generalización).*
*Veamos por inducción sobre la longitud de la demostración que $\Sigma \vdash (F \to G)$. Si $n = 1$ entonces $G_1 = G$ es un axioma o $G \in \Sigma\{F\}$. Si $G = F$ ya vimos que $G \to G$ es un teorema de la lógica proposicional y por tanto también es un teorema de la lógica de primer de orden. Si $G \neq F$:*

1. *$\Sigma \vdash (G \to (F \to G))$ axioma 1.*
2. *$\Sigma \vdash G$ ya que $G$ es axioma o $G \in \Sigma$.*
3. *$\Sigma \vdash (F \to G)$ mp 1,2.*

*Suponemos ahora que el teorema se cumple para cualquier demostración con una longitud menor que n. Si G es axioma o $G \in \Sigma \cup \{F\}$ utilizamos la demostración anterior. Si G ha sido obtenido mediante modus ponens entonces existen $G_m$ y $(G_m \to G)$ tales que $\Sigma \cup \{F\} G_m$ y $\Sigma \cup \{F\} \vdash (G_m \to G)$(observemos que $m < n$). Veamos que $\Sigma \vdash G$:*

1. *$\Sigma(F \to G_m)$ por hipótesis de inducción.*
2. *$\Sigma \vdash (F \to (G_m \to G))$ por hipótesis de inducción.*
3. *$\Sigma \vdash ((F \to (G_m \to G)) \to ((F \to G_m) \to (F \to G)))$ axioma 2 (sustituyendo A por F, B por $G_m$ y C por G).*
4. *$\Sigma \vdash ((F \to G_m) \to (F \to G))$ mp 3,2.*
5. *$\Sigma \vdash (F \to G)$ mp 4,1.*

*Si G ha sido obtenido por generalización entonces G es de la forma $(\forall x)H$ donde x no es una variable en ninguna fórmula de $\Sigma \cup \{F\}$ además existe una demostración menor que n que pruebe $\Sigma \cup \{F\} \vdash H$. Veamos que $\Sigma \vdash G$:*

1. *$\Sigma \vdash (F \to H)$ por hipótesis de inducción.*

2. $\Sigma \vdash (\forall x)(F \to H)$ *generalización 1.*

3. $\Sigma \vdash ((\forall x)(F \to H) \to (F \to (\forall x)H))$ *axioma 5(recordemos que x no tiene apariciones libres en F, luego no es una variable libre de F).*

4. $\Sigma \vdash (F \to (\forall x)H)$ *mp 3 y 2.*

**Definición 2.37.** *El conjunto $\Sigma$ es inconsistente si existe una fórmula F tal que $\Sigma \vdash F$ y $\Sigma \vdash (\neg F)$.*
*El conjunto $\Sigma$ es consistente si no es inconsistente.*

**Definición 2.38.** *Una fórmula F es consecuencia lógica(semántica) de un conjunto de fórmulas $\Sigma$ si todas las realizaciones de $\Sigma$ son realizaciones del conjunto unitario $\{F\}$ y denotaremos $\Sigma \models F$.*
*Si una fórmula F no es consecuencia lógica de un conjunto de fórmulas $\Sigma$ escribiremos $\Sigma \not\models F$.*

**Definición 2.39.** *Un conjunto de fórmulas $\Sigma$ es completo si, para cualquier fórmula F, o F o $(\neg F)$ pertenecen al conjunto $\Sigma$.*

**Teorema 2.4.** *Si $\Sigma \vdash F$ entonces $\Sigma \models F$.*

**Demostración.** *Veamos por inducción sobre la longitud de la demostración que si $\Sigma \vdash F$ entonces $\Sigma \models F$. Si la demostración tiene un único término $A_1 = F$ entonces F es un axioma o $F \in \Sigma$.*
*Si F es un axioma por el lema 2.13 sabemos que $\mathcal{M}_A(F) = 1$ para cualquier estructura $\mathcal{M}$ y cualquier asignación A en $\mathcal{M}$.*
*Si $F \in \Sigma$. Sea $(\mathcal{M}, A)$ una realización tal que para todo $x \in \Sigma$ $\mathcal{M}_A(x) = 1$. Como $F \in \Sigma$ entonces $\mathcal{M}_A(F) = 1$.*
*Supongamos ahora que para toda sucesión con menos de n términos se cumple el teorema.*
*Sea $A_1, A_2, A_3, ..., A_n = F$ una demostración de n términos veamos que $\Sigma \models F$.*
*Si F es un axioma o $F \in \Sigma$ es el mismo raonamiento que el caso base. Si no es el caso entonces F ha sido obtenido mediante modus ponens o generalización.*
*Si F ha sido obtenida mediante modus ponens entonces existen*
*$A_i = (A_j \to F)$ y $A_j$ con $i, j < n$ tales que, por hipótesis de inducción*
*$\mathcal{M}_A((A_j \to F)) = 1$ y $\mathcal{M}_A(A_j) = 1$, por lo tanto $\mathcal{M}_A(F) = 1$.*
*Si F ha sido obtenida mediante generalización entonces F es de la forma*

*$(\forall x)G$ y existe $A_j = G$ con $j < 1$ tal que, por hipótesis de inducción, $\mathcal{M}_A(G) = 1$. Por definición $\mathcal{M}_A((\forall x)G) = 1$ si y solo si para todo $a \in M$ $\mathcal{M}_{A[x/a]}(G) = 1$. Recordemos que la variable $x$ no tiene apariciones libres en $G$, por tanto no es una variable libre en $G$, entonces las asignaciones $A$ y $A[x/a]$ coinciden sobre las variables libres de $G$, luego*
*$\mathcal{M}_A(G) = \mathcal{M}_{A[x/a]}(G) = 1$.*

**Teorema 2.5.** *Sea $L$ un lenguaje de primer orden con una cantidad finita o numerable de símbolos de función, relación y constantes. Si existe una $L$-estructura $\mathcal{M}$ y una asignación $A$ en $\mathcal{M}$ tal que $\mathcal{M}_A(x) = 1$ para todo $x \in \Sigma$ entonces el conjunto de fórmulas $\Sigma$ es consistente.*

**Demostración.** *Veamos que si existe un par $(\mathcal{M}, A)$ tal que $\mathcal{M}_A(x) = 1$ para todo $x \in \Sigma$ entonces $\Sigma$ es consistente. Para ello probaremos que si $\Sigma$ es inconsistente no existe ningún par $(\mathcal{M}, A)$ tal que $\mathcal{M}_A(x) = 1$ para todo $x \in \Sigma$.*
*Si $\Sigma$ fuera inconsistente existiría una fórmula $F$ tal que $\Sigma \vdash F$ y $\Sigma \vdash (\neg F)$. Por el teorema anterior $\Sigma \models F$ y $\Sigma \models (\neg F)$. Si existiera al menos un par $(\mathcal{M}, A)$ tal que $\mathcal{M}_A(x) = 1$ para todo $x \in \Sigma$ entonces $\mathcal{M}_A(F) = 1$ y $\mathcal{M}_A((\neg F)) = 1$, lo cual es imposible. Por lo tanto si $\Sigma$ es inconsistente no existe ningún par $(\mathcal{M}, A)$ tal que $\mathcal{M}_A(x) = 1$ para todo $x \in \Sigma$.*

**Lema 2.5.** *Sean $L$ un lenguaje de primer orden con una cantidad finita o contable de símbolos de función, relación y constantes y $\Sigma$ un conjunto consistente de fórmulas de $L$, entonces $\Sigma$ está contenido en un conjunto completo consistente.*

**Demostración.** *Como hemos visto en el teorema 1.6, si $\Sigma$ consistente entonces para cualquier fórmula $F$ entonces $\Sigma \cup \{F\}$ o $\Sigma \cup \{(\neg F)\}$ es consistente, ya que si $\Sigma \cup \{F\}$ y $\Sigma \cup \{(\neg F)\}$ fueran inconsistentes llegaríamos a una contradicción utilizando los axiomas 1, 2 y 3 de la lógica de primer orden. Sea $F_0, F_1, F_2, ...$ la secuencia de los elementos del conjunto $\Sigma$ podemos ampliarla en el n-ésimo término con $F_n$ o $(\neg F)$ (eligiendo siempre la fórmula con la que obtendremos un nuevo conjunto consistente). Demostraremos el teorema por inducción.*
*Definimos $\Sigma_0$ de la siguiente manera:*

$$\Sigma_0 = \begin{cases} \Sigma \cup \{F\} & \text{si } \Sigma \cup \{F\} \text{es consistente} \\ \Sigma \cup \{(\neg F)\} & \text{si } \Sigma \cup \{(\neg F)\} \text{es consistente} \end{cases} \tag{2.14}$$

*Definimos $\Sigma_n$ de la siguiente manera:*

$$\Sigma_n = \begin{cases} \Sigma_{n-1} \cup \{F_n\} & \text{si } \Sigma_{n-1} \cup \{F_n\}\text{si es consistente} \\ \Sigma_{n-1} \cup \{(\neg F_n)\} & \text{si } \Sigma_{n-1} \cup \{(\neg F_n)\}\text{es consistente} \end{cases} \tag{2.15}$$

*Sea $\Sigma^+ = \bigcup \Sigma_n$, veamos que $\Sigma$ está contenido en el conjunto completo $\Sigma^+$.*
*Por definición del conjunto $\Sigma^+$ vemos que $\Sigma \subset \Sigma_0 \subset \Sigma_1 \subset \Sigma_2 \subset ...\Sigma^+$.*
*Y $\Sigma^+$ es un conjunto completo, ya que para cualquier fórmula $F_n$, o bien $F_n \in \Sigma_n \subset \Sigma^+$, o bien $(\neg F_n) \in \Sigma_n \subset \Sigma^+$.*
*Veamos por inducción sobre n que $\Sigma^+$ es consistente.*
*Para $n = 0$ veamos que $\Sigma_0$ es consistente.*
*El conjunto $\Sigma$ es consiste según el enunciado y hemos probado(en la demostración del teorema 1.6) que $\Sigma \cup \{F_0\}$ o $\Sigma \cup \{(\neg F_0)\}$ es consistente. Usando la definición de $\Sigma_0$ concluimos que $\Sigma_0$ es consistente (es consistente por que hemos podido definirlo de tal manera que sea consistente).*
*Veamos que si $\Sigma_n$ es consistente entonces $\Sigma_{n+1}$ es consistente.*
*El conjunto $\Sigma_n$ es consiste por hipótesis y hemos probado(en la demostración del teorema 1.6) que $\Sigma_n \cup \{F_{n+1}\}$ o $\Sigma_n \cup \{(\neg F_{n+1})\}$ es consistente. Usando la definición de $\Sigma_{n+1}$ concluimos que $\Sigma_{n+1}$ es consistente (es consistente por que hemos podido definirlo de tal manera que sea consistente).*

**Lema 2.6.** *Sean L un lenguaje de primer orden con una cantidad finita o contable de símbolos de función, relación y constantes y $\Sigma$ un conjunto consitente de fórmulas de L entonces existe una realización para $\Sigma$.*

**Demostración.** *Por el lema anterior podemos extender el conjunto $\Sigma$ a un conjunto $\Sigma^+$ consistente y completo. Construimos una L-estructura $\mathcal{M} = (M, I)$ y A una asignación donde el dominio M es el conjunto de todos los términos cerrados del lenguaje, es decir, términos sin variables. Observemos que M es un conjunto numerable. Para la función I tenemos:*

- *$I(c) = c$ si c es un símbolo de constante.*
- *$I(f(t_1, t_2, t_3, ..., t_n)) = f(I(t_1), I(t_2), I(t_3), ..., I(t_n)))$ si f es una función de aridad n y $t_1, t_2, t_3, ..., t_n$ términos cerrados.*
- *Para un predicado p $I(p)((t_1, t_2, t_3, ..., t_n))$ es verdad ($(t_1, t_2, t_3, ..., t_n)$ están relacionados por $I(p)$) si $\Sigma \vdash p(t_1, t_2, t_3, ..., t_n)$.*

*A partir de la estructura $\mathcal{M}$ vamos a definir la estructura $\bar{\mathcal{M}} = (\bar{M}, \bar{I})$.*
*Sean $t_1$ y $t_2$ términos definimos en el conjunto M la relación binaria de*

*la siguiente manera:* $\sim (t_1, t_2)$*(habitualmente escribimos* $t_1 \sim t_2$*) si y solo si* $\Sigma \vdash (t_1 = t_2)$*(por los axiomas 6,7 y 8 sabemos que es una relación de equivalencia en M).*
*Tomamos el cociente* $\bar{\mathcal{M}} = \mathcal{M}/\sim$ *Veamos que* $\bar{\mathcal{M}}$ *es un modelo para* $\Sigma^+$ *y por tanto también para* $\Sigma$*.*
*Veamos que* $\bar{\mathcal{M}}(x) = 1$ *si y solo si* $x \in \Sigma^+$*(solamente necesitamos probar la implicación indirecta). Sea* $F \in P_k \subset \mathcal{P}$ *una fórmula de* $\Sigma^+$ *veamos por inducción sobre k que* $\bar{\mathcal{M}}(F) = 1$*.*
*Si* $k = 0$ *entonces F es una fórmula átomica, es decir, F es* $(t_1 = t_2)$ *con* $t_1$ *y* $t_2$ *términos o F es un predicado.*
*Supongamos que F es de la forma* $(t_1 = t_2)$*.*
$F \in \Sigma^+$ *si y solo si* $\Sigma^+ \vdash F$ *si y solo si* $t_{12}$*(es decir, la clase de* $t_1$ *es la clase de* $t_2$*) si y solo si* $\bar{\mathcal{M}}(t_1) = \bar{\mathcal{M}}(t_2)$ *si y solo si* $\bar{\mathcal{M}}((t_1 = t_2)) = 1$*.*
*Si F es un predicado ya hemos visto por construcción que se cumple.*
*Supongamos que para todo* $k < n$ *se cumple el teorema, es decir, si*
$F \in P_k \subset \mathcal{P}$ *entonces* $\bar{\mathcal{M}}(F) = 1$*.*
*Sea F una fórmula de la forma* $(\neg G)$*.*
$(\neg G) \in \Sigma^+$ *si y solo si* $G \notin \Sigma^+$ *por ser* $\Sigma^+$ *consistente,* $G \notin \Sigma^+$ *si solo si* $\Sigma^+ \nvdash G$ *si y solo si* $\bar{\mathcal{M}}(G) = 0$ *por hipótesis de inducción. Por definición* $\bar{\mathcal{M}}(G) = 0$ *si y solo si* $\bar{\mathcal{M}}((\neg G)) = 1$*.*
*Sea F una fórmula de la forma* $(G \to H)$*. Veamos que si* $F \in \Sigma^+$ *entonces* $\bar{\mathcal{M}}(F) = 1$*.*
*Por ser* $\Sigma^+$ *un conjunto completo tenemos estas cuatro posibilidades:*

- $\{G, H\} \subset \Sigma^+$.
- $\{G, (\neg H)\} \subset \Sigma^+$.
- $\{(\neg G), H\} \subset \Sigma^+$.
- $\{(\neg G), (\neg H)\} \subset \Sigma^+$.

*Si* $\{G, H\} \subset \Sigma^+$ *entonces* $\bar{\mathcal{M}}(H) = 1$ *por hipótesis de inducción, luego* $\bar{\mathcal{M}}(F) = 1$ *por definición.*
*Si* $\{(\neg G)\} \in \Sigma^+$ *entonces* $\bar{\mathcal{M}}(\neg G) = 1$ *por hipótesis, luego* $\bar{\mathcal{M}}(G) = 1$ *y* $\bar{\mathcal{M}}(F) = 1$*.*
*Si* $\{G, (\neg H), (G \to H)\} \subset \Sigma^+$ *entonces* $\Sigma^+ \vdash H$ *(usando modus ponens) y* $\Sigma^+ \vdash (\neg H)$*, luego* $\Sigma^+$ *es inconsistente, por lo tanto* $\{G, (\neg H)\} \not\subset \Sigma^+$*.*
*Si F es de la forma* $(\forall x)G$ *veamos que* $G \in \Sigma^+$*:*

1. $\Sigma^+ \vdash (\forall x)G$ *ya que* $(\forall x)G \in \Sigma^+$.

2. $\Sigma^+ \vdash ((\forall x)G \to G[x/x])$ *axioma 4.*

3. $\Sigma^+ \vdash G[x/x]$ *mp 1,2.*

*Observemos que* $G[x/x] = G$. *Por ser* $\Sigma^+$ *completo entonces* $G \in \Sigma^+$ *o* $(\neg G) \in \Sigma^+$. *Por ser* $\Sigma^+$ *consistente* $G \in \Sigma^+$. *Para una asignación* $A$ *cualquiera tenemos* $\bar{\mathcal{M}}_{\mathcal{A}}((\forall x)G)$ *si y solo si para todo* $a \in \bar{M}$ *tenemos* $\bar{\mathcal{M}}_{A[x/a]}(G)$ *y esto último se cumple por hipótesis.*
*Hemos probado que* $\bar{\mathcal{M}}$ *es modelo para* $\Sigma^+$, *por lo tanto también es modelo para* $\Sigma$.

**Teorema 2.6.** *Sea* $L$ *un lenguaje de primer orden con una cantidad finita o contable de símbolos de constantes, funciones y predicados entonces: si* $\Sigma \models F$ *entonces* $\Sigma \vdash F$.

**Demostración.** *Si* $\Sigma$ *es inconsistente entonces* $\Sigma \vdash F$ *para cualquier fórmula* $F$ *de la lógica de primer orden(por el lema 1.5, que solo usa la definición de conjunto inconsistente y los axiomas 1,2 y 3).*
*Si* $\Sigma$ *es consistente entonces existe al menos una interpretación* $(\mathcal{M}, A)$ *tal que* $\mathcal{M}_A(x) = 1$ *para todo* $x \in \Sigma$. *Como* $\Sigma \models F$ *entonces* $\mathcal{M}_A(F) = 1$, *por lo tanto* $\mathcal{M}_A(\neg F) = 0$. *Es decir, no existe ningún par* $(\mathcal{M}, B)$ *tal que* $\mathcal{M}_B(x) = 1$ *para todo* $x \in \Sigma \cup \{(\neg F)\}$, *luego* $\Sigma \cup \{(\neg F)\}$ *es inconsistente.*
*Por ser* $\Sigma \cup \{(\neg F)\}$ *inconsistente podremos deducir de él cualquier fórmula, por lo tanto si* $C$ *es un axioma* $\Sigma \cup \{(\neg F)\} \vdash C$ *y* $\Sigma \cup \{(\neg F)\} \vdash (\neg C)$. *Veamos que* $\Sigma \vdash F$.

1. $\Sigma \vdash ((\neg F) \to (\neg C))$ *aplicando el teorema de la deducción a* $\Sigma \cup \{(\neg F)\} \vdash (\neg C)$.

2. $\Sigma \vdash (((\neg F) \to (\neg C)) \to (C \to F))$ *axioma 3.*

3. $\Sigma \vdash (C \to F)$ *mp 1,2.*

4. $\Sigma \vdash C$ *por ser* $C$ *un axioma.*

5. $\Sigma \vdash F$ *mp 3,4.*

# Capítulo 3

# Fundamentación de las Matemáticas

*Los matemáticos Zermelo(1871-1953) y Fraenkel(1891-1965) plantearon una lista de axiomas que fundamentaron las matemáticas de manera que, junto con el axioma de elección, se construyen todos los conceptos, resultados y teoremas que se conocen de la matemáticas utilizando solamente la noción de conjunto como concepto primitivo no definido.*

## 3.1. Sistema axiomático de la teoría de conjuntos de Zermelo-Fraenkel.

*La teoría de conjuntos se formaliza con el lenguaje $L = \{\in\}$ de primer orden, siendo $\in$ un predicado binario(escribiremos $x \in y$ o $x \notin y$ en vez de $\in (x, y)$ o $(\neg(\in (x, y)))$). Distintos autores dan diferentes conjuntos de axiomas de Zermelo-Fraenkel. Aquí escribiremos los axiomas de Zermelo-Fraenkel, ZF, según el libro [3].*

1. *Axioma del conjunto vacío.*
   *Existe un conjunto $\emptyset$ sin ningún elemento.*

$$(\exists x)(\forall u)(u \notin x).$$

2. *Axioma de extensionalidad.*
   *Si dos conjuntos tienen los mismos conjuntos como elementos entonces*

*los dos conjuntos son iguales.*

$$(\forall x)(\forall y)((\forall u)((u \in x) \longleftrightarrow (u \in y)) \rightarrow (x = y)).$$

*Definimos el símbolo* $\subseteq$ *de la siguiente manera:*

$$(\forall x)(\forall y)((x \subseteq y) \longleftrightarrow (\forall z)((z \in x) \rightarrow (z \in y))).$$

3. *Axioma de formación de pares. Definimos el par no ordenado formado por los conjuntos x e y(escrito habitualmente como* $\{x, y\}$*).*

$$(\forall x)(\forall y)(\exists z)(\forall u)((u \in z) \longleftrightarrow ((u = x) \vee (x = y))).$$

4. *Axioma del conjunto potencia o axioma de las partes del conjunto. Existe un conjunto x que contiene a cualquier subconjunto de cualquier conjunto.*

$$(\forall x)(\exists y)(\forall u)((u \in y) \longleftrightarrow (\forall v)((v \in u) \rightarrow (v \in x))).$$

*A partir de ahora llamaremos conjunto de partes de un conjunto cualquiera X al conjunto* $\mathcal{P}(X)$ *cuyos elementos son los subconjuntos de X.*

$$(\forall x)(\exists y)((y = \mathcal{P}(x)) \longleftrightarrow (\forall z)((z \in y) \longleftrightarrow (z \subseteq x))).$$

5. *Axioma del conjunto unión.*
*Dado un conjunto x existe un conjunto cuyos elementos son los elementos de los elementos de x.*

$$(\forall x)(\exists y)(\forall u)((u \in y) \longleftrightarrow (\exists v)((u \in v) \wedge (v \in x))).$$

*Dado un conjunto x definimos el conjunto* $\bigcup x$ *como la unión de los conjuntos pertenecientes al conjunto x:*

$$(\forall x)(\forall y)((y = \bigcup x) \longleftrightarrow (\forall z)((z \in y) \longleftrightarrow (\exists t)((t \in x) \wedge (z \in t)))).$$

*Por ejemplo* $\bigcup\{x, y\} = x \cup y$.

6. *Axioma del infinito.*
*Este axioma garantiza la existencia de un conjunto con una cantidad infinita de elementos.*

$$(\exists x)((\exists u)((u \in x) \wedge (\forall v)(v \notin u)) \wedge (\forall u)((u \in x) \rightarrow$$
$$(\exists v)((v \in x) \wedge (\forall w)((w \in v) \longleftrightarrow ((w \in u) \vee (w = u)))))).$$

7. *Axioma de reemplazamiento.*
   *Este axioma nos garantiza que la imagen de un conjunto por una función definida a través de una fórmula es también un conjunto.*

   $$(\forall x_1)(\forall x_2)(\forall x_3)...(\forall x_n)((\forall y)(\exists! v F(u,v,x_1,x_2,x_3,...,x_n)) \to (\forall x)(\exists y)(\forall v)((v \in y) \longleftrightarrow (\exists u)((u \in x) \wedge (F(u,v,x_1,x_2,x_3,...,x_n))))).$$

8. *Axioma de regularidad.*
   *Este axioma impide que un conjunto pueda pertenecerse a si mismo y además para para cualquier conjunto no vacío $x$ existe un conjunto $y$ tal que $y \in x$ y $x \cap y = \emptyset$.*

$(\forall x)((\exists u)(u \in x) \to (\exists v)((v \in x) \wedge (\forall w)(\neg((w \in x) \wedge (w \in v))))).$

**Definición 3.1.** *De los axiomas de Zermelo-Fraenkel se deduce el esquema axiomatico de separación en el que para un predicado $p$ tenemos:*
$(\forall x)(\exists y)(\forall z)((z \in y) \longleftrightarrow ((z \in x) \wedge p(z)))$.
*El esquema axiomático de separación permite concluir que los elementos de un conjunto que cumplen una fórmula es también un conjunto.*
*Definimos el conjunto $\bigcap x$ como el conjunto cuyos elementos son los elementos de los elementos de $x$, es decir*

$$\bigcap x = \{t | (\exists y)((t \in y) \wedge (y \in x))\}.$$

*La intersección entre dos conjuntos $X$ e $Y$ la definimos como $\bigcap Z$ donde $Z = \{X, Y\}$ (escribiremos $X \cap Y$). La obtención del esquema axiomático de separación no nos detendremos a*

**Lema 3.1.** *Si $x_0, x_1, x_2, ...$ son conjuntos entonces no se puede dar el caso $x_{i+1} \in x_i$ para todo $n \in \mathbb{N}$, es decir, no existe la cadena infinita $...x_2 \in x_1 \in x_0$.*

**Demostración.** *Supongamos que $x = \{x_n | n \in \mathbb{N}\}$ es un conjunto. Por el axioma de regularidad debe existir un $x_i \in x$ tal que $x_i \cap x = \emptyset$, mas para todo $i \in \mathbb{N}$ $x_{i+1} \in x_i$ y $x_{i+1} \in x$, luego $x \cap x_i \neq \emptyset$ para todo $i \in \mathbb{N}$. Por lo tanto $x = \{x_n | n \in \mathbb{N}\}$ no es un conjunto.*

**Lema 3.2.** *Si $x$ es un conjunto entonces $\{x\}$ y $x \cup \{x\}$ son conjuntos.*

**Demostración.** *Si $x$ es conjunto entonces por el axioma de formación de pares $\{x, x\}$ es un conjunto y por el conjunto de extensionalidad $\{x, x\} = \{x\}$, luego $\{x\}$ es un conjunto y finalmente por el axioma del conjunto unión concluimos que $x \cup \{x\}$ es un conjunto.*

**Definición 3.2.** *Sea $x$ un conjunto definimos el átomo como el conjunto $\{x\}$ y el par ordenado $(x, y)$ como el conjunto $\{\{x\}, \{x, y\}\}$.*
*Daremos una breve explicación al hecho de que si $x$ e $y$ son conjuntos entonces el par ordenado $(x, y)$ también es un conjunto.*
*Como $x$ e $y$ son conjuntos entonces por el axioma de formación de pares $\{x, y\}$ es un conjunto y por el axioma de las partes del conjunto $\mathcal{P}(\{x, y\})$ también es un conjunto. Finalmente usamos el esquema axiomático de separación para concluir que $(x, y)$ es un conjunto.*

**Lema 3.3.** *Si $(x, y)$ y $(x', y')$ son pares ordenados tales que $(x, y) = (x', y')$ entonces $x = x'$ e $y = y'$.*

**Demostración.** *Si $(x, y)$ y $(x', y')$ son pares ordenados tales que $(x, y) = (x', y')$ entonces $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$ y por el axioma de extensionalidad $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$ si y solamente si, o bien $\{x\} = \{x'\}$ y $\{x, y\} = \{x', y'\}$, o bien $\{x\} = \{x', y'\}$ y $\{x, y\} = \{x'\}$.*
*Si $x = y$ entonces $(x, x) = \{\{x\}, \{x, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$, luego $\{\{x\}\} = \{x', \{x', y'\}\}$, por lo tanto el conjunto $\{\{x'\}, \{x', y'\}\}$ tiene un único elemento, es decir $\{x'\} = \{x', y'\}$ y por el axioma de extensionalidad $x' = y'$ y por consiguiente $(x', x') = \{\{x'\}\}$. Por el axioma de extensionalidad $\{\{x\}\} = \{\{x'\}\}$ si y solo si $\{x\} = \{x'\}$ y por el axioma de extensionalidad una vez más $\{x\} = \{x'\}$ si y solo si $x = x'$.*
*Si $x \neq y$ entonces el conjunto $\{\{x\}, \{x, y\}\}$ tiene dos elementos distintos. Si $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$ entonces el conjunto $\{\{x'\}, \{x', y'\}\}$ tiene dos elementos distintos, luego $x' \neq y'$. Los conjuntos $\{x\}$ y $\{x'\}$ tienen cada uno un único elemento y los conjuntos $\{x, y\}$ y $\{x', y'\}$ tiene dos elementos diferentes, luego $\{x\} \neq \{x', y'\}$ y $\{x, y\} \neq \{x'\}$, por lo tanto si $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$ entonces $\{x\} = \{x'\}$ y $\{x, y\} = \{x', y'\}$, usando dos veces más el axioma de extensionalidad obtenemos $x = x'$ e $y = y'$ para concluir que si $(x, y) = (x', y')$ entonces $x = x'$ e $y = y'$.*

**Definición 3.3.** *Dados dos conjuntos $X$ e $Y$ definimos a partir de los pares ordenados el conjunto producto cartesiano $X \times Y$ como el conjunto cuyos elementos son todos los pares ordenadores $(x, y)$ tales que $x \in X$ e $y \in Y$, es decir $X \times Y = \{(x, y) | (x \in X) \wedge (y \in Y)\}$.*
*Veamos que el producto cartesiano $X \times Y$ es un conjunto. Por el axioma de unión $X \cup Y$ es un conjunto y usando dos veces el axioma del conjunto potencia $\mathcal{P}(\mathcal{P}(X \cup Y))$ es un conjunto. El conjunto $X \times Y$ es un conjunto formado por elementos de $\mathcal{P}(\mathcal{P}(X \cup Y))$ que cumplen una cierta propiedad.*

**Ejemplo 3.1.** *Sean $X = \{x\}$ e $Y = \{y\}$ dos conjuntos.*
*Usando el axioma del conjunto unión obtenemos el conjunto $X \cup Y = \{x, y\}$ y por el axioma del conjunto potencia obtenemos el conjunto de partes*
$\mathcal{P}(X \cup Y) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$ *y*
$\mathcal{P}(\mathcal{P}(X \cup Y)) = \{\emptyset, \{\emptyset\}, \{\{x\}\}, \{\{y\}\}, \{\{x, y\}\},$
$\{\emptyset, \{x\}\}, \{\emptyset, \{y\}\}, \{\emptyset, \{x, y\}\}, \{\{x\}, \{y\}\}, \{\{x\}, \{x, y\}\}, \{\{y\}, \{x, y\}\},$
$\{\emptyset, \{x\}, \{y\}\}, \{\emptyset, \{x\}, \{x, y\}\}, \{\emptyset, \{y\}, \{x, y\}\}, \{\{x\}, \{y\}, \{x, y\}\}, \mathcal{P}(X \cup Y)\}$.
*El conjunto $X \times Y \subset \mathcal{P}(\mathcal{P}(X \cup Y))$ es $\{\{\{x\}, \{x, y\}\}\}$.*

**Definición 3.4.** *Una relación(binaria) $\mathcal{R}$ en un conjunto $A$ es subconjunto de $A \times A$. Si $(x, y) \in R$ escribiremos $xRy$ y si $(x, y) \notin R$ escribiremos $x\not{R}y$.*
*Una relación $R$ es reflexiva en un conjunto $X$ si $xRx$ para todo $x \in X$.*
*Una relación $R$ es simétrica en un conjunto $X$ si para todo $x, y \in X$ tales que $xRy$ entonces $yRx$.*
*Una relación $R$ es antisimétrica en un conjunto $X$ si para todo $x, y \in X$ tales que $xRy$ entonces $y\not{R}x$.*
*Una relación $R$ es transitiva en un conjunto $X$ si para todo $x, y, z \in X$ tales que $xRy$ e $yRz$ entonces $xRz$.*
*Una relación $R$ es una relación de equivalencia en un conjunto $X$ si es reflexiva, simétrica y transitiva en $X$.*
*Una relación $R$ es una relación de orden en un conjunto $X$ si es reflexiva, transitiva y antisimétrica.*

**Definición 3.5.** *Una correspondencia $F$ entre los conjuntos $X$ e $Y$ es cualquier subconjunto $F \subset X \times Y$.*

**Definición 3.6.** *Dados los conjuntos $X$ e $Y$ y una correspondencia $F \subset X \times Y$ definimos los conjuntos dominio de F(habitualmente escribiremos dom(F) para referirnos al dominio de F) e imagen o rango de F(habitualmente escribiremos im(F) para referirnos a la imagen de F) como sigue:*

- $dom(F) = \{x \in X | (\exists y)((y \in Y) \wedge ((x, y) \in F))\}$.
  *Veamos que $dom(F)$ es un conjunto. Usando dos veces el axioma de unión tenemos $\bigcup\bigcup F$ siendo $dom(F) = X \cap (\bigcup\bigcup F)$.*
  *Por ejemplo si $X = \{x_1, x_2\}$ y $F = \{\{\{x_1\}, \{x_1, y\}\}\}$ entonces $\bigcup F = \{\{x_1\}, \{x_1, y\}\}$ y $\bigcup\bigcup F = \{x_1, x_1, y\}$.*
  *Por lo tanto $X \cap (\bigcup\bigcup F) = \{x_1\} = dom(F)$.*

- $im(F) = \{y \in Y | (\exists x)((x \in X) \wedge ((x, y) \in F))\}$.
  *El conjunto imagen es un conjunto, pues es $Y \cap (\bigcup\bigcup F)$.*

**Definición 3.7.** *Definimos el conjunto correspondencia inversa $F$ de la siguiente manera:*

$$F^{-1} = \{(y, x) \in Y \times X | (x, y) \in X \times Y\}.$$

*Diremos que una correspondecia $F$ es unívoca si para cada $x \in X$ existe a lo sumo un $y \in Y$ tal que $(x, y) \in F$, es decir si $(x, y), (x, z) \in F$ entonces $y = z$.*
*Si las correspondencia $F$ y $F^{-1}$ son unívocas entonces $F$ es biunívoca.*
*Si el conjunto $G$ es una correspondencia entre los conjuntos $Y$ y $Z$ definimos la composición de $F$ y $G$ como el conjunto*

$$G \circ F = \{(x, z) | (\exists y)(((x, y) \in F) \wedge ((y, z) \in G))\}.$$

*Observemos que el conjunto $G \circ F$ es una correspondencia entre los conjuntos $X$ y $Z$, ya que es un subconjunto de $X \times Z$.*

**Definición 3.8.** *Una función $F$ entre dos conjuntos $X$ e $Y$ es una correspondencia entre $X$ e $Y$ unívoca cuyo dominio es el conjunto $X$ y para cada $x \in X$ existe un único $y \in Y$ tal que $(x, y) \in F$.*
*Si $(x, y) \in F$ escribiremos $F(x) = y$.*
*Una función es inyectiva si para todo si para todo $x, x' \in X$ tal que $F(x) = F(x')$ se cumple $x = x'$.*
*Una función es sobreyectiva si para todo $y \in Y$ existe $x \in X$ tal que $F(x) = y$.*
*Una función es biyectiva si es inyectiva y sobreyectiva.*

**Observación 3.1.** *Daremos una breve explicación para mostrar que si $F$ y $G$ son correspondencias entonces $F^{-1}$ y $G \circ F$ son conjuntos.*
*Hemos definido $F^{-1}$ como*

$$\{u \in \mathcal{P}(\mathcal{P}(\bigcup\bigcup F)) | (\exists v)(\exists w)((u = (v, w)) \wedge ((w, v) \in F))\}.$$

*Como $F$ es un conjunto entonces por el axioma de unión $\bigcup\bigcup F$ es un conjunto y por el axioma del conjunto potencia $\mathcal{P}(\mathcal{P}(\bigcup\bigcup F))$, finalmente por el esquema axiomático de separación $F^{-1}$ es un conjunto.*
*Hemos definido $G \circ F$ como*

$$\{z \in \mathcal{P}(\mathcal{P}(\bigcup\bigcup(F \cup G))) | (\exists u)(\exists v)(\exists w)((((u, v) \in G) \wedge ((v, w) \in F)) \wedge (z = (u, w)))\}.$$

*Como $F$ y $G$ son conjuntos entonces por el axioma unión $\bigcup\bigcup(F \cup G)$ es un conjunto y por el axioma de partes $\mathcal{P}(\mathcal{P}(\bigcup\bigcup(F \cup G)))$ es un conjunto, finalmente por el esquema axiomático de separación $G \circ F$ es un conjunto.*

## 3.2. Sistema de Peano y los números naturales.

Los axiomas de Peano nos van permitir la construcción de forma teórica del conjunto de los números naturales.
Un sistema de Peano es una terna $(\mathbb{N}, 0, S)$ tal que:

1. $0 \in \mathbb{N}$.
2. $((x \in \mathbb{N}) \to (S(x) \in \mathbb{N}))$.
3. $(\forall x)(\forall y)((S(x) = S(y)) \to (x = y))$.
4. $(\neg(\exists x)(S(x) = 0))$.
5. Principio de inducción.
   Para cada $X \subseteq \mathbb{N}$ tenemos
   $(((0 \in X) \wedge ((\forall n)((n \in X) \to (S(n) \in X)))) \to (X = \mathbb{N}))$.

**Observación 3.2.** *La terna $(\mathbb{N}, 0, S)$ es el par $(\mathbb{N}, (0, S))$, es decir, la terna $(\mathbb{N}, 0, S)$ es el conjunto $\{\{\mathbb{N}\}, \{\mathbb{N}, \{\{0\}, \{0, S\}\}\}\}$.*

**Lema 3.4.** *En un sistema de Peano cada elemento distinto de cero es un sucesor y para cada elemento $n$ tenemos $S(n) \neq n$.*

**Demostración.** *Definimos el conjunto $X$ formado por el cero y por todos los sucesores de otros elementos, esto es*

$$X = \{n \in \mathbb{N} | (n = 0) \vee (\exists m)((m \in \mathbb{N}) \wedge (n = S(m)))\}.$$

*Puesto que $X \subseteq \mathbb{N}$ solo es necesario ver que se cumple el principio de inducción. El elemento $0 \in X$ y si tomamos un elemento de $X$ también está su sucesor, puesto que los elementos de $X$(excluyendo el cero) son aquellos elementos de $\mathbb{N}$ que son sucesor de otro. Por lo tanto $X = \mathbb{N}$ por el principio de inducción.*
*Probaremos por el principio de inducción que $S(n) \neq n$ para todo $n \in \mathbb{N}$.*
*Definimos $Y$ como el conjunto $\{n \in \mathbb{N} | S(n) \neq n\}$.*
*El elemento $0$ pertenece al conjunto $Y$ ya que por el axioma 4 de Peano $0$ no es sucesor de ningún elemento y por consiguiente tampoco es sucesor de sí mismo.*
*Veamos que si $n \in Y$ entonces $S(n) \in Y$. Para probar ésto último basta*

*probar que si* $S(n) \neq n$ *entonces* $S(S(n)) \neq S(n)$.
*El axioma* $(\forall x)(\forall y)((S(x) = S(y)) \rightarrow (x = y))$ *prueba que si* $S(n) \neq n$ *entonces* $S(S(n)) \neq S(n)$.
*Por el principio de inducción* $Y = \mathbb{N}$.

**Teorema 3.1.** *Existe al menos un sistema de Peano.*

**Demostración.** *El axioma del infinito nos garantiza la existencia de un conjunto* $I$ *tal que* $\emptyset \in I$ *y* $(\forall n)((n \in I) \rightarrow (n \cup \{n\} \in I))$.
*Como* $I$ *es un conjunto entonces* $\mathcal{P}(I)$ *también lo es por el axioma de las partes del conjunto. Usando el esquema axiomático de separación definimos la familia de conjuntos* $\mathcal{F}$ *de la siguiente manera:*

$$\mathcal{F} = \{X \subseteq I | (\emptyset \in X) \wedge (\forall n)((n \in X) \rightarrow n \cup \{n\} \in X)\}.$$

*Definimos* $\mathbb{N} = \bigcap \mathcal{F}$, $0 = \emptyset$ *y* $S = \{(n, m) \in \mathbb{N} \times \mathbb{N} | m = n \cup \{n\}\}$.
*Veamos que* $(\mathbb{N}, 0, S)$ *es un sistema de Peano:*

1. $\emptyset \in \bigcap \mathcal{F} = \mathbb{N}$ *ya que para cualquier conjunto* $X$ *de* $\mathcal{F}$ *tenemos* $\emptyset \in X$.

2. *Sea* $n \in \mathbb{N} = \bigcap \mathcal{F}$. *Usando las definiciones de* $\mathcal{F}$ *e* $I$ *vemos que* $(\forall X)((X \in \mathcal{F}) \rightarrow (n \cup \{n\} \in X))$ *por lo tanto* $n \cup \{n\} \in \bigcap \mathcal{F} = \mathbb{N}$.

3. *Veamos que si* $S(m) = S(n)$ *entonces* $n = m$. *Si* $m \cup \{m\} = n \cup \{n\}$ *entonces por el axioma de extensionalidad* $m \in n \cup \{n\}$ *y* $n \in m \cup \{m\}$, *es decir, o bien* $n = m$, *o bien* $n \in m$ *y* $m \in n$.
   *El caso* $m \in n$ *y* $n \in m$ *no es factible, ya que por el lema 3.1 no se puede dar el caso* $...m \in n \in m \in n$.

4. *El cero no es sucesor de ningún número, ya que el sucesor de cualquier número es un conjunto no vacío(*$S(n) = n \cup \{n\}$*).*

5. *Sea* $X \subseteq \mathbb{N}$. *Veamos que si se cumple* $((0 \in X) \wedge (\forall n)((n \in X) \rightarrow (S(n) \in X)))$ *entonces* $X = \mathbb{N}$.
   *Para ver que* $X = \mathbb{N}$ *solo hay que probar que* $\mathbb{N} \subset X$.
   *Por definición del conjunto* $\mathcal{F}$ $\mathbb{N} = \bigcap \mathcal{F}$ *es el conjunto tal que* $0 \in \mathbb{N}$ *y si un elemento pertenece a* $\mathbb{N}$ *entonces su sucesor también lo está. Vemos que* $\mathbb{N} \subset X$, *luego* $X = \mathbb{N}$.

El siguiente teorema junto con el corolario que lo sigue nos permitirán definir de manera recursiva la suma y el producto en $\mathbb{N}$.

**Teorema 3.2.** ***(de Recursión).*** *Sean $(\mathbb{N}, 0, S)$ un sistema de Peano, $E$ un conjunto cualquiera y $h : E \longrightarrow E$ una función. Entonces existe una única función $f : \mathbb{N} \longrightarrow E$ tal que $f(0) = a$ y $f(S(n)) = h(f(n))$ para todo $n \in \mathbb{N}$.*

**Demostración.** *Definimos el conjunto $\mathcal{A}$ cuyos elementos son las funciones $p$ tales que:*

1. *$dom(p) \subseteq \mathbb{N}$ y $im(p) \subseteq E$.*

2. *$0 \in dom(p)$ y $p(0) = a$.*

3. *$(\forall n)((S(n) \in \mathbb{N}) \rightarrow ((n \in dom(p)) \wedge (p(S(n)) = h(p(n)))))$.*

*Probaremos brevemente que $\mathcal{A}$ es un conjunto.*
*Como $\mathbb{N}$ y $E$ son conjuntos entonces $\mathbb{N} \times E$ también es un conjunto y por el axioma de las partes del conjunto $\mathcal{P}(\mathbb{N} \times E)$ es un conjunto, finalmente por el esquema axiomático de separación $\mathcal{A}$ es un conjunto.*
*Veamos que para todo $p, q \in \mathcal{A}$ y $n \in \mathbb{N}$ si $n \in dom(p) \cap dom(q)$ entonces $p(n) = q(n)$.*
*Definimos el conjunto*
*$X = \{n \in \mathbb{N} | (\forall p, q \in \mathcal{A})[(n \in dom(p) \cap dom(q)) \rightarrow (p(n) = q(n))]\}$. Vemos que $0 \in X$, ya que $p, q \in \mathcal{A}$ y $p(0) = q(0) = a$. Si $n \in X$, $p, q \in \mathcal{A}$ y $S(n) \in dom(p) \cap dom(q)$ entonces $p(S(n)) = h(S(n))$ ya que $p \in \mathcal{A}$, como $p(n) = q(n)$ tenemos $p(S(n)) = h(p(n)) = h(q(n))$ y finalmente tenemos $p(S(n)) = q(S(n))$ debido a que $q \in \mathcal{A}$. Vemos que si $n \in X$ entonces $S(n) \in X$ y por el principio de inducción tenemos $X = \mathbb{N}$.*
*Acabamos de probar que el conjunto $\mathcal{A}$ tiene a lo sumo un elemento. Puesto que $\{(0, a)\} \in \mathcal{A}$ podemos afirmar que $\mathcal{A}$ es distinto al conjunto vacío $\emptyset$.*
*Sea $f = \bigcup \mathcal{A} = \{(n, w) | (\exists p)((p \in \mathcal{A}) \rightarrow ((n \in dom(p)) \wedge (p(n) = w)))\}$. Si $(n, w), (n, \hat{w}) \in f$ entonces por definición de $f$ existen $p, q \in \mathcal{A}$ tales que $(u, w) \in p$ y $(u, \hat{w}) \in q$ y por lo visto en el primer párrafo de la demostración $p(u) = q(u)$, por lo tanto $w = \hat{w}$, luego $f$ es una función. Veamos que $f \in \mathcal{A}$:*

1. *$dom(f) \subseteq (\bigcup dom(p))$ con $p \in A$, luego $\bigcup dom(f) \subseteq \mathbb{N}$ y $im(f) \subseteq (\bigcup im(p))$ con $p \in A$, luego $\bigcup im(f) \subseteq E$.*

2. *Para todo $p \in \mathcal{A}$ tenemos $0 \in dom(p)$ y $p(0) = a$, luego $0 \in dom(f)$ y $f(0) = a$.*

3. *Tomamos $n \in \mathbb{N}$ y $S(n) \in dom(f)$. Como $S(n) \in dom(f)$ existe $p \in \mathcal{A}$ tal que $S(n) \in dom(p)$,luego $n \in dom(p)$ y $p(S(n)) = h(p(n))$. Por lo*

*tanto* $(S(n), h(p(n))) \in f$ *y* $p(n) = f(n)$ *por definición de f, luego* $(\forall n)((n \in \mathbb{N}) \to ((n \in dom(f)) \wedge (f(S(n)) = h(f(n)))))$.

*Veamos por el principio de inducción que* $dom(f) = \mathbb{N}$.
*Como* $0 \in dom(p)$ *para todo* $p \in \mathcal{A}$ *y* $\mathcal{A} \neq \emptyset$ *entonces* $0 \in dom(f)$. *Si* $n \in dom(f)$ *entonces existe una función* $p \in \mathcal{A}$ *con* $n \in dom(p)$. *Tomando* $q = p \cup \{(S(n), h(p(n)))\} \in \mathcal{A}$ *vemos que* $S(n) \in dom(q) \subseteq dom(f)$.
*Luego* $dom(f) = \mathbb{N}$

**Corolario 3.1.** *Para dos conjuntos cualesquiera Y y E y funciones* $g : Y \longrightarrow E$, $h : E \times Y \longrightarrow E$ *existe una única función* $f : \mathbb{N} \times Y \longrightarrow E$ *que satisface* $f(0, y) = g(y)$ *y* $f(S(n), y) = h(f(n, y), y)$.

**Demostración.** *Para cada* $y \in Y$ *definimos la función* $h_y : E \longrightarrow E$ *mediante la fórmula* $h_y(w) = h(w, y)$. *Por el teorema de recursión sabemos que existe una única función* $f_y : \mathbb{N} \longrightarrow E$ *tal que* $f_y(0) = g(y)$ *y*
$f_y(S(n)) = h_y(f_y(n)) = h(f_y(n), y)$.
*Sea* $f(n, y) = f_y(n)$ *veamos que* $f(0, y) = g(y)$ *y* $f(S(n), y) = h(f(n, y), y)$.
*Por definión* $f(0, y) = f_y(0)$ *y* $f_y(0) = g(y)$, *luego* $f(0, y) = g(y)$.
*Por definición* $f(S(n), y) = f_y(S(n))$ *y*
$f_y(S(n)) = h_y(f_y(n)) = h(f_y(n), y) = h(f(n, y), y)$, *luego*
$f(S(n), y) = h(f(n, y), y)$.

**Lema 3.5.** *Si existen dos sistemas de Peano* $(\mathbb{N}_1, 0_1, S_1)$ *y* $(\mathbb{N}_2, 0_2, S_2)$ *entonces existe una biyección* $\Pi : \mathbb{N}_1 \longrightarrow \mathbb{N}_2$ *tal que* $\Pi(0_1) = 0_2$ *y* $\Pi(S_1(n)) = S_2(\Pi(n))$ *para todo* $n \in \mathbb{N}_1$, *es decir, los sistemas de Peano son únicos salvo isomorfismos.*

**Demostración.** *Por el teorema de recursión en* $(\mathbb{N}_1, 0_1, S_1)$ *con* $E = \mathbb{N}_2$, $a = 0$ *y* $h = S_2$ *sabemos que existe una única función* $\Pi$ *que satisface* $\Pi(0_1) = 0_2$ *y* $\Pi(S_1(n)) = S_2\Pi(n)$ *para todo* $n \in \mathbb{N}_1$. *Veamos ahora que* $\Pi$ *es una función sobreyectiva e inyectiva.*
*Veamos que la función* $\Pi$ *es sobreyectiva:*
*Como* $\Pi(0_1) = 0_2$ *entonces* $0_2 \in \Pi[\mathbb{N}_2]$. *Si* $m \in \Pi[\mathbb{N}_2]$ *entonces existe* $n \in \mathbb{N}_1$ *tal que* $\Pi(n) = m$, *luego* $S_2(\Pi(n)) = S_2(m) = \Pi(S_1(n))$, *por lo tanto* $S_2(m) \in \Pi[\mathbb{N}_1]$. *Aplicando el principio de inducción obtenemos* $\Pi[\mathbb{N}_1] = \mathbb{N}_2$.
*Veamos que la función* $\Pi$ *es inyectiva:*
*Sea* $X = \{(n \in \mathbb{N}_1) | (\forall m)((m \in \mathbb{N}_1) \to ((\Pi(m) = \Pi(n)) \to (m = n)))\}$.
*Veamos que* $0_1 \in X$ *y si* $n \in X$ *entonces* $S_1(n) \in X$.
*Veamos que* $0_1 \in X$*:*

*Sea $m \neq 0_1$, por el lema 3.4 existe $\hat{m} \in \mathbb{N}_1$ tal que $S_1(\hat{m}) = m$, luego $\Pi(m) = \Pi(S_1(\hat{m})) = S_2(\Pi(\hat{m})) \neq 0_2$. Por lo tanto si $\Pi(m) = \Pi(0_1) = 0_2$ entonces $m = 0_1$ y $0_1 \in X$.*
*Veamos que si $n \in X$ entonces $S_1(n) \in X$:*
*Probaremos que si $n \in X$ y $\Pi(m) = \Pi(S_1(n))$ entonces $m = S_1(n)$.*
*Por hipótesis $\Pi(m) = \Pi(S_1(n)) = S_2(\Pi(n)) \neq 0_2$, por lo tanto $m \neq 0_1$. Por el lema 3.4 sabemos que existe $\hat{m} \in \mathbb{N}_1$ tal que $S_1(\hat{m}) = m$. Como $\Pi(m) = \Pi(S_1(\hat{m})) = S_2(\Pi(\hat{m}))$ y $\Pi(m) = \Pi(S_1(n)) = S_2(\Pi(n))$ por hipótesis entonces $S_2(\Pi(\hat{m})) = S_2(\Pi(n))$, luego $\Pi(\hat{m}) = \Pi(n)$, por lo tanto $\hat{m} = n$ ya que $n \in X$ y finalmente vemos que $m = S_1(\hat{m}) = S_1(n)$. Por el principio de inducción concluimos que $X = \mathbb{N}_1$.*

## 3.3. Suma y producto de los números naturales.

**Definición 3.9.** *Definimos la suma en $\mathbb{N}$ como la función $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que $+(n, 0) = 0$ para todo $n \in \mathbb{N}$ y $+(n, S(m)) = S(+(n, m))$ para todo $(n, m) \in \mathbb{N} \times \mathbb{N}$.*
*Veamos que existe la función suma. Sea $g_1 : \mathbb{N} \longrightarrow \mathbb{N}$ la función identidad y $h_1 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ la función que a cada par $(z, n)$ le corresponde $S(z)$, es decir $h_1 = \{((z, n), w) \in (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} | w = S(z)\}$.*
*El corolario 3.1 nos garantiza que existe una única función $f_1 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f_1(0, n) = g_1(n)$ y $f_1(S(m), n) = h_1(f_1(m, n), n)$.*
*Finalmente definimos la función suma de la siguiente manera:*

$$+ = \{((n, m), w) | ((m, n), w) \in f_1\}.$$

**Definición 3.10.** *Definimos la función producto en $\mathbb{N}$ como la función*
*$* : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que $*(n, 0) = 0$ para todo $n \in \mathbb{N}$ y*
*$*(n, S(m)) = +(*(n, m), n)$.*
*Veamos que la función producto está bien definida.*
*Sean $g_2 : \mathbb{N} \times \{0\} \longrightarrow \mathbb{N}$ una función tal que $g_2(n) = 0$ para todo $n \in \mathbb{N}$ y $h_2$ la función suma.*
*El corolario 3.1 nos garantiza que existe una única función $f_2 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f_2(0, n) = g_2(n)$ y $f_2(S(m), n) = h_2(f_2(m, n), n)$.*

*Finalmente definimos la función multiplicación de la siguiente manera:*

$$* = \{((n,m),w)|((m,n),w) \in f_2\}.$$

Escribiremos $n+m$ y $n*m$ en lugar de $+(n,m)$ y $*(n,m)$.
De la definicion de suma obtenemos las dos siguientes propiedades $(S1)$ y $(S2)$:

1. $(S1)$ $n+0=n$.
2. $(S2)$ $n+S(m)=S(n+m)$.

De la definicion de producto obtenemos las dos siguientes propiedades $(P1)$ y $(P2)$:

1. $(P1)$ $n*0=0$.
2. $(P2)$ $n*S(m)=(n*m)+n$.

**Teorema 3.3.** ***(Asociatividad)*** *La función suma es asociativa, es decir, para todo $m,n,k \in \mathbb{N}$ se cumple $(n+m)+k=n+(m+k)$.*

**Demostración.** *Lo demostraremos utilizando el principio de inducción.*
*Fijados $m$ y $n$ en $\mathbb{N}$ definimos el conjunto*
*$X=\{k \in \mathbb{N}|(m+n)+k=n+(m+k)\}$. Para $k=0$ tenemos*
*$(n+m)+0=n+m=n+(m+0)$, luego $0 \in X$.*
*Veamos que $(n+m)+S(k)=n+(m+S(k))$ asumiendo que para un $k$ se cumple $(n+m)+k=n+(m+k)$.*
*Por la propiedad $(S2)$ de la suma tenemos $(n+m)+S(k)=S((n+m)+k)$, como $(n+m)+k=n+(m+k)$ entonces $S((n+m)+k)=S(n+(m+k))$ y otra vez por la propiedad $(S2)$ de la suma tenemos*
*$S(n+(m+k))=n+S(m+k)=n+(n+S(k))$.*
*Por el principio de inducción $X=\mathbb{N}$.*

**Lema 3.6.** *Para todo natural $n$ se cumple $0+n=n$.*

**Demostración.** *Lo demostraremos utilizando el principio de inducción, para ello definimos el conjunto*
*$X=\{n \in \mathbb{N}|0+n=0\}$.*
*El elemento $0$ pertenece a $X$ por la propiedad $(S1)$ de la suma, es decir se cumple $0+0=0$.*

*Veamos que si* $0 + n = n$ *entonces* $0 + S(n) = S(n)$. *Por la propiedad* $(S2)$ *de la suma vemos que* $0 + S(n) = S(0 + n)$, *como* $0 + n = n$ *entonces* $S(0 + n) = S(n)$, *luego* $0 + S(n) = S(n)$ *y* $S(n) \in X$.
*Por el principio de inducción* $X = \mathbb{N}$.

**Lema 3.7.** *Para todo* $m, n \in \mathbb{N}$ *se cumple* $n + S(m) = S(n) + m$.

**Demostración.** *Demostraremos el lema utilizando el principio de inducción.*
*Fijando* $n$ *en* $\mathbb{N}$ *definimos el conjunto* $X = \{m \in \mathbb{N} | n + S(m) = S(n) + m\}$.
*El elemento* $0$ *pertenece al conjunto* $X$ *ya que por la propiedad* $(S2)$ *de la suma se cumple* $n + S(0) = S(n + 0)$ *y por la propiedad* $(S1)$ *de la suma* $S(n + 0) = S(n) = S(n) + 0$.
*Veamos que si existe* $m \in \mathbb{N}$ *tal que* $n + S(m) = S(n) + m$ *entonces* $n + S(S(m)) = S(n) + S(m)$.
*Por la propiedad* $(S2)$ *de la suma* $n + S(S(m)) = S(n + S(m))$, *como* $n+S(m) = S(n)+m$ *entonces* $S(n+S(m)) = S(S(m)+n)$ *y por la propiedad* $(S2)$ *de la suma* $S(S(m) + n) = S(m) + S(n)$, *luego* $n + S(S(m)) = S(n) + S(m)$, *por consiguiente* $S(m) \in \mathbb{N}$.
*Utilizando el principio de inducción se concluye* $X = \mathbb{N}$.

**Teorema 3.4.** *La función suma es conmutativa, es decir* $n + m = m + n$.

**Demostración.** *Demostraremos el teorema utilizando el principio de inducción.*
*Fijado un* $n$ *en* $\mathbb{N}$ *y definimos el conjunto* $X = \{m \in \mathbb{N} | n + m = m + n\}$.
*Por el lema 3.6 el elemento* $0$ *pertenece a* $X$.
*Veamos que si* $n + m = m + n$ *entonces* $n + S(m) = S(m) + n$.
*Por la propiedad* $(S2)$ *de la suma* $n + S(m) = S(n + m)$, *como* $n + m = m + n$ *entonces* $S(n + m) = S(m + n)$ *y por la propiedad* $(S2)$ *de la suma* $S(m + n) = m + S(n)$. *Aplicando el lema 3.7 vemos que* $m + S(n) = S(m) + n$, *concluyendo* $n + S(m) = S(m) + n$ *y* $S(m) \in X$.
*Por el principio de inducción* $X = \mathbb{N}$.

Denotaremos por 1 al elemento $S(0)$ y observemos que $S(n) = n + 1$, ya que por la propiedad $(P2)$ obtenemos $n + S(0) = S(n + 0)$ y por la propiedad $(P1)$ $n + 0 = n$, luego $n + 1 = S(n)$.

**Lema 3.8.** *Para todo* $n \in \mathbb{N}$ *se tiene* $0 * n = 0$.

**Demostración.** *Probaremos el lema utilizando el principio de inducción.*
*Definimos el conjunto* $X = \{n \in \mathbb{N} | n * 0 = 0\}$. *Para* $n = 0$ *basta aplicar la*

*propiedad* $(P1)$ *del producto y ver que* $0 * 0 = 0$.
*Veamos que si* $0 * n = 0$ *entonces* $0 * S(n) = 0$.
*Por la propiedad* $(P2)$ *del producto* $0 * S(n) = (0 * n) + 0$, *como* $0 * n = 0$ *entonces*
$(0 * n) + 0 = 0 + 0$ *y por el lema 3.6* $0 + 0 = 0$, *luego* $0 * S(n) = 0$ *y* $S(n) \in X$.
*Por el principio de inducción* $X = \mathbb{N}$.

**Teorema 3.5.** *La función producto es distributiva por la derecha, es decir, para todo* $n, m, k \in \mathbb{N}$ *se cumple* $(n + m) * k = (n * k) + (m * k)$.

**Demostración.** *Demostraremos el teorema usando el principio de inducción.*
*Fijados dos elementos de* $\mathbb{N}$ $n$ *y* $m$ *definimos el conjunto*
$X = \{k \in \mathbb{N} | (n + m) * k = (n * k) + (m * k)\}$.
*Para* $k = 0$ *vemos que* $(n + m) * k = 0$ *por la propiedad* $(P2)$, *por otra parte, por la propiedad* $(P1)$ *del producto* $n * 0 = 0$ *y* $m * 0 = 0$ *y por* $(S1)$ $0 + 0 = 0$, *luego* $(n + m) * k = 0 = (n * k) + (m * k)$, *es decir* $0 \in X$.
*Veamos que si* $(n + m) * k = (n * k) + (m * k)$ *entonces*
$(n + m) * S(k) = (n * S(k)) + (m * S(k))$.
*Por* $(P2)$ *vemos que* $(n + m) * S(k) = (n + m) * k + (n + m)$.
*Como* $(n + m) * k = (n * k) + (m * k)$ *entonces*
$(n + m) * k + (n + m) = ((n * k) + (m * k)) + (n + m)$.
*Por las propiedades asociativa y conmutativa de la suma*
$((n * k) + (m * k)) + (n + m) = ((n * k) + n) + ((m * k) + m)$.
*Usando la propiedad* $(P2)$ *del producto obtenemos*
$((n * k) + n) + ((m * k) + m) = (n * S(k)) + (m * S(k))$ *concluyendo*
$(n + m) * S(k) = (n * S(k)) + (m * S(k))$ *y* $S(k) \in X$.
*Por el principio de inducción* $X = \mathbb{N}$.

**Teorema 3.6.** *La función multiplicación es distributiva respecto de la suma, es decir, para todo* $n, m, k \in \mathbb{N}$ *se cumple* $n * (m + k) = (n * m) + (n * k)$.

**Demostración.** *Probaremos el teorema usando el principio de inducción.*
*Fijados dos elementos de* $\mathbb{N}$ $n$ *y* $m$ *definimos el conjunto*
$X = \{k \in \mathbb{N} | n * (m + k) = (n * m) + (n * k)\}$. *El elemento* $0$ *pertenece al conjunto* $X$ *ya que por la propiedad* $(S1)$ *de la suma* $n * (m + 0) = n * m$ *y* $n * m = (n * m) + 0 = (n * m) + (n * 0)$, *luego* $n * (m + 0) = (n * m) + (n * 0)$.
*Veamos que si* $n * (m + k) = (n * m) + (n * k)$ *entonces*
$n * (m + S(k)) = (n * m) + (n * S(k))$.

*Por la propiedad* $(S2)$ *de la suma*
$n * (m + S(k)) = n * S(m + k) = (n * (m + k)) + n$. *Como*
$n*(m+k) = (n*m)+(n*k)$ *entonces* $(n*(m+k))+n = ((n*m)+(n*k))+n$, *por el teorema de la asociatividad de la suma*
$((n * m) + (n * k)) + n = (n * m) + ((n * k) + n)$ *y por la propiedad* $(P2)$ *del producto concluimos* $(n*m)+((n*k)+n) = (n*m)+(n*S(k))$ *y* $S(k) \in X$.
*Por el principio de inducción* $X = \mathbb{N}$.

**Teorema 3.7.** *El producto tiene elemento unidad, siendo este el elemento* 1, *es decir, para todo* $n \in \mathbb{N}$ *se cumple* $n * 1 = n = 1 * n$.

**Demostración.** *Por la propiedad* $(P2)$ *del producto vemos que*
$n * 1 = (n * 0) + n$ *y por la propiedad* $(P1)$ *del producto* $(n * 0) + n = 0 + n$.
*Por el lema 3.6* $0 + n = n$, *luego* $n * 1 = n$.
*Utilizaremos el principio de inducción para probar* $1 * n = n$ *para todo* $n \in \mathbb{N}$.
*Definimos el conjunto* $X = \{n \in \mathbb{N} | 1 * n = n\}$.
*El elemento* 0 *pertenece al conjunto* $X$ *por la propiedad* $(P1)$ *del producto.*
*Veamos que si* $1 * n = n$ *entonces* $1 * S(n) = S(n)$.
*Recordando que* $S(n) = n + 1$ *vemos que* $1 * S(n) = 1 * (n + 1)$. *Por la propiedad distributiva del producto respecto de la suma tenemos*
$1 * (n + 1) = (1 * n) + (1 * 1)$. *Por otra parte hemos probado que* $(n * 1) = 1$ *para todo* $n \in \mathbb{N}$, *luego* $1 * 1 =$ *y por consiguiente* $(1 * n) + (1 * 1) = (1 * n) + 1$.
*Como* $1 * n = n$ *entonces* $(1 * n) + 1 = n + 1 = S(n)$ *y* $1 * S(n) = S(n)$, *luego* $S(n) \in \mathbb{N}$.
*Por el principio de inducción* $X = \mathbb{N}$.

**Lema 3.9.** *La función multiplicación es asociativa, es decir, para todo* $m, n, k \in \mathbb{N}$ *se cumple* $n * (m * k) = (n * m) * k$.

**Demostración.** *Probaremos el lema utilizando el principio de inducción.*
*Fijados n y m en* $\mathbb{N}$ *definimos el conjunto* $X = \{k \in \mathbb{N} | n*(m*k) = (n*m)*k\}$.
*El elemento* 0 *pertenece al conjunto* $X$ *ya que por la propiedad* $(P1)$ *del producto obtenemos* $n * (m * 0) = n * 0 = 0 = (n * m) * 0$.
*Veamos que si* $n*(m*k) = (n*m)*k$ *entonces* $n*(m*S(k)) = (n*m)*S(k)$.
*Por la propiedad* $(P2)$ *del producto* $n * (m * S(k)) = n * ((m * k) + m)$ *y por la propiedad distributiva del producto respecto de la suma obtenemos*
$n * ((m * k) + m) = (n * (m * k)) + (n * m)$. *Como* $n * (m * k) = (n * m) * k$ *entonces* $(n*(m*k))+(n*m) = ((n*m)*k)+(n*m)$ *y por la propiedad* $(P2)$ *del producto* $((n * m) * k) + (n * m) = (n * m) * S(k)$. *Finalmente concluimos*

*que* $n*(m*S(k)) = (n*m)*S(k)$ *y* $S(k) \in X$.
*Por el principio de inducción* $X = \mathbb{N}$.

**Lema 3.10.** *La función multiplicación es conmutativa, es decir para todo* $n, m \in \mathbb{N}$ *se cumple* $n*m = m*m$.

**Demostración.** *Demostraremos el teorema utlizando el principio de inducción.*
*Fijamos* $n \in \mathbb{N}$ *y definimos el conjunto* $X = \{m \in \mathbb{N} | n*m = m*n\}$. *El elemento* $0$ *pertenece al conjunto* $X$ *ya que por la propiedad* $(P1)$ *del producto y por el lema 3.8 se cumple* $n*0 = 0 = 0*n$.
*Veamos que si* $n*m = m*n$ *entonces* $n*S(m) = S(m)*n$ *y por consiguiente* $S(m) \in X$.
*Usando la propiedad del producto* $(P2)$ *vemos que* $n*S(m) = (n*m)+n$. *Como* $n*m = m*n$ *entonces* $(n*m)+n = (m*n)+n$. *En el teorema 3.7 hemos probado* $1*n = n$, *luego* $(m*n)+n = (m*n)+(1*n)$ *y usando la propiedad distributiva por la derecha concluimos* $(m*n)+(1*n) = (m+1)*n = S(m)*n$ *y* $S(m) \in \mathbb{N}$.
*Por el principio de inducción* $X = \mathbb{N}$.

*El par* $(\mathbb{N}, +)$ *es un semigrupo conmutativo con elemento neutro* $0$ *debido a las propiedades asociativa y conmutativa de la suma junto con la propiedad* $(S1)$ *de la suma.*
*La terna* $(\mathbb{N}, +, *)$ *es un semianillo conmutativo con elemento unidad por las propiedades distributivas, asociativa y conmutativa del producto y la existencia de elemento unidad.*

## 3.4. Ordenación de los números naturales.

**Definición 3.11.** *Definimos la relación menor que* $<$ *como el conjunto*

$$\{(n, m) \in \mathbb{N} \times \mathbb{N} | (\exists p)(((p \in \mathbb{N}) \wedge (n + p = m)) \wedge (p \neq 0))\}.$$

*y la relación menor o igual que* $\leq$ *como el conjunto*

$$\{(n, m) \in \mathbb{N} \times \mathbb{N} | (\exists p)((p \in \mathbb{N}) \wedge (n + p = m))\}.$$

**Lema 3.11.** ***(Propiedad cancelativa de la suma.)*** *Para todo* $m, n, p \in \mathbb{N}$ *si* $m + n = m + p$ *entonces* $n = p$.
*Si* $m \neq 0$ *entonces* $m + n \neq 0$.

**Demostración.** *Para probar que $m+n=m+p$ implica $n=p$ probaremos que $n \neq p$ implica $m+n \neq m+p$. Para ello fijamos $n, p \in \mathbb{N}$ tales que $n \neq p$ y definimos el conjunto $S_{n,p} = \{k \in \mathbb{N} | k+n \neq k+p\}$.*
*El elemento $0 \in S_{n,p}$ ya que $0+n = n \neq p = 0+p$, luego $0+n \neq 0+p$.*
*Veamos que si $k \in S_{n,p}$ entonces $S(k) \in S_{n,p}$.*
*Por la propiead conmutativa de la suma $S(k)+n = n+S(k)$ y por la propiedad $(S2)$ de la suma $n+S(k) = S(n+k)$. Por hipótesis de inducción y por ser $S$ una función inyectiva $S(n+k) \neq S(p+k)$ y otra vez por la propiedad $(S2)$ de la suma y por conmutatividad $S(p+k) = p+S(k)$, luego*
*$S(k)+n \neq S(k)+p$, por lo tanto $S(k) \in S_{n,p}$. Aplicando el axioma de inducción de Peano concluimos que $S_{n,p} = \mathbb{N}$.*
*Probamos ahora que si $m \neq 0$ entonces $m+n \neq 0$.*
*Como $m \neq 0$ sabemos por el lema 3.4 que existe $m'$ tal que $S(m') = m$. Por la propiedad conmutativa de la suma tenemos $m+n = n+m$, como $m = S(m')$ entonces $n+m = n+S(m')$. Por la propiedad $(S2)$ de la suma $n+S(m') = S(n+m')$. El axioma 4 de Peano nos garantiza que el elemento $0$ no es ningún sucesor, luego $0 \neq S(n+m')$ concluyendo así que si $m \neq 0$ entonces $m+n \neq 0$.*

*La propiedad cancelativa de la suma es fundamental en la demostración del siguiente lema.*

**Lema 3.12.** *El orden en $\mathbb{N}$ es total, es decir, para todo $m, n \in \mathbb{N}$ solamente una de las siguientes afirmaciones es válida:*

1. *$m < n$.*
2. *$m = n$.*
3. *$n < m$.*

**Demostración.** *Veamos que si $m < n$ o $n < m$ entonces no se puede dar el caso $m = n$.*
*Si $m < n$ entonces existe un $p \neq 0$ en $\mathbb{N}$ tal que $m+p = n$. Por otra parte $n = n+0$, luego $m+p = n+0$. Si $m = n$ por la propiedad cancelativa de la suma obtendríamos $p = 0$, lo cual es absurdo.*
*Razonando de forma similar vemos que si $n < m$ entonces no se puede dar el caso $m = n$.*
*Si $n < m$ entonces existe un $p \neq 0$ en $\mathbb{N}$ tal que $n+p = m$. Por otra parte $m = m+0$, luego $n+p = m+0$. Si $m = n$ por la propiedad cancelativa de*

*la suma obtendríamos $p = 0$, lo cual es absurdo.*
*Veamos que si $m < n$ entonces no se puede dar el caso $n < m$.*
*Si $m < n$ y $n < m$ entonces existen $p \neq 0$ y $p' \neq 0$ en $\mathbb{N}$ tales que $m + p = n$ y $n + p' = m$. Por lo tanto $(m + p) + p' = m$. Por la propiedad asociativa de la suma $m + (p + p') = m$. Como $m = m + 0$ entonces $m + (p + p') = m + 0$ y por la propiedad cancelativa de la suma vemos que $p + p' = 0$. En el lema 3.11 hemos probado que si $p \neq 0$ entonces $p + p' \neq 0$, luego $p = 0$, lo cual es absurdo.*
*Para demostrar que necesariamente se cumple una de las tres condiciones fijamos un $m \in \mathbb{N}$ y definimos el conjunto*

$$X_m = \{n \in \mathbb{N} | n < m, m < n \text{ o } m = n\}.$$

*Probaremos que $0 \in X_m$. Para $m = 0$ tomamos la igualdad $0 = 0$ para probar que $0 \in X_m$ y si $m \neq 0$ entonces $0 + m = m$, por lo tanto $0 < m$.*
*Veamos que si $n \in X_m$ entonces $S(n) \in X_m$.*
*Como $n \in X_m$ entonces, o bien $n < m$, o bien $m < n$, o bien $n = m$.*
*Si $m = n$ entonces $S(m) = S(n)$, luego $S(n) = m + 1$, por lo tanto existe $p \neq 0$ en $\mathbb{N}$ tal que $m + p = S(n)$, es decir $m < S(n)$ y $S(n) \in X_m$.*
*Si $m < n$ entonces existe $p \neq 0$ en $\mathbb{N}$ tal que $m+p = n$, luego $S(n) = S(m+p)$ y por la propiedad $(S2)$ de la suma $S(m + p) = m + S(p)$, por lo tanto $m + S(p) = S(n)$. Como $S(p) \neq 0$ entonces $m < S(n)$.*
*Si $n < m$ entonces existe $p \neq 0$ en $\mathbb{N}$ tal que $n + p = m$, como $p \neq 0$ entonces existe $p'$ tal que $S(p') = p$. Por lo tanto $n + S(p') = m$ y por la propiedad $(S2)$ de la suma $n + S(p') = S(n + p')$. Por conmutatividad $S(n + p') = S(p' + n) = p' + S(n) = m$. Si $p' = 0$ entonces $S(n) = m$ y si $p' \neq 0$ entonces $S(n) < m$, en ambos casos $S(n) \in X_m$.*
*Finalmente concluimos por el principio de inducción que $X_m = \mathbb{N}$.*

**Lema 3.13.** ***(Propiedad transitividad.)*** *Dados $m, n, p \in \mathbb{N}$ tales que $m < n$ y $n < p$ entonces $m < p$.*

**Demostración.** *Si $m < n$ y $n < p$ entonces existen $p_1 \neq 0$ y $p_2 \neq 0$ en $\mathbb{N}$ tales que $m + p_1 = n$ y $n + p_2 = p$, luego $(m + p_1) + p_2 = p$ y por la propiedad asociativa de la suma $m + (p_1 + p_2) = p$. Si $p_1 + p_2 = 0$ entonces $p_1 = 0$, por lo tanto $p_1 + p_2 \neq 0$, concluyendo así que $m < p$.*

**Lema 3.14.** *Dados $m, n, p \in \mathbb{N}$ entonces $m < n$ si y solo si $m + p < n + p$.*

**Demostración.** *Veamos que si $m < n$ entonces $m + p < n + p$.*
*Como $m < n$ entonces existe $p_1 \neq 0$ en $\mathbb{N}$ tal que $m + p_1 = n$, por lo tanto*

$n + p = (m + p_1) + p$. *Por asociatividad y conmutatividad*
$(m + p_1) + p = (m + p) + p_1$, *luego* $n + p = (m + p) + p_1$, *es decir*
$m + p < n + p$.
*Veamos que si* $m + p < n + p$ *entonces* $m < n$.
*Como* $m+p < n+p$ *entonces existe* $p_1 \neq 0$ *en* $\mathbb{N}$ *tal que* $(m+p)+p_1 = n+p$.
*Por asociatividad y conmutatividad* $(m + p) + p_1 = (m + p_1) + p$, *luego* $(m + p_1) + p = n + p$. *Por la propiedad cancelativa de la suma concluimos que* $m + p_1 = n$, *es decir* $m < n$.

**Lema 3.15.** *Sean* $m, n, p \in \mathbb{N}$ *con* $p \neq 0$ *entonces* $m < n$ *si y solo si* $m * p < n * p$.

**Demostración.** *Para probar que si* $m < n$ *entonces* $m * p < n * p$ *fijamos* $m, n \in \mathbb{N}$ *tales que* $m < n$ *y definimos el conjunto*

$$Z = \{p \in \mathbb{N} | m * p < n * p\} \cup \{0\}.$$

*El elemento* 0 *pertenece a Z. Recordando que* $S(0) = 1$, $m*1 = m$ *y* $n*1 = n$ *obtenemos que* $m * 1 = m < n = n * 1$.
*Veamos que si* $p \in Z$ *entonces* $S(p) \in Z$.
*Por la propiedad* $(P2)$ *del producto obtenemos* $m * S(p) = (m * p) + m$. *Por el lema anterior y por hipótesis* $(m * p) + m < (n * p) + m$.
*Por la propiedad conmutativa de la suma* $(n * p) + m = m + (n * p)$, *por el lema anterior como* $m < n$ *entonces* $m + (n * p) < n + (n * p) = (n * p) + n$.
*Finalmente por transitividad probamos* $m * S(p) < (n * p) + n = n * S(p)$.
*Por el axioma de inducción se concluye que* $Z = \mathbb{N}$.
*Para demostrar que si* $m * p < n * p$ *entonces* $m < n$ *probaremos que si no se cumple que* $m < n$ *entonces no se cumplirá* $m * p < n * p$.
*Si no se cumple* $m < n$ *entonces, bien* $m = n$, *bien* $n < m$.
*Si* $m = n$ *entonces* $m * p = n * p$, *luego no se cumple* $m * p < n * p$.
*Si* $n < m$ *entonces hemos demostrado que* $n * p < m * p$, *luego no se cumple* $m * p < n * p$.

**Teorema 3.8.** ***(Teorema del buen orden).*** *Sea S un subconjunto no vacío de* $\mathbb{N}$ *entonces existe* $m \in S$ *tal que* $m \leq n$ *para todo* $n \in S$.

**Demostración.** *Sea* $A = \{n \in m|$ *si* $m < n$ *entonces* $m \notin S\}$.
*Veamos que* $A \neq \mathbb{N}$. *Si* $A = \mathbb{N}$ *entonces* $S \subset A$, *es decir si* $u \in S$ *entonces* $u \in A$. *Por otra parte* $u < S(u)$ *y* $u \in S$ *y por definición del conjunto A*

*vemos que $S(u) \notin A$.*
*Veamos que $A \neq \emptyset$. El elemento $0$ es un elemento de $A$ ya que no existe $m \in S$ tal que $m < 0$.*
*Por el axioma de inducción existe $r \in A$ tal que $S(r) \notin A$.*
*Como $r \in A$ entonces no existe ningún $m \in S$ tal que $m < S(r)$, por otra parte como $S(r) \notin A$ entonces existe algún $m \in S$ tal que $m < S(r)$, lo que implica que $r \in S$. Finalmente concluimos que $r \in S \cap A$ y para todo $p < r$ $p \notin S$.*

**Definición 3.12.** *Sea $S$ un conjunto no vacío de $\mathbb{N}$ llamamos elemento mínimo de $S$ al elemento $m \in S$ tal que $m \leq n$ para todo $n \in S$. Escribimos $mín(S)$ para denotar al mínimo del conjunto $S$.*
*Si todos los subconjuntos no vacíos de un conjunto tienen elemento mínimo diremos que ese conjunto es un conjunto bien ordenado. Observemos que $\mathbb{N}$ es un conjunto bien ordenado.*

**Teorema 3.9.** ***(Principio fuerte de inducción.)*** *El conjunto $S = \mathbb{N}$ es el único subconjunto de $\mathbb{N}$ que satisface la siguiente propiedad:*
*"Para cada $n \in \mathbb{N}$, si todo número natural menor que $n$ pertenece a $S$ entonces $n \in S$".*

**Demostración.** *Supongamos que existe un subconjunto $S$ de $\mathbb{N}$ tal que $S \neq \mathbb{N}$ que satisface la propiedad entrecomillada.*
*Como $S \subset \mathbb{N}$ y $S \neq \mathbb{N}$ entonces existe un elemento $x \in \mathbb{N}$ tal que*
*$x \notin S$($x$ es un elemeto que pertenece al complementario de $S$). Por lo tanto el complementario de $S$ es un conjunto no vacío y por el teorema del buen orden dicho conjunto tendrá un minímo $m$ tal que todo elemento $n \in S$ cumple $n < m$, luego $m \in S$ por la propiedad entrecomillada, lo que es una contradicción.*

**Teorema 3.10.** ***(División de números naturales.)*** *Sean $m, n \in \mathbb{N}$ tal que $n \neq 0$ entonces existen dos elementos $q, r \in \mathbb{N}$ tales que $m = n * q + r$ con $r < n$. Los elementos $q$ y $r$ que verifican $m = n * q + r$ son únicos y se denominan, respectivamente, cociente y resto de la división euclídea de $m$ entre $n$.*

**Demostración.** *Fijamos un número natural $n$ tal que $n \neq 0$ y definimos el conjunto $M_n = \{m \in \mathbb{N} |$ existen $q$ y $r$ que cumplen $m = n * q + r$ y $r < n\}$.*
*El elemeto $0 \in M_n$, ya que tomando $q = 0$ y $r = 0$ comprobamos que*
*$0 * n + 0 = 0$ y $0 < n$.*

*Veamos que si* $m \in M_n$ *entonces* $S(m) \in M_n$. *Como* $S(m) = m + 1$ *entonces* $S(m) = n * q + (r + 1) =$, *es decir* $S(m) = n * q + S(r)$. *Es necesario que* $S(r) < n$ *para que* $S(m) \in M_n$.
*Si* $S(r) < n$ *entonces hemos probado que* $S(m) \in M_n$. *En el caso contrario, bien* $S(r) = n$, *bien* $n < S(r)$.
*Si* $S(r) = n$ *entnoces* $S(m) = n*q+S(r) = n*q+n$, *utilizando la existencia de elemento unidad en el producto y la propiedad distributiva por la izquierda obtenemos* $S(m) = n * (q + 1) = n * S(q) + 0$, *luego* $S(m) \in M_n$.
*El caso* $n < S(r)$ *no puede darse ya que no existe* $n \in \mathbb{N}$ *tal que* $r < n$ *y* $n < r + 1$.
*Por el axioma de inducción* $M_n = \mathbb{N}$.
*Para demostrar que el cociente y el resto de m entre n son únicos supondremos que no lo son, es decir, supondremos que* $q_1$,$q_2$,$r_1$ *y* $r_2$ *son números naturales tales que* $m = n * q_1 + r_1$, $m = n * q_2 + r_2$, $r_1 < n$ *y* $r_2 < n$.
*Como* $m = n * q_1 + r_1$ *y* $m = n * q_2 + r_2$ *entonces* $n * q_1 + r_1 = n * q_2 + r_2$.
*Si no se cumple* $r_1 = r_2$ *entonces, o bien* $r_1 < r_2$, *o bien* $r_2 < r_1$. *Suponemos que* $r_1 < r_2$, *es decir, existe un* $p \neq 0$ *en* $\mathbb{N}$ *tal que* $r_1 + p = r_2$, *luego* $n*q_1+r_1 = n*q_2+(r_1+p)$, *por conmutatividad y por la propiedad cancelativa de la suma* $n * q_1 = n * q_2 + p$. *Como* $p \neq 0$ *entonces* $n * q_2 < n * q_1$ *luego* $q_2 < q_1$ *por el lema 3.15, por consiguiente* $S(q_2) \leq q_1$.
*Si* $S(q_2) < q_1$ *entonces por el lema 3.15* $S(q_2) * n < q_1 * n$ *y por el lema 3.14* $S(q_2) * n + r_1 < q_1 * n + r_1$.
*Por otra parte* $S(q_2) * n + r_1 = (q_2 + 1) * n + r_1 = (q_2 * n + n) + r_1$, *luego* $(q_2 * n + n) + r_1 < q_1 * n + r_1 = q_2 * n + r_2$, *es decir* $(q_2*n+n)+r_1 = (q_2*n)+(n+r_1) < q_2*n+r_2$. *Por el lema 3.14* $n+r_1 < r_2$ *y finalmente vemos que* $n \leq n + r_2 < r_2$ *contradice la propiedad* $r_2 < n$.
*Si* $S(q_2) = q_1$ *entonces* $q_2 + 1 = q_1$, *es decir* $n * (q_2 + 1) + r_1 = n * q_2 + r_2$. *Por la propiedad distributiva del producto y la propiedad cancelativa de la suma deducimos* $n + r_1 = r_2$, *luego* $n \leq r_2$, *lo que contradice* $r_2 < n$, *es decir* $r_1 = r_2$.
*Como* $r_1 = r_2$ *entonces por la propiedad cancelativa de la suma aplicada a la igualdad* $n * q_1 + r_1 = n * q_2 + r_2$ *obtenemos* $n * q_1 = n * q_2$. *Si* $q_1 < q_2$ *entonces existe un* $p \neq 0$ *en* $\mathbb{N}$ *tal que* $q_1 + p = q_2$, *luego* $n*q_1 = n*q_2 = n*(q_1+p) = n*q_1+n*p$. *Por la propiedad cancelativa de la suma* $0 = n * p$, *como* $n \neq 0$ *entonces* $p = 0$, *lo cual es absurdo. Permutando los papeles de* $q_1$ *y* $q_2$ *comprobamos que no se cumple* $q_2 < q_1$ *concluyendo que* $q_1 = q_2$.

# Bibliografía


*[1]* Cameron, Peter J.,*(1999) Sets, Logic and Categories, Gran Bretaña: Springer-Verlag.*

*[2]* Moschovakis, Yiannis,*(2006) Notes on Set Theory, Estados Unidos: Springer-Verlag.*

*[3]* Hajnal,A. y Hamburger, P.,*(1999) Set Theory, Reino Unido: Cambridge University Press.*

*[4]* José F. Fernando,J. Manuel Gamboa y María Belén Rodrǵuez,*(2011)Matemáticas VOLUMEN 1, Espaanz y Torres.*

*[5]* Notas del profesor Alexander Kovacec, Universidade Coimbra.

*[6]* Notas del profesor Ignacio Villa Solis, Universidad Complutense.

*[7]* Notas de los profesores José A.Alonso Jiménez Andrés Cordón Franco, Universidad de Sevilla.