Matemática Discreta

bosquejo de apuntes

Doble Grado en Ing. Informática y Matemáticas

Lógica y Métodos Discretos

Curso: 1º del Doble Grado

autor:
francisco miguel garcía olmedo

18 de noviembre de 2017

Índice general

1. Nociones sobre Conjuntos **7**

1.1. Axiomas de Extensión y de Especificación . . . 7
1.2. Parejas no Ordenadas . . . 9
1.3. Uniones e Intersecciones . . . 10
1.4. Complementos y Potencias . . . 11
1.5. Parejas Ordenadas . . . 13
1.6. Relaciones . . . 13
1.7. Relaciones de Equivalencia . . . 15
1.8. Funciones . . . 15
1.9. Familias . . . 20
1.10. Números . . . 21
1.11. Los Axiomas de Peano . . . 22
1.12. Aritmética . . . 23
1.13. Relaciones de Orden . . . 24
1.14. Axioma de Elección . . . 26
1.15. Números Enteros . . . 26
1.16. Inmersión de ω en Z . . . 27

2. Inducción **29**

2.1. Los Postulados de Peano y la inducción finita . . . 29
2.2. Equivalencia entre Principios . . . 30
2.3. Teorema de Recursión . . . 33
2.4. Ejercicios de Inducción . . . 35

3. Relaciones de Recurrencia **39**

3.1. Introducción. . . . 39
3.2. Teoría de la Recurrencia Lineal Homogénea . . . 41
3.3. Teoría de la Recurrencia Lineal No Homogénea . . . 46
3.4. Ejemplos de Recurrencia Lineal Homogénea . . . 51
3.5. Ejemplos de Recurrencia Lineal No Homogénea . . . 56
3.6. Ejercicios . . . 62

4. Lenguajes **65**

4.1. Signos y Palabras . . . 65
4.2. Palabras Significativas . . . 66
4.3. Caracterización de las Palabras Significativas . . . 67
4.4. Fórmulas de un Lenguaje Proposicional . . . 70

5. Lógica Proposicional **71**
5.1. Lenguaje Proposicional . . . 71
5.2. Implicación Semántica . . . 73
5.3. Propiedades Básicas de la Implicación Semántica . . . 80
5.4. Forma Normal Conjuntiva . . . 86
5.5. Algoritmo de Davis & Putnam . . . 92
5.6. Ejercicios de Lógica Proposicional . . . 93

6. Retículos y Álgebras de Boole **97**
6.1. Conjuntos Ordenados . . . 97
6.2. Retículos . . . 100
6.3. Retículos Distributivos . . . 102
6.4. Retículos Complementados . . . 104
6.5. Álgebra de Boole . . . 105
6.6. Teoremas Fundamentales del Álgebra de Boole . . . 108
6.7. Subálgebras e Isomorfismos . . . 112
6.8. Representación Atómica de las Álgebras de Boole Finitas . . . 114
6.9. Expresiones Booleanas . . . 119

A. Alfabeto Griego **127**

B. Leyes de la Lógica Clásica **129**

C. Fórmulas Lógicamente Equivalentes **133**

D. Prontuario de cálculo clásico proposicional y de primer orden **135**

E. Polinomio interpolatorio de Lagrange **143**

Índice de figuras

3.1. Elecciones de $u_n^{(p)}$ según $f(n)$, si r no es sol. de la ecuación característica. 59

5.1. Tabla bidimensional de $\rightarrow$. 74
5.2. Tablas para la interpretación semántica de los símbolos lógicos 75

6.1. Diagrama de orden para el conjunto ordenado $\mathcal{P}(U)$. 98
6.2. Diagrama de orden para el conjunto $\{2, 3, 4, 6, 8, 12, 36, 60\}$ ordenado por $|$. 99
6.3. Diagrama de Hasse del Diamante y el Pentágono. 104
6.4. Funciones de conmutación de 2 variables. 106
6.5. Álgebras de Boole $\mathbf{F}(\mathbf{B_2}, \mathbf{2})$ 107
6.6. Álgebras de Boole de 8 elementos. 107
6.7. Propiedades básicas de la igualdad entre expresiones. 122
6.8. Propiedades adicionales de la igualdad entre expresiones. 122

Capítulo 1

Nociones sobre Conjuntos

1.1. Axiomas de Extensión y de Especificación

En el presente desarrollo de los rudimentos de la *Teoría de Conjuntos* consideramos primitivo el concepto de *conjunto* así como el de *pertenencia*. Si x pertenece a A (x es un *elemento* de A, x está *contenido* en A) escribimos abreviadamente $x \in A$. Otro concepto primitivo referido a conjuntos es el de la igualdad. El hecho de que dos conjuntos A y B sean iguales se representa simbólicamente como $A = B$. Es **imprescindible** para lo que sigue **suponer** que **existe al menos un conjunto**.

Existe una relación entre la pertenencia y la igualdad. Dicha relación queda explicitada en el siguiente principio que admitimos sin demostración.

Axioma 1 (de Extensión)**.** *Dos conjuntos son iguales si, y sólo si, tienen los mismos elementos.*

En definitiva, lo que estamos admitiendo es que un conjunto queda determinado por sus elementos. Esta no es una propiedad trivial, hay objetos que, tomados en lugar de los conjuntos, no la cumplen. Por ejemplo, "los ancestros de un ser humano". Acontece que hay seres humanos que teniendo los mismos ancestros no son idénticos. En efecto, si dos seres humanos son el mismo tienen los mismo ancestros (ésta es la parte "sólo si" y es verdadera); pero dos hermanos tienen los mismos ancestros y no son iguales (ésta es la parte "si" y es falsa).

Definición 1.1.1. El conjunto A es un *subconjunto* del conjunto B, si para todo x tal que $x \in A$ se cumple que $x \in B$. En este caso también decimos que A está *incluido* en B o que B *incluye* a A. Este hecho es representado como $A \subseteq B$. A es un subconjunto propio de B si $A \subseteq B$ y $A \neq B$.

Lema 1.1.1. *Sean A, B y C conjuntos. Entonces:*

1. $A \subseteq A$.
2. *Si* $A \subseteq B$ *y* $B \subseteq A$ *entonces* $A = B$.
3. *Si* $A \subseteq B$ *y* $B \subseteq C$ *entonces* $A \subseteq C$.

Lema 1.1.2. *Sean A, B y C tres conjuntos. Entonces:*

1. $A = A$.
2. *Si* $A = B$ *entonces* $B = A$.
3. *Si* $A = B$ *y* $B = C$ *entonces* $A = C$.

Todos los principios básicos de la teoría de conjuntos, con la sola excepción del *Axioma de Extensión*, están diseñados para la formación de nuevos conjuntos a partir de los originales. El primero y más importante de estos principios básicos en la manufactura de conjuntos dice, hablando toscamente, que cualquier cosa sensata que puede uno proponer para los elementos de un conjunto, define un conjunto, a saber, el subconjunto de aquellos elementos para los cuales la proposición es verdadera.

Ejemplo 1.1.1. Antes de formular este principio en términos precisos, enfocaremos un ejemplo heurístico. Sea A el conjunto de todos los hombres. La frase "x es casado" es verdadera para algunos de los elementos x de A y falsa para otros. El principio que estamos ilustrando es aquel que justifica el paso del conjunto A al subconjunto especificado por la cláusula dada (o sea, al conjunto de todos los hombres casados). La caracterización del subconjunto se indica usualmente con la notación

$$\{x \in A : x \text{ es casado}\}$$

Análogamente

$$\{x \in A : x \text{ no es casado}\}$$

es el conjunto de todos los solteros;

$$\{x \in A : \text{el padre de } x \text{ es } Adam\}$$

es el cojunto que contiene a *Caín* y *Abel* y nada más; y

$$\{x \in A : x \text{ es el padre de } Abel\}$$

es el conjunto que contiene a *Adam* y nada más.

Observación 1.1.1. Cuidado: una caja que contiene un sombrero y nada más, no es lo mismo que un sombrero y, análogamente, el último conjunto de la anterior lista de ejemplos no debe ser confundido con *Adam*. La analogía entre conjuntos y cajas tiene muchos puntos débiles, pero, a veces, proporciona un cuadro útil de las situación.

Definición 1.1.2. Una *proposición atómica* o *condición atómica* es una expresión de cualquiera de los tipos siguientes:

1. $x \in A$ (condición de pertenencia)
2. $A = B$ (condición de igualdad)

Definición 1.1.3 (*Proposición*)**.** Una *proposición* o *condición* es cualquier frase de uno de los tipos siguientes, y sólo de esos:

1. Una proposición atómica
2. "P o Q"
3. "P y Q"
4. "no P"
5. "si P, entonces Q"
6. "P si, y sólo si, Q"
7. "Existe x tal que P", abreviadamente "Existe x (P)"
8. "Para todo x, P", "Para todo x (P)"

donde tanto P como Q son proposiciones y x es una letra.

Observación 1.1.2. La condición "no $x \in A$" (resp. "no $A = B$") se representa usalmente como "$x \notin A$" (resp. "$A \neq B$").

Axioma 2 (de Especificación)**.** *A todo conjunto A y a toda condición $S(x)$ corresponde un conjunto B cuyos elementos son precisamente (exactamente) aquellos elementos x de A para los cuales se cumple $S(x)$.*

Observación 1.1.3. En el *axioma de especificación*, el simbolismo $S(x)$ se emplea queriendo indicar que la letra x es libre en la frase $S(x)$, es decir, x ocurre en $S(x)$ al menos una vez sin que haya sido introducida por alguna de las expresiones "existe x" o "para todo x".

Observación 1.1.4. Para representar al conjunto B al que se refiere el *axioma de especificación* usamos la notación $B = \{x \in A : S(x)\}$

Teorema 1.1.3. *No existe un conjunto que contenga a todos los conjuntos*

Demostración. Sea A un conjunto arbitrario y $S(x)$ la proposición $x \notin x$. A partir de A y $S(x)$ surge, por el axioma de especificación, el conjunto $B = \{x \in A : x \notin x\}$. Si $B \in A$, entonces, o $B \in B$ o bien $B \notin B$. En el primer caso, y dado que suponemos que $B \in A$, se tendrá que $B \notin B$ lo cual es absurdo. En el segundo caso se deduce que $B \in B$, lo que también es absurdo. Por tanto $B \notin A$ y hemos demostrado lo que se quería. □

Observación 1.1.5. Los clásicos leyeron el enunciado del Teorema 1.1.3 como "no hay universo" usando la palabra universo en el sentido de "universo de discurso", lo cual significa, en cualquier discusión particular, un conjunto que contiene a todos los objetos que intervienen en ese estudio. En tratamientos más antiguos (preaxiomáticos) a la teoría de conjuntos, se daba por supuesta la existencia de un universo, y el razonamiento anterior se conocía como *la paradoja de Russell*. La moraleja es que es imposible, especialmente en matemáticas, obtener algo a partir de nada. Para especificar un conjunto no basta pronunciar algunas palabras mágicas (las cuales pueden formar una frase tal como "$x \notin x$"); es necesario también disponer de un conjunto a cuyos elementos puedan aplicarse esas palabras mágicas.

1.2. Parejas no Ordenadas

Lema 1.2.1. *Existe un conjunto que no tiene elementos.*

Demostración. Sea A un conjunto —recordar que estamos suponiendo que existe al menos uno— y la proposición $x \neq x$. Por el axioma de especificación $B = \{x \in A : x \neq x\}$ es un conjunto y no puede tener elementos. □

Observación 1.2.1. El conjunto al que se refiere el Lema 1.2.1 es representado por el símbolo $\varnothing$. Utilizamos el artículo determinado porque según el axioma de extensión no puede haber otro conjunto que no tenga elemento alguno salvo $\varnothing$.

Lema 1.2.2. *Para todo conjunto A se cumple, $\varnothing \subseteq A$.*

Demostración. Si dado A, $\varnothing$ no fuera un subconjunto de A entonces existiría $x \in \varnothing$ tal que $x \notin A$ y esto es imposible porque $\varnothing$ no tiene elementos. Por tanto, $\varnothing \subseteq A$. □

¿Habrá suficientes conjuntos como para garantizar que todo conjunto es elemento de otro? ¿Y qué hay acerca de dos, tres o cuatro conjuntos? Necesitamos el siguiente axioma.

Axioma 3 (de Apareamiento)**.** *Para dos conjuntos cualesquiera hay otro al que pertenecen ambos.*

Lema 1.2.3. *Dados dos conjuntos a y b existe el conjunto que los tiene exactamente a ellos como elementos y lo representamos por $\{a, b\}$.*

Demostración. Por el axioma de apareamiento sea A un conjunto del que a y b son elementos. Por el axioma de especificación $\{x \in A : x = a \text{ o } x = b\}$ es un conjunto y no tiene más elementos que a a y b. □

Definición 1.2.1. Si a es un conjunto, al conjunto $\{a, a\}$ lo representamos por $\{a\}$ y nos referimos a él como *el simplete* de a.

Observación 1.2.2. Decir $\{a\} \subseteq A$ es equivalente a decir $a \in A$.

Ejemplo 1.2.1. Son ejemplos de conjuntos los siguientes: $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, $\{\{\{\varnothing\}\}\}$ y $\{\varnothing, \{\varnothing\}\}$.

1.3. Uniones e Intersecciones

Axioma 4 (de las Uniones)**.** *Para toda colección $\mathcal{C}$ de conjuntos existe un conjunto U tal que si $x \in X$ y $X \in \mathcal{C}$ entonces $x \in U$.*

Definición 1.3.1. Dada una colección de conjuntos $\mathcal{C}$, por el axioma de especificación y el de las uniones, existe el conjunto A que contiene exactamente a los elementos que pertenecen cuando menos a uno de los conjuntos de la colección dada. A es representado como $\bigcup \mathcal{C}$, o bien $\bigcup \{X : X \in \mathcal{C}\}$, o bien $\bigcup_{X \in \mathcal{C}} X$. Se le denomina la *unión* de los elementos de $\mathcal{C}$.

Lema 1.3.1. $\bigcup \varnothing = \varnothing$ *y* $\bigcup \{A\} = A$.

Observación 1.3.1. El conjunto $\bigcup \{X : X \in \{A, B\}\}$ se representa como $A \cup B$. Por tanto $A \cup B = \{x : x \in A \text{ o } x \in B\}$.

Teorema 1.3.2. *Para todo conjunto A, B y C se cumplen las siguientes propiedades:*

1. $A \cup \varnothing = A$
2. $A \cup B = B \cup A$ *(conmutatividad)*
3. $A \cup (B \cup C) = (A \cup B) \cup C$ *(asociatividad)*
4. $A \cup A = A$ *(idempotencia)*
5. $A \subseteq B$ *si, y sólo si,* $A \cup B = B$.

Observación 1.3.2. Es muy sugestivo el hecho de que $\{a, b\} = \{a\} \cup \{b\}$ y generalizando tendríamos $\{a, b, c\} = \{a\} \cup \{b\} \cup \{c\}$.

Definición 1.3.2. Dados dos conjuntos A y B definimos el conjunto *intersección* de ambos, que será notado como $A \cap B$ por la siguiente igualdad:

$$A \cap B = \{x \in A : x \in B\}$$

Teorema 1.3.3. *Para todo conjunto A, B y C se cumplen las siguientes propiedades:*

1. $A \cap \varnothing = \varnothing$
2. $A \cap B = B \cap A$ *(conmutatividad)*
3. $A \cap (B \cap C) = (A \cap B) \cap C$ *(asociatividad)*
4. $A \cap A = A$ *(idempotencia)*
5. $A \subseteq B$ *si, y sólo si,* $A \cap B = A$.

Definición 1.3.3. Dos conjuntos A y B son *disjuntos* si se cumple $A \cap B = \varnothing$.

Teorema 1.3.4 (leyes distributivas)**.** *Para todo conjunto A, B y C se cumple:*

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Observación 1.3.3. El concepto de intersección puede definirse para familias *no vacías* cualesquiera. El formato de esta definición es totalmente análogo al utilizado para la definición de unión.

Corolario 1.3.5. *Para todo conjunto A, B y C son equivalentes las siguientes afirmaciones:*

1. $(A \cap B) \cup C = A \cap (B \cup C)$
2. $(A \cap B) \cup C = A \cap (B \cup C)$ *sii* $C \subseteq A$

1.4. Complementos y Potencias

Definición 1.4.1. Dados dos conjuntos A y B la *diferencia* entre A y B, o también el *complemento relativo* de B respecto a A, es el conjunto $A \setminus B$ definido por:

$$A \setminus B = \{x \in A : x \notin B\}$$

Observación 1.4.1. Para contar con cierta facilidad en la exposición de los hechos básicos referidos al complemento relativo, supondremos que todos los conjuntos mencionados en esta sección son subconjuntos de un mismo conjunto E y que todos los complementos se forman con respecto a E. Esto no es esencial; pero la situación descrita es también la más frecuente. Puesto que E es fijo, resulta cómodo abreviar la notación escribiendo A' en lugar de $E \setminus A$.

Teorema 1.4.1. *Sean A y B conjuntos. Se cumple:*

1. $(A')' = A$
2. $\varnothing' = E$ *y* $E' = \varnothing$
3. $A \cap A' = \varnothing$ *y* $A \cup A' = E$
4. $A \subseteq B$ *si, y sólo si,* $B' \subseteq A'$.

Teorema 1.4.2 (leyes de De Morgan)**.** *Sean A y B conjuntos. Entonces:*

1. $(A \cup B)' = A' \cap B'$
2. $(A \cap B)' = A' \cup B'$

Observación 1.4.2. Las leyes de De Morgan se cumplen también para uniones e intersecciones de colecciones más grandes de conjuntos y no sólo para parejas. Esto conlleva que en la teoría, cuando se tiene un teorema, si en una ecuación o una inclusión concerniente a uniones, intersecciones y complementos de subconjuntos de E, reemplazamos cada conjunto por su complemento, intercambiamos uniones e intersecciones e invertimos todas las inclusiones, el resultado es otro teorema. Este hecho es conocido como *principio de dualidad* para conjuntos.

Teorema 1.4.3. *Sean A, B y C conjuntos. Entonces:*

1. $A \setminus B = A \cap B'$
2. $A \subseteq B$ *si, y sólo si,* $A \setminus B = \varnothing$.
3. $A \setminus (A \setminus B) = A \cap B$

4. $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$
5. $A \cap B \subseteq (A \cap C) \cup (B \cap C')$
6. $(A \cup C) \cap (B \cup C') \subseteq A \cup B$

Definición 1.4.2. Si A y B son conjuntos, la *diferencia simétrica* o *suma booleana* de A y B es el conjunto $A + B$ definido por la siguiente igualdad:

$$A + B = (A \setminus B) \cup (B \setminus A)$$

Teorema 1.4.4. *Sean A, B y C conjuntos. Entonces se cumple:*

1. $A + B = B + A$
2. $A + (B + C) = (A + B) + C$
3. $A + \varnothing = A$ *y* $A + A = \varnothing$
4. $A + B = (A \cup B) \setminus (A \cap B)$
5. $A \cap (B + C) = (A \cap B) + (A \cap C)$

Axioma 5 (de las potencias)**.** *Para cada conjunto existe una colección de conjuntos que contiene entre sus elementos a todos los subconjuntos del conjunto dado.*

Observación 1.4.3. En otras palabras, si E es un conjunto, entonces existe un conjunto $\mathcal{P}$ tal que si $X \subseteq E$, entonces $X \in \mathcal{P}$.

Observación 1.4.4. El conjunto descrito anteriormente puede ser más extenso de lo deseado, ya que puede contener otros elementos además de los subconjuntos de E. Esto se remedia fácilmente; basta aplicar el axioma de la especificación para formar el conjunto $\mathcal{P}(E)$ definido por la siguiente igualdad

$$\mathcal{P}(E) = \{X \in \mathcal{P} : X \subseteq E\}$$

Definición 1.4.3. Dado un conjunto E, el conjunto $\mathcal{P}(E)$ le denominamos *conjunto potencia* o *conjunto de partes* de E.

Ejemplo 1.4.1.

1. $\mathcal{P}(\varnothing) = \{\varnothing\}$
2. $\mathcal{P}(\{a\}) = \{\varnothing, \{a\}\}$
3. $\mathcal{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$

Teorema 1.4.5. *Sean A y B conjuntos. Entonces:*

1. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$
2. $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$
3. *Si* $A \subseteq B$, *entonces* $\mathcal{P}(A) \subseteq \mathcal{P}(B)$
4. $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ *si, y sólo si,* $A \subseteq B$ *o* $B \subseteq A$.
5. $\varnothing = \bigcap_{X \in \mathcal{P}(A)} X$
6. $A = \bigcup_{X \in \mathcal{P}(A)} X$
7. $A \subseteq \mathcal{P}(\bigcup_{X \in A} X)$

Ejercicio 1.4.1. Sean A, B, C conjuntos. Demostrar las siguientes propiedades:

1. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
2. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
3. $A = B$ siempre que $A + C = B + C$
4. $A \cap (B + C) = (A \cap B) + (A \cap C)$
5. $B \subseteq C$ siempre que $A \cup B \subseteq A \cup C$ y $A \cap B \subseteq A \cap C$.

1.5. Parejas Ordenadas

Definición 1.5.1. Dados a y b, la *pareja ordenada* de a y b, con primera coordenada a y segunda coordenada b, es el conjunto $\langle a, b\rangle$ definido por la igualdad:

$$\langle a, b\rangle = \big\{\{a\}, \{a, b\}\big\}$$

Teorema 1.5.1. *Si $\langle a, b\rangle$ y $\langle x, y\rangle$ son parejas ordenadas y $\langle a, b\rangle = \langle x, y\rangle$ entonces $a = x$ y $b = y$.*

Observación 1.5.1. Supongamos que A y B son conjuntos y que $a \in A$ y $b \in B$. Se cumple $\{a\} \subseteq A$ y $\{b\} \subseteq B$, por lo que $\{a, b\} \subseteq A \cup B$. Como $\{a\} \subseteq A \cup B$, entonces tenemos $\big\{\{a\}, \{a, b\}\big\} \subseteq \mathcal{P}(A \cup B)$, en otras palabras, $\big\{\{a\}, \{a, b\}\big\} \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big)$.

Definición 1.5.2. Sean A y B dos conjuntos. El *producto cartesiano* de A por B, $A \times B$, es el conjunto definido por la siguiente igualdad:

$$A \times B = \{\langle a, b\rangle : a \in A \text{ y } b \in B\}$$

Observación 1.5.2. El producto cartesiano de dos conjuntos y cualquier subconjunto suyo es un conjunto de parejas ordenadas,

Teorema 1.5.2. *Sean A y B dos conjuntos. $A \times B \subseteq \mathcal{P}\big(\mathcal{P}(A \cup B)\big)$.*

Ejercicio 1.5.1. Sean A, B, X e Y cuatro conjuntos. Entonces:

1. $(A \cup B) \times X = (A \times X) \cup (B \times X)$
2. $(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times Y)$
3. $(A \setminus B) \times X = (A \times X) \setminus (B \times X)$
4. Si $A = \varnothing$ o $B = \varnothing$ entonces $A \times B = \varnothing$
5. Si $A \subseteq X$ y $B \subseteq Y$, entonces $A \times B \subseteq X \times Y$ y recíprocamente (siempre que $A \times B \neq \varnothing$ o $A = B = \varnothing$)

1.6. Relaciones

En esta sección, y en lo que resta, emplearemos la palabra "relación" en lugar de emplear la expresión "relación binaria".

Definición 1.6.1. Una *relación* es cualquier conjunto, R de parejas ordenadas.

Observación 1.6.1. Si R es una relación y $\langle x, y\rangle \in R$, escribiremos para abreviar xRy y leeremos *x está relacionado con y mediante R*, o más sintéticamente *x está R con y*.

Ejemplo 1.6.1.

1. El conjunto $\varnothing$ es una relación.
2. Dados dos conjuntos X e Y, el conjunto $X \times Y$ es una relación. En particular, si X es un conjunto entonces $X \times X$ es una relación. A está última relación se la representa frecuentemente con el símbolo $\nabla(X)$ o simplemente ∇ si no hay peligro de confusión.
3. Si X es un conjunto no vacío, entonces $\{\langle x, y\rangle \in X \times X : x = y\}$ es una relación. Tal relación es denominada *la diagonal de* X y se representa como $\Delta(X)$ o simplemente Δ. Nótese que a esta relación se le podría llamar *la igualdad* en X y en ambos casos el artículo determinado está plenamente justificado.
4. Sea X un conjunto y sea R el conjunto:

   $$\{\langle x, A\rangle \in X \times \mathcal{P}(X) : x \in A\}$$

   Esta relación es la de pertenencia entre elementos de X y subconjuntos de X. En efecto, si $x \in X$ y $A \in \mathcal{P}(X)$, xRA significa lo mismo que $x \in A$.

Teorema 1.6.1. *Sea R una relación. $R \subseteq A \times A$, donde $A = \bigcup\bigcup R$.*

Ejemplo 1.6.2. Sea $X = \{a, b\}$. Entonces:

- $\mathcal{P}(X) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$
- La relación de pertenencia R es:

  $$\{\langle a, \{a\}\rangle, \langle b, \{b\}\rangle, \langle a, \{a, b\}\rangle, \langle b, \{a, b\}\rangle\},$$

  o sea,

  $$\{\{\{a\}, \{a, \{a\}\}\}, \{\{b\}, \{b, \{b\}\}\}, \{\{a\}, \{a, \{a, b\}\}\}, \{\{b\}, \{b, \{a, b\}\}\}\}$$

Se tiene entonces

$$\bigcup R = \{\{a\}, \{b\}, \{a, \{a\}\}, \{b, \{b\}\}, \{a, \{a, b\}\}, \{b, \{a, b\}\}\}$$

y

$$\bigcup\bigcup R = \{a, b, \{a\}, \{b\}, \{a, b\}\}$$

Si $A = \bigcup\bigcup R$, claramente se tiene $R \subseteq A \times A$.

Definición 1.6.2. Dada una relación R hay dos conjuntos distinguidos asociados a ella, a saber, su *dominio*, $\operatorname{dom} R$, y su *rango* o *codominio*, $\operatorname{ran} R$. Esto conjuntos quedan definidos por las siguientes igualdades:

$$\operatorname{dom} R = \{x : \text{existe } y(xRy)\} \qquad \text{y} \qquad \operatorname{ran} R = \{y : \text{existe } x(xRy)\}$$

A estos conjuntos también se les llama *proyecciones* de R sobre la primera y segunda coordenada respectivamente.

Ejemplo 1.6.3.

1. $\operatorname{dom} \varnothing = \varnothing$ y $\operatorname{ran} \varnothing = \varnothing$.
2. $\operatorname{dom} X \times Y = X$ y $\operatorname{ran} X \times Y = Y$.
3. $\operatorname{dom} \Delta(X) = X$ y $\operatorname{ran} \Delta(X) = X$.
4. Si R es la pertenencia en X entonces $\operatorname{dom} R = X$ y $\operatorname{ran} R = \mathcal{P}(X) \setminus \{\varnothing\}$.

Observación 1.6.2. Si la relación R es tal que $R \subseteq A \times B$, solemos decir que R es una relación de A a B, y si $A = B$, que R es una relación en A.

1.7. Relaciones de Equivalencia

Definición 1.7.1. Una relación R en un conjunto A es *reflexiva* si xRx, para todo $x \in A$, en otras palabras, si $\Delta(A) \subseteq R$. Es *simétrica* si xRy implica yRx y es *transitiva* si xRy e yRz implican xRz. Una relación que sea reflexiva, simétrica y transitiva se denomina *relación de equivalencia.*

Ejemplo 1.7.1. Dado un conjunto A, $\Delta(A)$ y $\nabla(A)$ son relaciones de equivalencia.

Ejercicio 1.7.1. Para cada una de las propiedades de la definición 1.7.1 encontrar una relación que cumpla dos de ellas y no cumpla la restante.

Definición 1.7.2. Sea A un conjunto. $\mathcal{C} \subseteq \mathcal{P}(A)$ es una *partición* de A si

1. Para todo $X \in \mathcal{C}$, $X \neq \varnothing$.
2. Para todo $X, Y \in \mathcal{C}$, si $X \neq Y$ entonces $X \cap Y = \varnothing$ (los elementos de $\mathcal{C}$ son disjuntos dos a dos).
3. $\bigcup_{X \in \mathcal{C}} X = A$

Definición 1.7.3. Sea R una relación de equivalencia en A. Para todo $x \in A$, el conjunto x/R, llamado *clase de equivalencia* de x por R, se define mediante la siguiente igualdad:

$$x/R = \{y \in A : \langle x, y\rangle \in R\}$$

usualmente se representa por A/R al conjunto de todas las clases de equivalencia y se le llama *conjunto conciente* de A por R.

Observación 1.7.1. Observar que para que A/R sea un conjunto es preciso disponer de un conjunto entre cuyos elementos escoger a los suyos y una fórmula para escogerlos. Consideremos la fórmula $S(X)$ siguiente "existe a tal que para todo y, $y \in X$ si, y sólo si, $\langle a, y\rangle \in R$". A/R sería pues $\{X \in \mathcal{P}(A) : S(X)\}$. Esto justifica que A/R es un conjunto.

Lema 1.7.1. *Sea A un conjunto y R una relación de equivalencia en A. El conjunto A/R es una partición de A.*

Definición 1.7.4. Sea A un conjunto y $\mathcal{C}$ una partición de A. La relación $A/\mathcal{C}$ es la definida por $xA/\mathcal{C}y$ si, y sólo si, existe $X \in \mathcal{C}$ tal que $x \in X$ e $y \in X$.

Lema 1.7.2. *Sea A un conjunto y $\mathcal{C}$ una partición de A. La relación $A/\mathcal{C}$ es una relación de eqivalencia.*

Teorema 1.7.3. *Sea A un conjunto y R una relación de equivalencia en A. Entonces $R = A/(A/R)$.*

Teorema 1.7.4. *Sea A un conjunto y $\mathcal{C}$ una partición de A. Entonces $\mathcal{C} = A/(A/\mathcal{C})$.*

1.8. Funciones

Definición 1.8.1. Sean X e Y conjuntos. Una *función* de X en Y es una relación f tal que $\operatorname{dom} f = X$ y tal que para cada $x \in X$ existe un único $y \in Y$ tal que $\langle x, y\rangle \in f$. La condición de unicidad se puede expresar también diciendo que si $\langle x, y\rangle \in f$ y $\langle x, z\rangle \in f$ entonces $y = z$. Para cada $x \in X$, el único $y \in Y$ tal que $\langle x, y\rangle \in f$ se representa como $f(x)$. El elemento y es conocido como el *valor* que la función f toma para el *argumento* x. Se dice también que f transforma a x en y

Observación 1.8.1. En lo sucesivo, si f es una función escribiremos $f(x) = y$ en lugar de $\langle x, y\rangle \in f$ o su variante xfy.

Observación 1.8.2. Las palabras *transformación*, *correspondencia* y *operador* son algunas de las muchas palabras que se usan como sinónimos de *función*. El símbolo

$$f\colon X \longrightarrow Y$$

se usa muy frecuentemente como abreviatura de "f es una función de X en Y". El conjunto de todas las funciones de X en Y es un subconjunto del conjunto $\mathcal{P}(X \times Y)$ y será denotado por Y^X.

Observación 1.8.3. Según nuestra definición, una función *no hace* nada sino que simplemente es. Muchos quedan insatisfechos con ésto, toda vez que el nombre de función y sus sinónimos más usados tienen un matiz de actividad. En estos círculos el término "función" queda para un objeto indefinido que de alguna manera es activo y llaman *gráfica* a lo que nosotros llamanos función.

Dada una función $f\colon X \longrightarrow Y$, es claro que $\operatorname{dom} f = X$. Sin embargo del rango no se puede afirmar en general más que $\operatorname{ran} f \subseteq Y$. Basándose en esto surgen las siguientes definiciones.

Definición 1.8.2. Sea $f\colon X \longrightarrow Y$ una función. Asociadas a f existen dos funciones

$$f_*\colon \mathcal{P}(X) \longrightarrow \mathcal{P}(Y) \text{ y } f^*\colon \mathcal{P}(Y) \longrightarrow \mathcal{P}(X)$$

definidas como sigue:

- Para todo $A \in \mathcal{P}(X)$, $f_*(A) = \{y \in Y\colon \text{ existe } x \in A \text{ tal que } f(x) = y\}$.
- Para todo $B \in \mathcal{P}(Y)$ $f^*(B) = \{x \in X\colon f(x) \in B\}$.

A f_* (resp. f^*) se le llama *imagen directa* (resp. *imagen inversa*) mediante f.

Observación 1.8.4. En la práctica, siempre que no haya peligro de confusión con los conceptos vistos y lo que vienen, muchos escribe f en lugar de f_* y f^{-1} en lugar de f^*. Nosotros no seguiremos aquí tal convenio.

Teorema 1.8.1. *Sea $f\colon X \longrightarrow Y$ una aplicación y $A, B \in \mathcal{P}(X)$. Entonces:*

1. $f_*(A \cup B) = f_*(A) \cup f_*(B)$
2. $f_*(A \cap B) \subseteq f_*(A) \cap f_*(B)$
3. $A \subseteq f^*\big(f_*(A)\big)$

Teorema 1.8.2. *Sea $f\colon X \longrightarrow Y$ una aplicación y $C, D \in \mathcal{P}(Y)$. Entonces:*

1. $f^*(C \cup D) = f^*(C) \cup f^*(D)$
2. $f^*(C \cap D) = f^*(C) \cap f^*(D)$
3. $f^*(Y \setminus B) = X \setminus f^*(B)$
4. $f^*\big(f_*(C)\big) \subseteq C$

Observación 1.8.5. Si $f\colon X \longrightarrow Y$ es una función, nótese que $\operatorname{ran} f = f_*(X)$ y que $f^*(Y) = X$. Sin embargo, no tiene porqué darse la igualdad $f_*(X) = Y$.

Definición 1.8.3. Sea $f\colon X \longrightarrow Y$ una función. f es *sobreyectiva* si $f_*(X) = Y$ y es *inyectiva* si para todo $y \in Y$, el conjunto $f^*(\{y\})$ es un simplete siempre que no sea vacío. Una función que sea simultáneamente inyectiva y sobreyectiva se denomina *biyectiva* o *biyección*.

Lema 1.8.3. *Sea $f\colon X \longrightarrow Y$ una función. Entonces son equivalentes las siguientes afirmaciones:*

1. *f es sobreyectiva*

2. *Para todo* $B \in \mathcal{P}(Y) \setminus \{\varnothing\}$, $f^*(B) \neq \varnothing$

3. *Para todo* $C \subseteq Y$, $f_*\big(f^*(C)\big) = C$.

Lema 1.8.4. *Sea* $f: X \longrightarrow Y$ *una función. Entonces son equivalentes las siguientes afirmaciones:*

1. f *es inyectiva*

2. *Para todo* $x, y \in A$, *si* $x \neq y$ *entonces* $f(x) \neq f(y)$.

3. *Para todo* $x, y \in A$, *si* $f(x) = f(y)$ *entonces* $x = y$.

4. *Para todo* $A \subseteq X$, $A = f^*\big(f_*(A)\big)$.

Ejemplo 1.8.1.

1. Si X es un subconjunto del conjunto Y, la aplicación $i: X \longrightarrow Y$ definida mediante $i(x) = x$ es un ejemplo de aplicación inyectiva que recibe el nombre particular de *inclusión*. En el caso en que el conjunto Y sea el propio conjunto X, a i se le llama *identidad* en X y se le representa por I_X o simplemente I.

2. Sea X un conjunto y R una relación de equivalencia en X. La aplicación $\pi: X \longrightarrow X/R$ definida por $\pi(x) = x/R$ es una función sobreyectiva, que recibe el nombre de *proyección canónica*, o simplemente *proyección*, de X en X/R.

3. Sean X e Y dos conjuntos, la aplicación $p_X: X \times Y \longrightarrow X$ definida por $p_X(x, y) = x$ es la función conocida como *proyección* de $X \times Y$ sobre la primera coordenada. Por supuesto que existe la proyección sobre la segunda coordenada y se define de forma análoga. Obsérvese que hemos escrito $p_X(x, y)$ cuando el rigor exige escribir $p_X(\langle x, y\rangle)$. Sin embargo, "todo el mundo" comete este abuso de notación con el fin de facilitar la escritura y dado que no hay peligro de confusión.

4. Sea $f: X \longrightarrow Y$ una función sobreyectiva. Sea g la aplicación de Y en $\mathcal{P}(X)$ tal que para cada $y \in Y$, $g(y)$ represente al conjunto de los $x \in X$ tales que $f(x) = y$. Entonces g es inyectiva, es decir, para todo u y v de Y, si $u \neq v$ entonces $g(u) \neq g(v)$.

Observación 1.8.6. La frase "la función f definida por..." es muy común cuando la condición que viene en lugar de los puntos suspensivos define inequívocamente a f y sólo a f. En la práctica usual de las matemáticas se define una función dando su dominio y describiendo, de forma unívoca, el valor y correspondiente a cada valor x.

Ejercicio 1.8.1. Demostrar que la proyección canónica no es en general inyectiva. Caracterizar a las relaciones de equivalencia tales que la proyección asociada es inyectiva.

Definición 1.8.4. Sea $f: X \longrightarrow Y$ una función y $A \subseteq X$. La función $g: A \longrightarrow Y$ definida por $g(x) = f(x)$, para todo $x \in A$ se denomina la *restricción* de f a A y se representa por $f|A$. Así pues $(f|A)(x) = f(x)$, para todo $x \in A$. A f se le llama *extesión* de g a X.

Observación 1.8.7. De la misma forma que la restricción de una función a un subconjunto de su dominio es única, las extensiones de una función pueden ser múltiples.

Definición 1.8.5. Sea $f: X \longrightarrow Y$ una función. Sea R_f la relación en X definida como aR_fb si, y sólo si, $f(a) = f(b)$.

Lema 1.8.5. *Sea* $f: X \longrightarrow Y$ *una función. La relación* R_f *es de equivalencia en* X.

Observación 1.8.8. En los ejemplos 1.8.1, el ejemplo 4 es tal que para cada $u \in Y$, $g(u)$ es una clase de equivalencia de R_f.

Definición 1.8.6. Llamemos temporalmente 2 al conjunto $\{0,1\}$. Sea X un conjunto y $A \subseteq X$. La *función característica* asociada a A, representada por χ_A, es la aplicación de X en 2 definida como

$$\chi_A(x) = \begin{cases} 1, \text{ si } x \in A, \\ 0, \text{ si } x \in X \setminus A. \end{cases}$$

Teorema 1.8.6. *Sea X un conjunto no vacío y $A, B \subseteq X$. Entonces:*

1. $\chi_A = \chi_B$ *si, y sólo si,* $A = B$.
2. $\chi_{A'} = 1 - \chi_A$.
3. $\chi_{A \cap B} = \chi_A \cdot \chi_B$.
4. $\chi_{A \cup B} + \chi_{A \cap B} = \chi_A + \chi_B$.
5. $\chi_{A \setminus B} = \chi_A - \chi_A \cdot \chi_B$.

Teorema 1.8.7. *Sea X un conjunto. La aplicación de $\mathcal{P}(X)$ en 2^X que a cada $A \subseteq X$ le asocia χ_A es una biyección.*

Ejercicio 1.8.2. Demostrar que:

1. $Y^{\varnothing}$ tiene exactamente un elemento, a saber, $\varnothing$, sea Y vacío o no.
2. Si X no es vacío entonces $\varnothing^X$ es vacío.

Observación 1.8.9. Si $f: X \longrightarrow Y$ es inyectiva entonces para todo $y \in \operatorname{ran} f$, $f^*(\{y\})$ es un conjunto con un elemento, a saber, $\{x\}$. En esta situación tiene sentido la siguiente definición.

Definición 1.8.7. Sea $f: X \longrightarrow Y$ una función inyectiva. Definimos la función $f^{-1}: \operatorname{ran} f \longrightarrow X$ como $f^{-1}(y) = x$ si, y sólo si, $f(x) = y$.

Definición 1.8.8. Sean X, Y y Z conjuntos y $f: X \longrightarrow Y$ y $g: W \longrightarrow Z$ funciones tales que $\operatorname{ran} f \subseteq \operatorname{dom} g$ entonces representamos por $g \circ f$ a la función de X en Z definida como $g \circ f(x) = g\big(f(x)\big)$ y la denominamos función *compuesta* de f con g.

Observación 1.8.10. En general, aún teniendo sentido $g \circ f$, $f \circ g$ no lo tendrá. Y si lo tuviera, ambas composiciones no coincidirán sino por una casualidad.

Lema 1.8.8. *Sean $f: X \longrightarrow Y$, $g: Y \longrightarrow Z$ y $h: Z \longrightarrow U$ tres aplicaciones. Entonces*

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Teorema 1.8.9. *Sea X un conjunto no vacío y $f: X \longrightarrow Y$. f es inyectiva si, y sólo si, existe $g: Y \longrightarrow X$ tal que $g \circ f = I_X$.*

Teorema 1.8.10. *Sea $f: X \longrightarrow Y$. f es sobreyectiva si, y sólo si, existe $g: Y \longrightarrow X$ tal que $f \circ g = I_Y$.*

Definición 1.8.9. Sea $f: X \longrightarrow Y$ una aplicación. Si $g: Y \longrightarrow X$ es tal que $g \circ f = I_X$ entonces a g se le denomina *inversa a izquierda* de f o *sección*. Si existe $h: Y \longrightarrow X$ tal que $f \circ h = I_Y$ entonces a h se le denomina *inversa a derecha* de f o *retracción*.

Lema 1.8.11. *Sea $f: X \longrightarrow Y$ una aplicación. Si g es una inversa a izquierda de f y h es una inversa a derecha, entonces $g = h$.*

Corolario 1.8.12. *Sea $f: X \longrightarrow Y$ una función. Entonces son equivalentes las siguientes afirmaciones:*

1. *f es biyectiva*

2. *Existe $g: Y \longrightarrow X$ tal que $f \circ g = I_Y$ y $g \circ f = I_X$*

La aplicación g es la aplicación f^{-1}.

Corolario 1.8.13. *La composición de dos aplicaciones inyectivas (resp. sobreyectivas, biyectivas) es una aplicación inyectiva (resp. sobreyectiva, biyectiva).*

Observación 1.8.11. La aplicación $f: \{a\} \longrightarrow \{b, c\}$ definida por $f(a) = b$ es inyectiva no sobreyectiva y sin embargo sólo tiene una inversa a izquierda, que es $g: \{b, c\} \longrightarrow \{a\}$ definida por $f(b) = f(c) = a$.

Teorema 1.8.14. *Sean $f: X \longrightarrow Y$ y $g: Y \longrightarrow Z$ dos aplicaciones. Entonces:*

1. *Para todo $A \subseteq X$, $(g \circ f)_*(A) = g_*\big(f_*(A)\big)$.*

2. *Para todo $B \subseteq Y$, $(g \circ f)^*(B) = f^*\big(g^*(B)\big)$.*

Corolario 1.8.15. *Sean $f: X \longrightarrow Y$ y $g: Y \longrightarrow Z$ dos biyecciones. Entonces $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Definición 1.8.10. Sean $f: A \longrightarrow C$ y $g: B \longrightarrow D$ dos aplicaciones. Definimos la aplicación $f \times g: A \times B \longrightarrow C \times D$ como $f \times g(a, b) = \langle f(a), g(b) \rangle$

Lema 1.8.16. *Sean $f: A \longrightarrow C$ y $g: B \longrightarrow D$ dos aplicaciones. Entonces:*

1. *$f \circ p_A = p_B \circ (f \times g)$*

2. *$g \circ p_C = p_D \circ (f \times g)$*

Ejercicio 1.8.3.

1. Sean $f: A \longrightarrow C$, $g: B \longrightarrow D$, $h: C \longrightarrow E$ y $k: D \longrightarrow F$. Entonces

$$(h \circ f) \times (k \circ g) = (h \times k) \circ (f \times g)$$

2. Si X e Y son conjuntos entonces $I_X \times I_Y = I_{X \times Y}$.

3. Sea $f: X \longrightarrow Y$ una función. f es inyectiva si, y sólo si, para todo $A, B \in \mathcal{P}(X)$, $f_*(A \cap B) = f_*(A) \cap f_*(B)$.

4. Sea $f: X \longrightarrow Y$ una función. f es inyectiva si, y sólo si, para todo $A \subseteq X$, $f_*(X \setminus A) \subseteq Y \setminus f_*(A)$.

5. Sea $f: X \longrightarrow Y$ una función. f es sobreyectiva si, y sólo si, para todo $A \subseteq X$, $Y \setminus f_*(A) \subseteq f_*(X \setminus A)$.

Teorema 1.8.17. *Sean X e Y conjuntos, R una relación de equivalencia en X y $f: X \longrightarrow Y$ una aplicación. Si xRy implica $f(x) = f(y)$, entonces existe una única aplicación $g: X/R \longrightarrow Y$ tal que $f = g \circ \pi_R$. Además:*

1. *Si f es sobreyectiva entonces g es sobreyectiva.*

2. *Si para todo $x, y \in X$, $f(x) = f(y)$ implica xRy, entonces g es inyectiva.*

Corolario 1.8.18. *Sea $f: X \longrightarrow Y$ una aplicación. Si π_{R_f} es la proyección canónica de X sobre X/R_f e i es la inclusión de $\operatorname{ran} f$ en Y, entonces $f = i \circ g \circ \pi_{R_f}$,*

1.9. Familias

Hay ocasiones en las que el rango de una función se considera más importante que la función misma. Cuando éste es el caso, tanto la terminología como la notación sufre alteraciones radicales.

Definición 1.9.1. Sea I un conjunto no vacío, que llamaremos ahora *conjunto de índices* y a sus elementos *índices*, X un conjunto al que llamaremos *conjunto indexado* y $x: I \longrightarrow X$ una aplicación a la que llamaremos ahora *familia*. En esta situación en lugar de $x(i)$ escribimos x_i y es llamado *término de la familia*. Una familia no vacía es cualquier familia para la que el conjunto de índices es no vacío.

Observación 1.9.1. Dada una familia como la de la definición, una forma inaceptable, pero generalmente aceptada, de representar a la familia es $\{x_i\}_{i\in I}$. En el colmo de la parquedad se escribe a veces solamente $\{x_i\}$. Se habla, por ejemplo, de una familia $\{A_i\}$ de subconjunto de X refiriéndose a una función de un conjunto I en $\mathcal{P}(X)$. Nosotros usaremos la notación $\langle x_i : i \in I\rangle$.

Definición 1.9.2. Sea X un conjunto, I un conjunto de índices y $\langle A_i : i \in I\rangle$ una familia de subconjuntos de X. La unión del rango de la familia es llamada *unión de la familia* y se representa con la simbología $\bigcup_{i\in I} A_i$ o simplemente $\bigcup_i A_i$.

Observación 1.9.2.

1. Todo conjunto $\mathcal{C}$ es el rango de una familia. Para ello basta tomar como conjuntos de índices al propio conjunto $\mathcal{C}$.

2. Tiene sentido hablar de una unión vacía y es vacía.

Lema 1.9.1 (ley asociativa generalizada)**.** *Sea $\langle I_j : j \in J\rangle$ una familia de conjuntos, $K = \bigcup_{j\in J} I_j$ y $\langle A_k : k \in K\rangle$ otra familia. Entonces*

$$\bigcup_{k\in K} A_k = \bigcup_{j\in J}\left(\bigcup_{i\in I_j} A_i\right)$$

Ejercicio 1.9.1. Enunciar y demostrar una versión generalizada de la ley conmutativa.

Definición 1.9.3. Sea X un conjunto, I un conjunto no vacía de índices y $\{A_i\}$ una familia de subconjuntos de X. La intersección del rango de la familia es llamada *intersección de la familia* y se representa con la simbología $\bigcap_{i\in I} A_i$ o simplemente $\bigcap_i A_i$.

Lema 1.9.2. *Sea $\langle A_i : i \in I\rangle$ una familia de subconjuntos de X y $B \subseteq X$. Entonces*

1. $B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I}(B \cap A_i)$
2. $B \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I}(B \cup A_i)$

Lema 1.9.3. *Sean $\langle A_i : i \in I\rangle$ y $\langle B_j : j \in J\rangle$ dos familias. Entonces*

1. $(\bigcup_{i\in I} A_i) \cap (\bigcup_{j\in J} B_j) = \bigcup_{\langle i,j\rangle\in I\times J}(A_i \cap B_j)$
2. *Si ambas familias son no vacías, entonces* $(\bigcap_{i\in I} A_i) \cup (\bigcap_{j\in J} B_j) = \bigcap_{\langle i,j\rangle I\times J}(A_i \cup B_j)$

Observación 1.9.3. Usualmente se escribe $\bigcup_{i,j}$ en lugar de $\bigcap_{\langle i,j\rangle\in I\times J}$.

Definición 1.9.4. El *producto cartesiano* de la familia $\langle X_i : i \in I\rangle$ es el conjunto de todas las familias $\langle x_i : i \in I\rangle$ tales que $x_i \in X_i$, para todo $i \in I$. El producto cartesiano de $\langle X_i : i \in I\rangle$ se representará por $\prod_{i\in I} X_i$ o simplemente $\prod_i X_i$.

Observación 1.9.4. Es necesario observar que:

1. Si X es un conjunto y la familia $\{X_i\}_{i\in I}$ cumple $X_i = X$, para todo $i \in I$, entonces $\prod_{i\in I} X_i = X^I$.

2. Si $I = \{a\}$ entonces $\prod_{i\in I} X_i = X_a$.

3. Si $I = \{a, b\}$ entonces existe una biyección entre $\prod_{i\in I} X_i$ y $X_a \times X_b$. Por tanto, pueden ser considerados el mismo conjunto.

Ejercicio 1.9.2. Demostrar que:

1. $(\bigcup_{i\in I} A_i) \times (\bigcup_j B_j) = \bigcup_{i,j}(A_i \times B_j)$

2. Si las familias son no vacías, $(\bigcap_{i\in I} A_i) \times (\bigcap_j B_j) = \bigcap_{i,j}(A_i \times B_j)$

3. Si la familia es no vacía, $\bigcap_{i\in I} X_i \subseteq X_j \subseteq \bigcup_{i\in I} X_i$, para todo $j \in J$.

1.10. Números

Definición 1.10.1. Sea x un conjunto. Definimos el conjunto *sucesor* de x , representado por x^+, mediante la siguiente igualdad:

$$x^+ = x \cup \{x\}$$

Observación 1.10.1. En el ámbito de la *Teoría de Conjuntos* acostumbramos a representar, en ocasiones, a $\varnothing$ por el símbolo 0. En realidad este convenio notacional es parte de otro más amplio. Por ejemplo:

1. $0 = \varnothing$

2. $1 = 0^+ (= \{0\})$

3. $2 = 1^+ (= \{0, 1\})$

4. $3 = 2^+ (= \{0, 1, 2\})$

y así sucesivamente.

De lo dicho no se deduce que esta construcción pueda ser llevada al infinito. Necesitamos hacer una nueva suposición, que lleva el nombre de *Axioma del Infinito*.

Definición 1.10.2. Un *conjunto de sucesores* es cualquier conjunto A que cumpla las siguientes condiciones:

1. $0 \in A$

2. Si $x \in A$ entonces $x^+ \in A$.

Axioma 6 (del Infinito)**.** *Exite un conjunto de sucesores A.*

Lema 1.10.1. *La intersección de toda familia no vacía de conjuntos de sucesores es un conjunto de sucesores.*

Definición 1.10.3. Representamos por ω a la intesección de todos los conjuntos de sucesores incluidos en A. Por su parte ω^* será la abreviatura de $\omega \setminus \{0\}$.

Lema 1.10.2. *Si B es un cojunto de sucesores entonces $\omega \subseteq B$.*

Definición 1.10.4. Un *número natural* es cualquier elemento de ω.

Definición 1.10.5. Una *sucesión* es cualquier familia cuyo conjunto de índices es ω o un elemento de ω. En el primer caso decimos que es *infinita* y en el segundo que es *finita*.

Observación 1.10.2. Si $n^+ \in \omega$ y $\{A_i\}_{i\in n}$ es una familia de conjuntos, entonces:

1. la unión de la sucesión es denotada por $A_0 \cup \cdots \cup A_n$ o $\bigcup_{i=0}^{n} A_i$.
2. la intersección de la sucesión es denotada por $A_0 \cap \cdots \cap A_n$ o $\bigcap_{i=0}^{n} A_i$.
3. el producto cartesiano de la sucesión es denotada por $A_0 \times \cdots \times A_n$ o $\prod_{i=0}^{n} A_i$.

y en el caso en que la sucesión sea infinita entonces usamos respectivamente la notación:

1. $A_0 \cup A_1 \cup A_2 \cup \cdots$ o $\bigcup_{i=0}^{\infty} A_i$.
2. $A_0 \cap A_1 \cap A_2 \cap \cdots$ o $\bigcap_{i=0}^{\infty} A_i$.
3. $A_0 \times A_1 \times A_2 \times \cdots$ o $\prod_{i=0}^{\infty} A_i$.

1.11. Los Axiomas de Peano

Lema 1.11.1. *El conjunto ω tiene las siguientes propiedades:*

P*1)* $0 \in \omega$

P*2) Si $n \in \omega$, entonces $n^+ \in \omega$.*

P*3) Si $S \subseteq \omega$, $0 \in S$ y si $n^+ \in S$ siempre que $n \in S$, entonces $S = \omega$.*

Observación 1.11.1. La propiedad 3 de 1.11.1 es conocida como *Principio de Inducción Matemática.*

Lema 1.11.2 (propiedad P4)**.** *Para todo $n \in \omega$, $n^+ \neq 0$.*

Lema 1.11.3. *Sea $n \in \omega$. Si $m \in n$ entonces $n \notin m$.*

Definición 1.11.1. Un conjunto E es *transitivo* si $x \in y$ e $y \in E$ implica $x \in E$.

Lema 1.11.4. *Todo número natural es transitivo.*

Teorema 1.11.5 (propiedad P5)**.** *Si $m, n \in \omega$ y $m^+ = n^+$ entonces $m = n$.*

Las propiedades P1 a P5 son conocidas como los *Axiomas de Peano*, y usualmente se les considera como la fuente del conocimiento matemático. A partir de ellos (junto con los principios de la teoría de los conjuntos que hemos presentado) es posible definir a los enteros, a los números racionales, a los números reales y a los números complejos, así como deducir sus propiedades aritméticas y analíticas.

La inducción se usa para demostrar resultados y también para definir, *definir por inducción.* A tal fin damos el siguiente teorema, conocido como *Teorema de Inducción.*

Teorema 1.11.6 (Teorema de Inducción)**.** *Sea X un conjunto, $a \in X$ y $f: X \longrightarrow X$. Existe una función $u: \omega \longrightarrow X$ tal que $u(0) = a$ y que para todo $n \in \omega$, $u(n^+) = f\big(u(n)\big)$.*

Ejercicio 1.11.1. Demostrar que:

1. Si $n \in \omega$ entonces $n \neq n^+$.
2. Si $n \in \omega$ y $n \neq 0$ entonces existe $m \in \omega$ tal que $n = m^+$.
3. ω es transitivo.
4. Si E es un subconjunto no vacío de algún número natural, entonces existe un elemento k en E tal que $k \in m$ siempre que m sea un elemento de E distinto de k.

1.12. Aritmética

Vamos a ver varios ejemplos de utilización del *teorema de inducción* en el ámbito de la aritmética.

Corolario 1.12.1. *Sea $m \in \omega$ y $f{:}\omega \longrightarrow \omega$ definida como $f(k) = k^+$. Existe una aplicación $s_m{:}\omega \longrightarrow \omega$ tal que $s_m(0) = m$ y $s_m(n^+) = \big(s_n(n)\big)^+$.*

Observación 1.12.1. Para cada $m, n \in \omega$, en lugar de $s_m(n)$ escribimos $m + n$.

Teorema 1.12.2. *Para todo $m, n, k \in \omega$ se cumple:*

1. $(k + m) + n = k + (m + n)$
2. $0 + n = n$
3. $m^+ + n = (m + n)^+$
4. $m + n = n + m$

Corolario 1.12.3. *Sea $m \in \omega$. Existe una aplicación $p_m{:}\omega \longrightarrow \omega$ tal que $p_m(0) = 0$ y $p_m(n^+) = p_m(n) + m$.*

Observación 1.12.2. Para cada $m, n \in \omega$, en lugar de $p_m(n)$ escribimos $m \cdot n$, aunque habitualmente se suprime el punto y se escribe mn.

Teorema 1.12.4. *Para todo $m, n, k \in \omega$ se cumple:*

1. $(km)n = k(mn)$
2. $0n = 0$
3. $m^+n = mn + n$
4. $mn = nm$
5. $k(m + n) = km + kn$

Corolario 1.12.5. *Sea $m \in \omega$. Existe una aplicación $e_m{:}\omega \longrightarrow \omega$ tal que $e_m(0) = 1$ y $e_m(n^+) = e_m(n)m$.*

Observación 1.12.3. Para cada $m, n \in \omega$, en lugar de $e_m(n)$ escribimos m^n. Las propiedades de esta función, en cuanto a su enunciado y demostración, pueden ser dejadas como ejercicio.

Definición 1.12.1. Dados dos números naturales $m, n \in \omega$, m y n son *comparables* si se cumple una de las siguientes propiedades:

- $m \in n$
- $m = n$
- $n \in m$

Teorema 1.12.6. *Para todo $m, n \in \omega$, m y n son comparables. Además se da exactamente una de las tres propiedades que definen el concepto de comparabilidad.*

Corolario 1.12.7. *Sean $m, n \in \omega$ tales que $m \neq n$. Son equivalentes las siguientes afirmaciones:*

1. $m \in n$
2. $m \subset n$

Definición 1.12.2. Definimos la relación $\leq$ en ω como $m \leq n$ si $m \in n$ o $m = n$ y la relación $<$ como $m < n$ si $m \in n$.

Observación 1.12.4. Ambas relaciones son transitivas, ninguna es simétrica y $<$ no es reflexiva, mientras que $\leq$ si lo es.

Lema 1.12.8. *Para todo $x, y \in \omega$, si $x \leq y$ e $y \leq x$ entonces $x = y$.*

Definición 1.12.3. Un conjunto E es *finito* si existen $n \in \omega$ y una función $f: n \longrightarrow E$ tal que f es biyección. E es *infinito* si no es finito.

Teorema 1.12.9. *Sea A un conjunto no vacío de números naturales. Entonces:*

1. *Existe $m \in A$ tal que $m \leq x$, para todo $x \in A$.*
2. *Si A es finito, entonces existe $m \in A$ tal que $x \leq m$, para todo $x \in A$.*

Teorema 1.12.10. *ω es infinito.*

Lema 1.12.11. *Si E es biyectivo con dos números naturales, entonces esto números coinciden.*

Definición 1.12.4. Si E es un conjunto finito, el *número de elementos* de E es el número natural al que es equivalente.

Ejercicio 1.12.1. Sean $m, n, k \in \omega$. Demostrar que:

1. Si $nk = mk$ y $k \neq 0$ entonces $n = m$.
2. Si $m < n$ entonces $m + k < n + k$.
3. Si $m + k < n + k$ entonces $m < n$.
4. Si $m < n$ y $k \neq 0$ entonces $mk < nk$.
5. Si $mk < nk$ y $k \neq 0$ entonces $m < n$.
6. Sea $S \subseteq \omega$. Si $n \in S$ siempre que $m \in S$, para todo $m < n$, entonces $S = \omega$.

1.13. Relaciones de Orden

Definición 1.13.1. Una relación R en un conjunto X es *antisimétrica* si para todo $x, y \in X$, $x = y$ siempre que xRy e yRx. R es una *relación de orden* en X si R es reflexiva, antisimétrica y transitiva. Un *conjunto ordenado* es un par $\langle X, R \rangle$, donde X es un conjunto y R es una relación de orden en X.

Observación 1.13.1. Se acostumbra a representar a las relaciones de orden con el símbolo $\leq$ y la expresión $x \leq y$ se lee "x es menor o igual que y" o "y es mayor o igual que x". Con esta notación, $x < y$ significa $x \leq y$ y $x \neq y$.

Definición 1.13.2. Sea X un conjunto y R una relación de orden en X. R es un *orden total* si para todo $x, y \in X$, xRy o yRx. Una *cadena* o *conjunto totalmente ordenado* es un conjunto ordenado $\langle X, R \rangle$ tal que R es un orden total.

Ejemplo 1.13.1.

1. Dado un conjunto X, la relación $\subseteq$ en $\mathcal{P}(X)$ es una relación de orden.
2. Sean X e Y dos conjuntos y F el conjunto de funciones cuyo dominio es un subconjunto de X y cuyo codominio es un subconjunto de Y. Sea R la relación en F definida por fRg siempre que $\operatorname{dom} f \subseteq \operatorname{dom} g$ y $f(x) = g(x)$, para todo $x \in \operatorname{dom} f$ —en realidad, fRg sii $f \subseteq g$—. R es una relación de orden en F.

3. $\langle \omega, \leq \rangle$ es un conjunto ordenado.

4. Sea el conjunto $\omega \times \omega$ con la relación $\langle a, b \rangle R \langle x, y \rangle$ sii, por definición, $(2a+1)2^y \leq (2x+1)2^b$.

Definición 1.13.3. Sean $\langle X_1, \leq_1 \rangle$ y $\langle X_2, \leq_2 \rangle$ conjuntos ordenados. En $X_1 \times X_2$ definimos las relaciones binarias $\leq_p$ y $\leq_l$ como sigue:

- $\langle a, b \rangle \leq_p \langle c, d \rangle$ sii, por def., $a \leq_1 c$ y $b \leq_2 d$.
- $\langle a, b \rangle \leq_l \langle c, d \rangle$ sii, por def., $(a \neq c$ y $a \leq_1 c)$ o $(a = c$ y $b \leq_2 d)$.

Lema 1.13.1. *Sean $\langle X_1, \leq_1 \rangle$ y $\langle X_2, \leq_2 \rangle$ conjuntos ordenados. Entonces $\langle X_1 \times X_2, \leq_p \rangle$ y $\langle X_1 \times X_2, \leq_l \rangle$ son conjuntos ordenados.*

Observación 1.13.2. A $\leq_p$ se le llama *orden producto* y a $\leq_l$ se le llama orden *orden lexicográfico*.

Definición 1.13.4. Sea $\langle X, \leq \rangle$ un conjunto ordenado y $A \subseteq X$. $x \in X$ es un *mayorante* (resp. *minorante*) de A sii, por def., para todo $a \in A$, $a \leq x$ (resp. $x \leq a$).

Definición 1.13.5. Sea $\langle X, \leq \rangle$ un conjunto ordenado y $A \subseteq X$. $a \in A$ es un elemento *maximal* (resp. *minimal*) de A sii, por def., para todo $x \in A$, $x = a$ siempre que $a \leq x$ (resp. $x \leq a$).

Definición 1.13.6. Sea $\langle X, \leq \rangle$ un conjunto ordenado y $A \subseteq X$. $a \in A$ es un *máximo* (resp. *mínimo*) de A sii, por def., para todo $x \in A$, $x \leq a$ (resp. $a \leq x$).

Lema 1.13.2. *Si un conjunto tiene mínimo (resp. máximo) éste es único.*

Definición 1.13.7. Sea $\langle X, \leq \rangle$ un conjunto ordenado y $A \subseteq X$. $x \in X$ es el *supremo* (resp. *ínfimo*) de A si x es el mínimo (resp. máximo) de los mayorantes (resp. minorantes).

Lema 1.13.3. *Sea $\langle X, \leq \rangle$ un conjunto ordenado, $A \subseteq X$ y $x \in X$. Son equivalentes las siguientes afirmaciones:*

1. *x es el ínfimo (resp. supremo) de A.*
2. *x es un minorante (resp. mayorante) de A y para todo minorante (resp. mayorante) y de A se cumple $y \leq x$ (resp. $x \leq y$).*

Definición 1.13.8. Sea $\langle X, R \rangle$ un conjunto ordenado. Dicho conjunto está *bien ordenado* si todos los subconjuntos no vacíos de X tienen mínimo.

Lema 1.13.4. *Si $\langle X, R \rangle$ es un conjunto bien ordenado entonces X tiene mínimo.*

Lema 1.13.5. *Todo conjunto bien ordenado está totalmente ordenado.*

Ejemplo 1.13.2.

1. $\langle \omega, \leq \rangle$ es un conjunto bien ordenado y, por tanto, totalmente ordenado.
2. El conjunto $\omega \times \omega$ con el orden $\langle a, b \rangle R \langle x, y \rangle$ sii, por definición, $(2a+1)2^y \leq (2x+1)2^b$ no está bien ordenado. Una forma de poner ésto de manifiesto es que $\langle a, b+1 \rangle \leq \langle a, b \rangle$, para todo a y b. Se deduce que $\omega \times \omega$ no tiene mínimo y por tanto (ver Lema 1.13.4) no puede ser bien ordenado. No obstante algunos subconjuntos de $\omega \times \omega$ si tienen mínimo. Por ejemplo, sea A el conjunto de todos aquellos elementos $\langle a, b \rangle$ tales que $\langle 1, 1 \rangle R \langle a, b \rangle$. Sin embargo, A con la misma relación de orden no está bien ordenado porque aún posee subconjuntos sin mínimo. Por ejemplo, considerar el conjunto de todas aquellas parejas $\langle a, b \rangle$ de A tales que $\langle a, b \rangle \neq \langle 1, 1 \rangle$.
3. $\omega \times \omega$ está ordenado con su orden lexicográfico.

1.14. Axioma de Elección

En esta pequeña sección enunciamos el controvertido *Axioma de Elección*. Un principio que admitimos sin demostración, muy utilizado en la matemática que conocemos y que tiene gran cantidad de enunciados equivalentes. Esto significa que dichos enunciados se deducen de los supuestos y teoremas anteriores junto al Axioma de Elección; y que si el axioma de elección fuese sustituido por cualquiera de estos enunciados, entonces tendría demostración.

Axioma 7 (de Elección)**.** *El producto cartesiano de cualquier familia no vacía de conjuntos no vacíos es no vacío.*

Observación 1.14.1.

1. Es inmediato, y no requiere mayor análisis, el darse cuenta de que el Axioma de Elección puede enunciarse también diciendo que "Para toda familia $\{A_i\}_{i\in I}$ existe una función $f: I \longrightarrow \bigcup_{i\in I} A_i$ tal que para todo $i \in I$, $f(i) \in A_i$". En definitiva, se observa que el mensaje de este enunciado es que, dada una familia arbitraria, se puede elegir un elemento en cada miembro de la familia simultáneamente. La dificultad de llevar esto a cabo no radica en el caso en que I sea finito, sino en los casos en que esto no ocurre.
2. A la función que se menciona en la observación anterior del se le llama *función de elección.*

Los siguientes son enunciados equivalentes al Axioma de Elección y que, tal como hemos enfocado la teoría, hemos de llamarlos teoremas. Las demostraciones son obviadas por el momento.

Teorema 1.14.1 (lema de Zorn)**.** *Si X es un conjunto ordenado tal que toda cadena en X tiene un mayorante en X, entonces X tiene un elemento maximal.*

Teorema 1.14.2 (del buen ordenamiento)**.** *Para todo conjunto no vacío X existe una relación de orden $\leq$ en X tal que $\langle X, \leq\rangle$ está bien ordenado.*

1.15. Números Enteros

Definición 1.15.1. Definimos en el conjunto $\omega \times \omega$ la relación $\sim$ como sigue:

$$\langle m, n\rangle \sim \langle r, s\rangle \text{ sii } m + s = n + r$$

Al conjunto $\omega\times\omega/\sim$ lo representamos como Z y le llamamos conjunto de los números *enteros*. Un *número entero*, o simplemente un *entero*, será cualquier elemento de Z.

Lema 1.15.1. *$\sim$ es una relación de equivalencia en $\omega \times \omega$.*

Definición 1.15.2. Definimos en Z las operaciones $\boxplus$ y $\boxdot$ como sigue:

$$\langle r, s\rangle/\sim \boxplus \langle u, v\rangle/\sim = \langle r + u, s + v\rangle/\sim \text{ y } \langle r, s\rangle/\sim \boxdot \langle u, v\rangle/\sim = \langle ru + sv, rv + su\rangle/\sim$$

Observación 1.15.1. Las respectivas definiciones de $\boxplus$ y $\boxdot$ están dadas sobre clases de equivalencia y hechas tomando un representante de las mismas. Resulta imprescindible demostrar que las definiciones no dependen del representante elegido. Esto se podría ver de otra forma, a saber, definir las operaciones en $\omega \times \omega$ y ver que $\sim$ es compatible con ella.

Lema 1.15.2. *Sean $m_i, n_i, u_i, v_i \in \omega$, $i \in \{1, 2\}$. Si $\langle m_1, n_1\rangle \sim \langle m_2, n_2\rangle$ y $\langle u_1, v_1\rangle \sim \langle u_2, v_2\rangle$, entonces*

1. $\langle m_1 + u_1, n_1 + v_1\rangle \sim \langle m_2 + u_2, n_2 + v_2\rangle$
2. $\langle m_1u_1 + n_1v_1, m_1v_1 + n_1u_1\rangle \sim \langle m_2u_2 + n_2v_2, m_2v_2 + n_2u_2\rangle$

El siguiente lema tiene una demostración fácil pero laboriosa. Se puede dejar como ejercicio.

1.16. Inmersión de ω en Z

Teorema 1.16.1. *Para todo $\langle m,n\rangle \in \omega\times\omega$ existe $\langle x,y\rangle \in \langle m,n\rangle/\sim$ tal que $x=0$ o $y=0$.*

Ejercicio 1.16.1. Si la demostración del teorema 1.16.1 se ha llevado a cabo por inducción, dar un método efectivo para calcular el representante con una componenete nula en la clase de equivalencia.

Teorema 1.16.2. *Para todo $m,n\in\omega$ se cumple:*

1. $\langle m,0\rangle/\sim = \langle n,0\rangle/\sim$ *si, y sólo si,* $m=n$
2. $\langle 0,m\rangle/\sim = \langle 0,n\rangle/\sim$ *si, y sólo si,* $m=n$
3. $\langle m,0\rangle/\sim = \langle 0,n\rangle/\sim$ *si, y sólo si,* $m=n=0$

Observación 1.16.1. Con este resultado tenemos que el representante de cada clase con una componente nula, cuya existencia garantiza el teorema 1.16.1, es único cumpliendo esta condición.

Teorema 1.16.3. $Z = \{\langle m,0\rangle/\sim : m\in\omega\}\cup\{\langle 0,n\rangle/\sim : n\in\omega^*\}$.

Teorema 1.16.4. *Sea $j:\omega\longrightarrow Z$ la función definida como $j(n)=\langle n,0\rangle/\sim$. Entonces:*

1. *j es inyectiva*
2. $j(n+m)=j(n)\boxplus j(m)$
3. $j(nm)=j(n)\boxdot j(n)$

Definición 1.16.1. Para todo $m,n\in\omega$ convenimos en representar al entero $\langle m,n\rangle/\sim$ como $-(\langle n,m\rangle/\sim)$. Además, convenimos en llamar n al entero $j(n)$ y $-n$ al entero $-j(n)$.

Observación 1.16.2. Obsérvese que $-0=0$ y también que la igualdad del teorema 1.16.3 se puede expresar ahora como $Z=j_*(\omega)\cup -j_*(\omega^*)$. Obsérvese también que esta unión es disjunta, como se deduce del teorema 1.16.2.

Observación 1.16.3. Si $z,w\in Z$ en lo sucesivo escribiremos $z-w$ en lugar de $z\boxplus(-w)$. Además, en virtud del teorema 1.16.4 no hay peligro en escribir en lo sucesivo $+$ (resp. $\cdot$) en lugar de $\boxplus$ (resp. $\boxdot$).

Ejercicio 1.16.2. Demostrar que:

1. $\boxplus$ y $\boxdot$ son asociativas y conmutativas
2. $\boxdot$ es distributiva respecto a $\boxplus$
3. Para todo $z\in Z$, $z+0=z$
4. Para todo $z\in Z$, $z+1=z$
5. Para todo $z\in Z$, $z-z=0$
6. Para todo $z\in Z$, $z\cdot 0=0$
7. Para todo $z,w\in Z$, $z\cdot w=0$ implica $z=0$ o $w=0$
8. Para todo $z,w\in Z$, $(-z)\cdot w=-(z\cdot w)$
9. Para todo $z\in Z$, $-(-z)=z$
10. Para todo $z,w\in Z$, $(-z)\cdot(-w)=z\cdot w$

Capítulo 2

Inducción

2.1. Los Postulados de Peano y la inducción finita

Puede que la función más conocida de las matemáticas sea la llamada *función sucesor de Peano*. Giuseppe Peano fue un matemático italiano nacido en 1858 y fallecido en 1932. Dicha función, representada por s, asigna su siguiente a cada número natural. Puede ser considerada como "la función que cuenta".

Definición 2.1.1. La *función sucesor de Peano* es la función:

$$s: \omega \longrightarrow \omega$$

definida[1] como $s(n) = n^+$, donde $n^+ = n \cup \{n\}$.

En términos de la función s existe una colección de "propiedades básicas" que caracterizan al "conjunto" de los números naturales ω. Estas propiedades se conocen con el nombre de *Postulados de Peano*.

Teorema 2.1.1. *Las siguientes afirmaciones, conocidas como postulados de Peano, son ciertas:*

P.1) $0 \in \omega$

P.2) Si $n \in \omega$, *entonces* $s(n) \in \omega$.

P.3) No existe $n \in \omega$ *tal que* $0 = s(n)$.

P.4) Si $s(n) = s(m)$, *entonces* $n = m$.

P.5) Si $P \subseteq \omega$ *y cumple las siguientes condiciones:*

a) $0 \in P$

b) $s(n) \in P$ *siempre que* $n \in P$

entonces $P = \omega$.

El postulado P.5 se conoce como el *principio de inducción finita*.

Teorema 2.1.2 (*Principio del Buen Orden*)**.** *Todo conjunto de números naturales no vacío tiene un elemento mínimo.*

[1] Siguiendo el desarrollo de la teoría de conjuntos, a la postre se comprueba que $s(n) = n + 1$.

Demostración. Sea S un conjunto de números naturales que no tiene elemento mínimo. Sea $P(n)$ el enunciado "no existe ningún número menor o igual que n que pertenezca a S" y sea, por el axioma de especificación, el conjunto:

$$P = \{n \in \omega : P(n)\}$$

y obsérvese que según la hipótesis, $m \in S$ sii $m \notin P$. (**Paso base**) Así pues, si $0 \notin P$ es porque $0 \in S$ y como todos los números naturales son mayores o iguales que 0, entonces S tendría mínimo; por tanto, $0 \in P$. (**Hipótesis de Inducción**) Supongamos ahora que $n \in P$; si $s(n) \notin P$ sería porque existe $k_n \leq s(n)$ tal que $k_n \in S$. Pero $n \in P$ y por tanto ningún número inferior o igual a n puede pertener a S. Siendo $s(n)$ el único número menor o igual que $s(n)$ que no es menor o igual que n, $s(n)$ sería un elemento de S y sería, por tanto, el menor elemento de S, lo que contradice lo supuesto sobre S. Deducimos que si $n \in P$ entonces $s(n) \in P$. Por el principio de inducción finita se tiene que $P = \omega$, de donde $S = \varnothing$. Ello concluye la demostración. □

Observación 2.1.1. Obsérvese que la demostración dada del Teorema 2.1.2 es una consecuencia del Principio de Inducción Finita.-

Teorema 2.1.3 (*Segundo Principio de Inducción Finita*)**.** *Si para todo número natural*[2] n *se cumple:*

$$n \in P \text{ siempre que } n \subseteq P \tag{2.1}$$

Entonces $P = \omega$.

Demostración. Sea el conjunto $J = \omega \setminus P$. Si J no fuera vacío, tomaríamos su elemento mínimo, que existe en virtud del Teorema 2.1.2, al que llamaremos j_0. Caben dos posibilidades:

1. $j_0 = 0$; al ser $0 = \varnothing$, se cumple $j_0 \subseteq P$. Según la hipótesis, debe cumplirse entonces $j_0 \in P$. Así, j_0 debe ser y no ser elemento de J, lo cual es absurdo; por tanto $J = \varnothing$ y $P = \omega$.

2. $j_0 \neq 0$; si j_0 es el más pequeño de los elementos de J quiere decir que ninguno de los inferiores son elementos de dicho conjunto, es decir, $\{0, \ldots, j_0 - 1\} \subseteq P$ o en nuestro lenguaje $j_0 \subseteq P$. Por la hipótesis del teorema se deduce entonces que $j_0 \in P$. Como en el caso anterior este absurdo conduce a que $J = \varnothing$ y por ende $P = \omega$.

Al no haber otro caso que los recogidos en la enumeración anterior, en los supuesto del teorema se debe cumplir $P = \omega$, como queríamos demostrar. □

Observación 2.1.2. Obsérvese que si un subconjunto de números naturales P cumple la condición (2.1) necesariamente debe contar con 0 entre sus elementos. En efecto, sea cual sea P siempre se cumplirá $\varnothing \subseteq P$, por lo que en virtud de la condición (2.1) se debe cumplir $\varnothing \in P$, esto es, $0 \in P$.

Observación 2.1.3. Obsérvese que la demostración dada del Teorema 2.1.3 es una consecuencia del Principio del Buen Orden.-

2.2. Equivalencia entre Principios

Hagamos una síntesis de los principios nombrados hasta ahora:

1. **Principio de Inducción Finita**; Si $P \subseteq \omega$ y cumple las siguientes condiciones:

   a) $0 \in P$

   b) $s(n) \in P$ siempre que $n \in P$

   entonces $P = \omega$.

[2] Según el modelo que tenemos de ω, también representado como ω, $0 = \varnothing$ y si $n \neq 0$ entonces $n = \{0, \ldots, n-1\}$.

2. **Principio del Buen Orden**; Todo conjunto de números naturales no vacío tiene un elemento mínimo.

3. **Segundo Principio de Inducción Finita**; Si $P \subseteq \omega$ y cumple que:

$$\text{Para todo número natural } n,\ n \in P \text{ siempre que } n \subseteq P \tag{2.2}$$

   Entonces $P = \omega$.

Teorema 2.2.1. *Si es válido el principio del buen orden entonces es válido el principio de inducción finita.*

Demostración. Supongamos que todo conjunto no vacío de números naturales tiene un elemento mínimo (principio del buen orden). Sea ahora $P \subseteq \omega$ tal que:

1. $0 \in P$
2. $s(n) \in P$ siempre que $n \in P$

Supongamos que $\omega \setminus P$ es no vacío. Por el principio del buen orden sea m el mínimo de $\omega \setminus P$. Como $0 \in P$ entonces $0 \notin \omega \setminus P$, por lo que $m \neq 0$. Existirá entonces $q \in \omega$ tal que $s(q) = m$, de donde $q < m$. Tenemos entonces que $q \notin \omega \setminus P$, por lo que $q \in P$ y de ello se deduce, por las propiedades de P, que $m \in P$. Esto contradice que $m \in \omega \setminus P$ y la contradicción establece que $\omega \setminus P$ es vacío, o sea, que $P = \omega$. □

Teorema 2.2.2. *Si es válido el segundo principio de inducción finita entonces es válido el principio del buen orden.*

Demostración. Supongamos válido el segundo principio de inducción y sea A un subconjunto del conjunto de los números naturales. Supongamos que A no tiene mínimo y sea $P = \omega \setminus A$. Sea $n \in \omega$ tal que $n \subseteq P$. Si $n \in A$ entonces n es el mínimo de A, de donde $n \notin A$ y por tanto $n \in P$. Por el segundo principio de inducción, $P = \omega$ y de ello se deduce que $A = \varnothing$. Tenemos así una demostración de la afirmación contrarecíproca del principio del buen orden, es decir, dicho principio es válido. □

Corolario 2.2.3. *Son equivalentes los siguientes principios:*

1. *El principio de inducción finita.*
2. *El principio del buen orden.*
3. *El segundo principio de inducción finita.*

Demostración. El principio de inducción finita implica el principio del buen orden (Teorema 2.1.2). El principio del buen orden implica el segundo principio de inducción finita (Teorema 2.1.3). El segundo principio de inducción finita implica el principio del buen orden (Teorema 2.2.2). Finalmente, el principio del buen orden implica el principio de inducción finita (Teorema 2.2.1). □

El principio de inducción ha sido difundido enunciándolo sobre enunciados proposicionales y no referidos necesariamente a 0 como primer natural de validez. En lo que sigue derivaremos dichas presentaciones.

En lo que sigue nos referiremos a los enunciado $P(i)$ dependientes de números naturales i que pueden ser evaluados como verdaderos o falsos como *enunciados proposicionales* o *fórmulas proposicionales* (cfr. Capítulo 5).

Teorema 2.2.4. *Sea $P(i)$ un enunciado proposicional e $i_0 \in \omega$. Supongamos que:*

1. *$P(i_0)$ es cierto (paso base).*

2. *Para todo todo $k \in \omega$ tal que $i_0 \leq k$, $P(k+1)$ es cierto siempre que $P(k)$ sea cierto (hipótesis de inducción).*

entonces $P(i)$ es cierto para todo $i \in \omega$ tal que $i_0 \leq i$.

Demostración. Consideremos $Q(i) = P(i_0 + i)$. Así pues, para demostrar que $P(i)$ es cierta para todo número natural i tal que $i_0 \leq i$, basta con demostrar que $Q(i)$ es cierta para todo $i \in \omega$. Definamos

$$Q = \{i \in \omega : Q(i) \text{ es cierto}\}$$

Si la condición 1) del teorema es cierta, entonces $Q(0) = P(i_0)$ es cierta; por tanto, $0 \in Q$. Sea ahora $i \in \omega$ fijo pero arbitrario y supongamos que $Q(i)$ es cierta, es decir, que $P(i_0 + i)$ es cierta. Como $i_0 \leq i_0 + i$ y la condición 2) vale, entonces $P(i_0 + i + 1)$ es cierta o equivalentemente $Q(i+1)$ es cierta. Así, a Q pertence $s(k) = i + 1$ siempre que a Q pertenezca i. Por el postulado P.5 debe cumplirse $Q = \omega$. En consecuencia, si las condiciones 1) y 2) se dan, $Q(i)$ es cierto para todo $i \in \omega$; es decir, $P(i)$ es cierto para todo $i \in \omega$ tal que $i_0 \leq i$. □

Ejemplo 2.2.1. Para todo $n \in \omega$ tal que $0 \leq n$ es cierta la igualdad (la igualdad es representada por $P(n)$):

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \tag{2.3}$$

Solución. En efecto, (paso base) para $i = 1$ el miembro de la izquierda de la ecuación 2.3) es 1 y el de la derecha es $\frac{1(1+1)}{2} = 2/2 = 1$; por tanto $P(1)$ es cierta. (Paso de inducción) Supongamos que $1 \leq k$ y que $P(k)$ es cierta (hipótesis de inducción) y demostremos que de ello se deduce que $P(k+1)$ es cierta. Un razonamiento que sirve de demostración es el siguiente:

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= (\sum_{i=1}^{k} i) + (k+1), \text{ por definición} \\
&= \frac{k(k+1)}{2} + (k+1), \text{ por hip. de inducción} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{(k+2)(k+1)}{2}
\end{aligned}$$

Por el *primer principio de inducción finita*, $P(n)$ es cierta para todo $1 \leq n$. □

Ejemplo 2.2.2. Probar que el producto de tres números naturales consecutivos cualesquiera es divisible por 6.

Solución. Sean los siguientes polinomios:

- $q(x) = 3(x+1)(x+2)$
- $p(x) = x(x+1)(x+2)$

Veamos por inducción que para todo $n \in \omega$, $6 \mid q(n)$. Como $q(0) = 6$ está claro que lo que se quiere demostrar vale para $n = 0$ (**caso base**). Supongamos que $0 \leq n$ y que $6 \mid q(n)$ (**hip. inducción**); veamos ahora que $6 \mid q(n+1)$. Se tiene que

$$\begin{aligned}
q(n+1) - q(n) &= 3(n+2)(n+3) - 3(n+1)(n+2) \\
&= 3(n+2)(n+3-(n+1)) \\
&= 3(n+2)2 \\
&= 6(n+2)
\end{aligned}$$

por lo que evidentemente $6 \mid q(n+1)-q(n)$; pero si $6 \mid q(n)$ y $6 \mid q(n+1)-q(n)$, se deduce que $6 \mid q(n+1)$, como queríamos demostrar.

Veamos ahora, también por inducción, que para todo $n \in \omega$ se cumple $6 \mid p(n)$. Se tiene que $6 \mid p(0)$ pues $p(0) = 0$ (**caso base**). Supongamos que $0 \leq n$ y que $6 \mid p(n)$ (**hip. inducción**); veamos ahora que $6 \mid p(n+1)$. Se tiene que:

$$\begin{aligned} p(n+1) - p(n) &= (n+1)(n+2)(n+3) - n(n+1)(n+2) \\ &= (n+3-n)(n+2)(n+3) \\ &= 3(n+1)(n+2) \\ &= q(n) \end{aligned}$$

Por lo antes demostrado se tiene que $6 \mid p(n+1) - p(n)$, y de ello y la hipótesis de inducción se deduce que $6 \mid p(n+1)$, como queríamos demostrar. □

Teorema 2.2.5. *Sea $P(i)$ un enunciado proposicional e $i_0 \in \omega$. Si para todo número natural n, $P(n)$ es cierto siempre que $P(i)$ sea cierto para todo $i \in \omega$ tal que $i_0 \leq i < n$, entonces $P(i)$ es cierto para todo $i \in \omega$ tal que $i_0 \leq i$.*

Demostración. Consideremos $Q(i) = P(i_0 + i)$. Desmostrar que $P(i)$ es cierto para todo $i \in \omega$ tal que $i_0 \leq i$ equivale a demostrar que $Q(i)$ es cierto para todo $i \in \omega$. Sea

$$Q = \{k \in \omega : Q(k) \text{ es cierto}\}$$

y sea $n \in \omega$ tal que $n \subseteq Q$, es decir, $Q(j) = P(i_0 + j)$ es cierto para todo $j \in n$ o equivalentemente $P(i)$ es cierto para todo $i \in \omega$ tal que $i_0 \leq i < i_0 + n$. Por la hipótesis del teorema, $P(i_0 + n)$ es cierto, o sea, $Q(n)$ es cierto o equivalentemente $n \in Q$. Por el Teorema 2.1.3 concluimos que $Q = \omega$, es decir, que $P(i)$ es cierto para todo $i \in \omega$ tal que $i_0 \leq i$. □

Ejemplo 2.2.3. Todo número natural mayor que 1 puede ser expresado como producto de números primos.

Solución. Supongamos que n es un número natural superior a 1 y supongamos que para todo $1 < k < n$, k puede ser expresado como un producto de números primos (**hip. de induc.**). Demostraremos que n puede ser expresado como un producto de números primos. Como n es natural, será primo o no lo será. Si n es primo, es producto de un número primo, a saber, él mismo; así pues la propiedad del enunciado resulta cierta en este caso. Si n no es primo es porque es producto de dos números naturales a y b, que cumplirán $1 < a \leq b < n$. Por la hipótesis de inducción tanto a como b pueden ser expresados como producto de números primos. El producto de los primos que descomponen a a por el de los que descomponen a b es un producto de primos que expresa a $n = ab$ y queda demostrado que la propiedad del enunciado es cierta para n. De esto se deduce que el enunciado es cierto vía el segundo principio de inducción finita. □

2.3. Teorema de Recursión

La inducción se usa para demostrar resultados y también para definir, *definir por recursión.* A tal fin damos una versión particular del conocido como *teorema de recursión.*

Teorema 2.3.1 (de recursión)**.** *Sea X un conjunto, $a \in X$ y $f : X \longrightarrow X$ una función. Existe una única función $u : \omega \longrightarrow X$ tal que $u(0) = a$ y que para todo $n \in \omega$, $u(n^+) = f\big(u(n)\big)$.*

Demostración. Consideremos la colección $\mathcal{C}$

$$\mathcal{C} = \{A \in \mathcal{P}(\omega \times X) : \langle 0, a\rangle \in d \text{ y } \langle n^+, f(x)\rangle \in d \text{ siempre que } \langle n, x\rangle \in d\}$$

La colección $\mathcal{C}$ es no vacía porque $\omega \times X$ es uno de sus elementos. Entonces $u = \bigcap \mathcal{C}$ es un subconjunto de $\omega \times X$ y por tanto es una relación. Supuesta la existencia de la función del enunciado, es claro que cualquier otra que cumpliera sus condiciones debebería de coincidir con ella. Resulta sencillo comprobar que $u \in \mathcal{C}$, por lo que sólo falta demostrar que u es una función tal que $\operatorname{dom} u = \omega$ y $\operatorname{ran} u \subseteq X$. En otras palabras, tenemos que demostrar que para todo $n \in \omega$ existe un único $x \in X$ tal que $\langle n, x\rangle \in u$. Esto se lleva a cabo, una vez más, mediante el *principio de inducción*. Sea

$$S = \big\{n \in \omega\colon \text{ existe } x\big(\langle n, x\rangle \in u \text{ y para todo } y(x = y \text{ siempre que } \langle n, y\rangle \in u)\big)\big\}$$

Veamos que $0 \in S$. Si no fuese así, existiría $z \in X$ tal que $a \neq z$ y $\langle 0, z\rangle \in u$. Consideremos el conjunto $u \setminus \{\langle 0, z\rangle\}$. Al ser $a \neq z$, $\langle 0, a\rangle \in u \setminus \{\langle 0, z\rangle\}$. Por otra parte, si $\langle n, x\rangle \in u \setminus \{\langle 0, z\rangle\}$ entonces $\langle n^+, f(x)\rangle \in u \setminus \{\langle 0, z\rangle\}$. La razón es que $n^+ \neq 0$ —y por tanto el elemento descartado de u no es éste. Se deduce que $u \setminus \{\langle 0, z\rangle\} \in \mathcal{C}$. Esto es absurdo porque $u \setminus \{\langle 0, z\rangle\} \subseteq u$ y $u \setminus \{\langle 0, z\rangle\} \neq u$, contradiciendo el hecho de que u es el conjunto más pequeño de $\mathcal{C}$, y debemos concluir entonces que $0 \in S$.

Supongamos ahora que $n \in S$, con lo cual estamos suponiendo que existe un único $x \in X$ tal que $\langle n, x\rangle \in u$. Como $\langle n, x\rangle \in u$, se deduce que $\langle n^+, f(x)\rangle \in u$. Si $n^+ \notin S$ es que existe y diferente de x tal que $\langle n^+, y\rangle \in u$. Considérese, en este caso, $u \setminus \{\langle n^+, y\rangle\}$. Dado que $n^+ \neq 0$, se tiene $\langle 0, a\rangle \in u \setminus \{\langle n^+, y\rangle\}$. Por otra parte, si $\langle m, t\rangle \in u \setminus \{\langle n^+, y\rangle\}$ entonces caben dos posibilidades:

1. $m = n$; en cuyo caso $t = x$ y como $f(x) \neq y$ entonces $\langle m^+, f(t)\rangle \in u \setminus \{\langle n^+, y\rangle\}$.

2. $m \neq n$; entonces $m^+ \neq n^+$. Por tanto, $\langle m^+, f(t)\rangle \in u \setminus \{\langle n^+, y\rangle\}$.

Se deduce que $u \setminus \{\langle n^+, y\rangle\} \in \mathcal{C}$, lo cual vuelve a contradecir el hecho de u es el conjunto más pequeño de $\mathcal{C}$. Por tanto, $n^+ \in S$.

□

Observación 2.3.1. Cada vez que se usa se usa el teorema 2.3.1, decimos que se ha hecho una definición por inducción.

En general es fácil de usar este teorema, aunque a veces las definiciones se pueden complicar. Es el caso de la función factorial y de la *sucesión de Fibonacci*.

Ejemplo 2.3.1. Sea $x = \omega \times \omega$, $a = \langle 1, 1\rangle$ y $f : x \longrightarrow x$ definida como $f(n, m) = \langle nm, n^+\rangle$. El teorema afirma que existe una única función

$$u\colon \omega \longrightarrow \omega \times \omega$$

que cumple $u(0) = \langle 1, 1\rangle$ y $u\big(s(n)\big) = f\big(u(n)\big)$, para todo $n \in \omega$. Representemos por fac a la función $\pi_1 \circ f$, donde π_1 es la proyección de $\omega \times \omega$ en su primera coordenada. A fac se le denomina *función factorial*. Es fácil demostrar que $\operatorname{fac}(0) = 1$ y (por inducción) que $\operatorname{fac}(n^+) = n^+ \operatorname{fac}(n)$.

Ejemplo 2.3.2. Sea $x = \omega \times \omega \times \omega$, $a = \langle 0, 1, 0\rangle$ y $f : x \longrightarrow x$ definida como $f(n, m, s) = \langle n + m, n, m\rangle$. El *teorema de recursión* afirma que existe una única función

$$u\colon \omega \longrightarrow \omega \times \omega \times \omega$$

que cumple $u(0) = \langle 0, 1, 0\rangle$ y $u\big(s(n)\big) = f\big(u(n)\big)$, para todo $n \in \omega$. Llamemos v a la composición $\pi_1 \circ f$, donde π_1 es la proyección de $\omega \times \omega \times \omega$ sobre su primera coordenada. A v se le denomina *sucesión de Fibonacci*. Es fácil demostrar que $v(0) = 0$, $v(1) = 1$ y (por inducción) que $v(n + 2) = v(n + 1) + v(n)$, para todo $i \in \omega$.

2.4. Ejercicios de Inducción

1. Demuestre que para todo número natural no nulo n se cumple:

$$\prod_{k=1}^{n}(1-\frac{1}{(k+1)^2}) = \frac{n+2}{2n+2}$$

2. Demuestre que para cualquier número natural n el número $n^2 - n$ es par. Utilice lo anterior para demostrar que para todo número natural n, $n^3 - 3n^2 - 4n$ es un múltiplo de 6.

3. Usar el teorema de inducción para demostrar que:

$$2^{n-1} \leq n!$$

para todo $n > 0$.

4. Utilizar el teorema de inducción para demostrar que:

$$\sqrt{n} < \sum_{i=1}^{n} \frac{1}{\sqrt{i}}$$

para todo $n \geq 2$.

5. Utilizar el teorema de inducción para demostrar que:

$$\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} \leq \frac{1}{\sqrt{n+1}}$$

para todo $n > 1$.

6. Utilizar el primer principio de inducción finita para demostrar que para todo número natural n es cierta la igualdad:

$$\sum_{i=0}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6}$$

7. Todo número natural mayor que 1 es divisible por al menos un número primo.

8. Usar el teorema de inducción para demostrar que $3^n + 7^n - 2$ es divisible por 8, para $n \geq 1$.

9. Usar el teorema de inducción para demostrar que $n^3 + 2n$ es divisible por 3, para $n \geq 1$.

10. Es cierto que de un número n en adelante se tiene que $n! > 100^n$. Encontrarlo y demostrar por inducción lo dicho a partir de ese número hallado.

11. Se ha dado una demostración falaz del enunciado falso siguiente: "Todos los niños tienen el mismo color de ojos". La demostración es como sigue. Si el grupo de niños es de 1 está claro que todos los del grupo tienen el mismo color de ojos. Supongamos el resultado cierto para todo grupo de tamaño n (con $n \geq 1$) y veamos que es cierto para $n + 1$. Si nos dan un grupo de $n + 1$ niños y los ordenamos por edad (digamos de menor a mayor), los n primeros tienen el mismo color de ojos al igual que los n últimos. Por tanto, todos los niños del grupo tienen el mismo color de ojos. Ahora bien, los niños forman un conjunto como los mencionados —de mayor o menor tamaño— por lo que el resultado está demostrado. Indique en el argumento dónde está el fallo.

12. Cualesquiera dos números naturales a y b tienen un mínimo común múltiplo, esto es, un número m que es múltiplo común a a y b y es menor o igual que cualquier otro múltiplo común a ambos.

13. Sea n un número natural y sea S un conjunto de números naturales menores que n. Demuestre que S es vacío o S tiene máximo.

14. Demuestre que para todo número natural n, $8^n - 3^n$ es múltiplo de 5.

15. Demuestre que para todo número natural n, $3^{4n} - 1$ es múltiplo de 5.

16. Demuestre que para todo número impar n, 9 divide a $4^n + 5^n$.

17. Sea p la función dada por:

$$p(a,0) = 0,$$
$$p(a,b) = \begin{cases} p\left(2a, \frac{b}{2}\right) & \text{si } b \text{ es par,} \\ p\left(2a, \frac{b-1}{2}\right) + a & \text{si } b \text{ es impar.} \end{cases}$$

Demuestre por inducción que para cualesquiera números naturales a y b, $p(a,b) = a \cdot b$.

18. Sea e la función dada por:

$$e(a,0) = 1,$$
$$e(a,b) = \begin{cases} e\left(a^2, \frac{b}{2}\right) & \text{si } b \text{ es par,} \\ e\left(a^2, \frac{b-1}{2}\right) a & \text{si } b \text{ es impar.} \end{cases}$$

Demuestre por inducción que para cualesquiera números naturales a y b, $e(a,b) = a^b$.

19. Demuestre que para todo número natural n:

$$\sum_{i=0}^{n} i!i = (n+1)! - 1$$

20. Demuestre que para para todo número natural n se cumple:

$$\sum_{i=0}^{n} 2i + 1 = (n+1)^2$$

21. Supongamos que disponemos en cantidad suficiente de sellos de 3 y 8 céntimos sólo. Demuestre que con esos sellos, una carta podría ser franqueada con una cántidad de céntimos superior a 13.

22. Definamos los *números de Fibonacci* como cualquier número de la sucesión:

$$F_n = \begin{cases} 0, & \text{si } n = 0; \\ 1, & \text{si } n = 1; \\ F_{n-1} + F_{n-2}, & \text{si } 1 < n; \end{cases}$$

Demuestre que para todo número natural n se cumple:

$$F_n < \left(\frac{5}{3}\right)^n$$

23. Definamos los *números de Lucas* como cualquier número de la sucesión:

$$L_n = \begin{cases} 2, & \text{si } n = 0; \\ 1, & \text{si } n = 1; \\ L_{n-1} + L_{n-2}, & \text{si } 1 < n; \end{cases}$$

Demuestre que para todo número natural n se cumple:

$$L_n < \left(\frac{7}{4}\right)^n$$

24. Sean $n_0, \ldots, n_d$ puntos distintos de un dominio de integridad $\mathbf{A}$ en cantidad igual a $d+1$ y sea el polinomio $g(x)$ en una variable definido por la siguiente igualdad:

$$g(x) = \prod_{i=0}^{d} (x - n_i)$$

Entonces:

$$g'(x) = \sum_{i=0}^{d} \prod_{\substack{j=0 \\ j \neq i}}^{d} (x - n_j)$$

Capítulo 3

Relaciones de Recurrencia

3.1. Introducción.

Es usual en el trabajo matemático y en las aplicaciones de sus resultados, necesitar construir un "objeto de tamaño $n+1$" a partir de otro similar de tamaño n, una vez determinado el objeto para un tamaño primero -0 ó 1-. En el presente capítulo, y en este orden de ideas, se abordará el estudio de funciones numéricas $a(n)$, $0 \leq n$, -o mejor a_n- donde a_n depende de algunos términos de entre $a_0, \ldots, a_{n-1}$. Este estudio se ha denominado clásicamente con el título de *Ecuaciones de Recurrencia* o *Ecuaciones de Diferencias* y supone en el fondo la versión discreta de la idea de ecuación diferencial ordinaria. A pesar de todo, nuestro enfoque no recurre a dicha teoría.

El estudio de las relaciones de recurrencia puede rastrearse hasta la relación de *Fibonacci*: $F_{n+2} = F_{n+1} + F_n$, $n \leq 0$; F_0, $F_1 = 1$, investigada por *Leonardo de Pisa* (1175-1250) en 1202. En su libro *Liber Abaci* se ocupó de un problema sobre el número de conejos que resultan en un año, si se comienza con una sola pareja que cría otra al final de cada mes. Cada nueva pareja comienza a reproducirse de igual manera al cabo de un mes del nacimiento, y se supone que ningún conejo muere durante el año dado. Así, al final del primer mes hay dos parejas de conejos, tres a los dos meses, cinco a los tres meses y así sucesivamente.

Esta misma sucesión aparece en los trabajos del matemático alemán *Johannes Kepler* (1571-1630), quién la utilizó en sus estudios sobre cómo pueden ordenarse las hojas de una planta o flor alrededor de su tallo. En 1844, el matemático francés *Gabriel Lamé* (1795-1870) utilizó la sucesión en su análisis de la eficiencia del *Algoritmo de Euclides*. Más tarde, *François Lucas* (1842-1891) dedujo varias propiedades de esta sucesión y fue el primero en llamarla *Sucesión de Fibonacci*.

Una *definición recursiva* de una sucesión especifica uno o varios términos iniciales y una regla para calcular el resto en función de términos anteriores. Esta forma de definir una sucesión resulta útil pra resolver problemas de conteo. La regla que define unos términos en función de los que preceden se llama *relación de recurrencia*.

Más concretamente, una relación de recurrencia para la sucesión $\{u_n\}$ es una ecuación que determina el término u_n en función de los términos anteriores, es decir, $u_0, u_1, \ldots, u_{n-1}$, para todos los números naturales n tales que $n \geq n_0$ siendo n_0 un número natural. Una sucesión es una *solución* de una relación de recurrencia si sus términos satisfacen la relación para todo entero positivo n.

Supongamos que nos enfrentamos al siguiente problema: un banco incrementa el capital depositado en un $6\,\%$ anual y compone mensualmente el interés. Si un depositario deposita 1000 euros en determinada fecha, ¿a cuánto ascenderá su depósito un año después?

Consideremos la situación abstracta que es modelada en el ejemplo 3.1.1 que sigue.

Ejemplo 3.1.1. Supongamos que a y c son constantes conocidas y consideremos las siguientes relaciones:

$$\begin{cases} u_0 = c \\ u_{n+1} - au_n = 0, \quad \text{para todo } n \geq 0 \end{cases} \tag{3.1}$$

La sucesión $\{x_n\}$ sugerida por:

$$\begin{aligned} x_0 &= c \\ x_1 &= ax_0 = ac \\ x_2 &= ax_1 = a(ac) = a^2c \\ x_3 &= ax_2 = a(a^2c) = a^3c \\ &\vdots \qquad\qquad \vdots \end{aligned}$$

es una solución a la relación de recurrencia 3.1. Es fácil conjeturar que la solución debe ser $\{x_n\}$, donde para todo natural n se cumple $x_n = c \cdot a^n$. Desmostremos por inducción que esto es así. En efecto, (paso base) para $n = 0$, $x_0 = ca^0 = c \cdot 1 = c$. Supongamos el resultado cierto para $k \geq 0$ y demostremos que también lo es para $k+1$. En efecto,

$$\begin{aligned} x_{k+1} &= ax_k && \text{por ser } \{x_n\} \text{ sol. de } (3{,}1) \\ &= a(ca^k) && \text{por la hip. de inducción} \\ &= ca^{k+1} && \text{agrupando factores.} \end{aligned}$$

Observación 3.1.1. Obsérvese que trivialmente la constante a puede ser traída a colación por ser la única raíz de $p(x) = x - a$, es decir, por ser la única solución de $x - a = 0$. En cuanto a c, es una constante arbitrariamente fijada o que viene dada por las condiciones de un problema concreto.

Ahora podemos abordar el problema introductorio en los siguientes términos.

Ejemplo 3.1.2. Un banco incrementa el capital depositado en un $6\,\%$ anual y compone mensualmente el interés. Si un depositario deposita 1000 euros en determinada fecha, ¿a cuánto ascenderá su depósito un año después?

Solución. La tasa de ingreso mensual será $6/12 = 0{,}5$, es decir, $0{,}5\,\%$. Entonces, el tanto por uno será $0{,}005$. Para $0 \leq n \leq 12$, representaremos por u_n el valor del depósito del depositario al cabo de n meses. Entonces, $u_{n+1} = u_n + 0{,}005u_n$ con lo que el problema que se plantea es:

$$\begin{cases} u_0 = 1000 \\ u_{n+1} = 1{,}005 \cdot u_n, \quad \text{para todo } 0 \leq n \leq 11 \end{cases} \tag{3.2}$$

Según lo dicho en el ejemplo 3.1.1, la solución al problema (3.2) es $x_n = 1000 \cdot 1{,}005^n$ medido en euros. Al cabo de un año, el capital del depositario será $x_{12} = 1000 \cdot 1{,}005^{12} = 1061{,}68$ euros. □

Ejemplo 3.1.3. Resolver la relación $u_n = u_{n-1} + 3n^2$, para todo $n \geq 1$. Particularizar la solución al caso $u_0 = 7$.

Solución. Sea $f(i) = 3i^2$ tiene lo siguiente:

$$\begin{aligned} u_1 &= u_0 + f(1) \\ u_2 &= u_1 + f(2) = u_0 + f(1) + f(2) \\ u_3 &= u_2 + f(3) = u_0 + f(1) + f(2) + f(3) \\ &\vdots \\ u_n &= u_{n-1} + f(n) = u_0 + \sum_{i=1}^{n} f(i) \end{aligned}$$

En este caso tenemos:

$$\begin{aligned} u_n &= u_0 + \sum_{i=1}^{n} f(i) \\ &= u_0 + 3\sum_{i=1}^{n} i^2 \\ &= u_0 + 3\frac{2n^3+3n^2+n}{6} \\ &= u_0 + \frac{1}{2}(2n^3+3n^2+n) \end{aligned}$$

En el caso $u_0 = 7$, tenemos:

$$u_n = 7 + \frac{1}{2}(2n^3+3n^2+n)$$

□

3.2. Teoría de la Recurrencia Lineal Homogénea

Definición 3.2.1. Sea k un número natural. Una relación de *recurrencia lineal homogénea* es cualquier igualdad de la forma:

$$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_ku_{n-k}, \text{ para todo } n \geq k \tag{3.3}$$

donde $a_1, \ldots, a_k$ son constantes. Si $a_k \neq 0$, el número k es denominado el *orden* de la relación de recurrencia 3.3. El polinomio:

$$p(x) = x^k - a_1x^{k-1} - a_2x^{k-2} - \cdots - a_k \tag{3.4}$$

es denominado *polinomio característico* de la relación de recurrencia 3.3. La ecuación $p(x) = 0$, es decir,

$$x^k - a_1x^{k-1} - a_2x^{k-2} - \cdots - a_k = 0 \tag{3.5}$$

es denominada *ecuación característica* de la relación de recurrencia 3.3. Una sucesión $\{x_n\}$ satisface la relación de recurrencia 3.3 sii, por definición, para todo $n \geq k$ se cumple $x_n - \sum_{i=1}^{k} a_ix_{n-i} = 0$, donde $a_0 = 1$. Solucionar la relación de recurrencia 3.3 es encontrar una sucesión que la satisfaga y entonces la misma se denomina *solución* de la relación de recurrencia lineal homogénea.

Ejemplo 3.2.1.

- Para el ejemplo de la relación de recurrencia:

  $$u_n = 1{,}005u_{n-1}$$

  se tiene:

  - orden: $k = 1$
  - coeficientes: $a_1 = 1{,}005$
  - polinomio característico: $p(x) = x - 1{,}005$
  - ecuación característica: $x - 1{,}005 = 0$
  - solución: $\{c \cdot 1{,}005^n\}$

  Obsérvese que $1{,}005$ es la única solución de la ecuación característica.

- Para el ejemplo:

  $$u_n = u_{n-1} + u_{n-2}$$

  se tiene:

- orden: $k = 2$
- coeficientes: $a_1 = 1$, $a_2 = 1$
- polinomio característico: $p(x) = x^2 - x - 1$
- ecuación característica: $x^2 - x - 1 = 0$
- solución: $\{f_n\}$ donde

$$f_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

para todo $n \geq 0$.

Obsérvese que $\frac{1+\sqrt{5}}{2}$ y $\frac{1-\sqrt{5}}{2}$ son las dos soluciones de la ecuación característica.

Definición 3.2.2. Sea una relación de recurrencia lineal homogénea como la recurrencia 3.3 y supongamos que es de orden k. La matriz

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

es denominada la *matriz compañera* de la recurrencia 3.3.

Observación 3.2.1. La matriz compañera de la recurrencia 3.3 cumple la siguiente igualdad:

$$\begin{pmatrix} u_n \\ u_{n-1} \\ \vdots \\ u_{n-(k-2)} \\ u_{n-(k-1)} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} u_{n-1} \\ u_{n-2} \\ \vdots \\ u_{n-(k-1)} \\ u_{n-k} \end{pmatrix}$$

por lo que representa a dicha relación de recurrencia, junto a algunas igualdades triviales más. Si representamos por A a la matriz compañera de la recurrencia 3.3, la anterior igualdad puede ser escrita como:

$$\mathbf{u_n} = A\mathbf{u_{n-1}}$$

Lema 3.2.1. *Sea A una matriz compañera y supongamos que*

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

con $a_k \neq 0$. Entonces:

1. *El polinomio característico de A es $x^k - a_1x^{k-1} - \cdots - a_{k-1}x - a_k$.*
2. *Todos los valores propias de A son no nulos.*
3. *Para todo valor propio r de A, la sucesión $\{x_n\}$ definida por $x_n = r^n$ es una solución de la relación de recurrencia $\mathbf{u_n} = A\mathbf{u_{n-1}}$.*

Demostración. La primera afirmación se demuestra por inducción sobre k, claramente cierto para $k = 1$. Supongamos cierta la igualdad para $k = n-1$ y sea $k = n$. Desarrollando $\det(xI - A)$ por la última columna, la hipótesis de inducción da:

$$\begin{aligned}\det(xI - A) &= (-1)^{2n}x(x^{n-1} - a_1x^{n-2} - \cdots - a_{n-1}) + (-1)^{n-1}(-a_n)(-1)^{n-1} \\ &= x(x^{n-1} - a_1x^{n-2} - \cdots - a_{n-1}) + (-1)^{2n-2}(-a_n) \\ &= x(x^{n-1} - a_1x^{n-2} - \cdots - a_{n-1}) - a_n \\ &= x^n - a_1x^{n-1} - \cdots - a_{n-1}x - a_n\end{aligned}$$

Al ser el polinomio característico $x^k - a_1x^{k-1} - \cdots - a_{k-1}x - a_k$ y ser $a_k \neq 0$, es imposible que sea 0 un valor propio. Además se deduce del primer apartado que cualquier valor propio r de A, $x_n = r^n$ satisface la relación de recurrencia:

$$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_ku_{n-k}.$$

□

Observación 3.2.2. Observe lo siguiente:

1. Como consecuencia del Lema 3.2.1, todo polinomio mónico

   $$p(x) = x^k - a_1x^{k-1} - \cdots - a_{k-1}x - a_k$$

   con término independiente a_k no nulo es el polinomio característico de la matriz compañera A de una relación de recurrencia lineal homogénea. Dicha matriz se denomina también *matriz compañera* de $p(x)$.

2. Del Lema 3.2.1 se deduce que si tenemos una relación de recurencia de orden k:

   $$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_ku_{n-k}$$

   entonces la ecuación característica de la matriz compañera puede obtenerse de la relación de recurrencia reemplazando u_i por r^i y dividiendo la ecuación resultante por r^{n-k}. Esta relación entre la relación de recurrencia y la ecuación característica de la matriz A puede entenderse como una razón de por qué para cada valor propio r, la sucesión $\{r^n\}$ es una solución de la recurrencia.

Teorema 3.2.2. *Para toda relación de recurrecia lineal homogénea como la recurrencia 3.3, si A es su matriz compañera entonces el conjunto de soluciones de $\mathbf{x_n} = A\mathbf{x_{n-1}}$ es un espacio vectorial de dimensión k.*

Demostración. Sea W el conjunto de soluciones $\{x_n\}$ de la relación de recurrencia 3.3. Claramente la suma (término a término) de dos de sus soluciones es una solución y el producto de cualquier escalar por una solución es una solución. Así pues, las soluciones forman un espacio vectorial. Consideremos ahora la función:

$$f: W \longrightarrow \mathbb{C}^k$$

definida por $f(\{x_n\}) = \langle x_{k-1}, \ldots, x_1, x_0\rangle$. Así definida, f es una aplicación lineal. Por otra parte, f es biyectiva puesto que dados unos valores iniciales $x_{k-1}, \ldots, x_1, x_0$, estos generan recursivamente una única sucesión $\{x_n\}$ que es solución de la ecuación (cfr. el Teorema 2.3.1 y ejemplos de aplicación). Así pues $\dim W = \dim \mathbb{C}^k = k$. □

Definición 3.2.3. Una base del espacio de soluciones de una relación de recurrencia 3.3 es denominado un *conjunto fundamental de soluciones*. Una combinación lineal de los elementos de un conjunto fundamental de soluciones es denominada *solución general* y si los valores iniciales son especificados, la solución queda determinada y se denomina *solución particular*. denomina

Observación 3.2.3. En virtud del Teorema 3.2.2, para resolver una relación lineal de recurrencia de orden k basta con encontrar k soluciones linealmente independientes. Una solución general es una combinación lineal genérica de esas k soluciones.

Lema 3.2.3. *Sean $c_0, \ldots, c_k$ escalares para todo $0 \le i \le k$. Si*

$$\sum_{i=0}^{k} c_i n^i = 0 \tag{3.6}$$

para todo natural n, entonces para todo $0 \le i \le k$, $c_i = 0$.

Demostración. Haciendo variar n entre los números del conjunto $\{1, \ldots, k+1\}$ en la expresión 3.6 obtenemos $k+1$ ecuaciones que constituyen un sistema homogéneo de $k+1$ ecuaciones en las incógnitas $c_0, c_1, \ldots, c_k$. La matriz A asociada a ese sistema es:

$$\begin{pmatrix} 1 & 1 & 1^2 & \cdots & 1^k \\ 1 & 2 & 2^2 & \cdots & 2^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & k+1 & (k+1)^2 & \cdots & (k+1)^k \end{pmatrix}$$

Esta matriz es una instancia de la *matriz de Vandermonde* y es bien conocido que:

$$\det A = \prod_{1 \le i < j \le k+1} (j - i)$$

y por tanto $\det A \neq 0$. En consecuencia el sistema

$$A\mathbf{c} = 0$$

donde $\mathbf{c} = \begin{pmatrix} c_0 & c_1 & \cdots & c_k \end{pmatrix}^t$, es compatible determinado y no tiene más que la solución nula, es decir, para todo $0 \le i \le k$ se cumple $c_i = 0$. □

Teorema 3.2.4. *Sea una relación como la relación lineal homogénea de recurrencia 3.3 con matriz compañera A. Supongamos que:*

1. *A es diagonalizable con valores propios $r_1, \ldots, r_t$*
2. *y para todo $1 \le i \le t$, la mulptiplicidad de r_i es m_i y $1 \le m_i$ (si A es diagonalizable, $m_1 + \ldots + m_t = k$).*

Entonces:

$$\langle \{r_i^n\}, \{n r_i^n\}, \ldots, \{n^{m_i - 1} r_i^n\} : 1 \le i \le t \rangle$$

es un sistema fundamental del conjunto de soluciones.

Demostración. En las hipótesis del teorema, el polinomio característico de A es

$$p(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_{k-1} x - a_k$$

Sea $1 \le i \le t$ y sea r_i el valor propio de multiplicidad $m_i \ge 1$. Se tiene que:

$$p(r_i) = p'(r_i) = \cdots = p^{m_i - 1)}(r_i) = 0$$

Definamos una nueva función $P_1(x)$ mediante:

$$\begin{aligned} P_1(x) &= x^{n-k} p(x) \\ &= x^n - a_1 x^{n-1} - \cdots - a_{k-1} x^{n-k+1} - a_k x^{n-k} \end{aligned}$$

Como $P_1'(x) = (n-k)x^{n-k-1}p(x) + x^{n-k}p'(x)$, es claro que $P_1'(r_i) = 0$ y entonces $P_2(r_i) = r_i P_1'(r_i) = 0$. Esto es:

$$nr_i^n - a_1(n-1)r_i^{n-1} - \cdots - a_{k-1}(n-k+1)r_i^{n-k+1} - a_k(n-k)r_i^{n-k} = 0$$

lo que demuestra que $\{nr_i^n\}$ es también una solución de la relación de recurrencia. Inductivamente, $P_j(x) = xP_{j-1}'(x)$ cumple $P_j(r_i) = 0$, lo que demuestra que $\{n^{j-i}r_i^n\}$ es también una solución para $1 \leq j \leq m_i$. Así pues, concluimos que $\{r_i^n\}, \{nr_i^n\}, \ldots, \{n^{m_i-1}r_i^n\}$ son m_i soluciones de la relación de recurrencia. Más aún, son linealmente independites pues si

$$\begin{aligned} 0 &= c_0 r_i^n + c_1 n r_i^n + \ldots + c_{m_i-1} n^{m_i-1} r_i^n \\ &= (c_0 + c_1 n + \ldots + c_{m_i-1} n^{m_i-1}) r_i^n \end{aligned}$$

conlleva que para todo natural n:

$$0 = c_0 + c_1 n + \ldots + c_{m_i-1} n^{m_i-1}$$

Esto implica que para todo $0 \leq j \leq m_i - 1$, $c_j = 0$ según lo establecido en el Lema 3.2.3. Así tenemos una base del espacio propio asociado a r_i. Al unir tales soluciones linealmente independientes para cada valor propio r_i, alcanzamos a tener un conjunto fundamental de soluciones de la relación de recurrencia. □

Corolario 3.2.5. *Sea la relación de recurrencia 3.3, supongamos que:*

- *su ecuación característica (ecuación 3.5) tiene t raíces distintas: $r_1, \ldots, r_t$,*
- *para todo $1 \leq i \leq t$, la mulptiplicidad de r_i es m_i y $1 \leq m_i$,*
- $m_1 + \ldots + m_t = k$
- *y $\{x_n\}$ una sucesión.*

Son equivalentes las siguientes afirmaciones:

1. *$\{x_n\}$ es una solución de la relación de recurrencia 3.3.*
2. *Para todo $1 \leq i \leq t$ y $0 \leq j \leq m_i - 1$, existen constantes α_{ij}, tales que para todo natural n:*

$$\begin{aligned} x_n = &(\alpha_{10} + \alpha_{11} n + \cdots + \alpha_{1(m_1-1)} n^{m_1-1}) r_1^n \\ &+ (\alpha_{20} + \alpha_{21} n + \cdots + \alpha_{2(m_2-1)} n^{m_2-1}) r_2^n \\ &\vdots \\ &+ (\alpha_{t0} + \alpha_{t1} n + \cdots + \alpha_{t(m_t-1)} n^{m_t-1}) r_t^n \end{aligned} \tag{3.7}$$

Ejemplo 3.2.2. Supongamos que las raíces de la ecuación característica de una relación de recurrencia lineal homogénea con coeficientes constantes son: 2, 2, 2, 5, 5 y 9; es decir, hay tres raíces distintas: la raíz 2 con multiplicidad 3, la raíz 5 con multiplicidad 2 y la raíz 9 con multiplicidad 1.

Solución. Según el Corolario 3.2.5 la forma general de la solución es:

$$(\alpha_{10} + \alpha_{11} n + \alpha_{12} n^2) 2^n + (\alpha_{20} + \alpha_{21} n) 5^n + \alpha_{30} 9^n$$

□

Ejemplo 3.2.3. Encuentre el número de Fibonacci que ocupa la posición 2000.

Solución. Consideramos la ecuación trivial extra $u_n = u_n$ junto con la ecuación dada:

$$\begin{cases} u_{n+1} &= u_n + u_{n-1} \\ u_n &= u_n \end{cases}$$

En la notación matricial:

$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix}$$

que es de la forma:

$$\mathbf{u_n} = \mathbf{A}\mathbf{u_{n-1}} = \mathbf{A}^n\mathbf{u_0}$$

donde $\mathbf{u_n} = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$, $\mathbf{u_0} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ y $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Así pues, el problema se reduce a calcular $\mathbf{A}^n$ y esto sabemos que pasa por diagonalizar la matriz. Un simple cálculo nos lleva a los valores propios $\lambda_1 = \frac{1}{2}(1+\sqrt{5})$ y $\lambda_2 = \frac{1}{2}(1-\sqrt{5})$ de $\mathbf{A}$ y sus vectores propios asociados $\mathbf{v_1} = \langle \lambda_1, 1 \rangle$ y $\mathbf{v_2} = \langle \lambda_2, 1 \rangle$, respectivamente. Por otra parte, la matriz de paso y su inversa hallamos que son:

$$\mathbf{P} = [\mathbf{v_1}\ \mathbf{v_2}] = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 1 & 1 \end{pmatrix} \qquad \mathbf{P}^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -\frac{1-\sqrt{5}}{2} \\ -1 & \frac{1+\sqrt{5}}{2} \end{pmatrix}$$

donde:

$$\mathbf{D} = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{pmatrix}$$

Así pues:

$$\mathbf{A}^n = \mathbf{P}\mathbf{D}^n\mathbf{P}^{-1} = \mathbf{P} \begin{pmatrix} \left(\frac{1+\sqrt{5}}{2}\right)^n & 0 \\ 0 & \left(\frac{1-\sqrt{5}}{2}\right)^n \end{pmatrix} \mathbf{P}^{-1}$$

Por ejemplo, si $n = 2000$, entonces:

$$\begin{aligned} \begin{pmatrix} x_{2001} \\ u_{2000} \end{pmatrix} &= \mathbf{x_{2000}} \\ &= \mathbf{A}^{2000} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \mathbf{P}\mathbf{D}^{2000}\mathbf{P}^{-1}\mathbf{x_0} \\ &= \frac{1}{\sqrt{5}} \begin{pmatrix} \lambda_1^{2001} - \lambda_2^{2001} \\ \lambda_1^{2000} - \lambda_2^{2000} \end{pmatrix} \end{aligned}$$

Esto da:

$$x_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

para todo número natural n. Obsérvese que como x_{2000} debe ser un entero, buscaremos el entero más cercano al gran número $\left(\frac{1+\sqrt{5}}{2}\right)^{2000}$, porque $\left(\frac{1-\sqrt{5}}{2}\right)^k$ es realmente muy pequeño cuando k es grande. Históricamente, el número $\frac{1+\sqrt{5}}{2}$, que es muy cercano a $\frac{x_{2001}}{x_{2000}}$, es denominado la *razón de oro*. □

3.3. Teoría de la Recurrencia Lineal No Homogénea

Definición 3.3.1. Sea k un número natural. Una relación de *recurrencia lineal no homogénea* de orden k es cualquier igualdad de la forma:

$$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_ku_{n-k} + f(n), \text{ para todo } n \geq k \tag{3.8}$$

donde $a_1, \ldots, a_k$ son constantes y $f(n)$ es una función no idénticamente nula que depende únicamente de n, que denominaremos *función de ajuste*. Su relación de recurrencia lineal homogénea asociada es:

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} \tag{3.9}$$

El orden, el polinomio característico y la ecuación característica de la relación de recurrencia 3.8 es el de la relación de recurrencia 3.9.

Teorema 3.3.1. *Si $\{x_n^{(p)}\}$ es una solución particular de la relación de recurrencia lineal no homogénea:*

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + f(n),$$

entonces toda solución es de la forma $\{x_n^{(p)} + x_n^{(h)}\}$, donde $\{x_n^{(h)}\}$ es una solución de la relación de recurrencia lineal homogénea asociada.

Demostración. Como $\{x_n^{(p)}\}$ es una solución particular de la relación de recurrencia lineal no homogénea, sabemos que

$$x_n^{(p)} = a_1 x_{n-1}^{(p)} + a_2 x_{n-2}^{(p)} + \cdots + a_k x_{n-k}^{(p)} + f(n)$$

Si $\{y_n\}$ es otra solución de la relación de recurrencia lineal no homogénea, sabemos que:

$$y_n = a_1 y_{n-1} + a_2 y_{n-2} + \cdots + a_k y_{n-k} + f(n)$$

Restando la primera de esta igualdades de la segunda, obtenemos que:

$$y_n - x_n^{(p)} = a_1(y_{n-1} - x_{n-1}^{(p)}) + a_2(y_{n-2} - x_{n-2}^{(p)}) + \cdots + a_k(y_{n-k} - x_{n-k}^{(p)})$$

Por tanto, $\{y_n - x_n^{(p)}\}$ es una solución de la relación de recurrencia lineal homogénea asociada, que denotamos por $\{x_n^{(h)}\}$. Por tanto, $y_n = x_n^{(p)} + x_n^{(h)}$ para todo natural n. □

Observación 3.3.1. Antes de abordar la demostración del Lema 3.3.2 analicemos un ejemplo. Considérese la relación de recurrencia lineal no homogénea:

$$u_n = 4u_{n-1} - 4u_{n-2} + (3 + 2n)s^n \tag{3.10}$$

donde s es una constante. Entonces para la recurrencia 3.10:

- $k = 2$.
- la ecuación característica de la recurrencia homogénea asociada es $x^2 - 4x + 4 = 0$.
- $q(n) = 2n + 3$, $d = \deg q(n) = 1$ y $d + 1 = 2$.

Para toda solución $\{x_n\}$ de la recurrencia 3.10 se cumple:

$$\begin{array}{rcrcrcl} x_n & - & 4x_{n-1} & + & 4x_{n-2} & = & (3+2n)s^n \\ & & sx_{n-1} & - & 4sx_{n-2} + 4sx_{n-3} & = & s(3+2(n-1))s^{n-1} = (3+2(n-1))s^n \end{array}$$

y restando ambas igualdades resulta:

$$x_n - (4+s)x_{n-1} + (4+4s)x_{n-2} - 4sx_{n-3} = 2s^n$$

de donde $\{x_n\}$ satisface la recurrencia:

$$u_n - (4+s)u_{n-1} + (4+4s)u_{n-2} - 4su_{n-3} = 2s^n$$

que tiene por ecuación característica:

$$(x^2 - 4x + 4)(x - s)$$

Repitiendo lo anterior para este nuevo caso, tenemos:

$$\begin{array}{rcrcrcrcr} x_n & - & (4+s)x_{n-1} & + & (4+4s)x_{n-2} & - & 4sx_{n-3} & = & 2s^n \\ & & sx_{n-1} & - & (4+s)sx_{n-2} & + & (4+4s)sx_{n-3} & - & 4s^2x_{n-4} \quad = \quad s2s^{n-1} = 2s^n \end{array}$$

y restando resulta que $\{x_n\}$ satisface la relación homogénea:

$$x_n - (4+2s)x_{n-1} + (4+8s+s^2)x_{n-2} - (8s+4s^2)x_{n-3} + 4s^2x_{n-4} = 0$$

que tiene por ecuación característica:

$$(x^2 - 4x + 4)(x-s)^2$$

Lo anterior inspira el enunciado del Lema 3.3.2 y su demostración.

Lema 3.3.2. *Sea la relación de recurrencia lineal no homogénea:*

$$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_ku_{n-k} + q(n)s^n, \tag{3.11}$$

donde, $a_k \neq 0$, s es una constante y $q(n)$ un polinomio en n no nulo tal que $\deg q(n) = d$. Si $\{x_n\}$ es una solución de la recurrencia 3.11 entonces satisface una relación de recurrencia cuya ecuación característica es:

$$(x^k - a_1x^{k-1} - \cdots - a_k)(x-s) = 0$$

y función de ajuste $p(n)s^n$, donde $p(n)$ es un polinomio en n tal que:

- $p(n) = 0$, *siempre que* $d = 0$
- $\deg p(n) = d-1$, *siempre que* $d > 0$.

Demostración. Supongamos que $q(n) = b_0 + b_1n + \cdots + b_dn^d$, donde $0 \leq d$ y $b_d \neq 0$. Si $\{x_n\}$ satisface la relación de recurrencia recurrencia 3.11, entonces:

$$x_n - a_1x_{n-1} - a_2x_{n-2} - \cdots - a_kk_{n-k} = q(n)s^n, \tag{3.12}$$

Sustituyendo n por $n-1$ en la relación 3.12 y multiplicando por s obtenemos:

$$sx_{n-1} - a_1sx_{n-2} - a_2sx_{n-2} - \cdots - a_ksk_{n-(k-1)} = q(n-1)s^{n-1}s = q(n-1)s^n \tag{3.13}$$

Restando de la igualdad 3.12 la igualdad 3.13 resulta:

$$x_n - (a_1+s)x_{n-1} - (a_2+a_1s)x_{n-2} - \cdots - a_ksx_{n-(k-1)} = p(n)s^n \tag{3.14}$$

donde $p(n) = q(n) - q(n-1)$. Hemos de distinguir dos casos:

- $d = 0$; entonces $q(n) = b_0$ y $p(n) = 0$.
- $d > 0$; entonces:

$$\begin{aligned} p(n) &= q(n) - q(n-1) \\ &= (b_0 + b_1n + \cdots + b_dn^d) - (b_0 + b_1(n-1) + \cdots + b_d(n-1)^d) \\ &= r(n) + \binom{d}{1}b_dn^{d-1} + (b_d - b_d\binom{d}{0})n^d \\ &= r(n) + db_dn^{d-1} + (b_d - b_d)n^d \\ &= r(n) + db_dn^{d-1} + 0n^d \\ &= r(n) + db_dn^{d-1} \end{aligned}$$

  donde $r(n)$ es un polinomio nulo o de grado menor que $d-1$. Hemos supuesto que $b_d \neq 0$ y que $d > 0$, de donde $db_d \neq 0$; como consecuencia $\deg p(n) = d-1$.

Para lo que resta, basta observar que la ecuación característica de la recurrencia 3.14, satisfecha por $\{x_n\}$, es:

$$(x^k - a_1x^{k-1} - \cdots - a_k)(x - s)$$

□

Teorema 3.3.3. *Sea la relación de recurrencia lineal no homogénea:*

$$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_ku_{n-k} + q(n)s^n, \tag{3.15}$$

donde, $a_k \neq 0$, s es una constante, $q(n)$ es un polinomio en n no nulo y $\deg q(n) = d$. Si $\{x_n\}$ es una solución de la recurrencia 3.15 entonces satisface una relación de recurrencia lineal homogéna cuya ecuación característica es

$$(x^k - a_1x^{k-1} - \cdots - a_k)(x - s)^{d+1} = 0$$

Demostración. Supongamos que $\{x_n\}$ es una solución de la recurrencia 3.15 en las condiciones del enunciado del teorema. Al ser $q(n)$ no nulo, se cumple $d \geq 0$. La demostración puede ser efectuada entonces por inducción sobre d. En el caso $d = 0$, el Lema 3.3.2 asevera que $\{x_n\}$ es solución de una relación de recurrencia de ecuación característica:

$$(x^k - a_1x^{k-1} - \cdots - a_k)(x - s) = 0$$

y función de ajuste $q(n)s^n = 0s^n = 0$, es decir, dicha relación es homogénea. Supongamos que $d \geq 1$ y que el resultado es cierto para $d - 1$. De nuevo por el Lema 3.3.2 tenemos que $\{x_n\}$ es solución de una relación de recurrencia de ecuación característica:

$$(x^k - a_1x^{k-1} - \cdots - a_k)(x - s) = 0$$

y función de ajuste $p(n)s^n$, donde $\deg p(n) = d-1$. Usando la hipótesis de inducción obtenemos que $\{x_n\}$ satisface entonces una relación de recurrencia lineal homogénea de ecuación característica:

$$(x^k - a_1x^{k-1} - \cdots - a_k)(x - s)(x - s)^d = 0$$

Por el *teorema de inducción*, el resultado es cierto. □

Corolario 3.3.4. *Sea la relación de recurrencia lineal no homogénea:*

$$u_n = a_1u_{n-1} + a_2u_{n-2} + \cdots + a_ku_{n-k} + q(n)s^n, \tag{3.16}$$

donde, $a_k \neq 0$, s es una constante y $q(n)$ es un polinomio. Entre las soluciones de la recurrencia 3.16 tiene una, $\{x_n^{(p)}\}$, de la forma:

$$x_n^{(p)} = n^m p(n)s^n \tag{3.17}$$

para todo natural n, donde m es la multiplicidad de s como raíz del polinomio característico de la recurrencia 3.16 y $p(n)$ es un polinomio de grado menor o igual que el grado de $q(n)$.

Demostración. En virtud del Lema 3.3.3, si $\{x_n\}$ es cualquier solución de la recurrencia 3.16 entonces también satisface una relación de recurrencia lineal homogénea cuya ecuación característica es:

$$(x^k - a_1x^{k-1} - \cdots - a_k)(x - s)^{d+1} = 0$$

Entonces podemos obtener una expresión no recurrente para $\{x_n\}$ que, por el Corolario 3.2.5, tendrá la forma:

$$\begin{aligned} x_n = {} & (\alpha_{10} + \alpha_{11}n + \cdots + \alpha_{1(m_1-1)}n^{m_1-1})r_1^n \\ & + (\alpha_{20} + \alpha_{21}n + \cdots + \alpha_{2(m_2-1)}n^{m_2-1})r_2^n \\ & \vdots \\ & + (\alpha_{t0} + \alpha_{t1}n + \cdots + \alpha_{t(m_t-1)}n^{m_t-1})r_t^n \end{aligned}$$

y en este momento procede distinguir si s es una solución de $x^k - a_1x^{k-1} - \cdots - a_k$, digamos —para fijar ideas— r_1, o no. En caso afirmativo la expresión es:

$$\begin{aligned} x_n = &(\alpha_{10} + \alpha_{11}n + \cdots + \alpha_{1(m_1-1)}n^{m_1-1})r_1^n \\ &+ (\alpha_{1m_1}n^{m_1} + \cdots + \alpha_{1(m_1+d)}n^{m_1+d})r_1^n \\ &+ (\alpha_{20} + \alpha_{21}n + \cdots + \alpha_{2(m_2-1)}n^{m_2-1})r_2^n \\ &\vdots \\ &+ (\alpha_{t0} + \alpha_{t1}n + \cdots + \alpha_{t(m_t-1)}n^{m_t-1})r_t^n \end{aligned} \tag{3.18}$$

y en caso negativo, la expresión es:

$$\begin{aligned} x_n = &(\alpha_{10} + \alpha_{11}n + \cdots + \alpha_{1(m_1-1)}n^{m_1-1})r_1^n \\ &+ (\alpha_{20} + \alpha_{21}n + \cdots + \alpha_{2(m_2-1)}n^{m_2-1})r_2^n \\ &\vdots \\ &+ (\alpha_{t0} + \alpha_{t1}n + \cdots + \alpha_{t(m_t-1)}n^{m_t-1})r_t^n \\ &+ (\alpha_{s0} + \alpha_{s1}n + \cdots + \alpha_{sd}n^d)s^n \end{aligned} \tag{3.19}$$

Como $\{x_n^{(h)}\}$ definida para todo n por

$$\begin{aligned} x_n = &(\alpha_{10} + \alpha_{11}n + \cdots + \alpha_{1(m_1-1)}n^{m_1-1})r_1^n \\ &+ (\alpha_{20} + \alpha_{21}n + \cdots + \alpha_{2(m_2-1)}n^{m_2-1})r_2^n \\ &\vdots \\ &+ (\alpha_{t0} + \alpha_{t1}n + \cdots + \alpha_{t(m_t-1)}n^{m_t-1})r_t^n \end{aligned} \tag{3.20}$$

es una solución de la recurrencia lineal homogénea asociada a la recurrencia 3.16, entonces (en virtud del Teorema 3.3.1) obtendremos que una solución particular de la recurrencia 3.10 es $\{x_n^{(p)}\}$ definida para todo n por:

$$\begin{aligned} x_n^{(p)} &= x_n - x_n^{(h)} \\ &= \begin{cases} n^{m_1}(\alpha_{1m_1} + \cdots + \alpha_{1(m_1+d)}n^d)r_1^n & \text{, si } s = r_1 \\ (\alpha_{s0} + \alpha_{s1}n + \cdots + \alpha_{sd}n^d)s^n & \text{, si } s \text{ no es ninguno de los } r_i \end{cases} \end{aligned}$$

y en todo caso

$$x_n^{(p)} = \begin{cases} n^{m_1}(\alpha_{1m_1} + \cdots + \alpha_{1(m_1+d)}n^d)r_1^n & \text{, si } s = r_1 \\ n^0(\alpha_{s0} + \alpha_{s1}n + \cdots + \alpha_{sd}n^d)s^n & \text{, si } s \text{ no es ninguno de los } r_i \end{cases}$$

□

Observación 3.3.2. Téngase en cuenta que:

- Podríamos dar una expresión general de los coeficientes de $p(n)$ en la solución particular de la igualdad 3.17, pero sería complicada. Para conocer el polinomio $p(n)$ en los casos prácticos, se lleva la solución 3.17 —con sus coeficientes indeterminados— a la ecuación de recurrencia y, efectuadas las operaciones, se llega a una igualdad entre polinomio del mismo grado: uno conocido y el otro desconocido. Ello produce un sistema de ecuaciones en los coeficientes indeterminados de $p(n)$ que, resuelto, permite conocerlos.
- La solución particular de la expresión 3.17 no puede adaptarse a condiciones iniciales arbitrarias; así pues, podría no ser la solución que se estuviese buscando.
- En ese caso sería imprescindible encontrar *todas* las soluciones mediante lo indicado por el Teorema 3.3.1 y luego seleccionar la específica cumpliendo las condiciones iniciales.

3.4. Ejemplos de Recurrencia Lineal Homogénea

En la presente sección abordamos el estudio y resolución de ejemplos concretos de relaciones de recurrencia lineales homogéneas. El estudio será llevado a cabo como aplicación del Corolario 3.2.5

Observación 3.4.1. Supongamos estar en el ambiente del Corolario 3.2.5 y revisemos los caso elementales:

- En el caso $k = 1$, el polinomio característico de la relación de recurrencia no tendrá más que una raíz, digamos r. Así, la expresión 3.7 se concreta en:

  $$x_n = \alpha r^n$$

  para todo natural n.

- En el caso $k = 2$, si el polinomio característico tiene coeficientes reales, respecto a sus raíces caben las siguientes posibilidades:

  - r_1 y r_2 son ambas reales y distintas; la expresión 3.7 se concreta en:

    $$x_n = c_1 r_1^n + c_2 r_2^n$$

    para todo natural n.
  - Si $r_1 = r_2$ y llamamos r a r_1, la expresión 3.7 se concreta en:

    $$x_n = (c_1 + c_2 n) r^n$$

    para todo natural n.
  - r_1 y r_2 complejas y conjugadas; si expresados en forma polar r_1 y r_2 son:

    $$r_1 = r(\cos\theta + i\sin\theta)$$
    $$r_2 = r(\cos\theta - i\sin\theta)$$

    entonces, según expresión 3.7:

    $$\begin{aligned} x_n &= c_1 r^n(\cos(n\theta) + i\sin(n\theta)) + c_2 r^n(\cos(n\theta) - i\sin(n\theta)) \\ &= r^n(c_1(\cos(n\theta) + i\sin(n\theta)) + c_2(\cos(n\theta) - i\sin(n\theta))) \\ &= r^n((c_1 + c_2)\cos(n\theta) + (c_1 - c_2)i\sin(n\theta)) \\ & r^n(k_1\cos(n\theta) + k_2\sin(n\theta)) \end{aligned}$$

    donde $k_1 = c_1 + c_2$ y $k_2 = (c_1 - c_2)i$.

- En el caso en que la ecuación característica (ecuación 3.5) tenga k raíces distintas: $r_1, \ldots, r_k$, la expresión 3.7 se concreta en:

  $$x_n = \alpha_1 r_1^n + \cdots + \alpha_k r_k^n$$

  para todo natural n.

Ejemplo 3.4.1. Resuelva la relación de recurrencia $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$. Particularice el resultado suponiendo que $F_0 = 0$ y $F_1 = 1$ (esta relación es conocida como *relación de Fibonacci* y su solución *sucesión de Fibonacci*).

Solución. La ecuación característica para este ejemplo es $r^2 - r - 1 = 0$ y sus raíces son $r_1 = \frac{1+\sqrt{5}}{2}$ y $r_2 = \frac{1-\sqrt{5}}{2}$. Como se tienen dos raíces reales distintas, $F_n = (\frac{1+\sqrt{5}}{2})^n$ y $F_n = (\frac{1-\sqrt{5}}{2})^n$ son soluciones; además, son linealmente independientes, pues una no es múltiplo de la otra. De este modo

$$F_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n \tag{3.21}$$

es la solución general, donde c_1 y c_2 son constantes arbitrarias. Si conocemos los valores de los dos primeros términos de la sucesión solución será posible determinar los valores de c_1 y c_2:

$$\begin{aligned} 0 = F_0 &= c_1 + c_2 \\ 1 = F_1 &= c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) \end{aligned}$$

Por tanto, $-c_1 = c_2$ y entonces:

$$\begin{aligned} 2 &= c_1(1+\sqrt{5}) - c_1(1-\sqrt{5}) \\ &= 2\sqrt{5}c_1 \end{aligned}$$

de donde

$$c_1 = \frac{1}{\sqrt{5}}$$

y en definitiva se tiene que la solución general será:

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

□

Ejemplo 3.4.2. Resuelva la relación de recurrencia dada por $u_{n+2} = 4u_{n+1} - 4u_n$, para todo $n \geq 0$. Particularice el resultado suponiendo que $n \geq 0$, $u_0 = 1$, $u_1 = 3$.

Solución. La relación de recurrencia dada es:

$$u_{n+2} - 4u_{n+1} + 4u_n = 0$$

para la que $k = n + 2 - n = 2$ y la ecuación característica es:

$$0 = x^2 - 4x + 4 = (x-2)^2$$

por lo que la solución general, según el Corolario 3.2.5, es de la forma:

$$(c_1 + c_2 n)2^n$$

Para particularizar la solución al caso de las condiciones iniciales dadas consideraremos lo siguiente:

$$\begin{aligned} 1 = u_0 &= (c_1 + 0c_2)2^0 = c_1 1 = c_1 \\ 3 = u_1 &= (c_1 + 1c_2)2^1 = (1 + c_2)2 \qquad\qquad \Rightarrow c_2 = \frac{1}{2} \end{aligned}$$

lo que nos lleva a:

$$\begin{aligned} x_n &= (1 + \frac{1}{2}n)2^n \\ &= 2^n + \frac{1}{2}n2^n \\ &= 2^n + n2^{n-1} \end{aligned}$$

por lo que la solución particular es para todo natural n:[1]

$$x_n = 2^n + n2^{n-1}$$

□

[1] Observar que para $n = 0$ aún tiene sentido $2^0 + 0 \cdot 2^{-1}$ y es $1 + 0 \cdot \frac{1}{2} = 1$.

Observación 3.4.2. En el que caso $k = 2$, suponiendo que el polinomio característico de la relación de recurrencia —que tendrá coeficientes reales— es irreducible, entonces no tendrá raíces reales y sí las dos complejas y distintas (si tiene una compleja, la otra debe ser la conjugada). En este caso aún es posible la resolución de la recurrencia, basta considerar que el cuerpo en el que se formula es el de los números complejos.

Antes de abordar el siguiente ejemplo debemos recordar algo sobre los número complejos:

1. Dado un número complejo $z = x + iy$, definimos $|z|$ por la siguiente igualdad:
$$|z| = \sqrt{x^2 + y^2}$$
2. Dado un número complejo $z = x + iy$, definimos $Re(z)$ e $Im(z)$ con las siguientes igualdades:
$$Re(z) = x \qquad\qquad Im(z) = y$$
3. Para todo número complejo z no nulo existen un número real r_z y un ángulo θ_z, expresado en radianes, tal que:
$$z = r_z(\cos\theta_z + i\sin\theta_z)$$
4. Dado un número complejo z no nulo,
$$r_z = |z|$$
$$\theta_z = \begin{cases} 2\arctan\frac{Im(z)}{Re(z)+|z|} & \text{, si } z \notin \mathbb{R}^- \\ \pi & \text{, si } z \in \mathbb{R}^- \end{cases}$$
5. El *Teorema de DeMoivre* que dice que si $z = r(\cos\theta + i\sin\theta)$ y n es un número natural, entonces:
$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

y recordar también la fórmula trigonométrica:

$$\operatorname{tg}(\frac{a}{2}) = \frac{\sin a}{1+\cos a}$$

Ejemplo 3.4.3. Calcule $(1 + i\sqrt{3})^{10}$

Solución. Sea $z = 1 + i\sqrt{3}$. Se tiene que $r_z = \sqrt{1^2 + (\sqrt{3})^2} = 2$. Por otra parte, dado que $z \notin \mathbb{R}^-$:

$$\frac{Im(z)}{Re(z)+|z|} = \frac{\sqrt{3}}{1+2} = \frac{\sqrt{3}}{3} = \frac{1}{\sqrt{3}}$$

y sabemos que $\arctan(1/\sqrt{3}) = \pi/6$. Mulitplicando por 2, resulta $\pi/3 = 2\arctan(1/\sqrt{3})$ y por tanto $\theta_z = \pi/3$. Entonces:

$$1 + i\sqrt{3} = 2(\cos(\pi/3) + i\sin(\pi/3))$$

y por tanto

$$\begin{aligned}(1 + i\sqrt{3})^{10} &= 2^{10}(\cos(10\pi/3) + i\sin(10\pi/3)) \\ &= 2^{10}(\cos((2\cdot 3 + 2\cdot 2)\pi/3) + i\sin((2\cdot 3 + 2\cdot 2)\pi/3)) \\ &= 2^{10}(\cos(2\pi + 4\pi/3) + i\sin(2\pi + 4\pi/3)) \\ &= 2^{10}(\cos(4\pi/3) + i\sin(4\pi/3)) \\ &= 2^{10}((-1/2) - i(\sqrt{3}/2)) \\ &= -2^9(1 + i\sqrt{3})\end{aligned}$$

□

Ejemplo 3.4.4. Encuentre la expresión polar de $z = 1 + i$

Solución. Sea $z = 1 + i$. Entonces: $|z| = \sqrt{2}$, $Re(z) = 1$ e $Im(z) = 1$. Se tiene lo siguiente:

$$\begin{aligned}\frac{1}{1+\sqrt{2}} &= \frac{2}{2\sqrt{2}+2}\\ &= \frac{\sqrt{2}}{2+\sqrt{2}}\\ &= \frac{\frac{\sqrt{2}}{2}}{1+\frac{\sqrt{2}}{2}}\\ &= \frac{\sin(\pi/4)}{1+\cos(\pi/4)}\\ &= \tan(\frac{\pi/4}{2})\end{aligned}$$

luego $\pi/4 = 2\arctan(\frac{1}{1+\sqrt{2}})$. Por tanto:

$$1 + i = \sqrt{2}(\cos(\pi/4) + i\sin(\pi/4))$$

□

Ejemplo 3.4.5. Resuelva la relación de recurrencia dada por $u_n = 2(u_{n-1} - u_{n-2})$, para todo $n \geq 2$. Particularice el resultado suponiendo que $u_0 = 1$, $u_1 = 2$.

Solución. La recurrencia propuesta es de orden 2 y su ecuación característica es:

$$0 = x^2 - 2x + 2$$

que tiene por soluciones $1 \pm i$. Según sabemos:

$$1 + i = \sqrt{2}(\cos(\pi/4) + i\sin(\pi/4))$$

De lo detallado en la observación 3.4.1 resulta entonces que:

$$x_n = (\sqrt{2})^n(k_1\cos(n\pi/4) + k_2\sin(n\pi/4))$$

Ahora bien:

$$\begin{aligned}1 = u_0 &= k_1\cos 0 + k_2\sin 0 = k_1 && \Rightarrow k_1 = 1\\ 2 = u_1 &= \sqrt{2}(\cos(\pi/4) + k_2\sin(\pi/4))\\ &= 1 + k_2 && \Rightarrow k_2 = 1\end{aligned}$$

Así pues, la solución general está dada por:

$$x_n = (\sqrt{2})^n(\cos(n\pi/4) + \sin(n\pi/4))$$

para todo número natural n. Observe que esta solución no contiene números complejos. Esto se debe a que los valores c_1 y c_2 de la observación 3.4.1 son complejos conjugados, y por tanto k_1 y k_2 son entonces reales. □

Ejemplo 3.4.6. Halle u_{12} si $u_{n+1}^2 = 5u_n^2$, $u_n \geq 0$, $n \geq 0$ y $u_0 = 2$.

Solución. No se trata de una relación de recurrencia lineal en u_n, pero se puede tratar como tal. Para ello hagamos un cambio de variable, a saber, $b_n = u_n^2$. Entonces la nueva relación es $b_{n+1} = 5b_n$, $n \geq 0$, $b_0 = 4$. La solución es entonces, $b_n = 4 \cdot 5^n$ y por tanto $u_n = 2\sqrt{5}^n$, $n \geq 0$. Así $u_{12} = 31250$. □

Ejemplo 3.4.7. Resuelva la relación de recurrencia:

$$u_n = nu_{n-1}, \text{ para todo } n \geq 1.$$

y particularice el resultado suponiendo $u_0 = 1$.

Solución. Se trata de una relación (lineal homogénea), pero **no** de coeficientes constantes. La resolveremos usando la inducción. Se tiene:

$$\begin{aligned}
u_0 &= 1 \\
u_1 &= 1 \cdot u_0 = 1 \\
u_2 &= 2u_1 = 2 \cdot 1 \\
u_3 &= 3u_2 = 3 \cdot 2 \cdot 1 \\
u_4 &= 4u_3 = 4 \cdot 3 \cdot 2 \cdot 1 \\
&\vdots \qquad\qquad \vdots
\end{aligned}$$

Es muy fácil demostrar por inducción que $u_n = n!$, o sea $\{u_n\}$ es la sucesión que cuenta el número de permutaciones de n objetos. □

Ejercicio 3.4.1. Considere las siguientes recurrencias:

$$\begin{aligned}
s_n &= 2s_{n-1} + s_{n-2} + 4t_{n-1}, \quad n \geq 2 \\
t_n &= s_{n-1} + t_{n-1}, \quad n \geq 2
\end{aligned}$$

y resuelva la primera.

Solución. Tenemos lo siguiente:

$$\begin{aligned}
s_n &= 2s_{n-1} + s_{n-2} + 4t_{n-1} \\
s_{n-1} &= 2s_{n-2} + s_{n-3} + 4t_{n-2}
\end{aligned}$$

Si restamos la segunda igualdad de la primera tenemos:

$$\begin{aligned}
s_n - s_{n-1} &= (2s_{n-1} + s_{n-2} + 4t_{n-1}) - (2s_{n-2} + s_{n-3} + 4t_{n-2}) \\
&= 2s_{n-1} - s_{n-2} - s_{n-3} + 4t_{n-1} - 4t_{n-2} \\
s_n &= 3s_{n-1} - s_{n-2} - s_{n-3} + 4t_{n-1} - 4t_{n-2} \\
&= 3s_{n-1} - s_{n-2} - s_{n-3} + 4(t_{n-1} - t_{n-2})
\end{aligned}$$

Por otra parte tenemos:

$$\begin{aligned}
t_n &= s_{n-1} + t_{n-1} \\
t_{n-1} &= s_{n-2} + t_{n-2} \\
t_{n-1} - t_{n-2} &= s_{n-2}
\end{aligned}$$

Ahora:

$$\begin{aligned}
s_n &= 3s_{n-1} - s_{n-2} - s_{n-3} + 4(t_{n-1} - t_{n-2}) \\
&= 3s_{n-1} - s_{n-2} - s_{n-3} + 4s_{n-2} \\
&= 3s_{n-1} + 3s_{n-2} - s_{n-3}
\end{aligned}$$

En definitiva:

$$s_n = 3s_{n-1} + 3s_{n-2} - s_{n-3}$$

recurrencia que tiene por ecuación característica:

$$\begin{aligned} 0 = x^3 - 3x^2 - 3x + 1 &= (x+1)(x^2 - 4x + 1) \\ &= (x+1)(x - 2 + \sqrt{3})(x - 2 - \sqrt{3}) \end{aligned}$$

y por tanto, sus soluciones son: -1, $2 \pm \sqrt{3}$. Así pues,

$$s_n = c_1(2+\sqrt{3})^n + c_2(2-\sqrt{3})^n + c_3(-1)^n$$

Abordando el problema matricialmente, tenemos que la recurrencia propuesta puede ser expresada mediante la igualdad siguiente:

$$\begin{pmatrix} u_n \\ u_{n-1} \\ t_n \end{pmatrix} = \begin{pmatrix} 2 & 1 & 4 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} u_{n-1} \\ u_{n-2} \\ t_{n-1} \end{pmatrix}$$

Si A es la matrix:

$$\begin{pmatrix} 2 & 1 & 4 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Resulta que el polinomio característico de A es:

$$\begin{aligned} p_A(\lambda) &= \lambda^3 - 3\lambda^2 - 3\lambda + 1 \\ &= (\lambda+1)(\lambda - 2 + \sqrt{3})(\lambda - 2 - \sqrt{3}) \end{aligned}$$

Por lo que A es diagonalizable y existen una matriz regular P y una matriz diagonal D tal que $D = P^{-1}AP$. En realidad:

$$D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2-\sqrt{3} & 0 \\ 0 & 0 & 2+\sqrt{3} \end{pmatrix}$$

$$P = \begin{pmatrix} -2 & 1-\sqrt{3} & 1+\sqrt{3} \\ 2 & -1-\sqrt{3} & -1+\sqrt{3} \\ 1 & 1 & 1 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} -\frac{1}{6} & \frac{1}{6} & \frac{1}{3} \\ \frac{1}{12}(1-\sqrt{3}) & \frac{1}{12}(-1-\sqrt{3}) & \frac{1}{3} \\ \frac{1}{12}(1+\sqrt{3}) & \frac{1}{12}(-1+\sqrt{3}) & \frac{1}{3} \end{pmatrix}$$

y por tanto:

$$A^n = PD^nP^{-1} = P \begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & (2-\sqrt{3})^n & 0 \\ 0 & 0 & (2+\sqrt{3})^n \end{pmatrix} P^{-1}$$

□

3.5. Ejemplos de Recurrencia Lineal No Homogénea

Observación 3.5.1. Considere lo siguiente:

1. Cuando $f(n) = b_t n^t + b_{t-1}n^{t-1} + \cdots + b_1 n + b_0$ estamos en el caso particular $s = 1$ de $f(n) = (b_t n^t + b_{t-1}n^{t-1} + \cdots + b_1 n + b_0)s^n$.

2. Cuando $f(n) = s^n$, estamos en el caso particular $b_i = 0$, para todo $1 \leq i \leq t$ y $b_0 = 1$.

3. En lo sucesivo a la solución particular la representaremos por $\{x_n^{(p)}\}$.

Ejemplo 3.5.1. Considere la relación de recurrencia:

$$u_n = 5u_{n-1} - 6u_{n-2} + f(n)$$

La ecuación característica de su relación de recurrencia homogénea asociada es:

$$0 = x^2 - 5x + 6 = (x-2)(x-3)$$

1. Si $f(n) = 2n^2$, entonces $x_n^{(p)} = c_2n^2 + c_1n + c_0$.
2. Si $f(n) = 5^n(3n^2 + 2n + 1)$, entonces $x_n^{(p)} = 5^n(c_2n^2 + c_1n + c_0)$.
3. Si $f(n) = 5^n$, entonces $x_n^{(p)} = c5^n$ (¿por qué?).
4. Si $f(n) = 2^n(3n + 1)$, entonces $x_n^{(p)} = 2^n n(c_1n + c_2)$ (¿por qué?).

Ejemplo 3.5.2. Considere la relación de recurrencia:

$$u_n = 6u_{n-1} - 9u_{n-2} + f(n)$$

La ecuación característica de su relación de recurrencia homogénea asociada es:

$$0 = x^2 - 6x + 9 = (x-3)^2$$

1. Si $f(n) = 3^n$, entonces $x_n^{(p)} = 3^n cn^2$.
2. Si $f(n) = 3^n(5n + 1)$, entonces $x_n^{(p)} = 3^n n^2(c_1n + c_0)$.
3. Si $f(n) = 2^n(5n + 1)$, entonces $x_n^{(p)} = 2^n(c_1n + c_0)$.

Ejemplo 3.5.3. Resuelva la relación $u_n = u_{n-1} + 3n^2$, para todo $n \geq 1$.

Solución. La ecuación característica de la recurrencia es $x - 1 = 0$, por lo que no tiene más que la solución 1 y es de multiplicidad 1. Para poder aplicar el Corolario 3.3.4 identifiquemos los valores s y t. Como $f(n) = 3n^2 = (3n^2)1^n$, entonces: $s = 1$ (que es raíz de mutiplicidad 1 de la ecuación característica) y $t = 2$, por lo que para todo natural n se tiene:

$$\begin{aligned}
x_n^{(p)} &= n^1(c_2n^2 + c_3n + c_4) \\
&= c_2n^3 + c_3n^2 + c_4n \\
x_{n-1}^{(p)} &= c_2(n-1)^3 + c_3(n-1)^2 + c_4(n-1) \\
&= c_2(n^3 - 3n^2 + 3n - 1) + c_3(n^2 - 2n + 1) + c_4(n-1) \\
&= c_2n^3 + (c_3 - 3c_2)n^2 + (3c_2 - 2c_3 + c_4)n + c_3 - c_2 - c_4 \\
x_n^{(p)} - x_{n-1}^{(p)} &= c_2n^3 + c_3n^2 + c_4n - c_2n^3 - (c_3 - 3c_2)n^2 - (3c_2 - 2c_3 + c_4)n - c_3 + c_2 + c_4 \\
&= 3c_2n^2 + (2c_3 - 3c_2)n - c_3 + c_2 + c_4
\end{aligned}$$

Al ser $\{x_n^{(p)}\}$ solución de la ecuación, se debe cumplir:

$$3c_2n^2 + (2c_3 - 3c_2)n - c_3 + c_2 + c_4 = 3n^2$$

de lo que surge el siguiente sistema:

$$\begin{aligned}
3c_2 &= 3 && \Rightarrow c_2 = 1 \\
2c_3 - 3c_2 &= 0 && \Rightarrow 2c_3 = 3 \quad \Rightarrow c_3 = \frac{3}{2} \\
c_4 + c_2 - c_3 &= 0 && \Rightarrow c_4 = c_3 - c_2 = \frac{3}{2} - 1 = \frac{1}{2}
\end{aligned}$$

En definitiva, para todo n:

$$\begin{aligned} x_n^{(p)} &= n(n^2 + \frac{3}{2}n + \frac{1}{2}) \\ &= n^3 + \frac{3}{2}n^2 + \frac{1}{2}n \\ &= \frac{1}{2}(2n^3 + 3n^2 + n) \end{aligned}$$

Por otra parte $\{x_n^{(h)}\}$ está definida por $x_n^{(h)} = c_1 1^r = c_1$, para todo natural n. Del Teorema 3.3.1 tenemos que la solución general es $\{x_n\}$ definida por $\{x_n^{(p)} + x_n^{(h)}\}$, es decir

$$x_n = c_1 + \frac{1}{2}(2n^3 + 3n^2 + n)$$

para todo número natural n. □

Ejemplo 3.5.4. Resuelva la relación de recurrencia $u_n = 3u_{n-1} + 5 \cdot 7^n$

Solución. La solución de la relación homogénea asociada es $u_n^{(h)} = c_1 \cdot 3^n$. Puesto que $f(n) = 5 \cdot 7^n$, buscamos una solución particular $u_n^{(p)}$ de la forma $c_2 \cdot 7^n$. Como $u_n^{(p)}$ debe ser una solución de la relación no homogénea dada, sustituimos $u_n^{(p)} = c_2 \cdot 7^n$ en la relación dada resultando:

$$c_2 \cdot 7^n - 3c_2 \cdot 7^{n-1} = 5 \cdot 7^n, \quad n \geq 1$$

Si dividimos entre 7^{n-1}, vemos que $7c_2 - 3c_2 = 5 \cdot 7$ por lo que $c_2 = 35/4$ y

$$a_n^{(p)} = \frac{35}{4}7^n = \frac{5}{4}7^{n+1}, \quad n \geq 0$$

La solución general es

$$x_n = c \cdot 3^n + \frac{5}{4}7^{n+1}$$

y ahora buscamos la particular de nuestro problema con la ayuda de los valores de frontera. Si $2 = x_0 = c_1 + \frac{5}{4}7$, entonces $c = -\frac{27}{4}$ y

$$x_n = \frac{5}{4}7^{n+1} - \frac{1}{4}3^{n+3}, \quad n \geq 0.$$

□

Ejemplo 3.5.5. Resuelva la relación de recurrencia $u_n = 3u_{n-1} + 5 \cdot 3^n$, donde $n \geq 1$ y $u_0 = 2$

Solución. Como en ejercicios anteriores, $x_n^{(h)} = c_1 3^n$, pero en este caso $x_n^{(h)}$ y $f(n)$ no son linealmente independientes. Como resultado, buscamos una solución particular $x_n^{(p)}$ de la forma $c_2 n 3^n$ (¿Qué ocurre si sustituimos $x_n^{(p)} = c_2 3^n$ en la relación dada?). Al sustituir $x_n^{(p)} = c_2 n 3^n$ en la relación dada obtenemos

$$\begin{aligned} c_2 n 3^n - 3c_2(n-1)3^{n-1} &= 5 \cdot 3^n \\ c_2 n - c_2(n-1) &= 5 \\ c_2 &= 5 \end{aligned}$$

Por lo tanto, para todo natural n se tiene $x_n = x_n^{(h)} + x_n^{(p)} = (c_1 + 5n)3^n$. Si $x_0 = 2$, la solución general queda particularizada en $x_n = (2 + 5n)3^n$, para todo natural n. □

Ejemplo 3.5.6. Dé el número de pasos mínimos necesarios para completar un juego de las *Torres de Hanoi* en función del número de discos n con los que cuente.

Solución. Para $n \geq 0$, sea u_n el número de movimientos necesarios para pasar los n discos de la vástago 1 a la vástago 3. Entonces para $n+1$ discos hacemos lo siguiente:

1. Pasamos los n discos de arriba desde el vástago 1 al vástago 2. Esto se realiza en u_n pasos.
2. Pasamos el disco más grande (el que hace de base de la torre) del vástago 1 al vástago 3. Esto se hace en un paso.
3. Por último pasamos, de nuevo, los n discos del vástago 2 sobre el disco mayor, que ahora está en la vástago 3. Esto requiere otros u_n movimientos.

Lo dicho sugiere la relación $u_{n+1} = 2u_n + 1$, donde $n \geq 0$ y $u_0 = 0$. Para $u_{n+1} - 2u_n = 1$, $x_n^{(h)} = c_1 2^n$. Como $f(n) = 1$ no es solución de $u_{n+1} - 2u_n = 0$, tomamos $x_n^{(p)} = c_2 \cdot 1^n = c_2$. De la relación anterior vemos que $c_2 = 2c_2 + 1$, por lo que $c_2 = -1$ y $x_n = c_1 2^n - 1$. De $0 = u_0 = c_1 - 1$ concluimos que $c_1 = 1$ y que $x_n = 2^n - 1$, $n \geq 0$. □

$f(n)$	$u_n^{(p)}$ de tanteo
c, constante	a, constante
cn	$c_0 n + c_1$
cn^2	$c_0 n^2 + c_1 n + c_2$
cn^t, t entero postivo	$c_t n^t + c_{t-1} n^{t-1} + \cdots + c_0$
cr^n, r constante	ar^n
$cn^t r^n$	$r^n(c_t n^t + c_{t-1} n^{t-1} + \cdots + c_0)$
$c \sin \alpha n$	$a \sin \alpha n + b \cos \alpha n$
$c \cos \alpha n$	$a \sin \alpha n + b \cos \alpha n$
$cr^n \sin \alpha n$	$r^n(a \sin \alpha n + b \cos \alpha n)$
$cr^n \cos \alpha n$	$r^n(a \sin \alpha n + b \cos \alpha n)$

Figura 3.1: Elecciones de $u_n^{(p)}$ según $f(n)$, si r no es sol. de la ecuación característica.

Teorema 3.5.1. *Sean las relaciones de recurrencia no homogénea siguientes:*

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + f(n), \tag{3.22}$$

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + g(n), \tag{3.23}$$

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + f(n) + g(n), \tag{3.24}$$

Si $\{x_n\}$ es una solución de la relación 3.22 e $\{y_n\}$ es una solución de la relación 3.23, entonces $\{x_n + y_n\}$ es una solución de la relación 3.24.

Demostración. Si $\{x_n\}$ es una solución de la relación 3.22 entonces.

$$y_n = a_1 y_{n-1} + a_2 y_{n-2} + \cdots + a_k y_{n-k} + f(n)$$

y si $\{u_n\}$ es una solución de la relación 3.23 entonces.

$$y_n = a_1 y_{n-1} + a_2 y_{n-2} + \cdots + a_k y_{n-k} + g(n)$$

Sumando ambas igualdades se tiene:

$$x_n + y_n = a_1(x_{n-1} + y_{n-1}) + a_2(x_{n-2} + y_{n-2}) + \cdots + a_k(x_{n-k} + y_{n-k}) + f(n) + g(n) = 0$$

De donde, $\{x_n + y_n\}$ es una solución de la relación 3.24. □

Ejercicio 3.5.1. Encuentre una expresión no recurrente para la sucesión definida por las siguientes igualdades:

$$\begin{aligned} u_0 &= 2, \\ u_1 &= 2, \\ u_n &= u_{n-2} + 2^n + (-1)^n, \text{ siempre que } n \geq 2. \end{aligned}$$

Solución. La recurrencia planteada en el enunciado es lineal no homogénea y, en este caso, $f(n) = 2^n + (-1)^n$. La ecuación característica asociada es:

$$x^2 - 1 = 0$$

que tiene como soluciones ± 1. Dado que -1 es solución de la ecuación característica, en parte según afirma el Corolario 3.3.4, tenemos que $\{x_n^{(p)}\}$, donde $x_n^{(p)} = c_3 2^n + c_4 n(-1)^n$ para todo natural n, es una solución particular de la recurrencia (-1 es raíz de la ecuación característica a la vez que parte de $f(n)$). También sabemos que $\{x_n^{(h)}\}$, donde $x_n^{(h)} = c_1(-1)^n + c_2$ para todo natural n, es una solución de la recurrencia homogénea asociada. Nuestra labor consiste ahora en encontrar los coeficientes involucrados, haciendo notar que el cálculo de los coeficientes c_3 y c_4 no requiere las condiciones iniciales (también llamadas "de frontera"). Para ello consideremos lo siguiente:

$$\begin{aligned} x_{n+2}^{(p)} &= c_3 2^{n+2} + c_4(n+2)(-1)^n \\ &= 4c_3 2^n + c_4(n+2)(-1)^n \end{aligned}$$

Por una parte $\{x_n^{(p)}\}$, al ser solución de la recurrencia, cumplirá:

$$x_{n+2}^{(p)} - x_n^{(p)} = 2^{n+2} + (-1)^{n+2}$$

Por otra, se tiene:

$$\begin{aligned} x_{n+2}^{(p)} - x_n^{(p)} &= 4c_3 2^n + c_4(n+2)(-1)^n - c_3 2^n - c_4 n(-1)^n \\ &= (4c_3 - c_3)2^n + (c_4(n+2) - c_4 n)(-1)^n \\ &= 3c_3 2^n + 2c_4(-1)^n \end{aligned}$$

y uniendo los dos resultados concluimos que:

$$3c_3 2^n + 2c_4(-1)^n = 4 \cdot 2^n + (-1)^n$$

Así pues, basta tomar $c_3 = \frac{4}{3}$ y $c_4 = \frac{1}{2}$ y en definitiva:

$$x_n^{(p)} = \tfrac{4}{3}2^n + \tfrac{1}{2}n(-1)^n$$

Ahora, según Teorema 3.3.1 compondremos la solución $\{x_n\}$ como suma, se decir, para todo número natural n: $x_n = x_n^{(h)} + x_n^{(p)}$. Según esto,

$$\begin{aligned} x_n &= x_n^{(h)} + x_n^{(p)} \\ &= c_1(-1)^n + c_2 + \frac{4}{3}2^n + \frac{1}{2}n(-1)^n \\ &= c_2 + \frac{4}{3}2^n + (\frac{1}{2}n + c_1)(-1)^n \end{aligned} \tag{3.25}$$

La expresión 3.25 representa la solución general de la relación de recurrencia. El cálculo de c_1 y c_2 requiere el uso de las condiciones iniciales. En efecto:

$$\begin{aligned} 2 = x_0 &= c_2 + \frac{4}{3} + c_1 \\ 2 = x_1 &= c_2 + \frac{4}{3}\cdot 2 + (\frac{1}{2} + c_1)(-1) \\ &= c_2 + \frac{8}{3} - \frac{1}{2} - c_1 \\ &= c_2 - c_1 + \frac{13}{6} \end{aligned}$$

y de aquí al siguiente sistema:

$$\left\{ \begin{array}{lcl} c_1 & + & c_2 = \frac{2}{3} \\ c_2 & - & c_1 = -\frac{1}{6} \end{array} \right.$$

que resuelto aporta $c_1 = \frac{5}{12}$ y $c_2 = \frac{1}{4}$. Llevando estos valores a la expresión 3.25 resulta:

$$\begin{aligned} x_n &= \frac{4}{3}2^n + (\frac{1}{2}n + \frac{5}{12})(-1)^n + \frac{1}{4} \\ &= \frac{2^{n+2}}{3} + (\frac{6n+5}{12})(-1)^n + \frac{1}{4} \\ &= \frac{2^{n+4}+3}{12} + (\frac{6n+5}{12})(-1)^n \end{aligned}$$

y entonces la **solución** es:

$$x_n = \frac{2^{n+4}+3}{12} + (\frac{6n+5}{12})(-1)^n$$

para todo número natural n. □

Ejercicio 3.5.2. Obtener dos soluciones distintas del problema de recurrencia lineal no homogénea siguiente:

$$x_n = 2x_{n-1} - x_{n-2} + (-2)^n$$

Solución. El enunciado plantea resolver la siguiente recurrencia lineal no homogénea:

$$x_n - 2x_{n-1} + x_{n-2} = (-2)^n$$

La ecuación característica de esta recurrencia es $x^2 - 2x + 1 = 0$, es decir, $(x-1)^2 = 0$. Por tanto, la ecuación tiene como raíz a 1 con multiplicidad 2. Así $\{x_n^{(h)}\}$ y $\{x_n^{(p)}\}$ vienen definidas para todo n según:

$$\begin{aligned} x_n^{(h)} &= c_1 + nc_2 \\ x_n^{(p)} &= c_3(-2)^n \end{aligned}$$

En esta situación está claro que:

$$\begin{aligned} x_{n+2}^{(p)} &= c_3(-2)^{n+2} \\ &= 4c_3(-2)^n \\ x_{n+1}^{(p)} &= c_3(-2)^{n+1} \\ &= -2c_3(-2)^n \end{aligned}$$

de donde:

$$x_n^{(p)} - 2x_{n-1}^{(p)} + x_{n-2}^{(p)} = (-2)^{n+2}$$

y por tanto:

$$\begin{aligned} 4(-2)^n &= (-2)^{n+2} \\ &= 4c_3(-2)^n - 2(-2c_3(-2)^n) + c_3(-2)^n \\ &= 9c_3(-2)^n \end{aligned}$$

de donde $c_3 = \frac{4}{9}$. Ahora, según Teorema 3.3.1 compondremos la solución $\{x_n\}$ como suma, se decir, para todo número natural n: $x_n = x_n^{(h)} + x_n^{(p)}$. Según esto, la solución general $\{x_n\}$ es la que viene definida para todo natural n por:

$$x_n = \frac{4}{9}(-2)^n + nc_2 + c_1$$

Para concluir el ejercicio ofrecemos dos soluciones particulares elegidas al azar, digamos, la que cumple $x_0 = 0$, $x_1 = 1$ y la que cumple $x_0 = 1$, $x_1 = 0$:

- $x_0 = 0$, $x_1 = 1$; tenemos:

$$\begin{aligned} 0 &= \frac{4}{9} + 0c_2 + c_1 && \Rightarrow c_1 = -\frac{4}{9} \\ 1 &= \frac{4}{9}(-2) + c_2 - \frac{4}{9} && \Rightarrow c_2 = \frac{7}{3} \end{aligned}$$

  y por tanto, para todo número natural n:

$$x_n = \frac{4}{9}(-2)^n + \frac{7}{3}n - \frac{4}{9}$$

- $x_0 = 1$, $x_1 = 0$; tenemos:

$$\begin{aligned} 1 &= \frac{4}{9} + 0c_2 + c_1 && \Rightarrow c_1 = \frac{5}{9} \\ 0 &= \frac{4}{9}(-2) + c_2 - \frac{5}{9} && \Rightarrow c_2 = \frac{3}{9} \end{aligned}$$

  y por tanto, para todo número natural n:

$$x_n = \frac{4}{9}(-2)^n + \frac{3}{9}n + \frac{5}{9}$$

□

3.6. Ejercicios

1. Resuelva la relación de recurrencia:

$$u_n = u_{n-1} + d$$

   y encuentre la solución particular que cumple $u_0 = a$, donde a es una constante (*progresión artimética*). (sol. $x_n = dn + a$)

2. Resuelva la relación de recurrencia:

$$u_n = ku_{n-1}$$

   y encuentre la solución particular que cumple $u_0 = a$, donde a es una constante (*progresión geométrica*). (sol. $x_n = ak^n$)

3. Resuelva la relación de recurrencia:

$$u_{n+2} - 6u_{n+1} + 9u_n = 0, \text{ para todo } n \geq 0.$$

   y encuentre la solución particular que cumple: $u_0 = 1$ y $u_1 = 6$.

4. Resuelva el problema de recurrencia:

$$u_{n+3} = 6u_{n+2} - 11u_{n+1} + 6u_n, \text{ para todo } n \geq 0.$$

y encuentre la solución particular que cumple: $u_0 = 2$, $u_1 = 5$ y $u_2 = 15$.

5. Encuentre la representación polar de los siguientes números complejos:

   a) $z_1 = -1 - i$ (sol. $r_1 = \sqrt{2}$ y $\theta_1 = -3\pi/4$)

   b) $z_2 = 2 + 2i$ (sol. $r_2 = 2\sqrt{2}$ y $\theta_2 = \pi/4$)

   c) $z_3 = -1 + i\sqrt{3}$ (sol. $r_3 = \sqrt{2}$ y $\theta_3 = 2\pi/3$)

   d) $z_4 = 1 - i\sqrt{3}$ (sol. $r_4 = \sqrt{2}$ y $\theta_4 = -\pi/3$)

   e) $z_5 = 2i\sqrt{3}$ (sol. $r_5 = 2$ y $\theta_5 = \pi/2$)

6. Resuelva la relación de recurrencia:

$$u_{n+2} = -4u_n$$

(sol. $x_n = 2^n(k_1 \cos \frac{n\pi}{2} + k_2 \sin \frac{n\pi}{2})$

7. Resuelva la relación de recurrencia:

$$u_{n+2} = -4u_{n+1} - 16u_n$$

(sol. $x_n = 4^n(k_1 \cos \frac{2n\pi}{3} + k_2 \sin \frac{2n\pi}{3})$

8. Dese una explicación de cada una de las afirmaciones hechas en el Ejemplo 3.5.1 y cada una de las hechas en el Ejemplo 3.5.2.

9. Resuelva la relación de recurrencia:

$$u_{n+2} = -4u_{n+1} - 3u_n + 5(-2)^n$$

(sol. $x_n = c_1(-3)^n + c_2(-1)^n - 5(-2)^n$)

10. Resuelva la relación de recurrencia:

$$u_{n+2} = -4u_{n+1} + 6\cos \frac{n\pi}{2} + 3\sin \frac{n\pi}{2}$$

(sol. $x_n = 2^n(c_1 \cos \frac{n\pi}{2} + c_2 \sin \frac{n\pi}{2}) + 2\cos \frac{n\pi}{2} + \sin \frac{n\pi}{2}$)

11. Resuelva la relación de recurrencia:

$$u_{n+2} = -4u_{n+1} - 16u_n + 4^{n+2}\cos \frac{n\pi}{2} - 4^{n+3}\sin \frac{n\pi}{2}$$

(sol. $x_n = 4^n(c_1 \cos \frac{n\pi}{2} + c_2 \sin \frac{n\pi}{2} + 4\cos \frac{n\pi}{2} + \sin \frac{n\pi}{2}$)

12. Resuelva la relación de recurrencia:

$$u_{n+2} = 6u_{n+1} - 9u_n + 3^n$$

(sol. $x_n = (c_1 + c_2 n + \frac{n^2}{18})3^n$)

13. Resuelva la relación de recurrencia:

$$u_{n+3} = -5u_{n+2} - 8u_{n+1} - 4u_n + 2(-1)^n + (-2)^{n+3}$$

(sol. $x_n = (1 - 2n)(-1)^n + (3 + 2n + n^2)(-2)^n$)

14. Resuelva el siguiente problema de recurrencia:

$$u_n - 2u_{n-1} = (n+5)3^n \tag{3.26}$$

15. Resuelva la recurrencia:

$$u_{n+2} = 2u_{n+1} - 4u_n, \text{ para todo } n \geq 0.$$

y encuentre la solución particular que cumple: $u_0 = 0$ y $u_1 = 1$.

16. Resuelva la recurrencia:

$$u_{n+1} = 3u_n + 2n, \text{ para todo } n \geq 0.$$

y encuentre la solución particular que cumple $u_1 = 3$.

17. Resuelva el problema de recurrencia:

$$u_n - 2u_{n-1} = 3^n, \text{ para todo } n \geq 1.$$

y encuentre la solución particular que cumple $u_1 = 5$.

18. Resuelva el problema de recurrencia:

$$u_{n+2} - 6u_{n-1} + 9u_n = 3 \cdot 2^n + 7 \cdot 3^n, \text{ para todo } n \geq 0.$$

y encuentre la solución particular que cumple $u_0 = 1$ y $u_1 = 4$.

19. Un ciudadano pide un préstamo de S cantidad de dinero a pagar en T plazos. Si I es el interés del préstamo por plazo, ¿qué pago constante P debe realizar al final de cada plazo? (sol. $P = SI(1-(1+I)^{-T})^{-1}$)

20. Para $n \geq 2$, supongamos que hay n personas en una fiesta y que cada una de ellas da la mano (exáctamente una vez) a todas las demás personas (y nadie estrecha su propia mano). Si u_n es el número de apretones de mano en esas condiciones, dar una expresión suya. (sol. $x_n = \frac{n(n-1)}{2}$), $n \geq 2$)

21. Para $n \geq 1$, sea C un conjunto que contiene 2^n números reales. ¿Cuántas comparaciones deben efectuarse entre pares de números de C para determinar los elementos máximo y mínimo de C?

22. Sea n cualquier número natural y consideremos x_n definido por:

$$x_n = \sum_{i=0}^{n} 2^{n-i}3^i$$

Encontrar el valor de x_n.

Capítulo 4

Lenguajes

4.1. Signos y Palabras

Definición 4.1.1. Un *monoide* es un álgebra $\mathbf{M} = \langle M, \circ, e\rangle$ de tipo $\langle 2, 0\rangle$ que cumple las siguientes propiedades:

1. para todo $x, y, z \in M$, $x \circ (y \circ z) = (x \circ y) \circ z$
2. para todo $x \in M$, $e \circ x = x = x \circ e$.

Observación 4.1.1. Es evidente que el elemento neutro de un monoide es único.

Definición 4.1.2. Sea S un conjunto no vacío, cuyos elementos serán llamados *signos*. Sea $\mathbf{L}_0(S)$ el monoide libre construido sobre S con conjunto base $L_0(S) = \bigcup_{n\in\omega} S^n$, cuyos elementos serán llamados *palabras* o *expresiones* y serán identificados por sucesiones finitas $A = \langle s_i\rangle_{0\leq i\leq n}$ de elementos de S; diremos que en la palabra $\langle s_i\rangle_{0\leq i\leq n}$ el símbolo s_i ocupa la posición i. Notaremos multiplicativamente la ley de composición en $L_0(S)$ y ésta será la yuxtaposición, es decir, AB será la sucesión obtenida por yuxtaposición de las sucesiones A y B en ese orden leyendo de izquierda a derecha. La palabra *vacía* $\varnothing$ es el elemento neutro en $\mathbf{L}_0(S)$. La *longitud* de $A \in L_0(S)$, en símbolos $\mathrm{l}(A)$, es el número de elementos de la sucesión A. Designamos por $L(S)$ al conjunto de las palabras no vacías de $L_0(S)$.

Observación 4.1.2.

1. La longitud de $\varnothing$ es 0 y es la única palabra con longitud igual a 0.
2. Las palabras de longitud 1 pueden ser identificadas con los signos.
3. Se cumple que $\mathrm{l}(AB) = \mathrm{l}(A) + \mathrm{l}(B)$.

Definición 4.1.3. Sea S un conjunto no vacío y supongamos que hay dada una aplicación $\mathrm{n}\colon S \longrightarrow \omega$. Notaremos con el mismo símbolo a su única extensión homomórfica a $L_0(S)$ en ω. n es llamada *función peso*.

Observación 4.1.3. Se tiene que $n(AB) = n(A) + n(B)$ y entonces:

$$\mathrm{n}(A) = \begin{cases} 0 & , \text{ si } A = \varnothing \\ \sum_{i=0}^{k} n(s_i) & , \text{ si } A = \langle s_i\rangle_{0\leq i\leq k} \end{cases}$$

Ejemplo 4.1.1. El contenido de la Definición 4.1.4 ejemplifica los contenidos de lo definido en la Definición 4.1.2 y la Definición 4.1.3.

Definición 4.1.4. Un *lenguaje proposicional* $\mathbf{L}$ es una terna $\langle X, Cons, a\rangle$ donde:

- $X \neq \varnothing$; sus elementos son denominados *enunciados atómicos*, *fórmulas atómicas*, *proposiciones atómicas*, o, simplemente *símbolos de variable proposicional*.
- $Cons$ es un conjunto finito no vacío (de constantes lógicas) tal que $Cons \cap X = \varnothing$.
- a es una aplicación $a: Cons \longrightarrow \omega^*$.
- $\mathrm{S}(\mathbf{L}) = X \cup Cons$ es el conjunto de *símbolos* del lenguaje.
- $\mathrm{Exp}(\mathbf{L})$ abreviará al conjunto $L(\mathrm{S}(\mathbf{L}))$.
- El *peso* asociado al lenguaje $\mathbf{L}$ es $n: \mathrm{S}(\mathbf{L}) \longrightarrow \omega$ definido como sigue:

$$n(x) = \begin{cases} 0 & \text{, si } x \in X \\ a(x) & \text{, si } x \in Cons \end{cases}$$

Definición 4.1.5. Sea $A \in L_0(S)$. Si $A = A'BA''$, la palabra B es un *segmento* de A y es un segmento *propio* sii, por definición, $A \neq B$. B es un segmento *inicial* (resp. *final*) de A sii, por definición, $A' = \varnothing$ (resp. $A'' = \varnothing$). Si $\mathrm{l}(A') = k$, decimos que B comienza en la posición $(k+1)$-ésima. Si $A = BCDEF$ (donde las palabras B, C, D, E, y F pueden ser vacías), se dice que los segmentos C y E son *disjuntos* en A.

4.2. Palabras Significativas

Definición 4.2.1. Sea S un conjunto no vacío y $\mathrm{n}: S \longrightarrow \omega$ una función peso. Una sucesión $\langle A_j \rangle_{0 \leq j \leq n}$ de elementos de $L_0(S)$ es *significativa* según o respecto a n sii, por definición, para cada $0 \leq i \leq n$ se cumple una de las siguientes condiciones:

1. $A_i \in S$ y $\mathrm{n}(A_i) = 0$
2. existen $p \in \omega^*$, $i_1, \ldots, i_p < i$ y $f \in S$ tales que $\mathrm{n}(f) = p$ y $A_i = fA_{i_1} \cdots A_{i_p}$

Una palabra es *significativa* según o respecto a n si existe al menos una sucesión significativa respecto a n de la que forma parte.

Observación 4.2.1. De la Definición 4.2.1 se deduce que es condición necesaria para ser palabra significativa el no ser la palabra vacía.

Lema 4.2.1. *Sea S un conjunto no vacío y $\mathrm{n}: S \longrightarrow \omega$ una función peso. Son equivalentes las siguientes afirmaciones:*

1. *Existe al menos una palabra significativa según n en $\mathbf{L}_0(S)$*
2. *$n^*(\{0\}) \neq \varnothing$*

Demostración. Sea A una palabra significativa según n en $\mathbf{L}_0(S)$. Para ella existirá al menos una sucesión significativa de $\langle A_j \rangle_{0 \leq j \leq n}$ de elementos de $L_0(S)$ de la que forma parte. Se cumple entonces que $A_0 \in S$ y $\mathrm{n}(A_0) = 0$, por lo que $n^*(\{0\}) \neq \varnothing$. Recíprocamente, si $n^*(\{0\}) \neq \varnothing$, sea $s \in S$ tal que $\mathrm{n}(s) = 0$. Se tiene que $\langle \langle s \rangle \rangle$ es una sucesión significativa de elementos de $L_0(S)$ que hace a $\langle s \rangle$ palabra significativa. □

Lema 4.2.2. *Sea $\mathrm{n}: S \longrightarrow \omega$ una función peso. Si $A_1, \ldots, A_p$ son palabras significativas de $L_0(S)$ respecto a n y $f \in S$ tal que $\mathrm{n}(f) = p$, entonces $fA_1 \cdots A_p$ es significativa.*

Ejemplo 4.2.1. Las palabras significativas respecto al peso n asociado al lenguaje proposicional $\mathbf{L} = \langle X, Cons, a \rangle$ existen y se denominan *fórmulas* de dicho lenguaje proposicional.

4.3. Caracterización de las Palabras Significativas

Definición 4.3.1. Sea $\mathrm{n}: S \longrightarrow \omega$ una función peso. Una palabra A de $L_0(S)$ es *equilibrada* respecto a n sii, por definición, cumple las siguientes propiedades:

1. $\mathrm{l}(A) = \mathrm{n}(A) + 1$

2. para todo segmento inicial propio y no vacío C de A se cumple $\mathrm{l}(C) \leq \mathrm{n}(C)$.

Observación 4.3.1. La condición 2) en la Definición 4.3.1 es equivalente a "para todo segmento inicial propio C de A se cumple $\mathrm{l}(C) \leq \mathrm{n}(C)$" pues $\mathrm{l}(\varnothing) = 0 = \mathrm{n}(\varnothing)$.

Observación 4.3.2. En virtud de la condición 1) en la Definición 4.3.1 es evidente que si A es equilibrada entonces $A \neq \varnothing$.

Teorema 4.3.1. *Sea* $\mathrm{n}: S \longrightarrow \omega$ *una función peso y* A *una palabra de* $L(S)$. *Si* A *es significativa respecto a* n *entonces* A *es equilibrada respecto a* n.

Demostración. Sea A una palabra significativa respecto a n que lo es por figurar en la sucesión significativa, por ejemplo, $\langle A_j \rangle_{0 \leq j \leq n}$. Demostremos que para todo $0 \leq k \leq n$ se tiene que la palabra A_k es equilibrada. Si $k = 0$, entonces $A = A_0$ y la única hipótesis posible es $0 = \mathrm{n}(A_0)$ (Definición 4.2.1); A_0 es equilibrada porque $\mathrm{l}(A_0) = 1$ y $\mathrm{n}(A_0) = 0$. Supongamos que $0 < k$ y que el resultado está establecido para todo $0 \leq j < k$. Si $\mathrm{n}(A_k) = 0$, la demostración es igual que para el caso $k = 0$. Si no es así, $A_k = fB_1 \cdots B_p$ donde $f \in S$ cumple $\mathrm{n}(f) = p$ y para todo todo $1 \leq j \leq p$ existe $i_j < k$ tal que $B_j = A_{i_j}$ siendo A_{i_j} equilibrada (según la hipótesis). Se tiene:

$$\begin{aligned}
\mathrm{l}(A_j) &= 1 + \sum_{j=1}^{p} \mathrm{l}(B_j) \\
&= 1 + \sum_{j=1}^{p} (\mathrm{n}(B_j) + 1) \\
&= 1 + p + \sum_{j=1}^{p} \mathrm{n}(B_j) \\
&= 1 + \mathrm{n}(A_k)
\end{aligned}$$

Por otra parte, sea C un segmento inicial no vacío y propio de A_k. Si no existe $m < p$ tal que B_m es un segmento de C, entonces $C = fD$ donde D es un segmento inicial de B_1. Si $D = \varnothing$, entonces $C = f$ y $l(C) = 1 \leq p = \mathrm{n}(C)$. Si $D \neq \varnothing$ entonces D es un segmento inicial propio y no vacío de la palabra significativa B_1:

$$\begin{aligned}
\mathrm{l}(C) &= 1 + \mathrm{l}(D) \\
&\leq p + \mathrm{n}(D) \\
&= \mathrm{n}(f) + \mathrm{n}(D) \\
&= \mathrm{n}(fD) \\
&= \mathrm{n}(C)
\end{aligned}$$

Si por contra existe algún $m < p$ tal que B_m es un segmento de C, sea q el mayor de los enteros m tales que $m < p$ y B_m es un segmento de C; se tiene entonces que $C = fB_1 \cdots B_q D$, donde D es un segmento

inicial propio de B_{q+1}. Entonces:

$$\begin{aligned} \mathrm{l}(C) &= 1 + (\sum_{j=1}^{q} \mathrm{l}(B_j)) + \mathrm{l}(D) \\ &\leq 1 + (\sum_{j=1}^{q} \mathrm{n}(B_j) + 1) + \mathrm{n}(D) \\ &\leq p + (\sum_{j=1}^{q} \mathrm{n}(B_j)) + \mathrm{n}(D) \\ &= \mathrm{n}(C) \end{aligned}$$

□

El enunciado recíproco del Teorema 4.3.1 es cierto. Para su demostración son necesarios algunos resultados previos.

Lema 4.3.2. *Sea* $\mathrm{n}: S \longrightarrow \omega$ *una función peso y* A *una palabra de* $L(S)$ *equilibrada según* n. *Para todo número natural* k *tal que* $0 \leq k < \mathrm{l}(A)$, *existe un único segmento* T *de* A *equilibrado según* n *que comienza en la posición* k *de* A.

Demostración. Si A es una palabra equilibrada de $L(S)$, entonces $0 < \mathrm{l}(A)$ (cfr. Observación 4.3.2), por lo que el enunciado de este lema tiene sentido. Demostremos en primer lugar la **existencia** de T. Sea $A = BC$, donde $\mathrm{l}(B) = k$ y $\mathrm{l}(C) = q$; así pues $q = \mathrm{l}(A) - k$ y por tanto $0 < q$. Para todo $0 \leq i \leq q$, sea C_i el segmento inicial de longitud i de C.[1] Sea

$$X = \{j \in \omega : 0 < j \leq q \text{ y para todo } 0 \leq h < j,\ \mathrm{l}(C_h) \leq \mathrm{n}(C_h)\}$$

Se tiene que $X \neq \varnothing$, pues $0 = l(C_0) \leq \mathrm{n}(C_0) = 0$, es decir, $1 \in X$; además X es finito (sus elementos no superan el valor q). Si $i = \max X$, se cumple que $\mathrm{l}(C_{i-1}) \leq \mathrm{n}(C_{i-1})$ y $\mathrm{l}(C_i) \geq \mathrm{n}(C_i) + 1$. Demostremos que C_i es equilibrada. La condición 2) de la Definición 4.3.1 se cumple por razón de la definición de i. Por otra parte, se tiene:

$$\begin{aligned} \mathrm{n}(C_i) + 1 &\leq \mathrm{l}(C_i) \\ &= \mathrm{l}(C_{i-1}) + 1 \\ &\leq \mathrm{n}(C_{i-1}) + 1 \\ &\leq \mathrm{n}(C_i) + 1 \end{aligned}$$

de lo que se deduce $\mathrm{l}(C_i) = \mathrm{n}(C_i) + 1$. La existencia queda probada tomando $T = C_i$. Para demostrar la **unicidad** basta observar que si T es una palabra equilibrada, ningún segmento inicial propio de T es equilibrado (cfr. Definición 4.3.1) □

Lema 4.3.3. *Sea* $\mathrm{n}: S \longrightarrow \omega$ *una función peso. Toda palabra* $A \in L(S)$ *equilibrada según* n *puede ser expresada de forma única de una de las siguientes formas:*

1. x, *siendo* $x \in S$ *y tal que* $n(x) = 0$, *siempre que* $l(A) = 1$.
2. $fA_1 \cdots A_p$, *donde para todo* $1 \leq i \leq p$ *se cumple que* A_i *es una palabra equilibrada según* n *y donde* $\mathrm{n}(f) = p$, *siempre que* $1 < l(A)$.

[1] Como B es un segmento inicial propio de A (recuérdese que $k < \mathrm{l}(A)$), se tiene:

$$\mathrm{l}(C_q) = \mathrm{l}(A) - \mathrm{l}(B) \geq \mathrm{n}(A) + 1 - n(B) = \mathrm{n}(C_q) + 1$$

Demostración. Si A es equilibrada, es no vacía y $0 < l(A)$. Si $l(A) = 1$, entonces existe un único $x \in S$ tal que $A = \langle x \rangle$ (o simplemente $A = x$ según nuestro convenio notacional) y $n(x) = 0$. Si $1 < l(A)$, sea f el signo inicial de A. Por el Lema 4.3.2, A puede ser expresada en la forma $fA_1 \cdots A_p$ donde para todo $1 \leq i \leq p$, A_i es equilibrada; para ello basta definir A_i como el único segmento equilibrado según n que comienza en la posición $k(i)$, donde:

$$k(i) = \begin{cases} 1 & \text{, si } i = 1 \\ 1 + \sum_{j<i} \mathrm{l}(A_j) & \text{, si } i > 1 \end{cases}$$

Por otra parte:

$$\begin{aligned} 1 + \sum_{i=1}^{p} \mathrm{l}(A_i) &= \mathrm{l}(A) \\ &= \mathrm{n}(A) + 1 \\ &= \mathrm{n}(f) + (\sum_{i=1}^{p} \mathrm{n}(A_i)) + 1 \\ &= \mathrm{n}(f) + (\sum_{i=1}^{p} (\mathrm{l}(A_i) - 1)) + 1 \end{aligned}$$

de donde se deduce que $\mathrm{n}(f) = p$. Para la unidad, supongamos que A se pudiese ser escrita como $gB_1 \cdots B_q$, donde para todo $1 \leq i \leq q$ se cumple que B_i es una palabra equilibrada según n. Como $gB_1 \cdots B_q = A = fA_1 \cdots A_p$ y A es una upla, se deduce que $f = g$ y por tanto $q = p$. Además, tanto A_1 como B_1 son equilibradas y comienzan en la posición 1; por el Lema 4.3.2 sabemos que $A_1 = B_1$. Si $p = 1$, el razonamiento está completo; pero si $1 < p$, supongamos en un razonamiento inductivo que $1 < i \leq p$ y que el resultado es cierto para todo j tal que $1 \leq j < i$, es decir, que para todo $1 \leq j < i$, $A_j = B_j$. Entonces tanto A_i como B_i son segmentos que comienzan en la misma posición y son ambos equilibrados. De nuevo por el Lema 4.3.2 concluimos que $A_i = B_i$. De ahí la unidad. □

Observación 4.3.3. Establecidos el Lema 4.3.2 y Lema 4.3.3 se deduce fácilmente (por recurrencia sobre la longitud de A) que toda palabra equilibrada A es significativa.

Teorema 4.3.4. *Sea* $\mathrm{n}: S \longrightarrow \omega$ *una función peso y* A *una palabra de* $L(S)$. *Son equivalentes las siguientes afirmaciones:*

1. A *es significativa respecto a* n.
2. A *es equilibrada respecto a* n

Demostración. El Teorema 4.3.1 permite conocer que la afirmación 2 es consecuencia de la afirmación 1. Supongamos ahora que A es una palabra de $L(S)$ equilibrada respecto a n. El razonamiento es por inducción sobre $\mathrm{l}(A)$. Si $\mathrm{l}(A) = 1$, sabemos por el Lema 4.3.3 que existe $x \in S$ y tal que $A = x$ y $n(x) = 0$; entonces $\langle A \rangle$ es una sucesión significativa y así A es una palabra significativa. Supongamos que $1 < \mathrm{l}(A)$ y que el resultado es cierto para toda palabra equilibrada de longitud inferior a la de A. De nuevo, por el Lema 4.3.3 sabemos que existe $f \in S$ tal que $\mathrm{n}(f) = p$ y palabras equilibradas A_i para todo $1 \leq i \leq p$ tales que $fA_1 \cdots A_p$. Por la hipótesis de inducción, para todo $1 \leq i \leq p$ resulta que A_i es significativa. Por el Lema 4.2.2 sabemos que $fA_1 \cdots A_p$ es significativa, es decir, que A es significativa. □

Por el 4.3.4 podemos reescribir el Lema 4.3.3 según reza en el enunciado del Corolario 4.3.5.

Corolario 4.3.5 (Principio de Lectura Única)**.** *Sea* $\mathrm{n}: S \longrightarrow \omega$ *una función peso. Toda palabra* $A \in L(S)$ *significativa según* n *puede ser expresada de forma única de una de las siguientes formas:*

1. x, *siendo* $x \in S$ *y tal que* $n(x) = 0$, *siempre que* $\mathrm{l}(A) = 1$.
2. $fA_1 \cdots A_p$, *donde para todo* $1 \leq i \leq p$ *se cumple que* A_i *es una palabra significativa según* n *y donde* $\mathrm{n}(f) = p$, *siempre que* $1 < \mathrm{l}(A)$.

4.4. Fórmulas de un Lenguaje Proposicional

Definición 4.4.1. Dado un lenguaje proposicional $\mathbf{L} = \langle X, Cons, a\rangle$ (cfr. la Definición 4.1.4), definimos:

$$\Phi_0 = X$$
$$\Phi_{i+1} = \Phi_i \cup \{fA_1\cdots A_p : f \in Cons \text{ y } n(f) = p \text{ y } A_1, \ldots, A_p \in \Phi_i\}$$

y finalmente:

$$\mathrm{P}(\mathbf{L}) = \bigcup_{i=0}^{\infty} \Phi_i$$

Definición 4.4.2. Dado un lenguaje proposicional $\mathbf{L} = \langle X, Cons, a\rangle$, *fórmula proposicional* o simplemente *fórmula* o *proposición* es cualquier palabra significativa del lenguaje proposicional $\mathbf{L}$.

Teorema 4.4.1. *Sea $\mathbf{L} = \langle X, Cons, a\rangle$ un lenguaje proposicional y A una palabra de $\mathrm{Exp}(\mathbf{L})$). Son equivalentes las siguientes afirmaciones:*

1. *A es una fórmula proposicional de $\mathbf{L}$.*
2. *$A \in P(\mathbf{L})$.*

Demostración. Supongamos que A es como dice el enunciado del teorema y que es significativa. El razonamiento es por inducción sobre $\mathrm{l}(A)$. Si $\mathrm{l}(A) = 1$, por el Corolario 4.3.5 sabemos que $A \in \mathrm{S}(\mathbf{L})$ y que $n(A) = 0$, por tanto $A \in X = \Phi_0$. Supongamos que $1 < \mathrm{l}(A)$ y que el resultado es cierto para cualquier palabra significativa de longitud menor que la de A. Por el Corolario 4.3.5 sabemos que A se puede expresar como $fA_1\cdots A_p$, donde para todo $1 \le i \le p$ se cumple que A_i es una palabra significativa según n y donde $\mathrm{n}(f) = p$. Por la hipótesis de inducción, para todo $1 \le i \le p$ existe k_i tal que $A_i \in \Phi_{k_i}$. Sea $k = \max\{k_1, \ldots, k_p\}$; se cumple entonces que para todo $1 \le i \le p$, $A_i \in \Phi_k$ y por tanto, $A \in \Phi_{k+1}$. En definitiva, hemos conluido que sea cual sea la longitud de A, $A \in P(\mathbf{L})$. La implicación recíproca es cierta por la propia Definición 4.2.1 o por el Lema 4.2.2. □

Definición 4.4.3. Sea $\mathbf{L} = \langle X, Cons, a\rangle$ un lenguaje proposicional, $f \in Cons$ tal que $n(x) = p$ y $\Gamma \subseteq \mathrm{Exp}(\mathbf{L})$. Γ es cerrado para f sii, por definición, para todo $A_1, \ldots, A_p \in \Gamma$, $fA_1\cdots A_p \in \Gamma$. Γ es cerrado para $Cons$ sii, por definición, Γ es cerrado para cada $f \in Cons$.

Teorema 4.4.2. *Sea $\mathbf{L} = \langle X, Cons, a\rangle$ un lenguaje proposicional. Entonces:*

$$\mathrm{P}(\mathbf{L}) = \bigcap\{\Gamma \subseteq \mathrm{Exp}(\mathbf{L}) : X \subseteq \Gamma \text{ y } \Gamma \text{ es cerrado para } Cons\}$$

Demostración. Existe al menos un subconjunto de $\mathrm{Exp}(L)$ cerrado para $Cons$ que contiene a X, a saber, $\mathrm{P}(L)$. Por tanto $\bigcap\{\Gamma \subseteq \mathrm{Exp}(\mathbf{L}) : X \subseteq \Gamma$ y Γ es cerrado para $Cons\}$ existe y es un subconjunto de $\mathrm{P}(L)$. Recíprocamente, si $\Gamma \subseteq \mathrm{Exp}(\mathbf{L})$, $X \subseteq \Gamma$ y Γ es cerrado para $Cons$ entonces evidentemente contiene como subconjunto a $\mathrm{P}(\mathbf{L})$. Así pues, $\mathrm{P}(\mathbf{L})$ es subconjunto de $\bigcap\{\Gamma \subseteq \mathrm{Exp}(\mathbf{L}) : X \subseteq \Gamma$ y Γ es cerrado para $Cons\}$ □

Definición 4.4.4. Dado un lenguaje proposicional $\mathbf{L} = \langle X, Cons, a\rangle$ y A una fórmula de $\mathbf{L}$, el conjunto de *subfórmulas* de A, en símbolos $\mathrm{sub}(A)$, es por definición:

$$\mathrm{sub}(A) = \begin{cases} \{A\}, & \text{si } A \in X, \\ \{A\} \cup (\bigcup_{i=1}^{r} \mathrm{sub}(A_i)), & \text{si } n(f) = r \text{ y } A = fA_1\cdots A_r \end{cases}$$

Sea $f \in Cons$, si $n(f) = r$ entonces $f \in A$ significa que existen $A_1, \ldots, A_r \in \mathrm{sub}(A)$ tales que $fA_1\cdots A_r \in \mathrm{sub}(A)$.

Capítulo 5

Lógica Proposicional

5.1. Lenguaje Proposicional

Definición 5.1.1. Un *lenguaje proposicional estándard* es un lenguaje proposicional $\mathbf{L} = \langle X, Cons, a\rangle$ cumpliendo que:

- X es numerable no finito. Sus elementos son representamos con las primeras letras minúsculas del alfabeto latino, subindicándolas si fuese preciso: a, b, c, a_0, a_1, a_2, etc.
- $Cons = \{N, C\}$.
- $a(N) = 1$ y $a(C) = 2$.

Para abreviar representamos por S al conjunto $S(\mathbf{L}) = X \cup Cons$ y lo llamamos *conjunto de símbolos* de $\mathbf{L}$.

Observación 5.1.1. Seal $\mathbf{L}$ el lenguaje proposicional standar y consideremos la siguiente sucesión de conjuntos definida recursivamente:

$$\begin{aligned}\Phi_0 &= X\\ \Phi_{i+1} &= \Phi_i \cup \{C\alpha\beta\colon \alpha, \beta \in \Phi_i\} \cup \{N\alpha\colon \alpha \in \Phi_i\}\end{aligned}$$

Por el Teorema 4.4.1 sabemos que una *fórmula proposicional* o simplemente *fórmula* o *proposición* del lenguaje proposicional standard es cualquier elemento del conjunto de expresiones:

$$\mathrm{P}(\mathbf{L}) = \bigcup_{i=0}^{\infty} \Phi_i$$

Por tanto, son *fórmulas proposicionales* del lenguaje proposicional:

- Cada uno de los símbolos de variable proposicional,
- la expresión $N\alpha$, siempre que α sea fórmula proposional y
- la expresión $C\alpha\beta$, siempre que α y β sean fórmulas proposionales.

y no hay otras fórmulas proposicionales distintas a las antes mencionadas. En el Capítulo 4 hemos justificado que sea cual sea la fórmula que consideremos, no existe más que una única forma de representarla; se trata del *principio de lectura única*.

Teorema 5.1.1. *Las fórmulas proposicionales están en cantidad numerable no finita.*

Demostración. Como

$$\bigcup_{i=0}^{\infty} \Phi_i$$

reune exáctamente a la totalidad de las fórmulas proposicionales (cfr. Definición 5.1.1), basta aplicar que la unión numerable de conjuntos numerables es numerable. Dicha unión no es finita porque no lo es Φ_0 en el lenguaje proposicional standard. □

Definición 5.1.2. Para cualesquiera fórmulas α y β, usaremos las siguientes representaciones:

- $(\neg\alpha)$ por $N\alpha$.
- $(\alpha \to \beta)$ por $C\alpha\beta$.
- $A\alpha\beta$ por $CN\alpha\beta$.
- $(\alpha \vee \beta)$ por $((\neg\alpha) \to \beta)$, es decir, por $CN\alpha\beta$.
- $K\alpha\beta$ por $NC\alpha N\beta$.
- $(\alpha \wedge \beta)$ por $(\neg(\alpha \to (\neg\beta)))$, es decir, por $NC\alpha N\beta$.
- $E\alpha\beta$ por $NCC\alpha\beta NC\beta\alpha$.
- $(\alpha \leftrightarrow \beta)$ por $((\alpha \to \beta) \wedge (\beta \to \alpha))$, es decir, por $NCC\alpha\beta NC\beta\alpha$.

Observación 5.1.2. En la práctica, al usar las representaciones de la Definición 5.1.2, suprimiremos paréntesis siempre que ello no suponga caer en ambigüedades.

Definición 5.1.3. Una fórmula del lenguaje proposiconal estándar $\mathbf{L}$ es un *literal* sii, por definición, pertenece al conjunto $\mathrm{L}(X)$ definido por la igualdad:

$$\mathrm{L}(X) = X \cup \{Nx : x \in X\}$$

Definición 5.1.4 $(\mathrm{V}(\varphi))$**.** Para cualquier fórmulas proposiconal φ definimos el conjunto de símbolos de variable que intervienen en φ, en símbolos $\mathrm{V}(\varphi)$, como sigue:

$$\mathrm{V}(\varphi) = \begin{cases} \mathrm{V}(a) & \text{, si } \varphi = a \in X \\ \mathrm{V}(\alpha) & \text{, si } \varphi = N\alpha \\ \mathrm{V}(\alpha) \cup \mathrm{V}(\beta) & \text{, si } \varphi = C\alpha\beta \end{cases}$$

Si Y es un conjunto de fórmulas, $\mathrm{V}_*(Y)$ es, por definición, el conjunto:

$$\bigcup\{V(\varphi) : \varphi \in Y\}$$

Definición 5.1.5 $(\mathrm{Com}(\varphi))$**.** Para cualquier fórmula proposiconal φ definimos la *complejidad* de φ, en símbolos $\mathrm{Com}(\varphi)$, como sigue:

1. $\mathrm{Com}(a) = 0$, para todo símbolo de variable a.
2. $\mathrm{Com}(N\alpha) = 1 + \mathrm{Com}(\alpha)$, siempre que α sea fórmula proposiconal.
3. $\mathrm{Com}(C\alpha\beta) = 1 + \mathrm{Com}(\alpha) + \mathrm{Com}(\beta)$, siempre que α y β sean fórmulas proposiconales.

5.2. Implicación Semántica

Observación 5.2.1. A lo largo de este tema y siguientes emplearemos a menudo la aritmética del cuerpo $\langle \mathbb{Z}_2, +, \cdot, 0, 1\rangle$ que está fijada por las siguientes tablas:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

de donde destacamos que para todo valor x e y escogidos en $\{0,1\}$: $x+x=0$ (el cuerpo es de característica 2) y $x^2=x$.

Definición 5.2.1. Una *valoración* o también *asignación*, representada por v es una aplicación que a cada proposición atómica, a, le hace corresponder un valor (de verdad) 0 ó 1.

Ejemplo 5.2.1. A modo de ejemplo de valoraciones ofrecemos los siguientes:

1. v_1 cumpliendo que para toda proposición atómica x, $v_1(x)=1$.
2. v_2 cumpliendo que para toda proposición atómica x, $v_2(x)=0$.
3. Dado cualquier número natural n y $A=\{a_0,\ldots,a_n\}$ cualquier conjunto de proposiciones atómicas con $n+1$ elementos, $v_A=\chi_A$.

Observación 5.2.2. Por el *principio de lectura única*, cada valoración v puede ser extendida de forma única a la totalidad de las fórmulas cumpliéndose, si dicha extensión es representada con la misma letra v, que:

- $v(\neg\alpha)=1$ sii $v(\alpha)=0$
- $v(\alpha\to\beta)=1$ sii $(v(\alpha)=0$ ó $v(\beta)=1)$

es decir, haciendo buena las tablas de las figuras 5.2(a) y 5.2(b). Usando la técnica *técnica interpolatoria de Lagrange* (cfr. Apéndice E) podemos encontrar una expresión aritmética que expresa la extensión de v. En efecto, considerando la tabla de la Figura 5.2(b), consideramos:

- $l_0(x)=\frac{x-1}{0-1}=x-1=x+1$
- $l_1(x)=\frac{x-0}{1-0}=x$

y componiendo esto para las parejas: $\langle 0,1\rangle$ y $\langle 1,0\rangle$ resulta:

$$\begin{aligned} N(x) &= 1l_0(x)+0l_1(x)\\ &= 1(x+1)+0x\\ &= x+1 \end{aligned}$$

Efectuando la interpolación por columnas sobre la tabla de la Figura 5.2(b) pero expresada bidimensionalmente en la Figura 5.1:

- en los puntos $\langle 0,1\rangle$ y $\langle 1,0\rangle$ queda como resultado $1(x+1)+0x=x+1$
- en los puntos $\langle 0,1\rangle$ y $\langle 1,1\rangle$ queda como resultado $1(x+1)+1x=x+1+x=1$

y considerando ahora de ello los puntos $\langle 0,x+1\rangle$ y $\langle 1,1\rangle$ que vienen dictados por las filas, queda al interpolar:

$$\begin{aligned} C(x,y) &= (x+1)l_0(y)+1l_1(y)\\ &= (x+1)(y+1)+1y\\ &= xy+y+x+1+y\\ &= xy+x+1 \end{aligned}$$

de donde:

$$v(\alpha \to \beta) = v(\alpha)v(\beta) + v(\alpha) + 1$$
$$v(\neg\alpha) = v(\alpha) + 1$$

En consecuencia, según la forma en que han sido definidas las conectivas derivadas a partir de N y C (cfr. Definición 5.1.2) debe cumplirse:

- $v(\alpha \vee \beta) = v(\alpha)v(\beta) + v(\alpha) + v(\beta)$
- $v(\alpha \wedge \beta) = v(\alpha)v(\beta)$
- $v(\alpha \leftrightarrow \beta) = v(\alpha) + v(\beta) + 1$

Así pues, y en resumen, se tiene que:

- $v(\neg\alpha) = 1$ sii, por def., $v(\alpha) = 0$
- $v(\alpha \to \beta) = 1$ sii, por def., $(v(\alpha) = 0$ ó $v(\beta) = 1)$
- $v(\alpha \vee \beta) = 1$ sii $(v(\alpha) = 1$ ó $v(\beta) = 1)$
- $v(\alpha \wedge \beta) = 1$ sii $(v(\alpha) = 1$ y $v(\beta) = 1)$
- $v(\alpha \leftrightarrow \beta) = 1$ sii $(v(\alpha) = v(\beta))$

y esta consideración, tan útil en la práctica, queda recogida en las tablas de la Figura 5.2.

Ejemplo 5.2.2. Sea v cualquier asignación. Entonces:

1. Evaluación de $\alpha \to (\beta \to \gamma)$:

$$\begin{aligned} v(\alpha \to (\beta \to \gamma)) &= v(\alpha)v(\beta \to \gamma) + v(\alpha) + 1 \\ &= v(\alpha)(v(\beta)v(\gamma) + v(\beta) + 1) + v(\alpha) + 1 \\ &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta) + v(\alpha) + v(\alpha) + 1 \\ &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta) + 1 \\ &= v(\alpha)v(\beta)(v(\gamma) + 1) + 1 \end{aligned}$$

2. Evaluación de $(\alpha \wedge \beta) \to \gamma$;

$$\begin{aligned} v((\alpha \wedge \beta) \to \gamma)) &= v(\alpha \wedge \beta)v(\gamma) + v(\alpha \wedge \beta) + 1 \\ &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta) + 1 \\ &= v(\alpha)v(\beta)(v(\gamma) + 1) + 1 \end{aligned}$$

Observación 5.2.3. Como muestra el Ejemplo 5.2.2, sea cual sea la asignación de variables que usemos dista mucho de evaluar de forma inyectiva pues hay bastantes fórmulas distintas, muy distintas, que quedarían evaluadas en un mismo valor.

→		
β \ α	0	1
0	1	0
1	1	1

Figura 5.1: Tabla bidimensional de →.

Lema 5.2.1 (de relevancia)**.** *Sea φ una fórmula proposicional y v, v' asignaciones de variables cualesquiera. Si*

$$v \restriction \mathrm{V}(\varphi) = v' \restriction \mathrm{V}(\varphi) \tag{5.1}$$

entonces $v(\varphi) = v'(\varphi)$.

Demostración. El razonamiento es por inducción sobre sobre la complejidad de φ. Supongamos que $n \geq 0$ y que (**hip. de inducción**) el resultado es cierto para para toda fórmula de complejidad menor que n. Caben tres posibilidades:

- $\varphi = a$, para cierto símbolo de variable a; así pues $\mathrm{V}(a) = \{a\}$. En este caso, la validez de la condición 5.1 se expresa como que $v(a) = v'(a)$, es decir, $v(\varphi) = v'(\varphi)$.
- $\varphi = N\alpha$; entonces $\mathrm{V}(\varphi) = \mathrm{V}(\alpha)$ y la hipótesis 5.1 conlleva $v \restriction \mathrm{V}(\alpha) = v' \restriction \mathrm{V}(\alpha)$. Como $\mathrm{Com}(\alpha) < \mathrm{Com}(\varphi)$, la hipótesis de inducción permite establecer $v(\alpha) = v'(\alpha)$ y por tanto:

$$\begin{aligned} v(\varphi) &= 1 + v(\alpha) \\ &= 1 + v'(\alpha) \\ &= v'(\varphi) \end{aligned}$$

- $\varphi = C\alpha\beta$; entonces $\mathrm{V}(\varphi) = \mathrm{V}(\alpha) \cup \mathrm{V}(\beta)$ y la hipótesis 5.1 conlleva $v \restriction \mathrm{V}(\alpha) = v' \restriction \mathrm{V}(\alpha)$ y $v \restriction \mathrm{V}(\beta) = v' \restriction \mathrm{V}(\beta)$. Dado que tanto α como β tienen memor complejidad que φ, la hipótesis de inducción implica que $v(\alpha) = v'(\alpha)$ y $v(\beta) = v'(\beta)$. Por tanto:

$$\begin{aligned} v(\varphi) &= v(C\alpha\beta) \\ &= v(\alpha)v(\beta) + v(\alpha) + 1 \\ &= v'(\alpha)v'(\beta) + v'(\alpha) + 1 \\ &= v'(C\alpha\beta) \\ &= v'(\varphi) \end{aligned}$$

  Así pues, el resultado es cierto para toda fórmula proposicional φ.

α	$\neg\alpha$
0	1
1	0

(a) negación

α	β	$\alpha \to \beta$
0	0	1
0	1	1
1	0	0
1	1	1

(b) implicación

α	β	$\alpha \vee \beta$
0	0	0
0	1	1
1	0	1
1	1	1

(c) disyunción

α	β	$\alpha \wedge \beta$
0	0	0
0	1	0
1	0	0
1	1	1

(d) conjunción

α	β	$\alpha \leftrightarrow \beta$
0	0	1
0	1	0
1	0	0
1	1	1

(e) equivalencia

Figura 5.2: Tablas para la interpretación semántica de los símbolos lógicos

□

Definición 5.2.2. Sea φ una fórmula del lenguaje proposicional. Entonces:

1. φ es una *fórmula satisfacible* sii, por def., existe (al menos) una valoración v tal que $v(\varphi) = 1$.
2. φ es una *fórmula refutable* sii, por def., $(\neg\varphi)$ es una fórmula satisfacible.
3. φ es una *fórmula tautológica*, *tautología* o *válida* sii, por def., para toda asignación v se cumple $v(\varphi) = 1$.
4. φ es una *contradicción* sii, por def., $(\neg\varphi)$ es una *tautología*.

Ejemplo 5.2.3. Para conocer ejemplos de tautologías de la lógica clásica y otros, consulte el Apéndice B.

Observación 5.2.4. Sea observado que:

- φ es una *fórmula refutable* sii existe (al menos) una valoración v tal que $v(\varphi) = 0$.
- En palabras sencillas, una tautología es una fórmula que se evalúa como verdadera, se evalúen como se evalúen las fórmulas atómicas que intervienen en su única escritura; "la verdad" viene exigida por su única estructura sintáctica, significa "la verdad" por su forma y no por el valor mutable de sus partes atómicas.
- Si una fórmula φ es satisfacible pero no tautología, entonces es también refutable.
- φ es una *contradicción* sii para toda valoración v se cumple la igualdad $v(\varphi) = 0$.
- Si una fórmula φ es refutable pero no contradicción, entonces es también satisfacible.

Definición 5.2.3. Dado un conjunto de fórmulas Γ —posiblemente vacío— y una fórmula φ decimos que Γ *implica semánticamente* a φ, abreviadamente $\Gamma \vDash \varphi$, si para toda valoración v se tiene $v(\varphi) = 1$ siempre que para toda fórmula γ de Γ valga la igualdad $v(\gamma) = 1$. Si Γ consta solamente de las fórmulas $\gamma_1, \ldots, \gamma_n$, en lugar de $\{\gamma_1, \ldots, \gamma_n\} \vDash \varphi$ escribimos $\gamma_1, \ldots, \gamma_n \vDash \varphi$ y cuando $\Gamma = \varnothing$ escribimos simplemente $\vDash \varphi$ en lugar de $\varnothing \vDash \varphi$.

Ejemplo 5.2.4.

1. Para cualquier tautología α, $\vDash \alpha$. En particular, para todo símbolo de variable proposicional, a, se cumple $\vDash a \to a$.
2. $\alpha, \alpha \to \beta \vDash \beta$; en efecto, sea v una asignación cualquiera a condición de que $v(\alpha) = v(\alpha \to \beta) = 1$ y demostremos que para una tal v debe cumplirse $v(\beta) = 1$. Basta considerar las siguientes igualdades:

$$\begin{aligned} 1 &= v(\alpha \to \beta) \\ &= v(\alpha)v(\beta) + v(\alpha) + 1 \\ &= 1 \cdot v(\beta) + 1 + 1 \\ &= v(\beta) + 0 \\ &= v(\beta) \end{aligned}$$

3. $\alpha \to (\beta \to \gamma), \alpha \to \beta, \alpha \vDash \gamma$; en efecto, sea v una asignación cualquiera a condición de que $v(\alpha \to (\beta \to \gamma)) = v(\alpha \to \beta) = v(\alpha) = 1$ y demostremos que para una tal v debe cumplirse $v(\beta) = 1$. Basta

considerar que por (2) se cumplirá $v(\beta) = 1$ y, además, las siguientes igualdades:

$$\begin{aligned} 1 &= v(\alpha \to (\beta \to \gamma)) && \text{hipótesis} \\ &= v(\alpha)v(\beta \to \gamma) + v(\alpha) + 1 \\ &= 1 \cdot v(\beta \to \gamma) + 1 + 1 && \text{pues } v(\alpha) = 1 \\ &= v(\beta \to \gamma) \\ &= v(\gamma) && \text{pues } v(\beta) = 1 \end{aligned}$$

4. $\alpha \to \beta, \beta \to \gamma \vDash \alpha \to \gamma$
5. $(\alpha \vee \beta) \wedge (\alpha \to \gamma) \wedge (\beta \to \gamma) \vDash \gamma$
6. $(\neg\alpha \vee \neg\beta) \wedge (\gamma \to \alpha) \wedge (\gamma \to \beta) \vDash \neg\gamma$
7. $(\alpha \vee \beta) \wedge (\alpha \to \varphi) \wedge (\beta \to \psi) \vDash \varphi \vee \psi$
8. $(\neg\alpha \vee \neg\beta) \wedge (\varphi \to \alpha) \wedge (\psi \to \beta) \vDash \neg\varphi \vee \neg\psi$
9. $a \vee b \nvDash a$; en efecto, suponiendo que $a \neq b$, sea una asignación v cualquiera a condición de que $v(b) = 1$ y $v(a) = 0$. Se cumple $v(a \vee b) = 1$ y, sin embargo, $v(a) = 0$.
10. $a \nvDash a \wedge b$

Lema 5.2.2. *Para toda fórmula α, α es tautología sii $\vDash \alpha$.*

Demostración. Si α es tautología, entonces para cualquier conjunto Γ de fórmulas, $\Gamma \vDash \alpha$ y en particular $\vDash \alpha$. Recíprocamente, si $\vDash \alpha$ y existiera una asignación v tal que $v(\alpha) = 0$, entonces debería existir $\gamma \in \varnothing$ tal que $v(\alpha) = 0$, con lo que estaríamos en el absurdo de que el cojunto vacío no sería vacío. En conclusión, para toda asignación v debe cumplirse que $v(\alpha) = 1$. □

Definición 5.2.4. Las fórmula α y β son *lógicamente equivalentes* o símplemente *equivalentes* si, y sólo si, por definición, $\vDash \alpha \leftrightarrow \beta$, es decir, sii $\alpha \leftrightarrow \beta$ es una tautología. La frase "α y β son *lógicamente equivalentes*" será abreviada ocasionalmente como $\alpha \equiv \beta$.

Ejemplo 5.2.5. Sean α, α', β, β' y γ fórmulas. Si α es logicamente equivalente a α' y β es lógicamente equivalente a β', entonces cada *item* subsiguiente enumera fórmulas lógicamente equivalentes:

1. α, α
2. α y β, tautologías cualesquiera.
3. $\alpha \vee \beta$, $\alpha' \vee \beta'$
4. $\alpha \wedge \beta$, $\alpha' \wedge \beta'$
5. $\alpha \to \beta$, $\neg(\alpha \wedge \neg\beta)$
6. $\neg\alpha \to \beta$, $\alpha \vee \beta$
7. $\alpha \vee (\beta \wedge \gamma)$, $(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
8. $\alpha \wedge (\beta \vee \gamma)$, $(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$

Lema 5.2.3. *La relación $\equiv$ entre fórmulas del lenguaje proposicional es una relación de equivalencia.*

Demostración. La demostración es un sencillo ejercicio. □

Teorema 5.2.4. *Sean α y β fórmulas de un lenguaje proposicional. Son equivalentes las siguientes afirmaciones:*

1. *α y β son lógicamente equivalentes*
2. *$\vDash \alpha \to \beta$ y $\vDash \beta \to \alpha$*
3. *$\alpha \vDash \beta$ y $\beta \vDash \alpha$*
4. *Para toda asignación v, $v(\alpha) = v(\beta)$*

Demostración. Supongamos que α y β son lógicamente equivalentes, es decir, que para todo asignación v se cumple $v(\alpha \leftrightarrow \beta)$. o equivalentemente $v(\alpha \to \beta) = v(\beta \to \alpha) = 1$, es decir, $\vDash \alpha \to \beta$ y $\vDash \beta \to \alpha$. Supongamos ahora que $\vDash \alpha \to \beta$ y $\vDash \beta \to \alpha$. Sea v una asignación cualquiera tal que $v(\alpha) = 1$. Como en particular, según la hipótesis $\vDash \alpha \to \beta$, para esa v se cumple $v(\alpha \to \beta) = 1$, deducimos por (2) que $v(\beta) = 1$. Acabamos de demostrar que $\alpha \vDash \beta$ y la demostración de $\beta \vDash \alpha$ es similar. Supongamos ahora qu $\alpha \vDash \beta$ y $\beta \vDash \alpha$ y tomemos una asignación v cualquiera. Caben dos posibilidades:

- $v(\alpha) = 1$; debido a la hipótesis $\alpha \vDash \beta$, debe cumplirse $v(\beta) = 1$.
- $v(\alpha) = 0$; por reducción al absurdo, dado que por hipótesis se cumple $\beta \vDash \alpha$, si $v(\beta) = 1$ entonces $v(\alpha) = 1$ y esto no ocurre en este caso y, por tanto, $v(\beta) = 0$.

Finalmente, supongamos que para toda valoración v, $v(\alpha) = v(\beta)$ y sea v una asignación cualquiera. En ese caso:

$$\begin{aligned} v(\alpha \to \beta) &= v(\alpha)v(\beta) + v(\alpha) + 1 \\ &= v(\alpha)^2 + v(\alpha) + 1 \\ &= v(\alpha) + v(\alpha) + 1 \\ &= 0 + 1 \\ &= 1 \end{aligned}$$

Análogamente tendremos que $v(\beta \to \alpha) = 1$ y, por tanto, $v(\alpha \leftrightarrow \beta) = 1$. □

Observación 5.2.5. Es claro que si α es una tautología y $\alpha \vDash \beta$, entonces β debe ser también una tautología; por lo que *a fortiori* si una fórmula es lógicamente equivalente a una tautología cualquiera, ella será una tautología; y más aún, cualesquiera dos tautologías son lógicamente equivalentes. Por demás existen fórmulas lógicamente equivalentes que no son tautologías, como se ha mostrado antes, y existen parejas de fómulas que no son lógicamente equivalentes. Sin ir más lejos, ninguna proposición atómica es lógicamente a otra salvo ella misma (si convenimos en admitir que la verdad y la falsedad son entes distintos).

Teorema 5.2.5. *Sean φ, ψ, ξ, α y β fórmulas del lenguaje proposcional. Si α es lógicamente equivalente a $\varphi \vee \psi$ y β lo es a $\varphi \vee \xi$ Entonces son lógicamente equivalentes las fórmulas:*

- $\varphi \vee (\psi \wedge \xi)$
- $\alpha \wedge \beta$

Demostración. Sea v una asignación cualquiera. Por la hipótesis del teorema sabemos que: $v(\alpha) =$

$v(\varphi \vee \psi)$ y $v(\beta) = v(\varphi \vee \xi)$. Se tiene lo siguiente:

$$\begin{aligned}
v(\varphi \vee (\psi \wedge \xi)) &= v(\varphi)v(\psi)v(\xi) + v(\varphi) + v(\psi)v(\xi) \\
&= v(\varphi)v(\psi)v(\xi) + v(\varphi) + v(\psi)v(\xi) + 0 + 0 + 0 \\
&= v(\varphi)v(\psi)v(\xi) + v(\varphi) + v(\psi)v(\xi) \\
&+ (v(\varphi)v(\psi)v(\xi) + v(\varphi)v(\psi)v(\xi)) \\
&+ (v(\varphi)v(\psi) + v(\varphi)v(\psi)) \\
&+ (v(\varphi)v(\xi) + v(\varphi)v(\xi)) \\
&= v(\varphi)v(\psi)v(\xi) + v(\varphi)v(\psi) + v(\varphi)v(\psi)v(\xi) \\
&+ v(\varphi)v(\xi) + v(\varphi) + v(\varphi)v(\xi) \\
&+ v(\varphi)v(\psi)v(\xi) + v(\varphi)v(\psi) + v(\psi)v(\xi) \\
&= v(\varphi)v(\psi)v(\xi) + v(\varphi)^2v(\psi) + v(\varphi)v(\psi)v(\xi) \\
&+ v(\varphi)^2v(\xi) + v(\varphi)^2 + v(\varphi)v(\xi) \\
&+ v(\varphi)v(\psi)v(\xi) + v(\varphi)v(\psi) + v(\psi)v(\xi) \\
&= (v(\varphi)v(\psi) + v(\varphi) + v(\psi))(v(\varphi)v(\xi) + v(\varphi) + v(\xi)) \\
&= v(\varphi \vee \psi)v(\varphi \vee \xi) \\
&= v(\alpha)v(\beta) \\
&= v(\alpha \wedge \beta)
\end{aligned}$$

y esto demuestra lo que se quería. □

Teorema 5.2.6. *Sean φ, ψ, ξ, α y β fórmulas del lenguaje proposcional. Si α es lógicamente equivalente a $\varphi \wedge \psi$ y β lo es a $\varphi \wedge \xi$ Entonces son lógicamente equivalentes las fórmulas:*

- $\varphi \wedge (\psi \vee \xi)$
- $\alpha \vee \beta$

Definición 5.2.5. Un conjunto Γ de fórmulas del lenguaje proposicional es *insatisfacible* sii, por def., para toda valoración v existe $\varphi_v \in \Gamma$ tal que $v(\varphi_v) = 0$. Un conjunto Γ de fórmulas del lenguaje es *satisfacible* cuando, y sólo cuando, no es insatisfacible.

Ejemplo 5.2.6.

1. El conjunto $\varnothing$ es satisfacible. En efecto, considérese cualquier asignación (cfr. Ejemplo 5.2.1) v. v satisface al conjunto $\varnothing$, pues si no lo satisfaciese sería porque existiera al menos un elemento α de $\varnothing$ tal que $v(\alpha) = 0$ y con ello el conjunto vacío habría de tener elementos, lo cual es absurdo.
2. Para todo símbolo de variable proposicional a, $\{a, \neg a\}$ es insatisfacible.
3. Cualquier conjunto que contenga a $\{a, \neg a\}$, siendo a un símbolo de variable proposicional cualquiera, es insatisfacible.

Observación 5.2.6. Sea observado que:

- Un conjunto Γ de fórmulas del lenguaje proposicional es satisfacible sii existe al menos una asignación v tal que para todo $\gamma \in \Gamma$, $v(\gamma) = 1$.
- Un conjunto Γ de fórmulas del lenguaje proposicional es satisfacible sii existe al menos una asignación v tal que $v_*(\Gamma) \subseteq \{1\}$. Nótese que si hubiésemos escrito $v_*(\Gamma) = \{1\}$, quedaría excluido el conjunto vacío, que es satisfacible, y no estaríamos ante una equivalencia.
- φ es satisfacible sii $\{\varphi\}$ es satisfacible.

- Según un *razonamiento por vacuidad*, el conjunto $\varnothing$ es satisfacible.
- Si Γ es un conjunto de fórmulas proposicionales, $\varphi \in \Gamma$ y φ es una tautología, entonces Γ es satisfacible sii $\Gamma \setminus \{\varphi\}$ es satisfacible.
- Si Γ es un conjunto de fórmula, $\varphi \in \Gamma$ y φ es una contradicción, entonces Γ es insatisfacible.

5.3. Propiedades Básicas de la Implicación Semántica

Definición 5.3.1 (satisfacibilidad finita)**.** Un conjunto Γ de fórmulas es *finitamente satisfacible* si, y sólo si, por definición, cualquier subconjunto finito Γ_f de Γ es satisfacible.

Lema 5.3.1. *Sea Γ un conjunto finitamente satisfacible de fórmulas y sea φ una fórmula. Entonces $\Gamma \cup \{\varphi\}$ es finitamente satisfacible o $\Gamma \cup \{\neg\varphi\}$ es finitamente satisfacible.*

Demostración. Demostraremos la afirmación contrarrecíproca. Supongamos que ni $\Gamma \cup \{\varphi\}$ ni $\Gamma \cup \{\neg\varphi\}$ son finitamente satisfacibles. Entonces existirán subconjuntos finitos Γ_1 y Γ_2 de Γ tales que $\Gamma_1 \cup \{\varphi\}$ y $\Gamma_2 \cup \{\varphi\}$ son insatisfacibles. Supongamos que la asignación v satisficiese a $\Gamma_1 \cup \Gamma_2$; entonces se tendría $v(\varphi) = 1 = v(\neg\varphi)$, lo cual es absurdo. Por tanto, $\Gamma_1 \cup \Gamma_2$ es insatisfacible, siendo un subconjunto finito de Γ. Así pues, Γ no podría ser finitamente satisfacible. □

Teorema 5.3.2 (de Compacidad)**.** *Sea Γ un conjunto de fórmulas proposicionales. Son equivalentes las siguientes afirmaciones:*

1. *Γ es satisfacible.*
2. *Γ es finitamente satisfacible.*

Demostración. Si Γ es satisfacible, también lo son sus subconjuntos y en particular sus subconjuntos finitos. Recíprocamente, supongamos que cada subconjunto finito de Γ es satisfacible. Consideremos los símbolos de variables proposicionales enumerados $\langle a_i \rangle_{i=0}^{\infty}$ y consideremos la siguiente definición recursiva:

$$\Delta_0 = \Gamma$$

$$\Delta_{i+1} = \begin{cases} \Delta_i \cup \{a_i\} & \text{, si es finitamente satisfacible,} \\ \Delta_i \cup \{\neg a_i\} & \text{, en otro caso.} \end{cases}$$

En virtud del Lema 5.3.1) sabemos que cada Δ_i es finitamente satisfacible. Sea $\Delta = \bigcup_i \Delta_i$, del que sabemos lo siguiente:

1. $\Gamma \subseteq \Delta$
2. Δ es finitamente satisfacible; en efecto, sea Δ_f un subconjunto finito de Δ. Como Δ_f es finito y para todo natural i, $\Delta_i \subseteq \Delta_{i+1}$, existirá un número natural j tal que $\Delta_f \subseteq \bigcup_{i=0}^{j} \Delta_i = \Delta_j$. Como en particular Δ_j es finitamente satisfacible, Δ_f es satisfacible.
3. Para todo símbolo de variable proposicional a_i, por construcción $a_i \in \Delta$ o $\neg a_i \in \Delta$ siendo esta disyunción lingüística exclusiva, pues Δ es finitamente satisfacible y si para cierto i, a_i y $\neg a_i$ perteneciese a Δ, $\{a_i, \neg a_i\}$ sería un subconjunto finito de Δ insatisfacible.

Consideremos ahora la asignación de variables v definida por la siguiente condición:

$$v(a_i) = \chi_{\Delta}(a_i)$$

y τ una función que aplica a cada símbolo de variable a el siguiente valor:

$$\tau(a) = \begin{cases} a & \text{, si } a \in \Delta \\ \neg a & \text{, si } \neg a \in \Delta \end{cases}$$

Sea $\varphi \in \Gamma$ y $Y = \{\tau(a) : a \in \mathrm{V}(\varphi)\}$. Entonces, por la definición de τ y v tenemos que:

- Si $\lambda \in Y$, entonces $v(\lambda) = 1$. En efecto, si $\lambda \in Y$ es porque existe $a \in \mathrm{V}(\varphi)$ tal que $\lambda = \tau(a)$; pero $\tau(a) \in \Delta$, luego $v(\lambda) = \chi_\Delta(\tau(a)) = 1$.

- $Y \subseteq \Delta$. En efecto, si $\lambda \in Y$ es porque existe $a \in \mathrm{V}(\varphi)$ tal que $\lambda = \tau(a)$; pero $\tau(a) \in \Delta$, luego $\lambda \in \Delta$.

- $\mathrm{V}(\varphi) = \mathrm{V}_*(Y)$. En efecto,

$$\begin{aligned} \mathrm{V}_*(Y) &= \bigcup\{\mathrm{V}(\lambda) : \lambda \in Y\} && \text{por definición} \\ &= \bigcup\{\mathrm{V}(\tau(a)) : a \in \mathrm{V}(\varphi)\} \\ &= \bigcup\{\{a\} : a \in \mathrm{V}(\varphi)\} && \text{pues } \mathrm{V}(\tau(a)) = \{a\} \\ &= \mathrm{V}(\varphi) \end{aligned}$$

- Para todo $\lambda \in Y$, $v(\lambda) = 1$. En efecto, para todo $\lambda \in Y$ existe $a \in \mathrm{V}(\varphi)$ tal que $\lambda = \tau(a)$; como para todo $a \in \mathrm{V}(\varphi)$, $\tau(a) \in \Delta$ entonces se cumple que $v(\lambda) = \chi_\Delta(\tau(a)) = 1$.

Como $\mathrm{V}(\varphi)$ es finito, $\mathrm{V}(\varphi) \cup \{\varphi\}$ es un subconjunto finito de Δ. Como Δ es finitamente satisfacible, $\mathrm{V}(\varphi) \cup \{\varphi\}$ es satisfacible, por lo que existe al menos una asignación v' que satisface a este conjunto. En particular, $v'(\varphi) = 1$ y además, para todo literal λ de Y, $v'(\lambda) = 1$. Así pues, $v \restriction \mathrm{V}(\varphi) = v' \restriction \mathrm{V}(\varphi)$ y por el Lema 5.2.1, deducimos que $v(\varphi) = v'(\varphi) = 1$. Como φ era una fórmula de Γ fija, pero arbitraria, hemos demostrado que v satisface a Γ, como se quería. □

Corolario 5.3.3. *Sea Γ un conjunto de fórmulas proposicionales. Son equivalentes las siguientes afirmaciones:*

1. *Γ es insatisfacible.*

2. *Existe un subconjunto finito de Γ que es insatisfacible.*

Definición 5.3.2. Dado un conjunto de fórmulas Γ del lenguaje, sea $\mathrm{Con}(\Gamma)$ el conjunto de fórmulas γ tales que $\Gamma \models \gamma$.

Ejemplo 5.3.1. $\mathrm{Con}(\varnothing)$ es el conjunto de las tautologías y, por tanto, es no vacío.

Lema 5.3.4. *Si Γ es instatisfacible entonces cualquier fórmula proposicional es elemento de $\mathrm{Con}(\Gamma)$.*

Demostración. Supongamos que Γ es insatisfacible y que φ es una fórmula proposicional. Si $\Gamma \not\models \varphi$, existiría al menos una asignación de variables tal que $v_*(\Gamma) \subseteq \{1\}$ y sin embargo $v(\varphi) = 0$. Así pues, Γ sería satisfacible, en contra de lo supuesto. Por tanto, no puede darse $\Gamma \not\models \varphi$ y entonces $\Gamma \models \varphi$. □

Teorema 5.3.5. *Para cualesquiera conjuntos de fórmula Γ y Δ son ciertas las siguientes afirmaciones:*

1. $\Gamma \subseteq \mathrm{Con}(\Gamma)$

2. *Si $\Gamma \subseteq \Delta$, entonces $\mathrm{Con}(\Gamma) \subseteq \mathrm{Con}(\Delta)$ (monotonía)*

3. $\mathrm{Con}(\mathrm{Con}(\Gamma)) \subseteq \mathrm{Con}(\Gamma)$

4. $\mathrm{Con}(\varnothing) \subseteq \mathrm{Con}(\Gamma)$

5. $\mathrm{Con}(\mathrm{Con}(\Gamma)) = \mathrm{Con}(\Gamma)$ *(idempotencia)*

Demostración. Si cualquiera de los conjuntos Γ o Δ fuera instatisfacible, todas las afirmaciones son trivialmente ciertas por lo que sabemos del Lema 5.3.4. Supongamos entonces que ambos conjuntos Γ y Δ son satisfacibles. En cuanto a la afirmación 1, sea v cualquier asignación que cumpla $v_*(\Gamma) \subseteq \{1\}$. Si $\gamma \in \Gamma$ entonces, en particular, $v(\gamma) = 1$. Esto significa que para todo $\gamma \in \Gamma$ se cumple $\Gamma \vDash \gamma$, o sea, $\Gamma \subseteq \mathrm{Con}(\Gamma)$. En cuanto a la afirmación 2, sea $\gamma \in \mathrm{Con}(\Gamma)$ y sea una cualquiera de las asignaciones v que cumplen $v_*(\Delta) \subseteq \{1\}$. Puesto que $\Gamma \subseteq \Delta$, es cierto que $v_*(\Gamma) \subseteq \{1\}$ y puesto que por hipótesis $\Gamma \vDash \gamma$, se tiene que $v(\gamma) = 1$. Hemos demostrado que si $\gamma \in \mathrm{Con}(\Gamma)$ entonces $\Delta \vDash \gamma$, es decir, $\gamma \in \mathrm{Con}(\Delta)$ o equivalentemente que $\mathrm{Con}(\Gamma) \subseteq \mathrm{Con}(\Delta)$. En cuanto a la afirmación 3, sea una cualquiera de las asignaciones v tales que $v_*(\Gamma) \subseteq \{1\}$; para cualquier $\varphi \in \mathrm{Con}(\Gamma)$ se cumplirá, por tanto, $v(\varphi) = 1$. Tenemos entonces que $v_*(\mathrm{Con}(\Gamma)) \subseteq \{1\}$, así si $\gamma \in \mathrm{Con}(\mathrm{Con}(\Gamma))$ entonces $v(\gamma) = 1$ y, por tanto, $\gamma \in \mathrm{Con}(\Gamma)$. Hemos demostrado que $\mathrm{Con}(\mathrm{Con}(\Gamma)) \subseteq \mathrm{Con}(\Gamma)$. La afirmación 4 es consecuencia de afirmación 2. Para afirmación 5, tengamos en cuenta que por la 1), $\Gamma \subseteq \mathrm{Con}(\Gamma)$ y entonces, por 2), $\mathrm{Con}(\Gamma) \subseteq \mathrm{Con}(\mathrm{Con}(\Gamma))$ y la igualdad se tiene entonces en virtud de 3). □

Definición 5.3.3. Sea Δ un conjunto de fórmulas. Δ es *cerrado* sii, por definición, $\mathrm{Con}(\Delta) = \Delta$.

Ejemplo 5.3.2.

1. No es cerrrado $\varnothing$, pues cualquier tautología es elemento de $\mathrm{Con}(\varnothing)$.

2. Sin embargo, $\mathrm{Con}(\varnothing)$ sí es cerrado puesto que $\mathrm{Con}(\mathrm{Con}(\varnothing)) = \mathrm{Con}(\varnothing)$ (cfr. 5) del Teorema 5).

3. En general, para todo conjunto Γ de fórmulas, $\mathrm{Con}(\Gamma)$ es cerrado.

4. $\mathrm{P}(\mathbf{L})$ es cerrado.

5. Para todo conjunto Γ de fórmulas, $\mathrm{Con}(\Gamma)$ y $\mathrm{P}(\mathbf{L})$ son ejemplos (no necesariamente distintos) de conjuntos cerrados que tienen a Γ como subconjunto, no necesariamente propio.

Teorema 5.3.6. *Para todo conjunto Γ de fórmulas:*

$$\mathrm{Con}(\Gamma) = \bigcap\{\Delta : \Delta \textit{ es cerrado y } \Gamma \subseteq \Delta\}$$

Demostración. En primer lugar, según es establecido en el Ejemplo 5.3.2, es no vacío el conjunto $\{\Delta : \Delta \text{ es cerrado y } \Gamma \subseteq \Delta\}$. Supongamos que Δ es cerrado y que $\Gamma \subseteq \Delta$. Al cumplirse $\Gamma \subseteq \Delta$, se tiene $\mathrm{Con}(\Gamma) \subseteq \mathrm{Con}(\Delta)$. Al ser Δ cerrado, $\mathrm{Con}(\Delta) = \Delta$ por lo que $\mathrm{Con}(\Gamma) \subseteq \Delta$. Así pues, $\{\Delta : \Delta \text{ es cerrado y } \Gamma \subseteq \Delta\}$ es no vacío y $\mathrm{Con}(\Gamma) \subseteq \bigcap\{\Delta : \Delta \text{ es cerrado y } \Gamma \subseteq \Delta\}$. Recíprocamente, $\mathrm{Con}(\Gamma)$ es cerrado y $\Gamma \subseteq \mathrm{Con}(\Gamma)$, por lo que $\bigcap\{\Delta : \Delta \text{ es cerrado y } \Gamma \subseteq \Delta\} \subseteq \mathrm{Con}(\Gamma)$. El resultado queda demostrado por doble inclusión. □

Observación 5.3.1. Obsérvese que en virtud de lo que establece el Teorema 5.3.6, $\mathrm{Con}(\varnothing) = \bigcap\{\Delta : \Delta \text{ es cerrado}\}$.

Corolario 5.3.7. *Para todo conjunto de fórmulas Δ cerrado y fórmulas φ y ψ:*

1. $\mathrm{Con}(\varnothing) \subseteq \Delta$.

2. $\psi \in \Delta$ *siempre que* $\varphi, \varphi \to \psi \in \Delta$.

Demostración. Como $\varnothing \subseteq \Delta$ y Δ es cerrado, se tiene:

$$\mathrm{Con}(\varnothing) \subseteq \mathrm{Con}(\Delta) = \Delta$$

Por otra parte, supongamos que $\varphi, \varphi \to \psi \in \Delta$. Entonces son ciertas las siguientes afirmaciones:

$$\begin{aligned} &\vDash \varphi \to ((\varphi \to \psi) \to \psi) \\ \Delta &\vDash \varphi \to ((\varphi \to \psi) \to \psi) \\ \Delta &\vDash \varphi \\ \Delta &\vDash (\varphi \to \psi) \to \psi \\ \Delta &\vDash \varphi \to \psi \\ \Delta &\vDash \psi \end{aligned}$$

Hemos concluido que $\psi \in \mathrm{Con}(\Delta)$, o sea, que $\psi \in \Delta$. □

Teorema 5.3.8. *Para cualesquiera fórmulas α, β y γ y conjunto de fórmulas Γ:*

1. *Si $\Gamma \vDash \alpha$ y $\Gamma \vDash \alpha \to \beta$, entonces $\Gamma \vDash \beta$ (regla del modus ponens)*
2. *Si $\Gamma \vDash \alpha \vee \beta$ y $\Gamma \vDash \neg\alpha \vee \gamma$ entonces $\Gamma \vDash \beta \vee \gamma$ (regla de resolución en log. proposicional)*

Demostración. Si $\Gamma \vDash \alpha$ y $\Gamma \vDash \alpha \to \beta$, entonces $\alpha, \alpha \to \beta \in \mathrm{Con}(\Gamma)$. Por 2) del Ejemplo 5.2.4 y la monotonía de Con, sabemos que $\beta \in \mathrm{Con}(\mathrm{Con}(\Gamma))$, es decir, $\beta \in \mathrm{Con}(\Gamma)$ o equivalentemente $\Gamma \vDash \beta$. Por otra parte, $\alpha \vee \beta$ (resp. $\neg\alpha \vee \gamma$) es lógicamente equivalente a $\neg\alpha \to \beta$ (resp. $\alpha \to \gamma$), por lo que $\vDash (\alpha \vee \beta) \to (\neg\alpha \to \beta)$ (resp. $\vDash (\neg\alpha \vee \gamma) \to (\alpha \to \gamma)$). Tenemos, pues,

1. $\Gamma \vDash \alpha \vee \beta$
2. $\vDash (\alpha \vee \beta) \to (\neg\alpha \to \beta)$
3. $\Gamma \vDash \neg\alpha \vee \gamma$
4. $\vDash (\neg\alpha \vee \gamma) \to (\alpha \to \gamma)$

Por esto, la regla del *modus ponens* y la monotonía, tenemos que $\Gamma \vDash \neg\alpha \to \beta$ y $\Gamma \vDash \alpha \to \gamma$. Por 10) del Ejemplo B.0.2 y la monotonía tenemos que $\Gamma \vDash (\neg\alpha \to \beta) \to (\neg\beta \to \alpha)$, por lo que $\Gamma \vDash \neg\beta \to \alpha$ y $\Gamma \vDash \alpha \to \gamma$. Por 2) del Ejemplo B.0.1 sabemos que en particular, $\vDash (\neg\beta \to \alpha) \to ((\alpha \to \gamma) \to (\neg\beta \to \gamma))$ por lo que $\Gamma \vDash (\neg\beta \to \alpha) \to ((\alpha \to \gamma) \to (\neg\beta \to \gamma))$. Aplicando dos veces la regla del *modus ponens* concluimos que $\Gamma \vDash \neg\beta \to \gamma$; pero al ser lógicamente equivalentes las fórmulas $\neg\beta \to \gamma$ y $\beta \vee \gamma$, lo que hemos demostrado es que $\Gamma \vDash \beta \vee \gamma$, como queríamos. □

Teorema 5.3.9. *Sea Γ un conjunto de fórmulas propicionales. Son equivalentes las siguientes afirmaciones:*

1. *Γ es insatisfacible*
2. *Existe una fórmula α tal que $\Gamma \vDash \alpha$ y $\Gamma \vDash \neg\alpha$.*
3. *Para toda fórmula proposicional β, $\Gamma \vDash \beta$.*

Demostración. Supongamos que Γ es insatisfacible y sea α el símbolo de variable a_0. Si $\Gamma \nvDash a_0$ es porque existe al menos una asignación de variables v tal que $v_*(\Gamma) \subseteq \{1\}$ y sin embargo $v(a_0) = 0$; en ese caso Γ no sería insatisfacible, en contra de lo supuesto. Por tanto, $\Gamma \vDash a_0$ y un razonamiento análogo conduce a que $\Gamma \vDash a_0$. Supongamos que existe una fórmula α tal que $\Gamma \vDash \alpha$ y $\Gamma \vDash \neg\alpha$. Sea β cualquier fórmula. Por 4) del Ejemplo B.0.2, tenemos que $\vDash \neg\alpha \to (\alpha \to \beta)$ y por monotonía que $\Gamma \vDash \neg\alpha \to (\alpha \to \beta)$. Aplicando dos veces la regla del *modus ponens* concluimos que $\Gamma \vDash \beta$. Finalmente, si para cualquier fórmula β se cumple $\Gamma \vDash \beta$ entonces, en particular para $\Gamma \vDash a_0 \wedge \neg a_0$. Por ello, si existiese aunque fuese una asignación de variables v tal que $v_*(\Gamma) \subseteq \{1\}$, entonces $1 = v(a_0 \wedge \neg a_0) = 0$ lo que es absurdo. Por tanto, en ese supuesto, Γ es necesariamente insatisfacible. □

Teorema 5.3.10 (de la deducción)**.** *Sea $\Gamma \cup \{\varphi, \psi\}$ un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1. $\Gamma, \psi \vDash \varphi$
2. $\Gamma \vDash \psi \to \varphi$

Demostración. Sea $\Gamma \cup \{\varphi, \psi\}$ un conjunto de fórmulas. Si alguno de los conjunto Γ o $\Gamma \cup \{\psi\}$ fuere insatisfacible, las dos afirmaciones son obviamente equialentes (¿por qué?). Supongamos, pues, que ni Γ ni $\Gamma \cup \{\psi\}$ son insatisfacibles. Ahora supongamos también que $\Gamma, \psi \vDash \varphi$ y que v es una asignación de variables cualquiera cumpliendo $v_*(\Gamma) \subseteq \{1\}$. Para v caben dos posibilidades:

- $v(\psi) = 0$; entonces

$$\begin{aligned} v(\psi \to \varphi) &= v(\psi)v(\varphi) + v(\psi) + 1 \\ &= 0v(\varphi) + 0 + 1 \\ &= 0 + 0 + 1 \\ &= 1 \end{aligned}$$

- $v(\psi) = 1$; entonces $v_*(\Gamma \cup \{\psi\}) \subseteq \{1\}$ (de hecho ambos conjuntos coinciden en este caso) y como estamos suponiendo que $\Gamma, \psi \vDash \varphi$, para v debe cumplirse que $v(\varphi) = 1$ y así $v(\psi \to \varphi) = 1$

como en cualquiera de los casos posibles hemos obtenido que $v(\psi \to \varphi) = 1$, entonces hemos demostrado que $\Gamma \vDash \psi \to \varphi$. Recíprocamente, supongamos que $\Gamma \vDash \psi \to \varphi$ y sea v una asignación de variables tal que $v_*(\Gamma \cup \{\psi\}) \subseteq \{1\}$. Entonces $v(\psi \to \varphi) = 1 = v(\psi)$, de donde $v(\varphi) = 1$. Hemos concluido, pues, que $\Gamma, \psi \vDash \varphi$. □

Corolario 5.3.11. *Para cualesquiera fórmulas $\gamma_1, \ldots, \gamma_n, \varphi$ $(2 \leq n)$ son equivalentes las siguientes afirmaciones:*

1. $\gamma_1, \ldots, \gamma_n \vDash \varphi$
2. $\gamma_1 \wedge \cdots \wedge \gamma_n \vDash \varphi$
3. $\vDash \gamma_1 \wedge \cdots \wedge \gamma_n \to \varphi$

Teorema 5.3.12. *Sea $\Gamma \cup \{\varphi\}$ un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1. $\Gamma \vDash \varphi$
2. $\Gamma \cup \{\neg\varphi\}$ *es insatisfacible.*

Demostración. Supongamos que $\Gamma \vDash \varphi$ y que v es una valoración cualquiera. Supongamos que para todo $\gamma \in \Gamma$, $v(\gamma) = 1$. Entonces $v(\varphi) = 1$, por lo que necesariamente debe cumplirse $v(\neg\varphi) = 0$. Así pues, $\Gamma \cup \{\neg\varphi\}$ es insatisfacible. Recíprocamente, sea v una valoración tal que para todo $\gamma \in \Gamma$, $v(\gamma) = 1$. Al ser $\Gamma \cup \{\neg\varphi\}$ insatisfacible, debe cumplirse $v(\neg\varphi) = 0$, o sea, $v(\varphi) = 1$ y de ahí que $\Gamma \vDash \varphi$. □

Corolario 5.3.13. *Sea $\Gamma \cup \{\varphi\}$ un conjunto de fórmulas proposicionales. Son equivalentes las siguientes afirmaciones:*

1. $\Gamma \vDash \varphi$
2. *Existe un subconjunto finito de Γ, Γ_f, tal que $\Gamma_f \vDash \varphi$.*

Demostración. Supongamos que $\Gamma \vDash \varphi$, entonces $\Gamma \cup \{\neg\varphi\}$ es insatisfacible. Por el Corolario 5.3.3 sabemos que existe un subcojunto finito Σ_f de $\Gamma \cup \{\neg\varphi\}$ que es insatisfacible. Sea Γ_f el conjunto $\Sigma_f \setminus \{\neg\varphi\}$, que es un subconjunto finito de Γ. Entonces, $\Gamma_f \cup \{\neg\varphi\}$ es insatisfacible (¿por qué?). Según el Teorema 5.3.12, se tendrá que $\Gamma_f \vDash \varphi$. Recíprocamente, supongamos que Γ_f es un subconjunto finito de Γ y que $\Gamma_f \vDash \varphi$. Esto equivale a que $\varphi \in \mathrm{Con}(\Gamma_f)$; pero por 2) del Teorema 5.3.5 sabemos que $\mathrm{Con}(\Gamma_f) \subseteq \mathrm{Con}(\Gamma)$ y por tanto $\varphi \in \mathrm{Con}(\Gamma)$, o sea, $\Gamma \vDash \varphi$. □

Corolario 5.3.14. *Sean Γ un conjunto de fórmulas proposicionales. Entonces:*

$$\mathrm{Con}(\Gamma) = \bigcup_{\substack{\Gamma_f \subseteq \Gamma \\ \Gamma_f \text{ finito}}} \mathrm{Con}(\Gamma_f) \qquad \textit{(finitariedad)}$$

Teorema 5.3.15. *Sea $\Gamma \cup \{\psi, \varphi\}$ un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1. $\Gamma, \psi \wedge \varphi \vDash \xi$
2. $\Gamma, \psi, \varphi \vDash \xi$

Corolario 5.3.16. *Para cualesquiera fórmulas $\gamma_1, \ldots, \gamma_n, \varphi$ $(2 \leq n)$ son equivalentes las siguientes afirmaciones:*

1. $\gamma_1, \ldots, \gamma_n \vDash \varphi$
2. $\{\gamma_1, \gamma_2, \ldots, \gamma_n, \neg\varphi\}$ *es insatisfacible*
3. $\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n \wedge \neg\varphi$ *es insatisfacible*

Teorema 5.3.17. *Sea $\Gamma \cup \{\psi, \varphi\}$ un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1. $\Gamma \vDash \psi$ *y* $\Gamma \vDash \varphi$
2. $\Gamma \vDash \psi \wedge \varphi$

Demostración. Supongamos que $\Gamma \vDash \psi$ y $\Gamma \vDash \varphi$. Por monotonía y al ser $\alpha \to (\beta \to (\alpha \wedge \beta))$ una tautología para cualesquiera fórmulas α y β, tenemos que:

$$\Gamma \vDash \psi \to (\varphi \to (\psi \wedge \varphi))$$

Por la primera suposición y el *modus ponens* deducimos que $\Gamma \vDash \varphi \to (\psi \wedge \varphi)$; por la segunda suposición y el *modus ponens* deducimos finalmente que $\Gamma \vDash \psi \wedge \varphi$. Recíprocamente, supongamos que $\Gamma \vDash \psi \wedge \varphi$. Como $(\alpha \wedge \beta) \to \alpha$ es una ley lógica para cualesquiera fórmulas α y β, tenemos en particular que $\Gamma \vDash (\psi \wedge \varphi) \to \psi$ y $\Gamma \vDash (\psi \wedge \varphi) \to \varphi$. Si $\Gamma \vDash \psi \wedge \varphi$, como suponemos por hipótesis, entonces $\Gamma \vDash \psi$ y $\Gamma \vDash \varphi$ por medio del *modus ponens*. □

Teorema 5.3.18. *Sea $\Gamma \cup \{\psi, \varphi, \xi\}$ un conjunto de fórmulas.*

1. *Si* $\Gamma, \psi \vDash \xi$ *y* $\Gamma, \varphi \vDash \xi$, *entonces* $\Gamma, \psi \vee \varphi \vDash \xi$.
2. *Si* $\Gamma \vDash \varphi$, *entonces* $\Gamma \vDash \varphi \vee \psi$

Demostración. Supongamos que $\Gamma, \psi \vDash \xi$ y $\Gamma, \varphi \vDash \xi$; entonces, por el *teorema de la deducción* (cfr. Teorema 5.3.10), $\Gamma \vDash \psi \to \xi$ y $\Gamma \vDash \varphi \to \xi$. Por 3) del Ejemplo B.0.4 tenemos que para cualesquier fórmulas $\alpha, \beta, \gamma, \vDash (\alpha \to \gamma) \to ((\beta \to \gamma) \to ((\alpha \vee \beta) \to \gamma))$. En particular y por la monotonía tenemos:

$$\Gamma \vDash (\psi \to \xi) \to ((\varphi \to \xi) \to ((\psi \vee \varphi) \to \xi))$$

Por *modus ponens* deducimos que $\Gamma \vDash (\psi \vee \varphi) \to \xi$ o equivalentemente $\Gamma, \psi \vee \varphi \vDash \xi$. Supongamos ahora que $\Gamma \vDash \varphi$. Por 1) del Ejemplo B.0.4 tenemos que para cualesquier fórmulas α, β, γ, $\alpha \to (\alpha \vee \beta)$. En particular y por la monotonía tenemos que $\Gamma \vDash \varphi \to (\varphi \vee \psi)$ y por *modus ponens* deducimos que $\Gamma \vDash \varphi \vee \psi$. □

5.4. Forma Normal Conjuntiva

El propósito de esta sección es describir un algoritmo preciso para obtener una fórmula en forma normal conjuntiva lógicamente equivalente a otra dada.

Definición 5.4.1. Sea el *lenguaje proposicional de la forma normal conjuntiva*, abreviadamente f.n.c., es un lenguaje proposicional $\mathbf{L_{KA}} = \langle X, Cons, a\rangle$ cumpliendo que:

- X es numerable no finito. Sus elementos serán son representados con las primeras letras minúsculas del alfabeto latino, subindicándolas si fuese preciso: a, b, c, a_0, a_1, a_2, etc.
- $Cons = \{A, K\}$.
- $a(A) = 1$ y $a(K) = 2$.

Observación 5.4.1.

1. Para abreviar ocasionalmente podríamos escribir simplemente $\mathrm{P}(\mathbf{L})$ en lugar de $\mathrm{P}(\mathbf{L_{KA}})$.
2. Los elementos de X en $\mathbf{L_{KA}}$ serán precisados más tarde.

Definición 5.4.2. Sea Δ un conjunto no vacío de fórmulas del lenguaje $\mathbf{L_{KA}}$. Definimos los siguientes conjuntos:

- $\mathrm{A}(\Delta) = \bigcap\{\Gamma\colon \Delta \subseteq \Gamma \subseteq \mathrm{P}(\mathbf{L})$ y Γ es cerrado bajo $A\}$
- $\mathrm{K}(\Delta) = \bigcap\{\Gamma\colon \Delta \subseteq \Gamma \subseteq \mathrm{P}(\mathbf{L})$ and Γ is closed under $K\}$
- $\Xi_{\mathrm{A}}(\Delta) = \bigcap\{\Gamma\colon \Delta \subseteq \Gamma \subseteq \mathrm{P}(\mathbf{L})$ and $\mathrm{A}\alpha\beta \in \Gamma$ whenever $\alpha \in \Gamma$ and $\beta \in \Delta\}$
- $\Xi_{\mathrm{K}}(\Delta) = \bigcap\{\Gamma\colon \Delta \subseteq \Gamma \subseteq \mathrm{P}(\mathbf{L})$ and $\mathrm{K}\alpha\beta \in \Gamma$ whenever $\alpha \in \Gamma$ and $\beta \in \Delta\}$

Definición 5.4.3. Sea $\alpha \in \mathrm{P}(\mathbf{L_{KA}})$. La fórmula α es una *forma normal conjuntiva* (resp. *cláusula*) sii, por definición, $\alpha \in \mathrm{K}(\mathrm{A}(X))$ (resp. $\alpha \in \Xi_{\mathrm{A}}(X)$). Por otra parte, α es una *forma normal conjuntiva a izquierdas* cuando, y sólo cuando, $\alpha \in \Xi_{\mathrm{K}}(\Xi_{\mathrm{A}}(X))$. En lo que sigue abreviaremos $\Xi_{\mathrm{K}}(\Xi_{\mathrm{A}}(X))$ por $\mathrm{lcnf}(X)$.

Para tener una medida del "volumen" de una fórmula, introducimos las funciones de *complejidad* y *longitud*.

Definición 5.4.4. Para cualquier α perteneciente a $\mathrm{P}(\mathbf{L_{KA}})$, la *complejidad* de α, $\mathrm{comp}(\alpha)$, es por definición:

$$\mathrm{comp}(\alpha) = \begin{cases} 0, & \text{if } \alpha \in X, \\ 1 + \mathrm{comp}(\varphi) + \mathrm{comp}(\psi), & \text{if } \alpha = A\varphi\psi \text{ or } \alpha = K\varphi\psi. \end{cases}$$

y la *longitud* de α, $\mathrm{lg}(\alpha)$, es por definición:

$$\mathrm{lg}(\alpha) = \begin{cases} 0, & \text{if } \alpha \in X, \\ 1 + \mathrm{máx}\{\mathrm{lg}(\varphi), \mathrm{lg}(\psi)\}, & \text{if } \alpha = A\varphi\psi \text{ or } \alpha = K\varphi\psi. \end{cases}$$

Nuestro objetivo ahora es, dada una fórmula φ de $\mathrm{P}(\mathbf{L_{KA}})$, encontrar otra φ_{cnf} perteneciente a $\mathrm{K}(\mathrm{A}(X))$ tal que ambas sean lógicamente equivalentes. Esto será la base del algoritmo y para ello lo primero es determinar cómo de alejada está φ de $\mathrm{K}(\mathrm{A}(X))$.

Definición 5.4.5. Sea α cualquier fórmula perteneciente a $\mathrm{P}(\mathbf{L_{KA}})$. La *alternancia* de α, $\mathrm{alt}(\alpha)$, es por definición:

$$\mathrm{alt}(\alpha) = \begin{cases} 0, & \text{si } \mathrm{K} \notin \alpha; \\ \max\{\mathrm{alt}(\varphi), \mathrm{alt}(\psi)\}, & \text{si } \alpha = \mathrm{K}\,\varphi\psi; \\ 1 + \max\{\mathrm{alt}(\varphi), \mathrm{alt}(\psi)\}, & \text{si } \alpha = \mathrm{A}\,\varphi\psi \text{ y } \mathrm{K} \in \alpha. \end{cases}$$

En el Lema 5.4.1 caracterizamos qué significa "pertenecer al cojunto $\mathrm{K}(\mathrm{A}(X))$" mediante la aplicación alt.

Lema 5.4.1. *Let $\alpha \in \mathrm{P}(\mathbf{L_{KA}})$. Son equivalentes las siguientes afirmaciones:*

1. $\mathrm{alt}(\alpha) = 0$.
2. $\alpha \in \mathrm{K}(\mathrm{A}(X))$.

Demostración. Sea α una fórmula tal que $\mathrm{alt}(\alpha) = 0$. Si $\mathrm{K} \notin \alpha$, entonces $\alpha \in \mathrm{A}(X)$ y así $\alpha \in \mathrm{K}(\mathrm{A}(X))$. Si $\mathrm{K} \in \alpha$, entonces $\alpha = \mathrm{K}\phi\psi$, donde $\mathrm{alt}(\phi) = \mathrm{alt}(\psi) = 0$. Por hipótesis de inducción, $\phi, \psi \in \mathrm{K}(\mathrm{A}(X))$ y entonces $\alpha \in \mathrm{K}(\mathrm{A}(X))$. El recíproco es de desmostración inmediata a partir de la Definición 5.4.5. □

Definición 5.4.6 (distributividad). Consideremos las siguientes reglas compuestas sobre relaciones binarias entre fórmulas de $\mathrm{P}(\mathbf{L_{KA}})$:

$$x_i \to_{dak} x_i \tag{5.2}$$

$$\frac{A\varphi\xi \to_{dak} \alpha \quad A\psi\xi \to_{dak} \beta}{AK\varphi\psi\xi \to_{dak} K\alpha\beta} \tag{5.3}$$

$$\frac{A\xi\varphi \to_{dak} \alpha \quad A\xi\psi \to_{dak} \beta}{A\xi K\varphi\psi \to_{dak} K\alpha\beta} \tag{5.4}$$

$$\frac{\varphi \to_{dak} \varphi' \quad \psi \to_{dak} \psi'}{A\varphi\psi \to_{dak} A\varphi'\psi'} \tag{5.5}$$

$$\frac{\varphi \to_{dak} \varphi' \quad \psi \to_{dak} \psi'}{K\varphi\psi \to_{dak} K\varphi'\psi'} \tag{5.6}$$

donde (5.3), (5.4) y (5.5) son aplicadas con la preferencia que indica el orden en las que han sido dadas. Siendo así, definimos la siguiente aplicación

$$\mathrm{dak}\colon \mathrm{P}(\mathbf{L_{KA}}) \longrightarrow \mathrm{P}(\mathbf{L_{KA}})$$

por

$$\mathrm{dak}(\varphi) = \psi, \text{ siempre que } \varphi \to_{dak} \psi$$

Observación 5.4.2. dak es realmente una aplicación pues se ha establecido una precedencia en las reglas en las que se basa su definición. Más aún, la transformada por dak de una fórmula resulta ser otra lógicamente equivalente.

Teorema 5.4.2. *Para toda $\zeta \in \mathrm{P}(\mathbf{L_{KA}})$, $\mathrm{dak}(\zeta) \equiv \zeta$, es decir $\mathrm{dak}(\zeta)$ y ζ son fórmulas lógicamente equivalentes.*

Demostración. Sea ζ perteneciente a $\mathrm{P}(\mathbf{L_{KA}})$ y tal que $\mathrm{comp}(\zeta) = n$. Supongamos, como hipótesis de inducción, que lo que se quiere probar es cierto para cualquier fórmula η tal que $\mathrm{comp}(\eta) < n$. Pueden darse varios casos:

1. $\zeta = x \in X$; como cualquier fórmula es lógicamente equivalente a ella misma y $\mathrm{dak}(\zeta) = \zeta$, se tiene el resultado para este caso.
2. $\zeta = AK\varphi\psi\xi$; suponemos que $\mathrm{dak}(A\varphi\xi) = \alpha$ y $\mathrm{dak}(A\psi\xi) = \beta$. Como la complejidad de cualquiera de las fórmulas $A\varphi\xi$ y $A\psi\xi$ es menor que la de ζ, $A\varphi\xi \equiv \alpha$ y $A\psi\xi \equiv \beta$. Por lo que afirma el Teorema 5.2.5 sabemos que $AK\varphi\psi\xi \equiv K\alpha\beta$, es decir, $AK\varphi\psi\xi \equiv \mathrm{dak}(AK\varphi\psi\xi)$.
3. $\zeta = A\xi K\varphi\psi$; este caso se demuestra análogamente al 2).

4. $\zeta = A\varphi\psi$; suponemos que $\mathrm{dak}(\varphi) = \varphi'$ y $\mathrm{dak}(\psi) = \psi'$. Como la complejidad de cualquiera de las fórmulas φ y ψ es menor que la de ζ, $\varphi \equiv \varphi'$ y $\psi \equiv \psi'$. Por lo ilustrado con el Ejemplo 5.2.5 sabemos que $A\varphi\psi \equiv A\varphi'\psi'$, es decir, $A\varphi\psi \equiv \mathrm{dak}(A\varphi\psi)$.

5. $\zeta = K\varphi\psi$; este caso se demuestra análogamente al 4).

□

Lema 5.4.3. *Sea α una fórmula cualquiera de $\mathrm{P}(\mathbf{L_{KA}})$. Si $\alpha \in \mathrm{A}(X)$ entonces $\mathrm{dak}(\alpha) = \alpha$*

Demostración. Supongamos que $\alpha \in \mathrm{A}(X)$ y que $\mathrm{comp}(\alpha) = n$. Razonando por inducción sobre $\mathrm{comp}(\alpha)$ demostraremos que $\mathrm{dak}(\alpha) = \alpha$. Supongamos que la implicación es cierta para toda fórmula $\beta \in \mathrm{A}(X))$ tal que $\mathrm{comp}(\beta) < n$. Si $\alpha \in \mathrm{A}(X)$, entonces son posibles dos situaciones:

1. $\alpha \in X$; si $x \in X$ y $\alpha = x$, entonces

$$\begin{aligned} \mathrm{dak}(\alpha) &= \mathrm{dak}(x) \\ &= x && \text{por Regla 5.2} \\ &= \alpha \end{aligned}$$

2. existen fórmulas φ y ψ de $\mathrm{A}(X)$ de complejidades menores que las de α tales que $\alpha = A\varphi\psi$. Como $K \notin \alpha$, para el cálculo de $\mathrm{dak}(\alpha)$ no es de aplicación más que la Regla 5.5. En efecto:

$$\begin{aligned} \mathrm{dak}(\alpha) &= \mathrm{dak}(A\varphi\psi) \\ &= A\,\mathrm{dak}(\varphi)\,\mathrm{dak}(\psi) && \text{por Regla 5.5} \\ &= A\varphi\psi && \text{por hip. induc.} \\ &= \alpha \end{aligned}$$

□

Observación 5.4.3. En el Lema 5.4.3 la condición $\alpha \in \mathrm{A}(X)$ es suficiente para que se de $\mathrm{dak}(\alpha) = \alpha$, pero no es necesaria. El Lema 5.4.4, que es consecuencia del Lema 5.4.3, da la condición necesaria y suficiente.

Lema 5.4.4. *Sea $\alpha \in \mathrm{P}(\mathbf{L_{KA}})$. Si $\alpha \in \mathrm{K}(\mathrm{A}(X))$ entonces $\mathrm{dak}(\alpha) = \alpha$.*

Demostración. Supongamos que $\alpha \in \mathrm{K}(\mathrm{A}(X))$ y que $\mathrm{comp}(\alpha) = n$. Razonando por inducción sobre $\mathrm{comp}(\alpha)$ demostraremos que $\mathrm{dak}(\alpha) = \alpha$. Supongamos que la implicación es cierta para toda fórmula $\beta \in \mathrm{K}(\mathrm{A}(X))$ tal que $\mathrm{comp}(\beta) < n$. Si $\alpha \in \mathrm{K}(\mathrm{A}(X))$, entonces son posibles dos situaciones:

1. $\alpha \in \mathrm{A}(X)$; que en este caso $\mathrm{dak}(\alpha) = \alpha$ es lo que establece el Lema 5.4.3.

2. existen fórmulas φ y ψ de $\mathrm{K}(\mathrm{A}(X))$ de complejidades menores que las de α tales que $\alpha = K\varphi\psi$. Para el cálculo de $\mathrm{dak}(\alpha)$ no es posible comenzar más que por la Regla 5.6. Así pues:

$$\begin{aligned} \mathrm{dak}(\alpha) &= \mathrm{dak}(K\varphi\psi) \\ &= K\,\mathrm{dak}(\varphi)\,\mathrm{dak}(\psi) && \text{por Regla 5.6} \\ &= K\varphi\psi && \text{por hip. induc.} \\ &= \alpha \end{aligned}$$

□

El significado esencial del Teorema 5.4.5 es que aplicando dak a una fórmula dada, digamos φ, el resultado está más cerca de $\mathrm{K}(\mathrm{A}(X))$ que φ, ello según la "medida" alt.

Teorema 5.4.5. *Sea α una fórmula cualquiera de $\mathrm{P}(\mathbf{L_{KA}})$. Entonces:*

$$\mathrm{alt}(\mathrm{dak}(\alpha)) = \begin{cases} 0, & \textit{si } \alpha \in \mathrm{K}(\mathrm{A}(X)); \\ \mathrm{alt}(\alpha) - 1, & \textit{en otro caso.} \end{cases}$$

Demostración. La demostración es sobre la complejidad de la fórmula. Sea α perteneciente a $\mathrm{P}(\mathbf{L_{KA}})$ y tal que $\mathrm{comp}(\alpha) = n$. Supongamos, como hipótesis de inducción, que lo que se quiere probar es cierto para cualquier fórmula β tal que $\mathrm{comp}(\beta) < n$. Pueden darse varios casos:

1. $\alpha = x \in X$; en este caso $\mathrm{dak}(\alpha) = x \in X$ y como quiera que $X \subseteq \mathrm{K}(\mathrm{A}(X))$ deducimos, según lo que establece el Lema 5.4.1, que $\mathrm{alt}(\alpha) = 0$ lo que demuestra el resultado en este caso.

2. $\alpha = AK\varphi\psi\xi$; en este caso tenemos que $\alpha \notin \mathrm{K}(\mathrm{A}(X))$ y que:

$$\begin{aligned} \mathrm{alt}(\alpha) &= 1 + \mathrm{máx}\{\mathrm{alt}(K\varphi\psi), \mathrm{alt}(\xi)\} \\ &= 1 + \mathrm{máx}\{\mathrm{alt}(\varphi), \mathrm{alt}(\psi), \mathrm{alt}(\xi)\} \end{aligned} \tag{5.7}$$

   Por otra parte, $\mathrm{dak}(\alpha) = K\,\mathrm{dak}(A\varphi\xi)\,\mathrm{dak}(A\psi\xi)$ por lo que:

$$\mathrm{alt}(\mathrm{dak}(\alpha)) = \mathrm{máx}\{\mathrm{alt}(\mathrm{dak}(A\varphi\xi)), \mathrm{alt}(\mathrm{dak}(A\psi\xi))\} \tag{5.8}$$

   Para abreviar, llamaremos β a $A\varphi\xi$ y γ a $A\psi\xi$. Tengamos en cuenta lo siguiente:

   a) $K \in \beta$; entonces $\mathrm{alt}(\beta) = 1 + \mathrm{máx}\{\mathrm{alt}(\varphi), \mathrm{alt}(\xi)\}$ y $\beta \notin \mathrm{K}(\mathrm{A}(X))$. Como $\mathrm{comp}(\beta) < \mathrm{comp}(\alpha)$, la hipótesis e inducción permite establecer que:

$$\begin{aligned} \mathrm{alt}(\mathrm{dak}(\beta)) &= \mathrm{alt}(\beta) - 1 \\ &= \mathrm{máx}\{\mathrm{alt}(\varphi), \mathrm{alt}(\xi)\} \end{aligned} \tag{5.9}$$

   b) $K \notin \beta$; entonces $\varphi, \xi, \beta \in \mathrm{A}(X)$. Según lo que establece el Lema 5.4.3, entonces $\mathrm{dak}(\beta) = \beta$ y, según el Lema 5.4.1,

$$\mathrm{alt}(\mathrm{dak}(\beta)) = \mathrm{alt}(\beta) = 0 \tag{5.10}$$

$$\mathrm{alt}(\varphi) = 0 \tag{5.11}$$

$$\mathrm{alt}(\xi) = 0 \tag{5.12}$$

   Analizaremos la igualdad 5.8 por casos:

   a) $K \in \beta$ y $K \in \gamma$; entonces:

$$\begin{aligned} \mathrm{alt}(\mathrm{dak}(\alpha)) &= \mathrm{máx}\{\mathrm{alt}(\mathrm{dak}(\beta)), \mathrm{alt}(\mathrm{dak}(\gamma))\} && \text{por (5.8)} \\ &= \mathrm{máx}\{\mathrm{alt}(\varphi), \mathrm{alt}(\psi), \mathrm{alt}(\xi)\} && \text{por (5.9)} \\ &= \mathrm{alt}(\alpha) - 1 \end{aligned}$$

   b) $K \notin \beta$ y $K \in \gamma$; entonces

$$\begin{aligned} \mathrm{alt}(\mathrm{dak}(\alpha)) &= \mathrm{máx}\{\mathrm{alt}(\mathrm{dak}(\beta)), \mathrm{alt}(\mathrm{dak}(\gamma))\} && \text{por (5.8)} \\ &= \mathrm{máx}\{0, \mathrm{alt}(\mathrm{dak}(\gamma))\} && \text{por (5.10)} \\ &= \mathrm{alt}(\mathrm{dak}(\gamma)) \\ &= \mathrm{máx}\{\mathrm{alt}(\psi), \mathrm{alt}(\xi)\} && \text{por (5.9)} \\ &= \mathrm{alt}(\psi) && \text{por (5.12)} \\ &= \mathrm{máx}\{0, \mathrm{alt}(\psi), 0\} \\ &= \mathrm{máx}\{\mathrm{alt}(\varphi), \mathrm{alt}(\psi), \mathrm{alt}(\xi)\} && \text{por (5.10) y (5.12)} \\ &= \mathrm{alt}(\alpha) - 1 && \text{por (5.7)} \end{aligned}$$

c) $K \in \beta$ y $K \notin \gamma$; esta situación es tratada como el caso del apartado 2*b*).

d) $K \notin \beta$ y $K \notin \gamma$; en este caso $\beta, \gamma \in \mathrm{A}(X)$ y $\alpha \in \mathrm{K}(\mathrm{A}(X))$. Por lo que afirma el Lema 5.4.4, $\mathrm{dak}(\alpha) = \alpha$ y, por lo que establece el Lema 5.4.1, $\mathrm{alt}(\alpha) = 0$; así pues, $\mathrm{alt}(\mathrm{dak}(\alpha)) = 0$

3. $\alpha = A\xi K\varphi\psi$; esta situación es tratada como el caso del apartado 2).

4. $\alpha = A\varphi\psi$, ni φ ni ψ comienzan por K pero $K \in \alpha$; sin pérdida de generalidad supongamos que $\mathrm{alt}(\psi) \leq \mathrm{alt}(\varphi)$, de donde $K \in \varphi$ y φ comienza por A, es decir $\varphi \notin \mathrm{K}(\mathrm{A}(X))$. Entonces $\mathrm{alt}(\alpha) = 1 + \mathrm{alt}(\varphi)$ y

$$\begin{aligned}
\mathrm{alt}(\mathrm{dak}(\alpha)) &= \mathrm{alt}(A\,\mathrm{dak}(\varphi)\,\mathrm{dak}(\psi)) \\
&= 1 + \mathrm{máx}\{\mathrm{alt}(\mathrm{dak}(\varphi)), \mathrm{alt}(\mathrm{dak}(\psi))\} \\
&= 1 + \mathrm{alt}(\mathrm{dak}(\varphi)) \\
&= 1 + \mathrm{alt}(\varphi) - 1 && \text{hip. de induc. y condiciones de } \varphi \\
&= \mathrm{alt}(\varphi) \\
&= \mathrm{alt}(\alpha) - 1
\end{aligned}$$

5. $\alpha = K\varphi\psi$; sin pérdida de generalidad supongamos que $\mathrm{alt}(\psi) \leq \mathrm{alt}(\varphi)$. Si $\mathrm{alt}(\varphi) = 0$, entonces $\mathrm{alt}(\psi) = 0$, $\varphi, \psi, \alpha \in \mathrm{K}(\mathrm{A}(X))$ y por tanto, $\mathrm{alt}(\alpha) = 0$ (cfr. Lema 5.4.1). Si $\mathrm{alt}(\varphi) \neq 0$, es decir $\varphi \notin \mathrm{K}(\mathrm{A}(X))$, entonces $\alpha \notin \mathrm{K}(\mathrm{A}(X))$. Así pues:

$$\begin{aligned}
\mathrm{alt}(\mathrm{dak}(\alpha)) &= \mathrm{alt}(K\,\mathrm{dak}(\varphi)\,\mathrm{dak}(\psi)) && \text{def. de } \mathrm{dak} \\
&= \mathrm{máx}\{\mathrm{alt}(\mathrm{dak}(\varphi)), \mathrm{alt}(\mathrm{dak}(\psi))\} && \text{def. de } \mathrm{alt} \\
&= \mathrm{alt}(\mathrm{dak}(\varphi)) \\
&= \mathrm{alt}(\varphi) - 1 && \text{hip. de induc. y condiciones de } \varphi \\
&= \mathrm{máx}\{\mathrm{alt}(\varphi), \mathrm{alt}(\psi)\} - 1 \\
&= \mathrm{alt}(\alpha) - 1 && \text{def. de } \mathrm{alt}
\end{aligned}$$

□

Observación 5.4.4. Como consecuencia del Teorema 5.4.5 se tiene que la condición suficiente del Lema 5.4.4 es también necesaria.

Corolario 5.4.6. *Sea α una fórmula cualquiera de $\mathrm{P}(\mathbf{L_{KA}})$. Son equivalentes las siguientes afirmaciones:*

1. $\mathrm{dak}(\alpha) = \alpha$
2. $\alpha \in \mathrm{K}(\mathrm{A}(X))$
3. $\mathrm{alt}(\alpha) = 0$

Demostración. Sea α una fórmula cualquiera de $\mathrm{P}(\mathbf{L_{KA}})$. Supongamos que $\mathrm{dak}(\alpha) = \alpha$. Según lo que afirma el Teorema 5.4.5, si $\alpha \notin \mathrm{K}(\mathrm{A}(X))$ entonces:

$$\begin{aligned}
\mathrm{alt}(\alpha) &= \mathrm{alt}(\mathrm{dak}(\alpha)) \\
&= \mathrm{alt}(\alpha) - 1
\end{aligned}$$

lo cual es absurdo y, por tanto, α debe ser un elemento de $\mathrm{K}(\mathrm{A}(X))$. Si $\alpha \in \mathrm{K}(\mathrm{A}(X))$ se tiene, según lo que afirma el Lema 5.4.1, que $\mathrm{alt}(\alpha) = 0$. Finalmente, si $\mathrm{alt}(\alpha) = 0$ entonces, según lo que afirma el Lema 5.4.1, $\alpha \in \mathrm{K}(\mathrm{A}(X))$ y por lo que asevera el Lema 5.4.4, $\mathrm{dak}(\alpha) = \alpha$. □

Ahora sabemos que dada una fórmula cualquiera, α, de $\mathrm{P}(\mathbf{L_{KA}})$ es posible obtener a partir de ella otra en forma normal conjuntiva por aplicación reiterada de la función dak. Además, el número de iteraciones necesarias es exactamente $\mathrm{alt}(\alpha)$. El Teorema 5.4.2 prueba que esa otra fórmula en forma normal conjuntiva es lógicamente equivalente a α, la fórmula de partida.

No obstante, para poder llevar a cabo el proceso antes detallado será preciso partir de una fórmula de $\mathrm{P}(\mathbf{L_{KA}})$, cuando lo habitual será contar con una fórmula de $\mathrm{P}(\mathbf{L})$. El remedio a esta situación es obtener a partir de la fórmula dada de $\mathrm{P}(\mathbf{L})$ otra perteneciente a $\mathrm{P}(\mathbf{L_{KA}})$ que sea lógica equivalente ella. Esta segunda sería la transformada a forma normal conjuntiva, obtiendo una tercera equivalente a la primera.

Definición 5.4.7 (eliminación de E y C). Sea la función

$$\mathrm{ece}\colon \mathrm{P}(\mathbf{L}) \longrightarrow \mathrm{P}(\mathbf{L})$$

definida por:

$$\mathrm{ece}(\zeta) = \begin{cases} x & \text{si } \zeta = x \text{ y } x \in X \\ KAN\,\mathrm{ece}(\varphi)\,\mathrm{ece}(\psi)AN\,\mathrm{ece}(\psi)\,\mathrm{ece}(\varphi), & \text{si } \zeta = E\varphi\psi \\ AN\,\mathrm{ece}(\varphi)\,\mathrm{ece}(\psi), & \text{si } \zeta = C\varphi\psi \\ N\,\mathrm{ece}(\varphi), & \text{si } \zeta = N\varphi \\ K\,\mathrm{ece}(\varphi)\,\mathrm{ece}(\psi), & \text{si } \zeta = K\varphi\psi \\ A\,\mathrm{ece}(\varphi)\,\mathrm{ece}(\psi), & \text{si } \zeta = A\varphi\psi \end{cases}$$

Definición 5.4.8 (profundización de N). Sea la función

$$\mathrm{brng}\colon \mathrm{P}(\mathbf{L}) \longrightarrow \mathrm{P}(\mathbf{L})$$

definida por:

$$\mathrm{brng}(\zeta) = \begin{cases} x & \text{si } \zeta = x \text{ y } x \in X \\ K\,\mathrm{brng}(\varphi)\,\mathrm{brng}(N\psi), & \text{si } \zeta = NC\varphi\psi \\ AK\,\mathrm{brng}(\varphi)\,\mathrm{brng}(N\psi)K\,\mathrm{brng}(\psi)\,\mathrm{brng}(N\varphi), & \text{si } \zeta = NE\varphi\psi \\ A\,\mathrm{brng}(N\varphi)\,\mathrm{brng}(N\psi), & \text{si } \zeta = NK\varphi\psi \\ K\,\mathrm{brng}(N\varphi)\,\mathrm{brng}(N\psi), & \text{si } \zeta = NA\varphi\psi \\ C\,\mathrm{brng}(\varphi)\,\mathrm{brng}(\psi), & \text{si } \zeta = C\varphi\psi \\ E\,\mathrm{brng}(\varphi)\,\mathrm{brng}(\psi), & \text{si } \zeta = E\varphi\psi \\ K\,\mathrm{brng}(\varphi)\,\mathrm{brng}(\psi), & \text{si } \zeta = K\varphi\psi \\ A\,\mathrm{brng}(\varphi)\,\mathrm{brng}(\psi), & \text{si } \zeta = A\varphi\psi \\ \mathrm{brng}(\varphi), & \text{si } \zeta = NN\varphi \end{cases}$$

Teorema 5.4.7. *Sea $Y = L(X)$ el conjunto de los literales del lenguaje proposicional estándard $\mathbf{L} = \langle X, Cons, a\rangle$, $Cons_1 = \{K, A\}$, $a_1 = a \restriction Cons_1$ y $\mathbf{L_{KAL}} = \langle Y, Cons_1, a_1\rangle$ el lenguaje proposicional de la forma normal conjuntiva sobre Y. Para todo $\alpha \in \mathrm{P}(\mathbf{L})$:*

1. $(\mathrm{brng} \circ \mathrm{ece})(\alpha) \in \mathrm{P}(\mathbf{L_{KAL}})$ *y*
2. $\alpha \equiv (\mathrm{brng} \circ \mathrm{ece})(\alpha)$.

Demostración. La demostración de este resultado es un ejercicio de inducción bastante sencillo, aunque algo tediosa. □

5.5. Algoritmo de Davis & Putnam

Hasta ahora hemos definido algunos conceptos que pasamos a recordar sintéticamente. Una fórmula λ es un *literal proposicional* sii, por def., existe una proposición atómica a tal que λ es la fórmula a o es la fórmula $\neg a$ (cfr. Definición 5.1.3). Una fórmula φ está en *forma normal conjuntiva*, abreviadamente f.n.c., sii, por def., es una conjunción de disyunciones de literales proposicionales del lenguaje, es decir, φ se escribe como:

$$\bigwedge_{i=0}^{n}(\lambda_{i,0} \vee \cdots \vee \lambda_{i,m_i})$$

donde cada $\lambda_{i,j}$ es un literal del lenguaje proposional (cfr. Definición 5.4.3). En tal caso llamamos *cláusula* o *conjunto* a cada fórmula $\lambda_{i,0} \vee \cdots \vee \lambda_{i,m_i}$ $(i = 0, \ldots, n)$. Dualmente, una fórmula φ está en *forma normal disyuntiva*, abreviadamente f.n.d., si es una disyunción de conjunciones de literales proposicionales del lenguaje, es decir, φ se escribe como:

$$\bigvee_{i=0}^{n}(\lambda_{i,0} \wedge \cdots \wedge \lambda_{i,m_i})$$

donde cada $\lambda_{i,j}$ es un literal del lenguaje proposional. En tal caso llamamos *disyunto* a cada fórmula $\lambda_{i,0} \wedge \cdots \wedge \lambda_{i,m_i}$ $(i = 0, \ldots, n)$.

Observación 5.5.1.

1. En este tema, y ocasionalmente con posterioridad, consideraremos a una cláusula como el conjunto de los literales que lo forman. Por tanto, las cláusulas generan conjuntos finitos y las veremos involucradas en expresiones de carácter conjuntista.

2. Al dar a una cláusula el carácter de conjunto, hay un trasiego unívoco entre cláusulas y conjuntos en ambos sentidos. Cabe pensar qué sería la cláusula asociada al conjunto vacío. Tiene interés y aporta ventaja simbólica aceptar la cláusula asociada al conjunto vacío; será la llamada *cláusula vacía* que representaremos por el símbolo $\square$ y que convenimos sea insatisfacible (pues, no hay literales para poderla satisfacer).

Definición 5.5.1. Dado un literal λ, definimos su *literal complementario* λ^c como sigue:

$$\lambda^c = \begin{cases} \neg a, & si\ \lambda = a \\ a, & si\ \lambda = \neg a \end{cases}$$

Definición 5.5.2. Sean α y β cláusulas. Entonces:

1. α es *tautológica* sii, por definición, existe un literal λ tal que $\{\lambda, \lambda^c\} \subseteq \alpha$.

2. α es *unit* sii, por definition, el conjunto de literales asociado a α es un simplete, es decir, su cardinal es igual a 1.

3. α es *ampliación* de β sii, por definición, $\alpha \subseteq \beta$.

4. El literal λ es *puro* en un conjunto de cláusas Σ sii, por definición, existe $\alpha_\lambda \in \Sigma$ tal que $\lambda \in \alpha_\lambda$ y para todo $\alpha \in \Sigma$, $\alpha \cap \{\lambda, \lambda^c\} \subseteq \{\lambda\}$. En otras palabras, λ es *puro* en un conjunto de cláusas Σ sii ocurre en al menos una cláusula y no aparece λ^c en ninguna de las cláusulas de Σ.

Lema 5.5.1 (Regla 1 o Regla de las Tautologías)**.** *Sea Σ un conjunto no vacío de cláusulas del lenguaje proposicional estándar. Si $\alpha \in \Sigma$ y α es tautológica, entonces son equivalentes las siguientes afirmaciones:*

1. *Σ es satisfacible.*

2. $\Sigma \setminus \{\alpha\}$ *es satisfacible.*

Teorema 5.5.2 (Regla 4 o Regla de Descomposición)**.** *Sea* Σ *un conjunto no vacío de cláusulas del lenguaje proposicional estándar y* λ *un literal. Sean* Σ_1 *y* Σ_2 *los conjuntos definidos por las siguientes igualdades:*

- $\Sigma_1 = \{\alpha \setminus \{\lambda^c\} : \alpha \in \Sigma,\ \lambda^c \in \alpha\} \cup \{\gamma : \gamma \in \Sigma,\ \gamma \cap \{\lambda, \lambda^c\} = \varnothing\}$
- $\Sigma_2 = \{\alpha \setminus \{\lambda\} : \alpha \in \Sigma,\ \lambda \in \alpha\} \cup \{\gamma : \gamma \in \Sigma,\ \gamma \cap \{\lambda, \lambda^c\} = \varnothing\}$

Son equivalentes las siguientes afirmaciones:

1. Σ *es satisfacible (resp. insatisfacible).*
2. Σ_1 *o* Σ_2 *(resp.* Σ_1 *y* Σ_2*) es satisfacible (resp. insatisfacible)*

Demostración. Supongamos que Σ es satisfacible y que lo evidencia la asignación v. Entonces, al cumplirse $\{\gamma : \gamma \cap \{\lambda, \lambda^c\} \subseteq \Sigma$ se tiene que para toda $\alpha \in \{\gamma : \gamma \cap \{\lambda, \lambda^c\} = \varnothing\}$, $v(\alpha) = 1$. □

Corolario 5.5.3 (Regla de la Cláusula Unit)**.** *Sea* Σ *un conjunto de cláusulas que cuenta entre sus elementos con una cláusula unit* λ *y sea* Σ' *el conjunto de cláusulas obtenido sustrayendo de* Σ *todas las ampliaciones de* λ*.*

1. *Si* $\Sigma' = \varnothing$*, entonces* Σ *es satisfacible*
2. *Si* $\Sigma' \neq \varnothing$*, sea* Σ'' *el conjunto que resulta de* Σ' *tras suprimir todas las ocurrencias de* λ^c *en las cláusulas de* Σ'*.* Σ'' *es insatisfacible si, y sólo si, lo es* Σ*.*

Corolario 5.5.4 (Regla del Literal Puro)**.** *Sea* Σ *un conjunto de cláusulas. Si* λ *es un literal puro de* Σ *y* Σ' *es el conjunto que resulta de* Σ *sustrayendo de éste todas las cláusulas que son ampliación de* λ*, entonces* Σ' *es insatisfacible si, y sólo si, lo es* Σ*.*

5.6. Ejercicios de Lógica Proposicional

1. Sean α, β, γ y δ fórmulas del lenguaje proposicional estándard. Demuestre que:

$$(((\alpha \to \beta) \to (\neg\gamma \to \neg\delta)) \to \gamma) \to \beta \vDash (\beta \to \alpha) \to (\delta \to \alpha)$$

2. Consideremos las fórmulas del lenguaje proposicional estándar:

   - $\alpha = a \to (b \wedge \neg c)$
   - $\beta = (a \leftrightarrow \neg b) \vee c$

   Encuentre una fórmula γ de dicho lenguaje tal que para cualquier asignación de variables v se cumpla $v(\gamma) = v(\alpha) + v(\alpha)v(\beta)$.

3. En el lenguaje proposicional estándar, sea α la fórmula:

$$(a \to (b \to (c \to d))) \to ((a \to b) \to (a \to (c \to d)))$$

   Demuestre que α es una fórmula tautológica.

4. Clasifique la siguiente fórmula del lenguaje proposicional estándar:

$$((((a \vee b) \wedge \neg c) \to d) \wedge (\neg d \wedge (b \vee a))) \to (c \vee e)$$

5. Estudie si cada una de las siguientes implicaciones semánticas es cierta o no. Cuando no lo sea, encuentre una asignación de variables que lo revele:

   a) $(a \wedge \neg b) \to (a \vee c) \vDash ((\neg a \vee b) \to (a \vee c)) \to (a \vee c)$

   b) $(a \vee d) \to (b \to c) \vDash ((a \vee d) \to \neg b) \to \neg c$

6. Sea Γ es siguiente conjunto de fórmulas del lenguaje proposicional estándard:

   $$\{\neg a \vee a \vee c, b \vee c, \neg a \vee c \vee d \vee e, \neg e, a \vee \neg c \vee \neg d, \neg a \vee \neg d, c \vee \neg d, a \vee d, \neg c \vee d\}$$

   Decida si Γ es o no satisfacible.

7. Decida si:

   $$(\neg a \to b) \wedge (c \to d), a \to c, (\neg b \wedge \neg c) \to d, b \to a, (d \wedge \neg c) \to a, a \to d \vDash a \wedge c \wedge d$$

8. Pruebe que:

   $$\vDash ((((a \to b) \to (\neg c \to \neg d)) \to c) \to e) \to ((e \to \neg b) \to ((e \to a) \to (d \to (a \wedge \neg b))))$$

9. Sean las siguientes fórmulas del lenguaje proposicional estándar:

   a) $\gamma_1 = (a \vee b) \to (c \vee d)$

   b) $\gamma_2 = (\neg a \wedge \neg d) \to (\neg c \wedge (c \vee e))$

   c) $\gamma_3 = a \to (\neg c \wedge \neg b \wedge (\neg d \vee b))$

   d) $\varphi = (d \to (b \vee a)) \to (d \wedge \neg(a \vee \neg b))$

   Estudie si $\gamma_1, \gamma_2, \gamma_3 \vDash \varphi$ y caso de **no** serlo, dé una asignación de variables que lo evidencie.

10. Sean las siguientes fórmulas del lenguaje proposicional estándar:

    a) $\gamma_1 = (r \vee t) \to (p \vee s)$

    b) $\gamma_2 = (\neg r \wedge \neg s) \to (\neg p \wedge (\neg p \to q))$

    c) $\gamma_3 = r \to (\neg(p \vee t) \to (\neg s \vee t))$

    d) $\varphi = \neg(s \to (t \vee r)) \vee (s \wedge \neg(t \to r))$

    Estudie si $\gamma_1, \gamma_2, \gamma_3 \vDash \varphi$ y caso de **no** serlo, dé una asignación de variables que lo evidencie.

11. Sean las siguientes fórmulas del lenguaje proposicional estándar:

    a) $\gamma_1 = (a \wedge b) \to (c \vee d)$

    b) $\gamma_2 = \neg((a \vee c \vee d) \wedge e)$

    c) $\varphi = (a \to b) \to (e \to \neg a)$

    Estudie si $\gamma_1, \gamma_2 \vDash \varphi$ y caso de **no** serlo, dé una asignación de variables que lo evidencie.

12. Sean α una fórmula del lenguaje proposicional estándard. Demuestre que son equivalentes las siguientes afirmaciones:

    a) α es una tautología.

    b) $\vDash \alpha$

13. ¿Es cierto que cualesquiera dos tautologías son lógicamente equivalentes? En caso de respuesta negativa, de un ejemplo que lo justifique.

14. Dado un conjunto de fórmulas Γ del lenguaje, sea $\mathrm{Con}(\Gamma)$ el conjunto de fórmulas γ tales que $\Gamma \vDash \gamma$. Si Γ y Δ son conjuntos de fórmulas, demuestre que:

    a) $\Gamma \subseteq \mathrm{Con}(\Gamma)$

    b) Si $\Gamma \subseteq \Delta$, entonces $\mathrm{Con}(\Gamma) \subseteq \mathrm{Con}(\Delta)$

    c) $\mathrm{Con}(\mathrm{Con}(\Gamma)) \subseteq \mathrm{Con}(\Gamma)$

    d) $\mathrm{Con}(\mathrm{Con}(\Gamma)) = \mathrm{Con}(\Gamma)$

15. Sea $\Gamma \cup \{\varphi\}$ un conjunto de fórmulas. Demuestre que son equivalentes las siguientes afirmaciones:

    a) $\Gamma \vDash \varphi$

    b) $\Gamma \cup \{\neg\varphi\}$ es insatisfacible

16. Sea $\Gamma \cup \{\psi, \varphi\}$ un conjunto de fórmulas. Demuestre que son equivalentes las siguientes afirmaciones:

    a) $\Gamma, \psi \wedge \varphi \vDash \xi$

    b) $\Gamma, \psi, \varphi \vDash \xi$

17. Demuestre que para cualesquiera fórmulas $\gamma_1, \ldots, \gamma_n, \varphi$ $(2 \leq n)$ son equivalentes las siguientes afirmaciones:

    a) $\gamma_1, \ldots, \gamma_n \vDash \varphi$

    b) $\{\gamma_1, \gamma_2, \ldots, \gamma_n, \neg\varphi\}$ es insatisfacible

    c) $\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n \wedge \neg\varphi$ es insatisfacible

18. Sea $\Gamma \cup \{\alpha, \beta, \gamma, \varphi, \psi, \xi\}$ un conjunto de fórmulas del lenguaje de proposicional estándar. Demuestre las siguientes reglas:

    a) Si $\Gamma \vDash \alpha$ y $\Gamma \vDash \alpha \to \beta$ entonces $\Gamma \vDash \beta$ (*regla de modus ponens*)

    b) Si $\Gamma \vDash \alpha \to \varphi$ y $\Gamma \vDash \neg\alpha \to \psi$ entonces $\Gamma \vDash \neg\psi \to \varphi$ (*regla de modus ponens generalizada*)

    c) Si $\Gamma \vDash \alpha \to \varphi$ y $\Gamma \vDash \neg\alpha \to \psi$ entonces $\Gamma \vDash \neg\varphi \to \psi$

    d) Si $\Gamma, \alpha \vDash \beta$ y $\Gamma, \beta \vDash \gamma$ entonces $\Gamma, \alpha \vDash \gamma$.

    e) Si $\Gamma, \alpha \vDash \beta \to \gamma$ y $\Gamma, \alpha \vDash \beta$ entonces $\Gamma, \alpha \vDash \gamma$.

    f) Si ξ es una tautología, $\Gamma, \xi \vDash \varphi$ sii $\Gamma \vDash \varphi$.

    g) Si $\Gamma, \alpha \vDash \varphi$ y $\Gamma, \neg\alpha \vDash \varphi$, entonces $\Gamma \vDash \varphi$.

    h) Si $\Gamma, \alpha \to \beta \vDash \varphi$ y $\Gamma, \beta \to \alpha \vDash \varphi$, entonces $\Gamma \vDash \varphi$

    i) Si $\Gamma, \alpha \to \beta \vDash \alpha$ entonces $\Gamma \vDash \alpha$

    j) Si $\Gamma, \psi \vDash \varphi$ entonces Si $\Gamma, \neg\varphi \vDash \neg\psi$.

    k) Si $\Gamma \vDash \varphi$ y $\Gamma \vDash \psi$, entonces $\Gamma \vDash \varphi \wedge \psi$.

    l) Si $\Gamma \vDash \varphi \wedge \psi$ entonces $\Gamma \vDash \varphi$.

    m) $\Gamma, \alpha, \beta \vDash \varphi$ sii $\Gamma, \alpha \wedge \beta \vDash \varphi$

    n) Si $\Gamma \vDash \alpha \vee \beta$ y $\Gamma \vDash \neg\alpha \vee \gamma$ entonces $\Gamma \vDash \beta \vee \gamma$ (*regla de resolución en log. proposicional*)

    ñ) Si $\Gamma, \alpha \vDash \varphi$ y $\Gamma, \beta \vDash \varphi$, entonces $\Gamma, \alpha \vee \beta \vDash \varphi$.

    o) Si $\Gamma \vDash \varphi$ entonces $\Gamma \vDash \varphi \vee \psi$

19. Llega un grupo de meteorólogos a la isla de los veraces y mendaces, insteresados en saber si durante la jornada anterior estuvo lloviendo en la misma. Encuentran a tres indígenas que dicen llamarse: Ana, Bruno y Carmen. Al ser preguntados por lo que interesa a los meteorólogos, las respuestas que dieron son las siguientes:

- Ana: “ayer no llovió aquí”
- Bruno: “ayer sí llovió aquí”
- Carmen: “si ayer llovió aquí, yo soy mendaz”

Averigüe el carácter de cada uno de los indígenas y si llovió o no la jornada anterior en la isla.

20. Dada una fórmula proposicional, ¿existe una única fórmula en forma normal conjuntiva lógicamente equivalente a ella? ¿Qué se puede decir de dos fórmulas para las que se encuentra una fórmula en forma normal conjuntiva lógicamente equivalente a ambas? Encontrar una fórmula en forma normal conjuntiva para las siguientes fórmulas:

   a) $\neg(a \leftrightarrow \neg(b \vee c))$
   b) $(a \to \neg(b \to (c \vee d))) \to \neg(a \to b)$

21. Dada una fórmula proposicional, ¿existe una única fórmula en forma normal conjuntiva lógicamente equivalente a ella? ¿Qué se puede decir de dos fórmulas para las que se encuentra una fórmula en forma normal conjuntiva lógicamente equivalente a ambas? Encontrar una fórmula en forma normal conjuntiva para las siguientes fórmulas:

   a) $\neg(a \leftrightarrow \neg(b \vee c))$
   b) $(a \to \neg(b \to (c \vee d))) \to \neg(a \to b)$

22. Considerar el conunto de cláusulas

$$\Gamma = \{a \vee \neg b \vee \neg c, \neg a \vee \neg b \vee c, a \vee b \vee \neg c \vee d, \neg d\}$$

    y decidir mediante el método de Davis y Putnam si Γ es satisfacible o no.

23. Considere el conjunto de cláusulas

$$\Gamma = \{b \vee \neg b \vee c, \neg a \vee \neg b \vee c, \neg b \vee a, b, \neg c\}$$

    y decida mediante el método de Davis y Putnam si Γ es satisfacible o no. Concluya razonadamente que

$$\vDash ((b \to a) \to (b \to (b \to c))) \to ((b \to a) \to (b \to c))$$

24. Considerar el conjunto de cláusulas

$$\Gamma = \{a \vee c, \neg b \vee c, d, \neg b \vee \neg c \vee e, b, \neg e\}$$

    y decidir mediante el método de Davis y Putnam si Γ es satisfacible o no. Concluir razonadamente que

$$\vDash ((a \to b) \to c) \to (d \to ((b \to (c \to e)) \to (b \to e)))$$

25. Haciendo uso del algoritmo de Davis y Putnam decida si son satisfacibles o no los siguientes conjuntos de cláusulas:

   a) $\Sigma_1 = \{\neg a \vee a \vee c, b \vee c, \neg a \vee c \vee d \vee e, \neg e, a \vee \neg c \vee \neg d\}$
   b) $\Sigma_2 = \Sigma_1 \cup \{\neg a \vee \neg d, c \vee \neg d\}$
   c) $\Sigma_3 = \Sigma_2 \cup \{a \vee d, \neg c \vee d\}$
   d) Justificar razonadamente que:

$$\vDash \Big(\big(((\varphi \to \psi) \to (\neg\chi \to \neg\theta)) \to \chi\big) \to \tau\Big) \to \big((\tau \to \varphi) \to (\theta \to \varphi)\big)$$

   e) Decidir si el siguiente conjunto de fórmulas es o no satisfacible:

$$\{(b \wedge \neg a \wedge \neg b) \to c, \neg c \to \neg(\neg a \wedge \neg b), c \to a, b \to a, (\neg a \vee \neg b \vee \neg c) \wedge (d \vee e), a \to (b \to c), d \to \neg e\}$$

   y caso de respuesta afirmativa, encuentre al menos una valoración que lo satisfaga.

Capítulo 6

Retículos y Álgebras de Boole

Este capítulo introduce el sistema algebraico llamado *retículo* . Desarrollamos las propiedades de los retículos y presentamos varios ejemplos de retículos (por ejemplo, el *retículo de las particiones*). Cuando son reforzados con postulados adicionales, los retículos se convierten en *álgebras de Boole*, estructuras algebraicas de importancia mayor para los científicos de la computación. Se derivan las propiedades de los subsistemas y los homomorfismos de las álgebras de Boole y se desmuestra que cada álgebra de Boole finita es isomorfa a cierta álgebra de conjuntos (y, por tanto, el cardinal de toda álgebra de Boole finita es una potencia de 2). Se demuestra también que cada álgebra de Boole de cardinalidad 2^r es isomorfa al producto directo de r álgebras de Boole de cardinal 2. El capítulo concluye con una discusión de las *funciones booleanas* y sus formas normales.

El concepto de retículo es importante en muchos aspectos de la teoría de máquinas de estados finitos. Las álgebras de Boole tienen un significado especial por su aplicabilidad directa a la teoría de conmutación y diseño lógico —como demostramos en posteriores secciones.

6.1. Conjuntos Ordenados

Definición 6.1.1. Un *conjunto ordenado* es cualquier estructura algebraica $\langle A, \leq \rangle$ cumpliendo:

1. A es un conjunto no vacío
2. $\leq$ es una relación binaria en A tal que:
   a) para todo $a \in A$, $a \leq a$ (*reflexividad*)
   b) para todo $a, b \in A$, si $a \leq b$ y $b \leq a$, entonces $a = b$ (*antisimetría*)
   c) para todo $a, b, c \in A$, si $a \leq b$ y $b \leq c$, entonces $a \leq c$ (*transitividad*).

Si $\langle A, \leq \rangle$ es un conjunto ordenado, entonces $\leq$ recibe el nombre de *orden* sobre A. $\langle A, \leq \rangle$ es un *conjunto totalmente ordenado* , y en ese caso $\leq$ es un *orden total* si para todo $a, b \in A$, $a \leq b$ o $b \leq a$. A veces escribimos $a < b$ (resp. $a > b$) para indicar que $a \leq b$ (resp. $a \geq b$), pero $a \neq b$.

Ejemplo 6.1.1. El ejemplo más familiar de orden total es el orden "menor o igual" sobre los enteros.

Ejemplo 6.1.2. Supongamos que tenemos dos conjuntos ordenados $\langle A_1, \leq_1 \rangle$ y $\langle A_2, \leq_2 \rangle$. Sea $\langle A_1 \times A_2, \leq \rangle$, donde $\langle a, b \rangle \leq \langle c, d \rangle$ sii, por definición, $a \leq_1 c$ y $b \leq_2 d$. Es fácil demostrar que $\langle A_1 \times A_2, \leq \rangle$ es un conjunto ordenado. $\leq$ es denominado *orden producto* sobre $A_1 \times A_2$. Sin embargo, sobre el producto $A_1 \times A_2$ el orden producto no es el más famoso, pues hay otro denominado *orden lexicográfico*, $\preceq$, que ha sido utilizado tanto o más incluso. El orden lexicográfico sobre $A_1 \times A_2$ se define como sigue:

$$\langle a_1, a_2 \rangle \preceq \langle b_1, b_2 \rangle \text{ sii, por def., } a_1 <_1 b_1 \text{ o } (a_1 = b_1 \text{ y } a_2 \leq_2 b_2)$$

Por supuesto que estas definiciones pueden ser generalizadas en el modo obvio a cualquier producto finito de conjuntos: $A_1 \times A_2 \times \cdots \times A_n$, con $n \geq 2$.

Observación 6.1.1. Para representar gráficamente los conjuntos ordenados finitos $\langle A, \leq \rangle$ se suele recurrir a su *diagrama de orden* o *diagrama de Hasse*. Para ello se disponen los elementos de A como etiquetas de puntos, de forma que:

- cada vértice etiquetado con a aparece debajo de cualquier otro vértice etiquetado con b tal que $a \leq b$ y $a \neq b$.
- aparece un eje del vértice etiquetado con a al vértice etiquetado con b, para todo b tal que: $a \neq b$, $a \leq b$, y no existe c distinto de ambos cumpliendo $a \leq c$ y $c \leq a$.
- no hay otros vértices ni otros ejes aparte de los mencionados.

Así pues, $a \leq b$ sii $a = b$ o se puede alcanzar el vértice a desde el b vía un camino descendente.

Ejemplo 6.1.3.

1. El conjunto $\mathcal{P}(U)$ de partes de conjunto U, también llamado conjunto potencia $\mathbf{2}^U$ sobre el conjunto universo U, dotado de la inclusión $\subseteq$ es un conjunto ordenado, el conjunto ordenado $\langle \mathcal{P}(U), \subseteq \rangle$. El diagrama de orden de $\langle \mathcal{P}(U), \subseteq \rangle$, donde $U = \{a, b, c, d\}$, aparece en la Figura 6.1.
2. El conjunto $\mathbb{N}$ de los números naturales junto a la relación $|$, donde $i|j$ sii i es un divisor de j, es un conjunto ordenado. La Figura 6.2 muestra esta misma relación sobre el conjunto $J = \{2, 3, 4, 6, 8, 12, 36, 60\}$ y así $\langle J, | \rangle$ es también un conjunto ordenado.

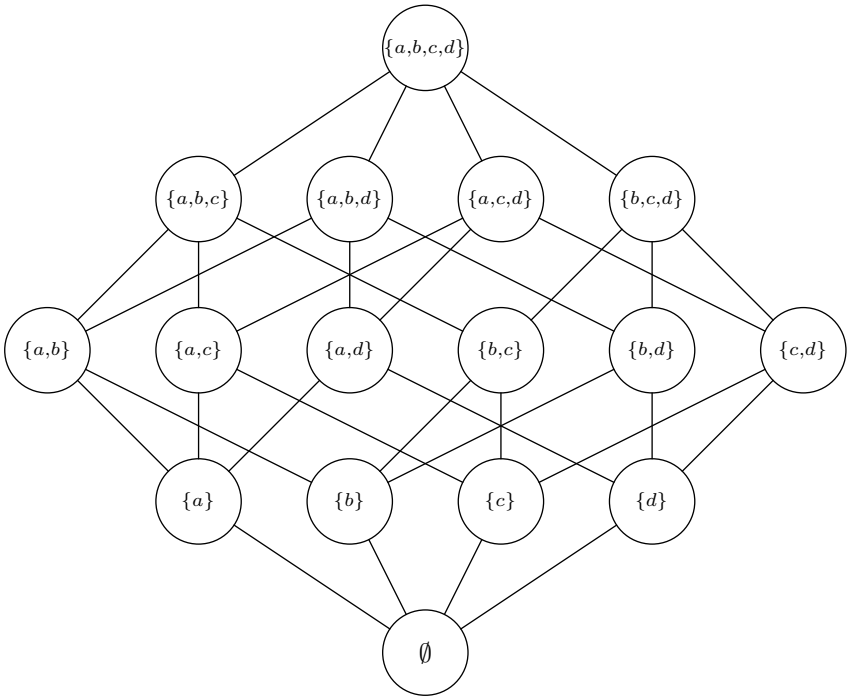


Figura 6.1: Diagrama de orden para el conjunto ordenado $\mathcal{P}(U)$.

Definición 6.1.2. Sea $\langle A, \leq \rangle$ un conjunto ordenado, S un subconjunto no vacío de A y $a \in A$. a es una *cota inferior* (resp. *cota superior*) de S si para todo $x \in S$, $a \leq x$ (resp. $x \leq a$). *mayorante* (resp. *minorante*) es sinónimo de cota superior (resp. cota inferior). a es *mínimo* (resp. *máximo*) de S si:

1. $a \in S$ y
2. a es cota inferior (resp. superior) de S

en tal caso abreviamos escribiendo $a = \min S$ (resp. $a = \max S$). a es *ínfimo* (resp. *supremo*) de S si:

1. a es cota inferior (resp. superior) de S y
2. para toda cota inferior (resp. superior) de S, a', se cumple $a' \leq a$ (resp. $a \leq a'$).

en tal caso abreviamos escribiendo $a = \inf S$ (resp. $a = \sup S$). $a \in S$ es *maximal* (resp. *minimal*) en S si para todo $x \in S$, $x \geq a$ (resp. $x \leq a$) implica $x = a$.

Ejemplo 6.1.4. En este ejemplo, sea $J = \{2, 3, 4, 6, 8, 12, 36, 60\}$ y $U = \{a, b, c, d\}$.

1. En el caso $\langle J, | \rangle$, las cotas superiores de $\{2, 3\}$ son exactamente los elementos del conjunto $\{6, 12, 36, 60\}$ y 4 no es cota superior (¿por qué?). La cotas inferiores de $\{8, 12\}$ son exactamente los elementos del conjunto $\{4, 2\}$ y las de $\{8, 4\}$ son exactamente los elementos del conjunto $\{4, 2\}$.
2. En el caso $\langle J, | \rangle$, $S = \{12, 36, 60\}$ tiene mínimo, el elemento 12, pero no tiene máximo. $S = \{2, 3, 6\}$ tiene máximo, el elemento 6, pero no tiene mínimo. $S = \{2, 3\}$ no tiene ni máximo ni mínimo, de hecho S no tiene cotas inferiores.
3. En el caso $\langle J, | \rangle$, $\inf \{4, 6\} = 2$ $\sup \{4, 6\} = 12$. Obsérvese que el conjunto de cotas superiores de $\{4, 6\}$ es $M = \{12, 36, 60\}$ y que $\min M = 12$. Por otra parte el conjunto de contas inferiores de $\{4, 6\}$ es $m = \{2\}$ y que el máximo de m es 2.
4. En el caso $\langle \mathcal{P}(U), \subseteq \rangle$ es fácil comprobar que el ínfimo de $\inf \{\{a, c\}, \{b, c, d\}\} = \{c\}$ y que $\sup \{\{a, c\}, \{b, c, d\}\} = \{a, b, c, d\}$. Si se observa con atención se verá que cada par de elementos de este poset tiene un supremo y un ínfimo. $\varnothing$ (resp. $\{a, b, c, d\}$) es un mínimo (resp. máximo) de $\mathcal{P}(U)$ ordenado por $\subseteq$.
5. En el caso $\langle J, | \rangle$ y tomando $S = \{2, 3, 6\}$, 2 y 3 son minimales y 6 es maximal. Si $S = \{2, 3\}$, entonces 2 y 3 son maximales y minimales a la vez.

Lema 6.1.1. *Sea $\langle A, \leq \rangle$ un conjunto ordenado y S un subconjunto no vacío de A. Si existe $\inf S$ (resp. $\sup S$), éste es el máximo (resp. mínimo) de las cotas inferiores (resp. superiores).*

Demostración. Es evidente a partir de las definiciones de ínfimo y supremo dadas en la Definición 6.1.2. □

Teorema 6.1.2. *Sea $\langle A, \leq \rangle$ un conjunto ordenado y S un subconjunto no vacío de A. Si S tiene mínimo (resp. máximo) éste es único.*

Demostración. Supongamos que $a, b \in A$ son ambos elementos mínimo (resp. máximo) de S. Entonces: $a, b \in S$, $a \leq b$ y $b \leq a$; por antisimetría se tendrá entonces $a = b$. □

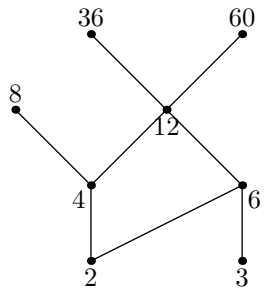


Figura 6.2: Diagrama de orden para el conjunto $\{2, 3, 4, 6, 8, 12, 36, 60\}$ ordenado por $|$.

Corolario 6.1.3. *Sea $\langle A, \leq \rangle$ un conjunto ordenado y S un subconjunto no vacío de A. Si existe* $\inf S$ *(resp.* $\sup S$*), entonces éste es único.*

Demostración. Es consecuencia inmediata del Lema 6.1.1 y el Teorema 6.1.2 y de las definiciones. □

Definición 6.1.3. Sea $\langle A, \leq \rangle$ un conjunto ordenado. $\langle A, \leq \rangle$ es un *conjunto bien ordenado*, y en tal caso $\leq$ es un *buen orden*, si para todo subconjunto no vacío S de A existe $a_s \in A$ tal que a_s es mínimo de S.

Observación 6.1.2. Es obvio que todo conjunto bien ordenado es totalmente ordenado.

Ejemplo 6.1.5. El ejemplo más familiar de buen orden es el orden "menor o igual" sobre los naturales.

6.2. Retículos

Definición 6.2.1. Un *retículo* es un álgebra $\mathbf{A} = \langle A, \vee, \wedge \rangle$ de tipo $\langle 2, 2 \rangle$ cumpliendo para todo $a, b, c \in A$:

R.1) $a \vee b = b \vee a$

R.2) $a \wedge b = b \wedge a$

R.3) $a \vee (b \vee c) = (a \vee b) \vee c$

R.4) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

R.5) $a \vee a = a$

R.6) $a \wedge a = a$

R.7) $a \vee (a \wedge b) = a$

R.8) $a \wedge (a \vee b) = a$

A las igualdades R.1 y R.2 (resp. R.3 y R.4, R.5 y R.6, R.7 y R.8) se les llama *leyes de commutatividad* (resp. *de asociatividad*, *de idempotencia*, *de absorción*).

Ejemplo 6.2.1. Si X es un conjunto entonces $\langle \mathcal{P}(X), \cup, \cap \rangle$ es un retículo.

Teorema 6.2.1 (de dualidad para retículos). *Sea $\mathbf{A} = \langle A, \vee, \wedge \rangle$ un álgebra de tipo $\langle 2, 2 \rangle$. Si $\mathbf{A}$ es un retículo entonces $\langle A, \wedge, \vee, \rangle$ es un retículo.*

Demostración. Es una consecuencia inmediata del hecho de que en la Definición 6.2.1 para propiedades definitorias están dadas por pares, obteniéndose una propiedad de la otra intercambiando entre sí los papeles de $\wedge$ y $\vee$. □

Lema 6.2.2. *Sea $\langle A, \vee, \wedge \rangle$ un retículo. Para todo $a, b \in A$ son equivalentes las siguientes afirmaciones:*

1. $a \wedge b = a$
2. $a \vee b = b$

Demostración. Supongamos que $a, b \in A$ y que $a \wedge b = a$. Entonces:

$$\begin{aligned} a \vee b &= (a \wedge b) \vee b && \text{por hipótesis} \\ &= b \vee (b \wedge a) && \text{por R.2 y R-1} \\ &= b && \text{R.7} \end{aligned}$$

La implicación recíproca está demostrada con ésta por dualidad. □

Teorema 6.2.3. *Sea* $\mathbf{A} = \langle A, \vee, \wedge \rangle$ *un retículo. Existe una relación de orden* $\leq$ *sobre* A *tal que para todo* $a, b \in A$*:*

1. $a \wedge b = \inf \{a, b\}$
2. $a \vee b = \sup \{a, b\}$

Demostración. Definamos sobre A la relación binaria:

$$a \leq b \text{ si, y sólo si, } a \wedge b = a \tag{6.1}$$

Demostremos en primer lugar que $\leq$, así definida, es una relación de orden. Es *reflexiva* porque según R.6 vale para todo $a \in A$ la igualdad $a \wedge a = a$. Es *antisimétrica*, porque si $a, b \in A$ y se cumple $a \leq b$ y $b \leq a$, entonces:

$$\begin{aligned} a &= a \wedge b && \text{por hipótesis} \\ &= b \wedge a && \text{por R.2} \\ &= b && \text{por hipótesis.} \end{aligned}$$

Es *transitiva* porque para todo $a, b, c \in A$, si $a \leq b$ y $b \leq c$ entonces:

$$\begin{aligned} a \wedge c &= (a \wedge b) \wedge c && \text{por hipótesis} \\ &= a \wedge (b \wedge c) && \text{por R.4} \\ &= a \wedge b && \text{por hipótesis} \\ &= a && \text{por hipótesis} \end{aligned}$$

Sean $a, b \in A$,

$$\begin{aligned} (a \wedge b) \wedge a &= a \wedge (b \wedge a) && \text{por R.4} \\ &= a \wedge (a \wedge b) && \text{por R.2} \\ &= (a \wedge a) \wedge b && \text{por R.4} \\ &= a \wedge b && \text{por R.6} \end{aligned}$$

de donde $a \wedge b \leq a$. De forma similar se demuestra que $a \wedge b \leq b$. Supongamos que $c \in A$ y cumple $c \leq a$ y $c \leq b$. Entonces

$$\begin{aligned} c \wedge (a \wedge b) &= (c \wedge a) \wedge b && \text{por R.4} \\ &= c \wedge b && \text{por hipótesis} \\ &= c && \text{por hipótesis} \end{aligned}$$

por lo que $c \leq a \wedge b$. En definitiva se ha demostrado que para todo $a, b \in A$,

$$a \wedge b = \inf \{a, b\} \tag{6.2}$$

según $\leq$. Por otra parte, según R.8, $a \wedge (a \vee b) = a$ y

$$\begin{aligned} b \wedge (a \vee b) &= b \wedge (b \vee a) && \text{por R.1} \\ &= b && \text{por R.8} \end{aligned}$$

luego $a \leq a \vee b$ y $b \leq a \vee b$. Además, si $c \in A$ cumple $a \leq c$ y $b \leq c$ entonces

$$\begin{aligned}(a \vee b) \vee c &= a \vee (b \vee c) && \text{por R.3}\\ &= a \vee c && \text{por el Lema 6.2.2}\\ &= c && \text{por el Lema 6.2.2}\end{aligned}$$

y por el Lema 6.2.2, $a \vee b \leq c$. En definitiva, tenemos que $a \vee b = \sup\{a, b\}$. □

Ejercicio 6.2.1. Sea $\langle A, \leq\rangle$ un conjunto ordenado tal que para todo $a, b \in A$ existe $\inf\{a, b\}$ y $\sup\{a, b\}$. En tal caso definimos dos operaciones binarias en A, representadas respectivamente por $\vee$ y $\wedge$, de la siguiente manera:

1. $a \wedge b = \inf\{a, b\}$
2. $a \vee b = \sup\{a, b\}$

Demostrar que:

1. Para todo $a, b \in a$, $a_1 \vee a_2 = a_1$ sii $a_2 \leq a_1$ sii $a_1 \wedge a_2 = a_2$.
2. $\langle A, \vee, \wedge\rangle$ es un retículo.
3. para todo $a, b \in A$, $a \wedge b = a$ sii $a \leq b$.

Hecho este ejercicio conocemos una definición alternativa, y equivalente, a la de retículo dada por nosotros.

Ejemplo 6.2.2. $\langle J, |\rangle$, donde $J = \{2, 3, 4, 6, 8, 12, 36, 60\}$, es un conjunto ordenado (Ejemplo 6.1.3(2) y Figura 6.2); pero no es retículo (¿por qué?).

6.3. Retículos Distributivos

Definición 6.3.1. Sea $\mathbf{A} = \langle A, \vee, \wedge\rangle$ un retículo. $\mathbf{A}$ es *distributivo* si cumple para todo $a, b, c \in A$:

1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Ejemplo 6.3.1.

1. Si X es un conjunto entonces $\langle \mathcal{P}(X), \cup, \cap\rangle$ es un retículo distributivo.
2. El Diamante (Figura 6.3(a)) y el Pentágono (Figura 6.3(b)) son retículos, pero ninguno de los dos son distributivos.

Definición 6.3.2. Sea $\mathbf{A} = \langle A, \vee, \wedge\rangle$ un retículo, $S \subseteq A$ y $S \neq \varnothing$. $\mathbf{S} = \langle S, \vee, \wedge\rangle$ es un subretículo de $\mathbf{A}$ si para todo $a, b \in S$, $a \vee b, a \wedge b \in S$.

Teorema 6.3.1. *Sea $\mathbf{A} = \langle A, \vee, \wedge\rangle$ un retículo. Son equivalentes las siguientes afirmaciones:*

1. *$\mathbf{A}$ es distributivo.*
2. *Ni el Diamante ni el Pentágono son subretículos de $\mathbf{A}$.*

Demostración. Supongamos que $\mathbf{A}$ es distributivo. Para el Diamante (Figura 6.3(a)):

$$\begin{aligned} a_1 \wedge (a_2 \vee a_3) &= a_1 \wedge a_4 \\ &= a_1 \\ &\neq a_0 \\ &= (a_1 \wedge a_2) \vee (a_1 \wedge a_3) \end{aligned}$$

en cuanto al Pentágono (Figura 6.3(b)):

$$\begin{aligned} b_2 \wedge (b_1 \vee b_3) &= b_2 \wedge b_4 \\ &= b_2 \\ &\neq b_1 \\ &= (b_2 \wedge b_1) \vee (b_2 \wedge b_3) \end{aligned}$$

Luego si contuviera como subretículo al Diamante o al Pentágono, no podría ser distributivo. Recíprocamente, supongamos primeramente que existiera $\{a, b, c\} \subseteq A$ tal que $a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c)$ y $c < a$. Hagamos

$$\begin{aligned} b_0 &= a \wedge b \\ b_1 &= c \vee (a \wedge b) \\ b_2 &= a \wedge (b \vee c) \\ b_3 &= b \\ b_4 &= b \vee c \end{aligned}$$

Entonces $S = \{b_0, b_1, b_2, b_3, b_4\}$ es un conjunto con 5 elementos cerrado para $\vee$ y $\wedge$; por lo que forma un subretículo de $\mathbf{A}$ isomorfo al representado en la Figura 6.3(b). Por tanto, podemos suponer que:

$$\text{Para todo } x, y, z \in A, \text{ si } z < x \text{ entonces } x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \tag{6.3}$$

Pero como $\mathbf{A}$ no es distributivo, debe existir $p, q, r \in A$ tal que $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$. Sea:

$$\begin{aligned} a_1 &= (q \wedge r) \vee (p \wedge (q \vee r)) \\ a_2 &= (r \wedge p) \vee (q \wedge (r \vee p)) \\ a_3 &= (p \wedge q) \vee (r \wedge (p \vee q)) \\ a_0 &= (p \wedge q) \vee (q \wedge r) \vee (r \wedge p) \\ a_4 &= (p \vee q) \wedge (q \vee r) \wedge (r \vee p) \end{aligned}$$

Se puede comprobar, usando 6.3, que a_0, a_1, a_2, a_3 y a_4 son distintos dos a dos y por consiguiente determinan un subretículo de $\mathbf{A}$ isomorfo al de la Figura 6.3(a). □

Lema 6.3.2. *Sea* $\mathbf{A} = \langle A, \vee, \wedge \rangle$ *un retículo. Son equivalentes las siguientes afirmaciones:*

1. *para todo* $x, y, z \in A$, $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee (x \wedge z))$
2. *para todo* $x, y, z \in A$, *si* $z \leq x$ *entonces* $(x \wedge y) \vee z = x \wedge (y \vee z)$

Demostración. Si $z \leq x$ entonces $z = x \wedge z$; así pues la implicación se deduce de la identidad. Recíprocamente, supongamos que la segunda afirmación vale. Como $x \wedge z \leq x$ tenemos $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee (x \wedge z))$. □

Definición 6.3.3. Un retículo $\mathbf{A} = \langle A, \vee, \wedge \rangle$ es *modular* si para todo $x, y, z \in A$ se cumple:

$$(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee (x \wedge z)) \tag{6.4}$$

Teorema 6.3.3. *Sea* $\mathbf{A} = \langle A, \vee, \wedge \rangle$ *un retículo. Entonces:*

1. $\mathbf{A}$ *es modular sii el Pentágono no es un subretículo suyo.*
2. *Si* $\mathbf{A}$ *es modular, entonces son equivalentes las siguientes afirmaciones:*
   a) $\mathbf{A}$ *es distributivo*
   b) *el Diamante no es un subretículo de* $\mathbf{A}$

Lema 6.3.4. *Sea* $\mathbf{A} = \langle A, \vee, \wedge \rangle$ *un retículo distributivo y* $a_1, \ldots, a_r, b_1, \ldots, b_s \in A$. *Entonces:*

$$(\bigwedge_{i=1}^{r} a_i) \vee (\bigwedge_{j=1}^{s} b_j) = \bigwedge_{i=1}^{r} (\bigwedge_{j=1}^{s} (a_i \vee b_j)) \tag{6.5}$$

$$(\bigvee_{i=1}^{r} a_i) \wedge (\bigvee_{j=1}^{s} b_j) = \bigvee_{i=1}^{r} (\bigvee_{j=1}^{s} (a_i \wedge b_j)) \tag{6.6}$$

Teorema 6.3.5. *Sea* $\mathbf{A} = \langle A, \vee, \wedge \rangle$ *un retículo distributivo y* $a_1, a_2, a_3 \in A$. *Son equivalentes las siguientes afirmaciones:*

1. $a_1 \vee a_2 = a_1 \vee a_3 \quad y \quad a_1 \wedge a_2 = a_1 \wedge a_3$
2. $a_2 = a_3$

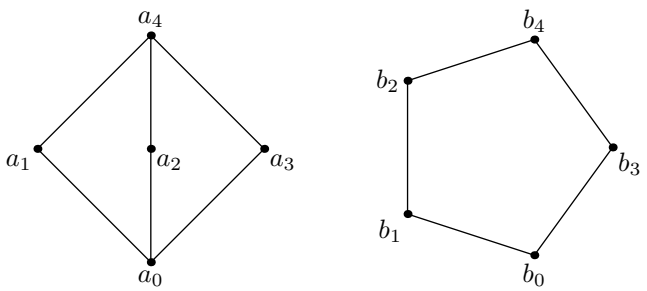
Demostración. Supongamos que $a_1 \vee a_2 = a_1 \vee a_3$ y $a_1 \wedge a_2 = a_1 \wedge a_3$. Entonces:

$$\begin{aligned} a_2 &= a_2 \vee (a_2 \wedge a_1) \\ &= a_2 \vee (a_3 \wedge a_1) \\ &= (a_2 \vee a_3) \wedge (a_2 \vee a_1) \\ &= (a_3 \vee a_2) \wedge (a_3 \vee a_1) \\ &= a_3 \vee (a_2 \wedge a_1) \\ &= a_3 \vee (a_3 \wedge a_1) \\ &= a_3 \end{aligned}$$

□

6.4. Retículos Complementados

Definición 6.4.1. Sea $\mathbf{A} = \langle A, \vee, \wedge, 1, 0 \rangle$ un álgebra de tipo $\langle 2, 2, 0, 0 \rangle$. $\mathbf{A}$ es un *retículo complementado* si:



(a) Diamante (b) Pentágono

Figura 6.3: Diagrama de Hasse del Diamante y el Pentágono.

1. $\langle A, \vee, \wedge \rangle$ es un retículo
2. 1 es máximo de $\mathbf{A}$ y 0 mínimo, según el orden derivado de las operaciones del retículo.
3. para todo $a \in A$ existe $\bar{a} \in A$ tal que

$$a \vee \bar{a} = 1 \qquad a \wedge \bar{a} = 0 \tag{6.7}$$

Lema 6.4.1. *Si $\langle A, \vee, \wedge, 1, 0 \rangle$ es un retículo complementado, también lo es $\langle A, \wedge, \vee, 0, 1 \rangle$.*

Teorema 6.4.2. *Sea $\mathbf{A} = \langle A, \vee, \wedge, 1, 0 \rangle$ un retículo complementado y distributivo. Para todo $a \in A$ no hay más que un elemento con las propiedades de $\bar{a}$ dadas en la ecuación 6.7.*

Teorema 6.4.3. *Sea $\mathbf{A} = \langle A, \vee, \wedge, 1, 0 \rangle$ un retículo complementado y distributivo. Para todo $a \in A$,*

$$\bar{\bar{a}} = a$$

Teorema 6.4.4. *Sea $\mathbf{A} = \langle A, \vee, \wedge, 1, 0 \rangle$ un retículo complementado y distributivo. Para todo $a, c \in A$,*

$$\overline{a \vee c} = \bar{a} \wedge \bar{c} \text{ y } \overline{a \wedge c} = \bar{a} \vee \bar{c}$$

Teorema 6.4.5. *Sea $\mathbf{A} = \langle A, \vee, \wedge, 1, 0 \rangle$ un retículo complementado. Para todo $a, c \in A$ son equivalentes las siguientes afirmaciones:*

1. $a \leq c$
2. $a \wedge \bar{c} = 0$
3. $\bar{a} \vee c = 1$

6.5. Álgebra de Boole

La siguiente definición es debida a Huntington en 1904 y tiene la propiedad de que ningún postulado incluido en ella es consecuencia de otros.

Definición 6.5.1. Un *álgebra de Boole* es un álgebra $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1 \rangle$ de tipo $\langle 2, 2, 1, 0, 0 \rangle$ cumpliendo para todo $a, b, c \in B$:

B.1) $a + b = b + a$

B.2) $a \cdot b = b \cdot a$

B.3) $a + (b \cdot c) = (a + b) \cdot (a + c)$

B.4) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

B.5) $a \cdot \bar{a} = 0$

B.6) $a + \bar{a} = 1$

B.7) $a + 0 = a$

B.8) $a \cdot 1 = a$

El álgebra de Boole $\mathbf{B}$ se denomina trivial cuando $0 = 1$.

Observación 6.5.1. En este tratado:

1. Consideraremos excluida de nuestras consideraciones el álgebra de Boole trivial.
2. Representaremos la operación $\cdot$ por la simple yuxtaposición de los elementos operados con ella.

Para establecer la consistencia de los postulados de la definición 6.5.1 debidos a *Huntington*, es necesario ofrecer al menos un ejemplo de estructura en la que se cumplan. Nosotros ofrecemos varios de interés de sugerente valor.

Ejemplo 6.5.1. Son álgebras de Boole (como ejercicio, comprobarlo) las siguientes estructuras:

1. El álgebra $\mathbf{B_2} = \langle B_2, +, \cdot, {}^{-}, 0, 1\rangle$ donde:
   - $B_2 = \{0, 1\}$
   - las operaciones: $+$, $\cdot$ y $^{-}$ son las dadas por las tablas:

x	$\bar{x}$
0	1
1	0

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

2. Sea U un conjunto —no vacío, si se desea un ejemplo de álgebra de Boole no trivial– y sea $\mathbf{2}^U$ el álgebra $\langle \mathcal{P}(U), \cup, \cap, ', \varnothing, U\rangle$. En la figura 6.6 se muestra el ejemplo de $\mathbf{2}^{\{0,1,2\}}$, que tiene un universo de 8 elementos. Así:
   - $\mathbf{2}^{\varnothing}$, tiene un universo de 1 elemento (¿por qué?).
   - $\mathbf{2}^{\{0,1\}}$, tiene un universo de $\mathrm{card}(\mathcal{P}(\{0,1\})) = 4$ elementos.
   - $\mathbf{2}^{\{0,1,2,3\}}$, tiene un universo de $\mathrm{card}(\mathcal{P}(\{0,1,2,3\})) = 16$ elementos.

   y constatamos de esta forma la facilidad para generar álgebras de Boole finitas con cardinal igual a una potencia de 2.
3. Sea $\mathbf{B}$ un álgebra de Boole y n un número natural. Se denomina *función booleana* o *función de conmutación* de n variables sobre $\mathbf{B}$ a cualquier función $f\colon B^n \longrightarrow B$. Hay dos ejemplos de funciones de conmutación para cualquier número de variables: la constantemente igual a 0 (representada como 0) y la constantemente igual a 1 (representada por 1). Sean f, g funciones de conmutación de n variables sobre el álgebra de Boole $\mathbf{B}$; definimos las siguientes operaciones:
   - $(f+g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)$, para todo $\langle x_1, \ldots, x_n\rangle \in B^n$.
   - $(f\cdot g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)\cdot g(x_1, \ldots, x_n)$, para todo $\langle x_1, \ldots, x_n\rangle \in B^n$.
   - $\bar{f}(x_1, \ldots, x_n) = \overline{f(x_1, \ldots, x_n)}$, para todo $\langle x_1, \ldots, x_n\rangle \in B^n$.

   Si $F(\mathbf{B}, n)$ es el conjunto de aplicaciones $f\colon B^n \longrightarrow B$, el álgebra $\langle F(\mathbf{B}, n), +, \cdot, {}^{-}, 0, 1\rangle$ es un álgebra de Boole que representamos por el símbolo $\mathbf{F(B, n)}$. Por ejemplo, si $n = 2$ y $\mathbf{B} = \mathbf{B_2}$ en la Figura 6.4 recogemos las $16 (= 2^4 = \mathrm{card}(B_2^{B_2\times B_2}))$ funciones de conmutación de 2 variables. y la representación

			$\cdot$		x_1		x_2	$\oplus$	$+$	$\downarrow$	$\equiv$	$\bar{x}_2$		$\bar{x}_1$	$\supset$	$\uparrow$	
x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Figura 6.4: Funciones de conmutación de 2 variables.

de $\mathbf{F(B_2, 2)}$ es dada en la figura 6.5.

4. Sea $D(30) = \{n \in \mathbb{N} : n|30\}$, es decir, $B = \{1, 2, 3, 5, 6, 10, 15, 30\}$ y para cualesquiera $m, n \in B$ sea $m + n = [m, n]$, $m \cdot n = (m, n)$ y $\bar{n} = 30/n$. Si representamos por 0 (resp. 1) al elemento $1 \in B$ (resp. $30 \in B$), el álgebra $\mathbf{D(30)} = \langle B, +, \cdot, ^-, 0, 1\rangle$. $\mathbf{D(m)}$ es álgebra de Boole sii $m = 1$ (álgebra trivial) o si m se expresa de la forma $\prod_{i=0}^{k} p_i$ donde: $0 \leq k$, p_i es primo para todo $0 \leq i \leq k$ y $p_i \neq p_j$, siempre que $0 \leq i < j \leq k$; éste es el caso de $30 = 2 \cdot 3 \cdot 5$, mostrado en la figura 6.6.

Además de la consistencia, es necesario considerar la cuestión de la independencia de los postulados. Por independencia se entiende que ninguno de los postulados se puede demostrar a partir de los otros. Los postulados que se presentan aquí son, de hecho, independientes. Sin embargo, una demostración de ello sería prolija y no es esencial para este estudio. No es necesario que se principie con un conjunto independiente de postulados. De hecho, algunos autores ahorran esfuerzos incluyendo como postulados ciertos teoremas que se desarrollarán más tarde. No obstante, prevalece la opinión de que la demostración de estos teoremas constituye la mejor introducción posible para el manejo del álgebra del Boole.

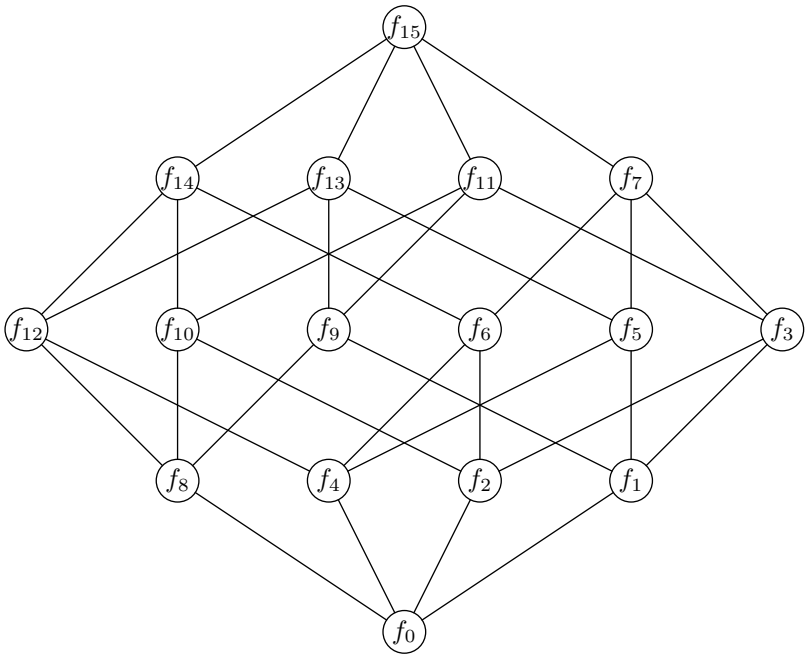


Figura 6.5: Álgebras de Boole $\mathbf{F(B_2, 2)}$.

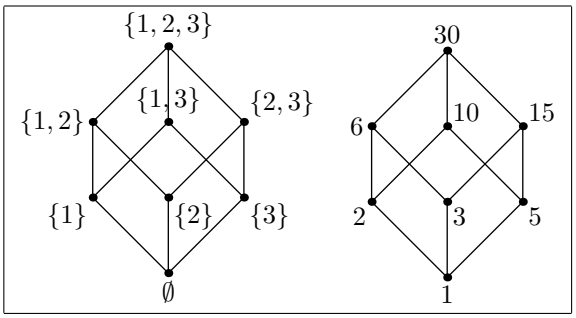


Figura 6.6: Álgebras de Boole de 8 elementos.

6.6. Teoremas Fundamentales del Álgebra de Boole

Observe que los postulados de Huntington se presentan en pares. Si se los examina cuidadosamente, se observa que en cada caso un postulado de un par se puede obtener a partir del otro intercambiando 0 y 1 junto con $+$ y $\cdot$. Cada teorema que se pueda demostrar mediante el álgebra de Boole tiene un dual o equivalente, que es también cierto. En otras palabras, cada paso de la demostración de un teorema se puede reemplazar por su dual, dando con ello una demostración del dual del teorema. En cierto sentido, esto duplica la capacidad para demostrar los teoremas. Cuando hayamos demostrado un teorema diremos que es cierto su dual por *dualidad*. La validez de lo dicho reside en el siguiente teorema

Teorema 6.6.1 (*de dualidad*). *Si* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *es un álgebra de Boole entonces* $\mathbf{B}^d = \langle B, \cdot, +, ^-, 1, 0\rangle$ *es un álgebra de Boole.*

Demostración. Es evidente tras constatar que los axiomas de álgebra de Boole están dados en parejas, intercambiando los papeles de $+$ y $\cdot$ (resp. 1 y 0) entre una pareja y otra. □

Lema 6.6.2. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole. Los elementos* 0 *y* 1 *son únicos.*

Demostración. Si además de 0 existiera otro elemento, digamos 0_1, con sus propiedades axiomáticas, entonces se tendría:

$$\begin{aligned} 0_1 &= 0 + 0_1 && \text{por B.7}\\ &= 0_1 + 0 && \text{por B.1}\\ &= 0 && \text{por B.7} \end{aligned}$$

El resto de la demostración es por dualidad. □

Lema 6.6.3. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole. Para cada elemento* $a \in B$, $a + a = a$ *y* $a \cdot a = a$.

Demostración.

$$\begin{aligned} a + a &= (a + a) \cdot 1 && \text{por B.8}\\ &= (a + a)(a + \bar{a}) && \text{por B.6}\\ &= a + a\bar{a} && \text{por B.3}\\ &= a + 0 && \text{por B.5}\\ &= a && \text{por B.7}\\ aa &= a && \text{por dualidad} \end{aligned}$$

□

Lema 6.6.4. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole. Para cada* $a \in B$, $a + 1 = 1$ *y* $a \cdot 0 = 0$.

Demostración.

$$\begin{aligned} a + 1 &= 1 \cdot (a + 1) && \text{por B.8}\\ &= (a + \bar{a})(a + 1) && \text{por B.5}\\ &= a + \bar{a} \cdot 1 && \text{por B.3}\\ &= a + \bar{a} && \text{por B.8}\\ &= 1 && \text{por B.6}\\ a \cdot 0 &= 0 && \text{por dualidad} \end{aligned}$$

□

Lema 6.6.5. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Si* $2 \leq \mathrm{Card}(B)$ *entonces* $1 \neq 0$ *y* $\bar{1} = 0$.

Demostración. Sea a un elemento cualquiera de B. Se tiene:

$$a \cdot 1 = a$$
$$a \cdot 0 = 0$$

Si suponemos que $1 = 0$ tendremos entonces que para todo $a \in B$, $a = 0$. Sin embargo estamos suponiendo que B tiene al menos 2 elementos. Esta contradicción solamente se puede salvar llegando a la conclusión de que $1 \neq 0$. Para la segunda aseveración tengamos en cuenta:

$$\begin{aligned} \bar{1} &= \bar{1} \cdot 1 && \text{por B.8} \\ &= 0 && \text{por B.5} \end{aligned}$$

□

Lema 6.6.6. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, b \in B$, $a + ab = a$ *y* $a(a + b) = a$.

Demostración.

$$\begin{aligned} a + ab &= a \cdot 1 + ab && \text{por B.8} \\ &= a(1 + b) && \text{por B.4} \\ &= a \cdot 1 && \text{por Lema 6.6.4} \\ &= a && \text{por B.8} \\ a(a + b) &= a && \text{por dualidad} \end{aligned}$$

□

Teorema 6.6.7. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, b \in B$, $ab + \bar{a}b = b = (a + b)(\bar{a} + b)$.

Demostración. Basta considerar:

$$\begin{aligned} ab + \bar{a}b &= ba + b\bar{a} && \text{por B.2} \\ &= b(a + \bar{a}) && \text{por B.4} \\ &= b \cdot 1 && \text{por B.6} \\ &= b && \text{por B.8} \\ (a + b)(\bar{a} + b) &= b && \text{por dualidad} \end{aligned}$$

□

Lema 6.6.8. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Sea* $a \in B$ *y supongamos que existe* $\tilde{a}$ *tal que* $a\tilde{a} = 0$ *y* $a + \tilde{a} = 1$, *entonces* $\tilde{a} = \bar{a}$.

Demostración. En los supuestos del enunciado:

$$\begin{aligned}
\tilde{a} &= 1 \cdot \tilde{a} && \text{por B.8}\\
&= (a + \bar{a})\tilde{a} && \text{por B.5}\\
&= a\tilde{a} + \bar{a}\tilde{a} && \text{por B.4}\\
&= 0 + \bar{a}\tilde{a} && \text{por hipótesis}\\
&= a\bar{a} + \bar{a}\tilde{a} && \text{por B.5}\\
&= (a + \tilde{a})\bar{a} && \text{por B.4}\\
&= 1 \cdot \bar{a} && \text{por hipótesis}\\
&= \bar{a} && \text{por B.8}
\end{aligned}$$

□

Lema 6.6.9. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a \in B$, $\bar{\bar{a}} = a$.

Demostración. Sea $a \in B$ y consideremos $\bar{a}$. Por B.1, B.2, B.5 y B.6 se tiene que $\bar{a}a = 0$ y $\bar{a} + a = 1$. Por el Lema 6.6.8, debe darse $a = \bar{\bar{a}}$. □

Lema 6.6.10. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, b, c \in B$, $a((a + b) + c) = a = ((a + b) + c)a$.

Demostración.

$$\begin{aligned}
a((a + b) + c) &= a(a + b) + ac && \text{por B.4}\\
&= a + ac && \text{por Lema 6.6.6}\\
&= a && \text{por Lema 6.6.6}
\end{aligned}$$

y

$$\begin{aligned}
a &= a((a + b) + c) && \text{por fase anterior}\\
&= ((a + b) + c)a && \text{por B.2}
\end{aligned}$$

□

Observación 6.6.1. El lector reconocerá el Teorema 6.6.11 como las *leyes asociativas* de + y ·. Algunos autores incluyen estas leyes entre los postulados del álgebra de Boole; aunque, como se ve en la demostración del teorema, esto es absolutamente innecesario, una redundancia.

Teorema 6.6.11. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, b, c \in B$, $(a+b)+c = a+(b+c)$ *y* $(ab)c = a(bc)$.

Demostración.

$$\begin{aligned}
(a+b)+c &= (a(a+(b+c))+b)+c && \text{por Lema 6.6.6}\\
&= (a(a+(b+c))+b(a+(b+c)))+c && \text{por Lema 6.6.10}\\
&= (a+b)(a+(b+c))+c && \text{por B.4}\\
&= (a+b)(a+(b+c))+c(a+(b+c)) && \text{por Lema 6.6.10}\\
&= ((a+b)+c)(a+(b+c)) && \text{por B.4}\\
&= ((a+b)+c)a+((a+b)+c)(b+c) && \text{por B.4}\\
&= a+((a+b)+c)(b+c) && \text{por Lema 6.6.10}\\
&= a+(((a+b)+c)b+((a+b)+c)c) && \text{por B.4}\\
&= a+(b+((a+b)+c)c) && \text{por Lema 6.6.10}\\
&= a+(b+c) && \text{por B.2 y Lema 6.6.6}\\
(ab)c &= a(bc) && \text{por dualidad}
\end{aligned}$$

□

Observación 6.6.2. Ahora que se han establecido las leyes de asociatividad, algunas expresiones pueden ser aliviadas de paréntesis como sigue:

$$(a+b)+c = a+b+c \tag{6.8}$$
$$(a\cdot b)\cdot c = abc \tag{6.9}$$

Teorema 6.6.12. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, b \in B$, $a + \bar{a}b = a + b$ *y* $a(\bar{a} + b) = ab$.

Demostración.

$$\begin{aligned}
a+\bar{a}b &= (a+\bar{a})(a+b) && \text{por B.3}\\
&= 1\cdot(a+b) && \text{por B.6}\\
&= a+b && \text{por B.8}\\
a(\bar{a}+b) &= ab && \text{por dualidad}
\end{aligned}$$

□

Observación 6.6.3. El Teorema 6.6.13 expresa las conocidas como *leyes de De Morgan*, que expresan el complemento de una suma (resp. producto) en función de los sumandos (resp. factores), mejor en función del complemento de los sumandos (resp. factores).

Teorema 6.6.13. *Sea* $\mathbf{B} = \langle B, +, \cdot, \bar{}, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, c \in B$, $\overline{a+c} = \bar{a}\bar{c}$ *y* $\overline{ac} = \bar{a}+\bar{c}$

Demostración. Por una parte se tiene:

$$\begin{aligned}
(a+b)+\bar{a}\bar{b} &= ((a+b)+\bar{a})((a+b)+\bar{b}) && \text{por B.3}\\
&= (\bar{a}+(a+b))(\bar{b}+(b+a)) && \text{por B.1}\\
&= 1\cdot 1 && \text{por Teorema 6.6.11 y Lema 6.6.4}\\
&= 1 && \text{por B.8}
\end{aligned}$$

y por otra:

$$\begin{aligned}(a+b)(\bar{a}\bar{b}) &= a(\bar{a}\bar{b}) + b(\bar{a}\bar{b}) && \text{por B.2 y B.4}\\ &= 0+0 && \text{por Teorema 6.6.11, B.5 y Lema 6.6.4}\\ &= 0 && \text{por B.7}\end{aligned}$$

Por el Lema 6.6.8, $(a+b) = \overline{(\bar{a}\bar{b})}$ y por el Lema 6.6.9 se tiene

$$\overline{a+b} = \bar{a}\bar{b}. \tag{6.10}$$

La segunda parte del teorema es cierta por dualidad; pero por motivos pedagógicos daremos una demostración directa por otro camino:

$$\begin{aligned}\overline{\bar{a}+\bar{b}} &= \bar{\bar{a}}\bar{\bar{b}} && \text{por 6.10}\\ &= ab && \text{por Lema 6.6.9}\end{aligned}$$

y por Lema 6.6.9,

$$\overline{ab} = \bar{a} + \bar{b}$$

□

Teorema 6.6.14. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, b, c \in B$, $ab + \bar{a}c + bc = ab + \bar{a}c$ *y* $(a+b)(\bar{a}+c)(b+c) = (a+b)(\bar{a}+c)$.

Demostración.

$$\begin{aligned}ab + \bar{a}c + bc &= ab + \bar{a}c + bc(a+\bar{a}) && \text{por B.6 y B.8}\\ &= ab + abc + \bar{a}c + \bar{a}bc && \text{por B.4}\\ &= ab(1+c) + \bar{a}c(1+b) && \text{por B.4 y B.8}\\ &= ab + \bar{a}c && \text{por Lema 6.6.4 y B.8}\\ (a+b)(\bar{a}+c)(b+c) &= (a+b)(\bar{a}+c) && \text{por dualidad}\end{aligned}$$

□

6.7. Subálgebras e Isomorfismos

Definición 6.7.1. Sean $\mathbf{B}$ y $\mathbf{C}$ álgebras de Boole y $f: B \longrightarrow C$. f es un *homomorfismo* de $\mathbf{B}$ en $\mathbf{C}$ sii, por def., f cumple:

$$\begin{aligned}f(x+y) &= f(x) + f(y)\\ f(\bar{x}) &= \overline{f(x)}\end{aligned}$$

Si además el homomorfismo f cumple ser una inyeccción (res. sobreyección, biyección), entonces se denomina *monomorfismo* (resp. *epimorfismo*, *isomorfismo*.

Teorema 6.7.1. *Sean* $\mathbf{B}$ *y* $\mathbf{C}$ *álgebras de Boole y* $f: B \longrightarrow C$. *Son equivalentes las siguientes afirmaciones:*

1. f *es un homomorfismo.*

2. *f cumple:*

$$f(x \cdot y) = f(x) \cdot f(y)$$
$$f(\bar{x}) = \overline{f(x)}$$

Demostración. Supongamos que f es un homorfismo entre álgebras de Boole y que $x, y \in B$. Entonces:

$$\begin{aligned} f(x \cdot y) &= f(\overline{\bar{x} + \bar{y}}) \\ &= \overline{f(\bar{x} + \bar{y})} \\ &= \overline{f(\bar{x}) + f(\bar{y})} \\ &= \overline{\overline{f(x)} + \overline{f(y)}} \\ &= \overline{\overline{f(x)} + \overline{f(y)}} \\ &= \overline{\overline{f(x)}} \cdot \overline{\overline{f(y)}} \\ &= f(x) \cdot f(y) \end{aligned}$$

Recíprocamente, supongamos cierta la segunda afirmación. Entonces:

$$\begin{aligned} f(x + y) &= f(\overline{\bar{x} \cdot \bar{y}}) \\ &= \overline{f(\bar{x} \cdot \bar{y})} \\ &= \overline{f(\bar{x}) \cdot f(\bar{y})} \\ &= \overline{\overline{f(x)} \cdot \overline{f(y)}} \\ &= \overline{\overline{f(x)}} + \overline{\overline{f(y)}} \\ &= f(x) + f(y) \end{aligned}$$

□

Corolario 6.7.2. *Sean* **B** *y* **C** *álgebras de Boole y $f: B \longrightarrow C$. Si f es un homomorfismo entonces:*

1. $f(0) = 1$.
2. $f(1) = 0$.

Demostración. Para la primera afirmación,

$$\begin{aligned} f(0) &= f(0 \cdot 1) \\ &= f(0 \cdot \bar{0}) \\ &= f(0) \cdot f(\bar{0}) \\ &= f(0) \cdot \overline{f(0)} \\ &= 0 \end{aligned}$$

y para la segunda,

$$\begin{aligned} f(1) &= f(\bar{0}) \\ &= \overline{f(0)} \\ &= \bar{0} \\ &= 1 \end{aligned}$$

□

6.8. Representación Atómica de las Álgebras de Boole Finitas

Definición 6.8.1. Sea $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ un álgebra de Boole y $a \in B$. a es un *átomo* si, y sólo si, por definición:

1. $a \neq 0$
2. para todo $x \in B$, $xa = a$ ó $xa = 0$

El conjunto de los átomos del álgebra de Boole $\mathbf{B}$ será representado por $\mathrm{Atm}(\mathbf{B})$. El elemento c de $\mathbf{B}$ es un *coátomo* sii, por def., es un átomo de $\mathbf{B}^d$.

Ejemplo 6.8.1.

1. En el álgebra de Boole $\mathbf{B_2}$, 1 es un átomo, su único átomo.
2. En el álgebra de Boole $\mathbf{2}^{\{1,2,3\}}$, $\{1\}$, $\{2\}$ y $\{3\}$ son átomos. De hecho éstos son sus únicos elementos cumplido la condición de ser átomo.
3. En el álgebra $\mathbf{F}(\mathbf{B_2}, \mathbf{2})$ los únicos elementos átomo son: f_1, f_2, f_4 y f_8.
4. En el álgebra de Boole de los divisores de 30 los únicos elementos cumpliendo la condición de ser átomo son: 2, 3 y 5.

Observación 6.8.1. El concepto de átomo tal y como ha sido expresado en la Definición 6.8.1 puede ser entendido desde otro punto de vista. Se trata realmente de una definición equivalente en términos de la relación de orden que subyace bajo la definición axiomática de álgebra de Boole. En la Definición 6.8.2 damos a conocer esa relación, en el Lema 6.8.1 expresamos una definición equivalente, en el Lema 6.8.2 demostramos que efectivamente la relación es de orden y, finalmente, en el Lema 6.8.3 damos la caracterización del concepto de átomo por medio del orden.

Definición 6.8.2. Sea $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ un álgebra de Boole. Definimos en B la relación binaria $\leq$ como sigue:

$$a \leq b \text{ sii, por definición, } ab = a$$

Lema 6.8.1. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole. Para todo* $a, b \in B$*, son equivalentes las siguientes afirmaciones:*

1. $a + b = b$
2. $ab = a$

Demostración. Sean $a, b \in B$. Supongamos que $a + b = b$, entonces:

$$\begin{aligned} ab &= a(a+b) && \text{por hipótesis} \\ &= a && \text{por Lema 6.6.6} \end{aligned}$$

Recíprocamente, si suponemos que $ab = a$ entonces:

$$\begin{aligned} a + b &= ab + b && \text{por hipótesis} \\ &= b + ba && \text{por B.1 y B.2} \\ &= b && \text{por Lema 6.6.6} \end{aligned}$$

□

Lema 6.8.2. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole. La relación* $\leq$ *es una relación de orden.*

Demostración. Sean $a, b, c \in B$. En virtud del Lema 6.6.3, $aa = a$, luego según $a \leq a$ (reflexividad). Supongamos que $a \leq b$ y $b \leq a$; por lo primero tenemos $ab = a$ y por lo segundo tenemos $ba = b$; por B.2 concluimos que $a = b$ (simetría). Supongamos, finalmente, que $a \leq b$ y $b \leq c$, es decir, que $ab = a$ y $bc = b$; entonces:

$$\begin{aligned} ac &= (ab)c && \text{por hipótesis} \\ &= a(bc) && \text{por Teorema 6.6.11} \\ &= ab && \text{por hipótesis} \\ &= a && \text{por hipótesis} \end{aligned}$$

es decir, $a \leq c$ (transitividad). □

Lema 6.8.3. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole y* $a \in B$ *tal que* $a \neq 0$. *Son equivalentes las siguientes afirmaciones:*

1. a *es un átomo.*
2. *para todo* $x \in B$, *si* $0 \leq x \leq a$ *entonces* $x = 0$ *ó* $x = a$.

Demostración. Supongamos que a es átomo, que $x \leq a$ y que $x \neq 0$; entonces $xa = x$. Por ser a átomo, ha de cumplirse $xa = 0$ o $xa = a$, pero lo primero es imposible puesto que estamos suponiendo $x \neq 0$ luego ha de darse lo segundo. Por tanto, $x = xa = a$. Recíprocamente, supongamos lo segundo y que $x \in B$; por Lema 6.6.6, $a + ax = a$ y por Lema 6.8.1, $xa \leq a$. Según la hipótesis, esto significa que $xa = 0$ o $xa = a$. Como la hipótesis general es que $a \neq 0$, lo anterior significa que a es átomo. □

Teorema 6.8.4. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole finita. Para todo* $x \in B$ *tal que* $x \neq 0$ *existe* $a \in \mathrm{Atm}(\mathbf{B})$ *tal que* $a \leq x$.

Demostración. Por reducción al absurdo supongamos que el resultado no es cierto; de donde existe $x_0 \in B$ tal que no existe ningún átomo a de $\mathbf{B}$ tal que $a \leq x$. Será posible encontrar $x_1 \in B$ tal que $0 < x_1 < x_0$ y, en general para todo natural i, encontraremos $x_{i+1} \in B$ tal que $0 < x_{i+1} < x_i < \cdots < x_1 < x_0$. La sucesión $\{x_i\}_i$ es una sucesión estrictamente decreciente de elementos no nulos de B, cuya existencia contradice la finitud de B. Esta situación sólo puede ser evitada estableciendo que para todo $x \in B$ tal que $x \neq 0$ debe existir $a \in B$ tal que $a \leq x$ y que impida el proceso anterior, es decir, $a \in \mathrm{Atm}(\mathbf{B})$. □

Teorema 6.8.5. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole finita. Para todo* $a_1, a_2 \in \mathrm{Atm}(\mathbf{B})$, *si* $a_1 a_2 \neq 0$ *entonces* $a_1 = a_2$.

Demostración. Por la definición de átomo (Definicion 6.8.1), $a_2 a_1 = a_1$ o $a_2 a_1 = 0$. Como lo segundo está excluido por hipótesis, tenemos que $a_2 a_1 = a_1$ y, simétricamente, que $a_2 a_1 = a_2$; por tanto, $a_1 = a_2$. □

Lema 6.8.6. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole. Si* $a, b, c \in B$ *son tales que* $ac = a$ *y* $bc = b$, *entonces* $(a + b)c = a + b$.

Demostración.

$$\begin{aligned} (a + b)c &= ac + bc && \text{por B.2 y B.4} \\ &= a + b && \text{por hipótesis} \end{aligned}$$

□

Lema 6.8.7. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole y* $a, b \in B$. *Son equivalentes las siguientes afirmaciones:*

1. $ab = a$
2. $a\bar{b} = 0$
3. $\bar{a} + b = 1$

Demostración. Supongamos que $ab = a$. Entonces tenemos:

$a\bar{b} = (ab)\bar{b}$	por hipótesis
$= a(b\bar{b})$	por Teorema 6.6.11
$= a \cdot 0$	por B5
$= 0$	por Lema 6.6.4

Supongamos que $a\bar{b} = 0$. Entonces tenemos:

$1 = \bar{0}$	por Lema 6.6.5 y Lema 6.6.9
$= \overline{a\bar{b}}$	por hipótesis
$= \bar{a} + \bar{\bar{b}}$	por Teorema 6.6.13
$= \bar{a} + b$	por Lema 6.6.9

Finalmente, supongamos que $\bar{a} + b = 1$. Entonces:

$a = a \cdot 1$	por B8
$= a \cdot (\bar{a} + b)$	por hipótesis
$= a\bar{a} + ab$	por B.4
$= 0 + ab$	por B.5
$= ab$	por B.7

□

Teorema 6.8.8. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole finita y* $x \in B$ *tal que* $x \neq 0$. *Si* $\{a_1, \ldots, a_k\} = \{a : a \in \mathrm{Atm}(\mathbf{B})$ *y* $a \leq x\}$, *entonces* $x = a_1 + \cdots + a_k$.

Demostración. Sea $y = a_1 + \cdots + a_k$. Por Lema 6.8.6, $yx = y$. Así pues, lo que resta es demostrar que $xy = x$, o mejor, según el Lema 6.8.7, que $x\bar{y} = 0$. Por reducción al absurdo, supongamos que $x\bar{y} \neq 0$; por el Teorema 6.8.4, existe un átomo a tal que $a \leq x\bar{y}$. Por el Lema 6.6.6, tenemos $x\bar{y} \leq x$ y $x\bar{y} \leq \bar{y}$, lo que por transitividad implica que $a \leq x$ y $a \leq \bar{y}$. Como $a \leq x$ existirá algún a_i tal que $a = a_i$ y, por tanto, por el Lema 6.6.6, $a \leq a_1 + \cdots + a_k = y$. Así tenemos que $a \leq y$ y $a \leq \bar{y}$; por el Lema 6.8.7

$$ay = a = a\bar{y} = 0$$

o sea, $a = 0$ lo cual es una contradicción. Por tanto, la hipótesis $x\bar{y} \neq 0$ debe ser falsa. □

Teorema 6.8.9. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole finita y* $a, a_1, \ldots, a_k \in \mathrm{Atm}(\mathbf{B})$. *Si* $x = a_1 + \cdots + a_k$ *y* $a \leq x$ *entonces existe* $1 \leq i \leq k$ *tal que* $a = a_i$.

Demostración. Supongamos que $a \leq x$, es decir $ax = a$. Entonces:

$$\begin{aligned} 0 \neq a & && \text{por ser } a \text{ átomo} \\ = a(a_1 + \cdots + a_k) & && \text{por ser } a = ax \\ = aa_1 + \cdots + aa_k & && \text{por B4} \end{aligned}$$

luego, existe $1 \leq i \leq k$ tal que $aa_i \neq 0$. Por el Teorema 6.8.5, $a = a_i$. □

Teorema 6.8.10. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole finita.* $\mathbf{B}$ *es isomorfa a* $\mathbf{2}^{\mathrm{Atm}(\mathbf{B})}$*, es decir, es isomorfa al álgebra*

$$\langle \mathcal{P}(\mathrm{Atm}(\mathbf{B})), \cup, \cap, ', \varnothing, \mathrm{Atm}(\mathbf{B})\rangle$$

Demostración. Consideremos la función:

$$h: B \longrightarrow \mathcal{P}(\mathrm{Atm}(\mathbf{B}))$$

definida por

$$h(x) = \begin{cases} \varnothing & \text{, si } x = 0 \\ \{a : a \in \mathrm{Atm}(\mathbf{B}), a \leq x\} & \text{, si } x \neq 0 \end{cases}$$

En virtud de los teoremas 6.8.8 y 6.8.9 sabemos, y es fácil comprobar, que h es una biyección. Lo que resta es demostrar que "respeta" las operaciones de $\mathbf{B}$. En primer lugar, es claro en virtud de B.8 que

$$h(1) = M \tag{6.11}$$

y, en virtud del Lema 6.6.4 y la Definición 6.8.1, que

$$h(0) = \varnothing \tag{6.12}$$

Consideremos ahora $x_1, x_2 \in B$, no nulos, y sea:

$$\begin{aligned} h(x_1) = M_1 = \{a_{11}, \ldots, a_{1k_1}\} \\ h(x_2) = M_2 = \{a_{21}, \ldots, a_{2k_2}\} \end{aligned}$$

Por tanto:

$$\begin{aligned} x_1 &= a_{11} + \cdots + a_{1k_1} \\ x_2 &= a_{21} + \cdots + a_{2k_2} \\ x_1 + x_2 &= a_{11} + \cdots + a_{1k_1} + a_{21} + \cdots + a_{2k_2} \end{aligned}$$

y así

$$h(x_1 + x_2) = M_1 \cup M_2 \tag{6.13}$$

Seguidamente, usando la propiedad distributiva (B.4), es legítimo escribir:

$$\begin{aligned} x_1 x_2 &= (a_{11} + \cdots + a_{1k_1})(a_{21} + \cdots + a_{2k_2}) \\ &= \sum_{i=1}^{k_1} \sum_{j=1}^{k_2} a_{1i} a_{2j} \end{aligned}$$

Por el Teorema 6.8.5,

$$a_{1i}a_{2j} = \begin{cases} 0 & \text{, si } a_{1i} \neq a_{2j} \\ a_{1i} & \text{, si } a_{1i} = a_{2j}. \end{cases}$$

Consecuentemente

$$h(x_1x_2) = M_1 \cap M_2 \tag{6.14}$$

Seguidamente supongamos que $x_2 = \bar{x}_1$. Entonces:

$$\begin{aligned} M_1 \cup M_2 &= h(x_1 + x_2) && \text{por 6.13} \\ &= h(x_1 + \bar{x}_1) && \text{por la hipótesis} \\ &= h(1) && \text{por B6} \\ &= M && \text{por 6.11} \end{aligned}$$

y

$$\begin{aligned} M_1 \cap M_2 &= h(x_1x_2) && \text{por 6.14} \\ &= h(x_1\bar{x}_1) && \text{por la hipótesis} \\ &= h(0) && \text{por B5} \\ &= \varnothing && \text{por 6.12} \end{aligned}$$

En consencuencia, $M_2 = M \setminus M_1$ y

$$h(\bar{x}_1) = M \setminus M_1 \tag{6.15}$$

Supongamos ahora que $x_1 = 0$ o $x_2 = 0$. Para fijar ideas sea $x_1 = 0$ (el caso $x_2 = 0$ se analiza de forma análoga); entonces:

$$\begin{aligned} h(0 + x_2) &= h(x_2) && \text{por B.7} \\ &= M_2 && \text{por la definición de } h \\ &= \varnothing \cup M_2 && \text{por B.7} \\ &= h(0) + h(x_2) && \text{por 6.12} \end{aligned} \tag{6.16}$$

y

$$\begin{aligned} h(0 \cdot x_2) &= h(0) && \text{por el Lema 6.6.4} \\ &= \varnothing && \text{por 6.12} \\ &= \varnothing \cap M_2 && \text{por el Lema 6.6.4} \\ &= h(0) \cap h(x_2) && \text{por 6.12} \end{aligned} \tag{6.17}$$

En virtud de las ecuaciones: 6.11, 6.12, 6.13, 6.14, 6.15, 6.16 y 6.17, h es un isomorfismo entre $\langle B, +, \cdot, ^-, 0, 1\rangle$ y el álgebra de Boole $\langle \mathcal{P}(\mathrm{Atm}(\mathbf{B})), \cup, \cap, ', \varnothing, \mathrm{Atm}(\mathbf{B})\rangle$. □

Corolario 6.8.11. *Sea* $\mathbf{B} = \langle B, +, \cdot, ^-, 0, 1\rangle$ *un álgebra de Boole finita. Son ciertas las siguientes afirmaciones:*

1. $\mathrm{Car}(B) = 2^{\mathrm{Car}(\mathrm{Atm}(\mathbf{B}))}$.
2. *Si* $\mathbf{A}$ *es un álgebra de Boole y* $\mathrm{Car}(A) = \mathrm{Car}(B)$, *entonces* $\mathbf{A}$ *es isomorfa a* $\mathbf{B}$.

Demostración. Por el Teorema 6.8.10 sabemos que el álgebra de Boole finita $\mathbf{B}$ es isomorfa al álgebra de Boole $\langle \mathcal{P}(\mathrm{Atm}(\mathbf{B})), \cup, \cap, ', \varnothing, \mathrm{Atm}(\mathbf{B})\rangle$. En particular se tiene de ello que B y $\mathcal{P}(\mathrm{Atm}(\mathbf{B}))$ son biyectivos, luego $\mathrm{Car}(B) = 2^{\mathrm{Car}(\mathrm{Atm}(\mathbf{B}))}$ y tenemos la demostración de 1). Si $\mathbf{A}$ es un álgebra de Boole tal que

$\mathrm{Car}(A) = \mathrm{Car}(B)$, entonces $2^{\mathrm{Car}(\mathrm{Atm}(\mathbf{A}))} = 2^{\mathrm{Car}(\mathrm{Atm}(\mathbf{B}))}$ por lo que $\mathrm{Car}(\mathrm{Atm}(\mathbf{A})) = \mathrm{Car}(\mathrm{Atm}(\mathbf{B}))$. Por tanto:

$$\begin{aligned}\mathbf{A} &\cong \langle \mathcal{P}(\mathrm{Atm}(\mathbf{A})), \cup, \cap, ', \varnothing, \mathrm{Atm}(\mathbf{A})\rangle \\ &\cong \langle \mathcal{P}(\mathrm{Atm}(\mathbf{B})), \cup, \cap, ', \varnothing, \mathrm{Atm}(\mathbf{B})\rangle \\ &\cong \mathbf{B}\end{aligned}$$

y ésta es la demostración de la afirmación 2). □

6.9. Expresiones Booleanas

Definición 6.9.1 (*lenguaje booleano*)**.** El *lenguaje booleano* es el lenguaje proposicional $\mathbf{L_B} = \langle X, Cons, a\rangle$ cumpliendo que:

- X es numerable no finito. Sus elementos son representamos con las últimas letras minúsculas del alfabeto latino, subindicándolas si fuese preciso: u, v, x, y, z x_0, x_1, x_2, etc.
- $Cons = \{A, K, N, \bot, \top\}$.
- $a(A) = a(K) = 2$, $a(N) = 1$ y $a(\bot) = a(\top) = 0$.

Para abreviar representamos por S al conjunto $S(\mathbf{L}) = X \cup Cons$ y lo llamamos *conjunto de símbolos* de $\mathbf{L_B}$.

Definición 6.9.2 (*expresión boolena*)**.** Designamos con el nombre de *expresión boolena* exáctamente a cualquier elemento de $\mathrm{P}(\mathbf{L_B})$ (cfr. Definición 4.4.1).

Observación 6.9.1. Seal $\mathbf{L}$ el lenguaje proposicional standar y consideremos la siguiente sucesión de conjuntos definida recursivamente:

$$\begin{aligned}\Phi_0 &= X \cup \{\top, \bot\} \\ \Phi_{i+1} &= \Phi_i \cup \{A\alpha\beta \colon \alpha, \beta \in \Phi_i\} \cup \{K\alpha\beta \colon \alpha, \beta \in \Phi_i\} \cup \{N\alpha \colon \alpha \in \Phi_i\}\end{aligned}$$

Por el Teorema 4.4.1 sabemos que una *expresión booleana* de $\mathrm{P}(\mathbf{L_B})$ es cualquier elemento del conjunto de expresiones:

$$\bigcup_{i=0}^{\infty} \Phi_i$$

Por tanto, son *expresiones booleanas*:

- Cada uno de los símbolos de variable,
- cada uno de los símbolos del conjunto $\{\top, \bot\}$,
- la expresión $N\alpha$, siempre que α sea una expresión booleana y
- las expresiones $A\alpha\beta$ y $K\alpha\beta$, siempre que α y β sean expresiones booleanas.

y no hay otras expresiones booleanas distintas a las antes mencionadas. En el Capítulo 4 hemos justificado que sea cual sea la expresión que consideremos, no existe más que una única forma de representarla; se trata del *principio de lectura única*.

Definición 6.9.3. Para cualesquiera expresiones α y β, usaremos las siguientes representaciones:

- (α') por $N\alpha$.

- $(\alpha + \beta)$ por $A\alpha\beta$.
- $(\alpha \cdot \beta)$ por $K\alpha\beta$.
- 0 por $\bot$, ocasionalmente.
- 1 por $\top$, ocasionalmente.

A veces escribimos la expresión booleana α como $\alpha(u_1, \ldots, u_k)$ para indicar que los símbolos de variable que aparecen en α están entre los símbolos $u_1, \ldots, u_k$ y no es necesario que todas ellos ocurran en α. Llamamos *literal* a los elementos del conjunto

$$X \cup \{(x'): x \in X\}$$

donde X representa al conjunto de símbolos de variable. Aquí $\alpha \equiv \beta$ significará igualdad sintáctica entre α y β.

Observación 6.9.2. En la práctica, al usar las representaciones de la Definición 6.9.3, suprimiremos paréntesis siempre que ello no suponga caer en ambigüedades.

Definición 6.9.4. Dada un álgebra de Boole $\mathbf{B}$, una expresión booleana $\alpha(u_1, \ldots, u_k)$ y un elemento $\langle b_1, \ldots, b_k \rangle \in B^k$, $\alpha(b_1, \ldots, b_k)$ se define de la siguiente forma:

$$\alpha^{\mathbf{B}}(b_1, \ldots, b_k) = \begin{cases} b_i & \text{, si } 1 \leq i \leq k \text{ y } \alpha \equiv x_i \\ \tau(b_1, \ldots, b_k) + \sigma(b_1, \ldots, b_k) & \text{, si } \alpha \equiv (\tau + \sigma) \\ \tau(b_1, \ldots, b_k) \cdot \sigma(b_1, \ldots, b_k) & \text{, si } \alpha \equiv (\tau \cdot \sigma) \\ \overline{\tau(b_1, \ldots, b_k)} & \text{, si } \alpha \equiv (\tau') \\ 0 & \text{, si } a \equiv \bot \\ 1 & \text{, si } a \equiv \top \end{cases}$$

Ejemplo 6.9.1. Consideremos las expresión booleana:

$$\begin{aligned} m_1(x,y,z) &\equiv \bar{x}\bar{y}z \\ e_1(x,y,z) &\equiv \bar{x}\bar{y} \\ h_1(x,y,z) &\equiv \bar{x} \\ k_1(x,y,z) &\equiv \bar{y} \\ g_1(x,y,z) &\equiv z \\ m_2(x,y,z) &\equiv \bar{x}y\bar{z} \\ m_4(x,y,z) &\equiv x\bar{y}\bar{z} \\ m_7(x,y,z) &\equiv xyz \\ s(x,y,z) &\equiv \bar{x}\bar{y}z + \bar{x}y\bar{z} + x\bar{y}\bar{z} + xyz \\ a(x,y,z) &\equiv yz + xz + xy \end{aligned}$$

Se tiene:

$$\begin{aligned} s(0,0,1) &= m_1(0,0,1) + m_2(0,0,1) + m_4(0,0,1) + m_7(0,0,1) \\ &= (e_1(0,0,1) \cdot g_1(0,0,1)) + m_2(0,0,1) + m_4(0,0,1) + m_7(0,0,1) \\ &= (h_1(0,0,1) \cdot k_1(0,0,1) \cdot g_1(0,0,1)) + m_2(0,0,1) + m_4(0,0,1) + m_7(0,0,1) \\ &= (\overline{x(0,0,1)} \cdot \overline{y(0,0,1)} \cdot z(0,0,1)) + m_2(0,0,1) + m_4(0,0,1) + m_7(0,0,1) \\ &= (\bar{0} \cdot \bar{0} \cdot 1) + m_2(0,0,1) + m_4(0,0,1) + m_7(0,0,1) \\ &= (1 \cdot 1 \cdot 1) + m_2(0,0,1) + m_4(0,0,1) + m_7(0,0,1) \\ &= 1 + m_2(0,0,1) + m_4(0,0,1) + m_7(0,0,1) \\ &= 1 \end{aligned}$$

y los siguientes ejemplos:

x	y	z	$s(x,y,z)$	$a(x,y,z)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Observación 6.9.3. La Definición 6.9.4 explica cómo hacer corresponder a la expresión $\alpha(u_1,\ldots,u_k)$ la aplicación $\alpha^{\mathbf{B}}$ de evaluación de α en los puntos de B^k. Así pues, α^k es una aplicación de B^k en B sin más que tener en cuenta el *principio de lectura única* y convenir en listar los símbolos de variable $u_1,\ldots,u_k$ en el orden en el que ocurren en la lista:

$$u, v, x, y, z, u_1, v_1, x_1, y_1, z_1, u_2, v_2, x_2, y_2, z_2, \ldots$$

Por ejemplo $y + x'$ determina la función $f(x,y) = y + x'$ y así $f(1,0) = 0$ y $f(0,1) = 1$.

Definición 6.9.5. Dada un álgebra de Boole $\mathbf{B}$ y una expresión booleana $\alpha(u_1,\ldots,u_k)$, definimos la función booleana $f_\alpha\colon B^k \longrightarrow B$ como sigue:

$$f_\alpha(b_1,\ldots,b_k) = \alpha^{\mathbf{B}}(b_1,\ldots,b_k)$$

Diremos que las expresiones booleanas $\alpha(u_1,\ldots,u_k)$ y $\beta(u_1,\ldots,u_k)$ son *iguales* (o *equivalentes*), en símbolos $\alpha(u_1,\ldots,u_k) = \beta(u_1,\ldots,u_k)$ o simplemente $\alpha = \beta$, sii, por def., $f_\alpha \restriction \{0,1\} = f_\beta \restriction \{0,1\}$.

Observación 6.9.4.

- En cualquier álgebra de Boole $\{0,1\}$ es cerrado para $+$, $\cdot$ y $^-$, por lo que para toda expresión $\alpha(u_1,\ldots,u_k)$ y toda álgebra de boole $\mathbf{B}$, $\mathrm{ran}(f_\alpha \restriction \{0,1\}) \subseteq \{0,1\}$.
- En un abuso de notación está permitido confundir $f_\alpha(u_1,\ldots,u_k) \restriction \{0,1\}$ con $\alpha(u_1,\ldots,u_k)$.

Ejemplo 6.9.2. Si $s(x,y,z)$ y $a(x,y,z)$ son los dados en el ejemplo 6.9.1, sabemos que $s(x,y,z) \neq a(x,y,z)$. Sin embargo, si $\alpha_1(x,y) \equiv x + xy$ y $\alpha_2(x,y) \equiv x$, entonces es fácil comprobar que $\alpha_1 = \alpha_2$. En efecto:

x	y	$\alpha_1(x,y)$	$\alpha_2(x,y)$
0	0	0	0
0	1	0	0
1	0	1	1
1	1	1	1

Ejemplo 6.9.3. Dadas expresiones booleanas α y β, puede ocurrir que $\alpha \not\equiv \beta$ y sin embargo $\alpha = \beta$. Por ejemplo, sea $a \equiv ((x_1 + x_2)')$ y $b \equiv ((x_1') \cdot (x_2'))$.

Teorema 6.9.1. *La igualdad, $=$, entre expresiones boolenas tiene las propiedades que recogen las tablas de la Figura 6.7 y la Figura 6.8.*

Definición 6.9.6. Para todo símbolo de variable u y expresión booleana $\alpha(u,u_1,\ldots,u_k)$, definimos su *expansión mediante* u, en símbolos $e_u(\alpha)$, por la igualdad sintáctica:

$$\mathrm{e}_u(\alpha) \equiv (\alpha(\bot,u_1,\ldots,u_k)\cdot u') + (\alpha(\top,u_1,\ldots,u_k)\cdot u)$$

Teorema 6.9.2. *Para todo símbolo de variable u y expresión booleana $\alpha(u, u_1, \ldots, u_k)$,*

$$\alpha(u, u_1, \ldots, u_k) = \mathrm{e}_u(\alpha)$$

Demostración. La demostración es por inducción sobre la complejidad de la expresión $\alpha(u, u_1, \ldots, u_k)$, que en esta demostración abreviaremos por $\alpha(u)$. Supongamos que α es una expresión booleana de complejidad n y que el resultado es cierto para toda expresión de complejidad inferior a la de α. Se pueden dar los siguientes casos:

1. $n = 0$; son posibles cuatro situaciones:

   - $\alpha \equiv u$; entonces $\alpha(0) = 0$, $\alpha(1) = 1$. Así pues:

   $$\begin{aligned}\alpha(u) &= u \\ &= (\bot \cdot u') + (\top \cdot u) \\ &= (\alpha(\bot) \cdot u') + (\alpha(\top) \cdot u) \\ &= e_u(\alpha(u))\end{aligned}$$

   - Que $u_i \not\equiv u$ y $\alpha \equiv v$, donde $v \in \{u_i, \bot, \top\}$; entonces $\alpha(0) = \alpha(1) = v$. Así pues:

   $$\begin{aligned}\alpha(u) &= v \\ &= v \cdot \top \\ &= v(u' + u) \\ &= vu' + vu \\ &= (\alpha(\bot) \cdot u') + (\alpha(\top) \cdot u) \\ &= e_u(\alpha(u))\end{aligned}$$

2. $\alpha(u) = (\sigma(u))'$. Como la complejidad de σ es menor que la de α, la hipótesis de inducción permite afirmar que:

   $$\sigma(u) = \mathrm{e}_u(\sigma)$$

leyes conmutativas	1. $x + y = y + z$	1'. $xy = yx$
leyes asociativas	2. $x + (y + z) = (x + y) + z$	2'. $x(yz) = (xy)z$
leyes distributivas	3. $x(y + z) = xy + xz$	3'. $x + yz = (x + y)(x + z)$
leyes de identidad	4. $x + 0 = x = 0 + x$	4'. $x1 = x = 1x$
leyes del complemento	5. $x + x' = 1$	5'. $xx' = 0$

Figura 6.7: Propiedades básicas de la igualdad entre expresiones.

leyes de involución	1. y 1'. $x'' = x$	
leyes de idempotencia	2. $x + x = x$	2'. $xx = x$
leyes de anulación	3. $x + 1 = 1$	3'. $x0 = 0$
leyes de absorción	4. $x + xy = x$	4'. $x(x + y) = x$
leyes de De Morgan	5. $(x + y)' = x'y'$	5'. $(xy)' = x' + y'$
leyes de simplificación	6. $xy + x'y = y$	6'. $(x + y)(x' + y) = y$

Figura 6.8: Propiedades adicionales de la igualdad entre expresiones.

Así pues:

$$\begin{aligned}
\alpha(u) &= (\sigma(u))' \\
&= ((\sigma(\bot)\cdot u') + (\sigma(\top)\cdot u))' \\
&= (\sigma(\bot)\cdot u')'(\sigma(\top)\cdot u)' \\
&= (\alpha(\bot) + u)(\alpha(\top) + u') \\
&= (\alpha(\bot)\cdot\alpha(\top)) + (\alpha(\bot)\cdot u') + (\alpha(\top)\cdot u) + (u\cdot u') \\
&= (\alpha(\bot)\cdot\alpha(\top)) + (\alpha(\bot)\cdot u') + (\alpha(\top)\cdot u) \\
&= ((\alpha(\bot)\cdot\alpha(\top))\cdot(u + u')) + (\alpha(\bot)\cdot u') + (\alpha(\top)\cdot u) \\
&= (\alpha(\bot)\cdot\alpha(\top)\cdot u) + (\alpha(\bot)\cdot\alpha(\top)\cdot u') + (\alpha(\bot)\cdot u') + (\alpha(\top)\cdot u) \\
&= ((\alpha(\bot)\cdot\alpha(\top)\cdot u) + (\alpha(\top)\cdot u)) + ((\alpha(\bot)\cdot\alpha(\top)\cdot u') + (\alpha(\bot)\cdot u')) \\
&= (\alpha(\top)\cdot u) + (\alpha(\bot)\cdot u')) \\
&= (\alpha(\bot)\cdot u')) + (\alpha(\top)\cdot u) \\
&= \mathrm{e}_u(\alpha)
\end{aligned}$$

3. $\alpha(u) = \sigma(u) + \tau(u)$; entonces la hipótesis de inducción vale para σ y τ, con lo que:

$$\begin{aligned}
\alpha(u) &= \sigma(u) + \tau(u) \\
&= e_u(\sigma) + e_u(\tau) \\
&= ((\sigma(\bot)\cdot u') + (\sigma(\top)\cdot u)) + ((\tau(\bot)\cdot u') + (\tau(\top)\cdot u)) \\
&= ((\sigma(\bot)\cdot u') + (\tau(\bot)\cdot u')) + ((\sigma(\top)\cdot u) + (\tau(\top)\cdot u)) \\
&= ((\sigma(\bot) + \tau(\bot))\cdot u') + ((\sigma(\top) + \tau(\top))\cdot u) \\
&= (\alpha(\bot)\cdot u') + (\alpha(\top)\cdot u) \\
&= e_u(\alpha)
\end{aligned}$$

4. $\alpha(u) = \sigma(u)\cdot\tau(u)$; entonces la hipótesis de inducción vale para σ y τ, con lo que:

$$\begin{aligned}
\alpha(u) &= \sigma(u)\cdot\tau(u) \\
&= e_u(\sigma)\cdot e_u(\tau) \\
&= ((\sigma(\bot)\cdot u') + (\sigma(\top)\cdot u))\cdot((\tau(\bot)\cdot u') + (\tau(\top)\cdot u)) \\
&= (\sigma(\bot)\cdot u'\cdot\tau(\bot)\cdot u') + (\sigma(\top)\cdot u\cdot\tau(\bot)\cdot u') \\
&+ (\sigma(\bot)\cdot u'\cdot\tau(\top)\cdot u) + (\sigma(\top)\cdot u\cdot\tau(\top)\cdot u) \\
&= (\sigma(\bot)\cdot\tau(\bot)\cdot u'\cdot u') + (\sigma(\top)\cdot\tau(\bot)\cdot u\cdot u') \\
&+ (\sigma(\bot)\cdot\tau(\top)\cdot u'\cdot u) + (\sigma(\top)\cdot\tau(\top)\cdot u\cdot u) \\
&= (\sigma(\bot)\cdot\tau(\bot)\cdot u') + (\sigma(\top)\cdot\tau(\bot)\cdot\bot) \\
&+ (\sigma(\bot)\cdot\tau(\top)\cdot\bot) + (\sigma(\top)\cdot\tau(\top)\cdot u) \\
&= (\sigma(\bot)\cdot\tau(\bot)\cdot u') + (\sigma(\top)\cdot\tau(\top)\cdot u) \\
&+ ((\sigma(\top)\cdot\tau(\bot)) + (\sigma(\bot)\cdot\tau(\top)))\cdot\bot \\
&= (\alpha(\bot)\cdot u') + (\alpha(\top)\cdot u) + \bot \\
&= (\alpha(\bot)\cdot u') + (\alpha(\top)\cdot u) \\
&= e_u(\alpha)
\end{aligned}$$

Así pues, sea cual sea la complejidad de la expresión α resulta que $\alpha = e_u(\alpha)$, como se quería demostrar. □

Definición 6.9.7. Para toda expresión booleana α e $i \in \{0,1\}$ definimos α^i por la siguiente igualdad:

$$\alpha^i = \begin{cases} \alpha' & \text{, si } i = 0 \\ \alpha & \text{, si } i = 1 \end{cases}$$

Corolario 6.9.3 (forma normal disyuntiva)**.** *Para todo número natural k, símbolos de variable u_i $(1 \leq i \leq k)$ y toda expresión booleana α:*

$$\alpha(u_1, \ldots, u_k) = \sum_{\langle i_1,\ldots,i_k\rangle \in \{0,1\}^k} \alpha(i_1, \ldots, i_k) \prod_{j=1}^{k} u_j^{i_j}$$

Demostración. La demostración es por inducción sobre el número n de símbolos de variable que intervienen en la expresión booleana [1] α. Para el **caso base**, si $n = 0$ entonces[2] caben dos posibilidades:

- $\alpha = \bot$; en este caso

$$\begin{aligned} \alpha &= \bot \\ &= \bot\top \\ &= \sum_{i \in \{0\}} \bot\top \end{aligned}$$

- $\alpha = \top$; en este caso

$$\begin{aligned} \alpha &= \top \\ &= \top\top \\ &= \sum_{i \in \{0\}} \top\top \end{aligned}$$

Supongamos que $0 < n$, que en α ocurren n símbolos de variable y que el resultado es cierto para cualquier expresión booleana en la que ocurren $n-1$ símbolos de variable. Por lo que asegura el Teorema 6.9.2, sabemos que:

$$\alpha(u_1, \ldots, u_n) = (\alpha(\bot, u_2, \ldots, u_n) \cdot u_1') + (\alpha(\top, u_2, \ldots, u_n) \cdot u_1)$$

y haciendo uso de la hipótesis de inducción tenemos:

$$\begin{aligned} \alpha(u_1, \ldots, u_n) &= (\alpha(\bot, u_2, \ldots, u_n) \cdot u') + (\alpha(\top, u_2, \ldots, u_n) \cdot u) \\ &= \left(\left(\sum_{\langle i_2,\ldots,i_n\rangle \in \{0,1\}^{n-1}} \alpha(\bot, i_2, \ldots, i_n) \prod_{j=2}^{n} u_j^{i_j} \right) \cdot u_1' \right) \\ &+ \left(\left(\sum_{\langle i_2,\ldots,i_n\rangle \in \{0,1\}^{n-1}} \alpha(\top, i_2, \ldots, i_n) \prod_{j=2}^{n} u_j^{i_j} \right) \cdot u_1 \right) \\ &= \sum_{\langle i_1,\ldots,i_n\rangle \in \{0,1\}^{n}} \alpha(i_1, \ldots, i_n) \prod_{j=1}^{n} u_j^{i_j} \end{aligned}$$

Esto demuestra lo que se quería para expresiones con un número de variables cualquiera. □

Corolario 6.9.4 (forma normal disyuntiva)**.** *Para todo número natural k, símbolos de variable u_i $(1 \leq i \leq k)$ y toda expresión booleana α:*

$$\alpha(u_1, \ldots, u_k) = \prod_{\langle i_1,\ldots,i_k\rangle \in \{0,1\}^k} \left(\alpha(i_1, \ldots, i_k) + \sum_{j=1}^{k} u_j^{i_j'} \right)$$

[1] A lo largo de la demostración hacemos uso de acordado en la Definición 6.9.3 respecto a nombrar ocasionalmente a $\bot$ (resp. $\top$) por 0 (resp. 1).

[2] Sea o no Y vacío, $Y^{\varnothing} = \{\varnothing\}$. Si $X \neq \varnothing$, $\varnothing^X = \varnothing$. Aquí estamos en el primero de los casos, o sea $\{\bot, \top\}^{\varnothing}$, pues no debemos olvidar que $0 = \varnothing$.

Demostración. α' es una expresión booleana y por el Corolario 6.9.3

$$\alpha(u_1, \ldots, u_k)' = \sum_{\langle i_1, \ldots, i_k \rangle \in \{0,1\}^k} \alpha(i_1, \ldots, i_k)' \prod_{j=1}^{k} u_j^{i_j} \tag{6.18}$$

Tomando el complemento en ambos miembros de (6.18) se obtiene lo que queremos. □

Observación 6.9.5. Lo que expresa el Corolario 6.9.3 es:

- En el caso $n = 1$;
$$\alpha(u) = (\alpha(\bot) + u)(\alpha(\top) + u')$$
- En el caso $n = 2$;
$$\alpha(u_1, u_2) = (\alpha(\bot, \bot) + u_1 + u_2)(\alpha(\bot, \top) + u_1 + u_2')(\alpha(\top, \bot) + u_1' + u_2)(\alpha(\top, \top) + u_1' + u_2')$$

Apéndice A

Alfabeto Griego

Nombre	Mayúscula	Minúscula	Pronunciación	orden LaTeX
alfa	A	α	a	`\alpha`
beta	B	β	b,v	`\beta`
gamma	Γ	γ	g	`\gamma`
delta	Δ	δ	d	`\delta`
epsilón	E	ϵ,ε	e breve	`\epsilon`, `\varepsilon`
dseta	Z	ζ	z,ds	`\zeta`
eta	H	η	e larga	`\eta`
theta	Θ	θ,ϑ	th	`\theta`, `\vartheta`
yota	I	ι	i	`\iota`
cappa	K	κ	k,c	`\kappa`
lambda	Λ	λ	l	`\lambda`
mu	M	μ	m	`\mu`
nu	N	ν	n	`\nu`
xi	Ξ	ξ	x suave	`\xi`
omicrón	O	o	o breve	o
pi	Π	π	p	`\pi`
ro	R	ρ	r	`\rho`
sigma	Σ	σ,ς	s	`\sigma`,`\varsigma`
tau	T	τ	t	`\tau`
upsilón	Υ	υ	y,u breve	`\upsilon`
fi	Φ	ϕ,φ	f,ph	`\phi`,`\varphi`
ji	C	χ	j,x fuerte	`\chi`
psi	Ψ	ψ	ps,bs	`\psi`
omega	Ω	ω	o larga	`\omega`

Apéndice B

Leyes de la Lógica Clásica

Ejemplo B.0.1. Ejemplos de tautologías son las siguientes fórmulas:

1. $\alpha \to \alpha$ (*ley de identidad*); en efecto, sea cual sea v,

$$\begin{aligned} v(\alpha \to \alpha) &= v(\alpha)v(\alpha) + v(\alpha) + 1 \\ &= v(\alpha) + v(\alpha) + 1 \\ &= 0 + 1 \\ &= 1 \end{aligned}$$

2. $(\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))$ (ley de silogismo fuerte); en efecto, para toda asignación de variables v:

$$v((\alpha \to \beta)v(\beta \to \gamma)) = v(\alpha)v(\beta) + v(\beta)v(\gamma) + v(\alpha) + v(\beta) + 1$$

y así:

$$\begin{aligned} v((\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))) &= v(\alpha \to \beta)v(\beta \to \gamma)(v(\alpha \to \gamma) + 1) + 1 \\ &= v(\alpha \to \beta)v(\beta \to \gamma)(v(\alpha)v(\gamma) + v(\alpha)) + 1 \\ &= (v(\alpha)v(\beta) + v(\beta)v(\gamma) + v(\alpha) + v(\beta) + 1)(v(\alpha)v(\gamma) + v(\alpha)) \\ &\quad + 1 \\ &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\gamma) + v(\alpha)v(\beta)v(\gamma) \\ &\quad + v(\alpha)v(\gamma) \\ &\quad + v(\alpha)v(\beta) + v(\alpha)v(\beta)v(\gamma) + v(\alpha) + v(\alpha)v(\beta) + v(\alpha) + 1 \\ &= 1 \end{aligned}$$

3. $\big(\alpha \to (\beta \to \gamma)\big) \to \big(\beta \to (\alpha \to \gamma)\big)$ (*ley de conmutación de premisas* o *cambio del antecedente*)
4. $(\beta \to \gamma) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$ (ley de silogismo débil)
5. $\alpha \to (\beta \to \alpha)$ (*ley de "a fortiori"* (con mayor razón) o *"verum sequitur ad quodlibet"* (la verdad se sigue de cualquiera)); en efecto, según el Ejemplo 5.2.2, sea cual sea v,

$$\begin{aligned} v(\alpha \to (\beta \to \alpha)) &= v(\alpha)v(\beta)v(\alpha) + v(\alpha)v(\beta) + 1 \\ &= v(\alpha)v(\beta) + v(\alpha)v(\beta) + 1 \\ &= 0 + 1 \\ &= 1 \end{aligned}$$

6. $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$ (*ley de Frege o autodistributiva*)

7. $\alpha \to ((\alpha \to \beta) \to \beta)$ (ley de *modus ponens*)

8. $(\alpha \to (\alpha \to \beta)) \to (\alpha \to \beta)$ (*ley de reducción de premisas*)

9. $((\alpha \to \beta) \to (\beta \to \alpha)) \to (\beta \to \alpha)$

10. $((\alpha \to \beta) \to \gamma) \to (\delta \to ((\beta \to (\gamma \to \varepsilon)) \to (\beta \to \varepsilon)))$

11. $\varepsilon \to ((\alpha \to \beta) \to ((\delta \to \alpha) \to (\beta \to \gamma)) \to (\alpha \to \gamma))$

12. $((\alpha \to \beta) \to \gamma) \to (((\beta \to \alpha) \to \gamma) \to \gamma)$ (ley de *Dummet*)

13. $((\alpha \to \beta) \to \beta) \to ((\beta \to \alpha) \to \alpha)$ (ley de *Tanaka*)

14. $\big((\alpha \to \beta) \to \alpha\big) \to \alpha$ (ley de *Peirce*)

15. $((((\varphi \to \psi) \to (\neg\alpha \to \neg\beta)) \to \alpha) \to \gamma) \to ((\gamma \to \varphi) \to (\beta \to \varphi))$ (ley de *Meredith*)

16. $((\alpha \to \gamma) \to \beta) \to (((\beta \to \alpha) \to \beta) \to \beta)$ (ley para la trivalencia del sistema BCK)

Cualquier fórmula anterior es satisfacible y no refutable. La negación de cualquiera de las fórmulas anteriores es un ejemplo de contradicción. Cualquier variable atómica es a la vez satisfacible y refutable.

Ejemplo B.0.2.

1. $\neg\neg\alpha \to \alpha$ (*ley de doble negación clásica o fuerte*)

2. $\alpha \to \neg\neg\alpha$ (*ley de doble negación intuicionista o minimal*)

3. $\neg\neg\neg\alpha \to \neg\alpha$ (ley de *Brouwer*)

4. $\neg\alpha \to (\alpha \to \beta)$ (*ley de Duns Scoto*) ; en efecto, para toda asignación de variables:

$$\begin{aligned} v(\alpha \to (\neg\alpha \to \beta)) &= v(\alpha)v(\neg\alpha \to \beta) + v(\alpha) + 1 \\ &= v(\alpha)(v(\neg\alpha)v(\beta) + v(\neg\alpha) + 1) + v(\alpha) + 1 \\ &= v(\alpha)((v(\alpha) + 1)v(\beta) + v(\alpha) + 1 + 1) + v(\alpha) + 1 \\ &= v(\alpha)(v(\alpha)v(\beta) + v(\beta) + v(\alpha)) + v(\alpha) + 1 \\ &= v(\alpha)^2 v(\beta) + v(\alpha)v(\beta) + v(\alpha)^2 + v(\alpha) + 1 \\ &= v(\alpha)v(\beta) + v(\alpha)v(\beta) + v(\alpha) + v(\alpha) + 1 \\ &= 0 + 0 + 1 \\ &= 1 \end{aligned}$$

5. $\alpha \to (\neg\alpha \to \neg\beta)$ (*ley débil de Duns Scoto*)

6. $(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)$ (*ley de "reductio ad absurdum" clásica o fuerte*)

7. $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$ (*ley de contraposición "tollendo tollens"*); en efecto, sea cual sea v,

$$\begin{aligned} v((\alpha \to \beta) \to (\neg\beta \to \neg\alpha)) &= v(\alpha \to \beta)v(\neg\beta \to \neg\alpha) + v(\alpha \to \beta) + 1 \\ &= (v(\alpha)v(\beta) + v(\alpha) + 1)(v(\neg\beta)v(\neg\alpha) + v(\neg\beta) + 1) \\ &+ (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\ &= (v(\alpha)v(\beta) + v(\alpha) + 1)((v(\beta) + 1)(v(\alpha) + 1) + v(\beta) + 1 + 1) \\ &+ (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\ &= (v(\alpha)v(\beta) + v(\alpha) + 1)(v(\alpha)v(\beta) + v(\alpha) + v(\beta) + 1 + v(\beta)) \\ &+ (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\ &= (v(\alpha)v(\beta) + v(\alpha) + 1)(v(\alpha)v(\beta) + v(\alpha) + 1) \\ &+ (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\ &= (v(\alpha)v(\beta) + v(\alpha) + 1) + (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\ &= 1 \end{aligned}$$

8. $(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$ (*ley de contraposición "ponendo ponens"*);
9. $(\alpha \to \neg\beta) \to (\beta \to \neg\alpha)$ (*ley de contraposición "ponendo tollens"*);
10. $(\neg\alpha \to \beta) \to (\neg\beta \to \alpha)$ (*ley de contraposición "tollendo ponens"*);
11. $(\alpha \to \beta) \to ((\alpha \to \neg\beta) \to \neg\alpha)$ (*ley "reductio ad absurdum" intuicionista o minimal*)
12. $(\neg\alpha \to \alpha) \to \alpha$ (*ley de Clavius*); en efecto, sea v una asignación de variables cualquiera:

$$\begin{aligned} v((\neg\alpha \to \alpha) \to \alpha) &= v((\neg\alpha \to \alpha))v(\alpha) + v((\neg\alpha \to \alpha)) + 1 \\ &= (v(\neg\alpha)v(\alpha) + v(\neg\alpha) + 1)v(\alpha) + (v(\neg\alpha)v(\alpha) + v(\neg\alpha) + 1)v(\alpha) + 1 \\ &= (v(\neg\alpha)v(\alpha) + v(\alpha))v(\alpha) + v(\neg\alpha)v(\alpha) + v(\alpha) + 1 \\ &= v(\neg\alpha)v(\alpha) + v(\alpha) + v(\neg\alpha)v(\alpha) + v(\alpha) + 1 \\ &= 0 + 0 + 1 \\ &= 1 \end{aligned}$$

13. $(\alpha \to \neg\alpha) \to \neg\alpha$ (*ley débil de Clavius*)
14. $\neg(\alpha \to \alpha) \to \beta$ (*ley "ex falso sequitur quodlibet"* (de lo falso se sigue cualquier cosa))
15. $\alpha \to (\neg\beta \to \neg(\alpha \to \beta))$
16. $(\alpha \to \beta) \to ((\neg\alpha \to \beta) \to \beta)$ (*ley del dilema*)
17. $(\alpha \to \beta) \to \big((\alpha \to \neg\beta) \to \neg\alpha\big)$
18. $(\alpha \to \gamma) \to ((\neg\alpha \to \beta) \to (\neg\beta \to \gamma))$ (ley de *modus ponens* generalizada)

Ejemplo B.0.3.

1. $(\alpha \wedge \beta) \to \alpha$
2. $(\alpha \wedge \beta) \to \beta$
3. $(\gamma \to \alpha) \to ((\gamma \to \beta) \to (\gamma \to (\alpha \wedge \beta)))$
4. $\alpha \to \big(\beta \to (\alpha \wedge \beta)\big)$

5. $(\beta \wedge \alpha) \to (\alpha \wedge \beta)$
6. $(\alpha \to (\beta \to \gamma)) \to ((\alpha \wedge \beta) \to \gamma)$ (*ley de importación*)
7. $((\alpha \wedge \beta) \to \gamma) \to (\alpha \to (\beta \to \gamma))$ (*ley de exportación*)
8. $(\alpha \to \beta) \to ((\alpha \wedge \gamma) \to (\beta \wedge \gamma))$
9. $((\alpha \to \beta) \wedge (\beta \to \gamma)) \to (\alpha \to \gamma)$ (*ley "ex toto"* o *transitividad de* $\to$)
10. $(\alpha \wedge (\alpha \to \beta)) \to \beta$ (*ley de "modus ponens"*)

Ejemplo B.0.4.

1. $\alpha \to (\alpha \vee \beta)$
2. $\beta \to (\alpha \vee \beta)$
3. $(\alpha \to \gamma) \to ((\beta \to \gamma) \to ((\alpha \vee \beta) \to \gamma))$
4. $(\alpha \to (\beta \vee \gamma)) \to ((\alpha \to \beta) \vee (\alpha \to \gamma))$
5. $(\alpha \to \beta) \vee (\beta \to \alpha)$
6. $(\beta \vee \alpha) \to (\alpha \vee \beta)$
7. $(\alpha \to \varphi) \to ((\beta \to \psi) \to ((\alpha \vee \beta) \to (\varphi \vee \psi)))$

Ejemplo B.0.5.

1. $\alpha \vee \neg\alpha$ (*ley "tertium non datur"* o *principio del tercio excluso*)
2. $\neg(\alpha \to \neg\alpha)$ (*principio de no contradicción*)
3. $(\alpha \wedge \neg\alpha) \to \beta$ (*principio de inconsistencia*)
4. $(\neg\beta \wedge (\alpha \to \beta)) \to \neg\alpha$ (*principio del "modus tollendo tollens"*)
5. $((\alpha \vee \beta) \wedge \neg\beta) \to \alpha$
6. $((\alpha \vee \beta) \wedge \neg\alpha) \to \beta$
7. $((\alpha \vee \beta) \wedge (\alpha \to \gamma) \wedge (\beta \to \gamma)) \to \gamma$
8. $((\neg\alpha \vee \neg\beta) \wedge (\gamma \to \alpha) \wedge (\gamma \to \beta)) \to \neg\gamma$
9. $((\alpha \vee \beta) \wedge (\alpha \to \varphi) \wedge (\beta \to \psi)) \to (\varphi \vee \psi)$
10. $((\neg\alpha \vee \neg\beta) \wedge (\varphi \to \alpha) \wedge (\psi \to \beta)) \to (\neg\varphi \vee \neg\psi)$
11. $\neg(\alpha \wedge \neg\alpha)$

Apéndice C

Fórmulas Lógicamente Equivalentes

Lema C.0.1. *Sean α, β y γ fórmulas. Entonces:*

1. $\alpha \equiv \alpha$
2. $\alpha \equiv \alpha \vee \alpha$
3. $\alpha \equiv \alpha \wedge \alpha$
4. $\alpha \wedge \beta \equiv \beta \wedge \alpha$
5. $\alpha \vee \beta \equiv \beta \vee \alpha$
6. $(\alpha \wedge \beta) \wedge \gamma \equiv \alpha \wedge (\beta \wedge \gamma)$
7. $(\alpha \vee \beta) \vee \gamma \equiv \alpha \vee (\beta \vee \gamma)$
8. $\neg\neg\alpha \equiv \alpha$
9. $\alpha \to \beta \equiv \neg\alpha \vee \beta$
10. $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$
11. $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$
12. $\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
13. $\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
14. $\alpha \equiv \alpha \vee (\beta \wedge \neg\beta)$
15. $\alpha \equiv (\alpha \vee \beta) \wedge (\alpha \vee \neg\beta)$
16. $\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha)$
17. $(\neg\alpha \vee \alpha) \wedge \beta \equiv \beta$
18. $(\neg\alpha \vee \alpha) \vee \beta \equiv \neg\alpha \vee \alpha$
19. $(\neg\alpha \wedge \alpha) \vee \beta \equiv \beta$
20. $(\neg\alpha \wedge \alpha) \wedge \beta \equiv \neg\alpha \wedge \alpha$

Apéndice D

Prontuario de cálculo clásico proposicional y de primer orden

definición de sustituir x por t en α (α_t^x)

1. Si $\alpha \in \mathrm{Atom}(\mathbf{L})$, α_t^x es la fórmula obtenida sustituyendo las ocurrencias de x en α por el término t.
2. $(\neg\alpha)_t^x$ es $\neg(\alpha_t^x)$
3. $(\alpha \to \beta)_t^x$ es $(\alpha_t^x \to \beta_t^x)$
4. $(\forall y\alpha)_t^x = \begin{cases} \forall y\alpha, & \text{si } x = y, \\ \forall y(\alpha_t^x), & \text{si } x \neq y. \end{cases}$

(consiste en leer la fórmula de izquierda a derecha y cuando encontremos una ocurrencia libre de x sustituirla por t. Luego continuar leyendo en el símbolo inmediatamente siguiente al último de la escritura del término recién sustituido. Continuamos esta operación y no operamos cuando encontremos una ocurrencia de x que sea ligada.)

definición de "x es sustituible por t en α"

1. Si $\alpha \in \mathrm{Atom}(\mathbf{L})$, x es sustituible por t en α
2. x es sustituible por t en $(\neg\alpha)$ si, y solamente si, x es sustituible por t en α
3. x es sustituible por t en $(\alpha \to \beta)$ si, y solamente si, x es sustituible por t en α y β
4. x es sustituible por t en la fórmula $\forall y\alpha$ si o bien:
   a) x no ocurre libremente en $\forall y\alpha$, o bien
   b) en t no tiene y ninguna ocurrencia y x es sustituible por t en α.

(x es sustituible por t en una fórmula si en ella x no ocurre libremente nunca en el radio de acción de un $\forall x_j$, donde x_j es una variable que ocurre en t.)

lema de re-reemplazamiento

$$\frac{\begin{array}{c} y \text{ sustituible por } z \text{ en } \alpha \\ z \text{ no ocurre libremente en } \alpha \end{array}}{(z \text{ es sustituible por } y \text{ en } \alpha_z^y) + (\alpha_z^y)_y^z = \alpha}$$

algunas abreviaturas

abreviatura	**fórmula**
$\alpha \vee \beta$	$\neg\alpha \to \beta$
$\alpha \wedge \beta$	$\neg(\alpha \to \neg\beta)$
$\alpha \leftrightarrow \beta$	$(\alpha \to \beta) \wedge (\beta \to \alpha)$
$\exists x\alpha$	$\neg(\forall x \neg\alpha)$

Axiomas

A1) $\alpha \to (\beta \to \alpha)$ (ley "*a fortiori*" o "*verum sequitur ad quodlibet*")

A2) $\big(\alpha \to (\beta \to \gamma)\big) \to \big((\alpha \to \beta) \to (\alpha \to \gamma)\big)$ (ley autodistributiva o *de Frege*)

A3) $(\neg\alpha \to \neg\beta) \to \big((\neg\alpha \to \beta) \to \alpha\big)$ (ley *"reductio ad absurdum"* clásica o fuerte)

A4) $\forall x\alpha \to \alpha_t^x$, siendo x sustituible por t en α;

A5) $\forall x(\alpha \to \beta) \to (\forall x\alpha \to \forall x\beta)$;

A6) $\alpha \to \forall x\alpha$, donde x no ocurre libremente en α.

A7) $x \approx x$;

A8) $x \approx y \to (\alpha \to \tilde{\alpha})$, donde α es cualquier fórmula atómica del lenguaje y $\tilde{\alpha}$ es obtenida de α reemplazando x, en cero o más (no necesariamente todos) lugares por y.

modus ponens (único motor de inferencia)

$$\frac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$

algunos sistemas equivalentes

$$\alpha \to (\beta \to \alpha)$$
$$\big(\alpha \to (\beta \to \gamma)\big) \to \big((\alpha \to \beta) \to (\alpha \to \gamma)\big)$$
$$(\neg\alpha \to \neg\beta) \to \big((\neg\alpha \to \beta) \to \alpha\big)$$

$$\alpha \to (\beta \to \alpha)$$
$$\big(\alpha \to (\beta \to \gamma)\big) \to \big((\alpha \to \beta) \to (\alpha \to \gamma)\big)$$
$$(\neg\beta \to \neg\alpha) \to (\alpha \to \beta)$$

$$(\alpha \to \beta) \to \big((\beta \to \gamma) \to (\alpha \to \gamma)\big)$$
$$(\neg\alpha \to \alpha) \to \alpha$$
$$\neg\alpha \to (\alpha \to \beta)$$

$$((((\varphi \to \psi) \to (\neg\alpha \to \neg\beta)) \to \alpha) \to \gamma) \to ((\gamma \to \varphi) \to (\beta \to \varphi))$$

consecuencia del lema de re-reemplazamiento

$$\frac{y \text{ no ocurre en } \varphi}{\forall y\varphi_y^x \vdash \forall x\varphi}$$

definición de $\vdash_t$ y Ded_t

$\Gamma \vdash_t \varphi$ (φ es *consecuencia tautológica* de Γ) si existe una lista finita $\langle \alpha_1, \ldots, \alpha_n \rangle$ tal que $\varphi = \alpha_n$ y para cada $1 \leq i \leq n$ se cumple una de las siguientes condiciones:

1. α_i es una instancia de alguno de los esquemas A1, A2 o A3
2. existen $1 \leq j, k < i$ tales que $\alpha_j = \alpha_k \to \alpha_i$

$$\mathrm{Ded}_t(\Gamma) = \{\varphi : \Gamma \vdash_t \varphi\}$$

noción de generalización de una fórmula

φ es *generalización* de ψ si $\varphi = \psi$ o existen $x_{i_0}, \ldots, x_{i_n}$ tales que $\varphi = \forall x_{i_0} \cdots \forall x_{i_n} \psi$

definición de $\vdash_\Upsilon$ y Ded_Υ

$\Gamma \vdash_\Upsilon \varphi$ (φ es *consecuencia tautológica* de Γ) si existe una lista finita $\langle \alpha_1, \ldots, \alpha_n \rangle$ tal que $\varphi = \alpha_n$ y para cada $1 \leq i \leq n$ se cumple una de las siguientes condiciones:

1. $\alpha_i \in \Gamma \cup \Upsilon$
2. existen $1 \leq j, k < i$ tales que $\alpha_j = \alpha_k \to \alpha_i$

$$\mathrm{Ded}_\Upsilon(\Gamma) = \{\varphi : \Gamma \vdash_\Upsilon \varphi\}$$

En nuestro curso Υ es el conjunto de las generalizaciones de A1–A6 o A1–A7. Una tal lista $\langle \alpha_1, \ldots, \alpha_n \rangle$ recibe el nombre de $\langle \Gamma, \Upsilon \rangle$-prueba de φ o simplemente Γ-prueba de φ.

propiedades elementales de Ded_t y Ded_Υ

1. $\Gamma \subseteq \mathrm{Ded}_t(\Gamma)$
2. Si $\Gamma \subseteq \Delta$ entonces $\mathrm{Ded}_t(\Gamma) \subseteq \mathrm{Ded}_t(\Delta)$
3. $\mathrm{Ded}_t\big(\mathrm{Ded}_t(\Gamma)\big) \subseteq \mathrm{Ded}_t(\Gamma)$
4. $\mathrm{Ded}_t(\Gamma) = \bigcup_{\Phi \in \mathcal{P}_f(\Gamma)} \mathrm{Ded}_t(\Phi)$
5. $\mathrm{Ded}_t(\Gamma) \subseteq \mathrm{Ded}_\Upsilon(\Gamma)$ (acotación funcional)
6. Si $\alpha, \alpha \to \beta \in \mathrm{Ded}_\Upsilon(\Gamma)$, entonces $\beta \in \mathrm{Ded}_\Upsilon(\Gamma)$ (ser cerrado por *modus ponens*)
7. $\Gamma \subseteq \mathrm{Ded}_\Upsilon(\Gamma)$ (acotación de los conjuntos de fórmulas por cerrados)
8. Si $\Gamma \subseteq \Delta$ entonces $\mathrm{Ded}_\Upsilon(\Gamma) \subseteq \mathrm{Ded}_\Upsilon(\Delta)$ (monotonía)
9. $\mathrm{Ded}_\Upsilon\big(\mathrm{Ded}_\Upsilon(\Gamma)\big) \subseteq \mathrm{Ded}_\Upsilon(\Gamma)$ (idempotencia)
10. $\mathrm{Ded}_\Upsilon(\Gamma) = \bigcup_{\Phi \in \mathcal{P}_f(\Gamma)} \mathrm{Ded}_\Upsilon(\Phi)$ (finitariedad)

algunas equivalencias elementales

fórmula	equivalente
$\neg\neg\alpha$	α
$\neg(\alpha \vee \beta)$	$\neg\alpha \wedge \neg\beta$
$\neg(\alpha \wedge \beta)$	$\neg\alpha \vee \neg\beta$
$\neg\alpha \vee \beta$	$\alpha \to \beta$
$\neg(\alpha \wedge \neg\beta)$	$\alpha \to \beta$
$\alpha \vee (\beta \wedge \gamma)$	$(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
$\alpha \wedge (\beta \vee \gamma)$	$(\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
$\alpha \wedge (\neg\beta \vee \beta \vee \gamma)$	α

regla de *modus ponens* generalizada

$$\frac{\begin{array}{c}\neg\alpha \to \beta \\ \alpha \to \gamma\end{array}}{\neg\beta \to \gamma}$$

regla de *resolución*

$$\frac{\begin{array}{c}\alpha \vee \beta \\ \neg\alpha \vee \gamma\end{array}}{\beta \vee \gamma}$$

teorema de la deducción

$$\frac{\Gamma \vdash \varphi \to \psi}{\Gamma, \varphi \vdash \psi} \quad \text{y} \quad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}$$

regla de generalización

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall x \varphi}$$

con tal de que $\Gamma \vdash \varphi$ esté avalada por al menos una Γ-prueba en la que no sea usada niguna hipótesis con ocurrencias libres de x.

regla de generalización particularizada (ver. 1)

$$\frac{\vdash \varphi}{\vdash \forall x \varphi}$$

regla de generalización particularizada (ver. 2)

$$\frac{\Theta \vdash \varphi}{\Theta \vdash \forall x \varphi} \quad \text{, donde } \Theta \text{ es un conjunto de sentencias}$$

regla T

$$\frac{\begin{array}{c}\Gamma \vdash \varphi_1 \\ \ldots \\ \Gamma \vdash \varphi_n \\ \varphi_1, \ldots, \varphi_n \vdash_t \psi\end{array}}{\Gamma \vdash \psi}$$

reglas de contraposición

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma, \neg\psi \vdash \neg\varphi} \qquad \frac{\Gamma, \neg\varphi \vdash \psi}{\Gamma, \neg\psi \vdash \varphi}$$

$$\frac{\Gamma, \varphi \vdash \neg\psi}{\Gamma, \psi \vdash \neg\varphi} \qquad \frac{\Gamma, \neg\varphi \vdash \neg\psi}{\Gamma, \psi \vdash \varphi}$$

regla de reducción al absurdo clásica

$$\frac{\Gamma, \neg\varphi \vdash \psi \quad \Gamma, \neg\varphi \vdash \neg\psi}{\Gamma \vdash \varphi}$$

regla de reducción al absurdo intuicionista

$$\frac{\Gamma, \varphi \vdash \psi \quad \Gamma, \varphi \vdash \neg\psi}{\Gamma \vdash \neg\varphi}$$

regla del silogismo

$$\frac{\Gamma \vdash \alpha \to \beta \quad \Gamma \vdash \beta \to \gamma}{\Gamma \vdash \alpha \to \gamma}$$

regla de isotonía

$$\frac{\Gamma \vdash \alpha \to \beta}{\Gamma \vdash (\gamma \to \alpha) \to (\gamma \to \beta)}$$

regla de antiisotonía

$$\frac{\Gamma \vdash \alpha \to \beta}{\Gamma \vdash (\beta \to \gamma) \to (\alpha \to \gamma)}$$

negación de la flecha

$$\frac{\Gamma \vdash \alpha \quad \Gamma \vdash \neg\beta}{\Gamma \vdash \neg(\alpha \to \beta)}$$

$$\frac{\Gamma \vdash \neg(\alpha \to \beta)}{\Gamma \vdash \alpha} \qquad \frac{\Gamma \vdash \neg(\alpha \to \beta)}{\Gamma \vdash \neg\beta}$$

regla A4

$\vdash \forall x\varphi \to \varphi_t^x$, si x es sustituible por t en φ

regla A4 especial

$$\vdash \forall x\varphi \to \varphi$$

regla E4

$\vdash \varphi_t^x \to \exists x\varphi$, si x es sustituible por t en φ

generalización de constantes

$\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash \forall y\varphi_y^c}$, si c no ocurre en Γ

(y no ocurre en φ y $\Gamma \vdash \forall y\varphi_y^c$ está avalada por un Γ-prueba en la que no interviene c)

regla C (versión 1)

$$\frac{\Gamma \vdash \varphi^x_c}{\Gamma \vdash \forall x\varphi}, \text{ si } c \text{ no ocurre en } \Gamma \cup \{\varphi\}$$

($\Gamma \vdash \forall x\varphi$ está avalada por un Γ-prueba en la que no interviene c)

regla EI

$$\frac{\Gamma, \varphi^x_c \vdash \psi}{\Gamma, \exists x\varphi \vdash \psi}, \text{ si } c \text{ no ocurre en } \Gamma \cup \{\varphi, \psi\}$$

($\Gamma, \exists x\varphi \vdash \psi$ está avalada por un Γ-prueba en la que no interviene c)

regla C (versión 2 incompleta)

$$\frac{\begin{array}{c}\Gamma \vdash \exists x\varphi \\ \Gamma, \varphi^x_c \vdash \psi\end{array}}{\Gamma \vdash \psi} \quad \text{si } c \text{ no ocurre en } \Gamma \cup \{\varphi, \psi\}$$

(si $\Gamma \vdash \exists x\varphi$ está avalada por al menos una prueba en la que no ocurre c, entonces $\Gamma \vdash \psi$ también lo estará)

regla C (equiparable a la de Mendelson)

$$\frac{\begin{array}{c}\exists x\varphi \in \Gamma \\ \Gamma, \varphi^x_c \vdash \psi\end{array}}{\Gamma \vdash \psi} \quad \text{si } c \text{ no ocurre en } \Gamma \cup \{\psi\}$$

($\Gamma \vdash \psi$ está avalada por un Γ-prueba en la que no interviene c)

regla de extensión

$$\frac{\varphi \vdash \psi}{\forall x\varphi \vdash \forall x\psi}$$

definición de $\exists!x\alpha$

$$\exists x\alpha \wedge \forall x\forall y\big(\alpha \wedge \alpha^x_y \to x \approx y\big)$$

(y es el primer s. de variable diferente de x que no ocurre en α)

1. $\vdash \forall x\exists! yx \approx y$
2. $\vdash \exists! x\alpha \leftrightarrow \exists x\forall y(\alpha^x_y \leftrightarrow x \approx y)$
3. $\vdash \forall x(\alpha \leftrightarrow \beta) \to (\exists! x\alpha \leftrightarrow \exists! x\beta)$
4. $\vdash \exists! x(\alpha \vee \beta) \to (\exists! x\alpha \vee \exists! x\beta)$
5. $\vdash \exists! x\alpha \leftrightarrow \exists x\big(\alpha \wedge \forall y(\alpha^x_y \to y \approx x)\big)$

(y es el primer s. de variable diferente de x que no ocurre en α)

algunas leyes lógicas con cuantificadores y/o igualdad

1. $\forall x\varphi \to \exists x\varphi$
2. $\exists x\forall y\varphi \to \forall y\exists x\varphi$

3. $\forall x \forall y (x \approx y \to y \approx x)$
4. $x \approx y \to (\forall z p(x,z) \to \forall z p(y,z))$
5. $\forall x \forall y \forall z \forall v \big(x \approx z \to (y \approx v \to f(x,y) \approx f(z,v))\big)$
6. $t_k \approx u \to \big(r(t_1,\ldots,t_k,\ldots,t_n) \to r(t_1,\ldots,u,\ldots,t_n)\big)$
7. $\forall x (x \approx x)$
8. $\forall x \forall y (x \approx y \to y \approx x)$
9. $\forall x \forall y \forall z \big(x \approx y \to (y \approx z \to x \approx z)\big)$
10. $\forall x \forall y \forall z \forall v \big(x \approx z \to (y \approx v \to f(x,y) \approx f(z,v))\big)$
11. $\forall x \forall y \forall z \forall v \big(x \approx z \to (y \approx v \to r(x,y) \approx r(z,v))\big)$
12. $x \approx y \to (\varphi \to \tilde{\varphi})$, donde $\tilde{\varphi}$ es cualquier fórmula obtenida a partir de φ reemplazando por el s. de variable y algunas de, pero no necesariamente todas, las ocurrencias libres del s. de variable x, a condición de x sea sustituible por y en la fórmula φ

equivalencia–negación

$$\frac{\vdash \alpha \leftrightarrow \alpha'}{\vdash \neg\alpha \leftrightarrow \neg\alpha'}$$

equivalencia-implicación

$$\frac{\vdash \alpha' \to \alpha \quad \vdash \beta \to \beta'}{\vdash (\alpha \to \beta) \to (\alpha' \to \beta')} \qquad \frac{\vdash \alpha \leftrightarrow \alpha' \quad \vdash \beta \leftrightarrow \beta'}{\vdash (\alpha \to \beta) \leftrightarrow (\alpha' \to \beta')}$$

lema de renombramiento de variables

$$\frac{\begin{array}{c} y \text{ sustituible por } z \text{ en } \beta \\ z \text{ no ocurre libremente en } \beta \\ \vdash \alpha \leftrightarrow \beta \end{array}}{\vdash \forall y \alpha \leftrightarrow \forall z (\beta)^y_z}$$

existencia de variante alfabética

$$\frac{\begin{array}{c} y \text{ s. variable y } t \text{ término} \\ \varphi \text{ fórmula} \end{array}}{\begin{array}{c} \text{existe } \varphi' \text{ tal que} \\ x \text{ es sustit. por } t \text{ en } \varphi' + \vdash \varphi \leftrightarrow \varphi' \end{array}}$$

leyes generales

1. $\neg \forall x \alpha \leftrightarrow \exists x \neg \alpha$
2. $\neg \exists x \alpha \leftrightarrow \forall x \neg \alpha$

y en el suspuesto de que x no ocurra libremente en α:

1. $\alpha \leftrightarrow \forall x \alpha$
2. $\alpha \leftrightarrow \exists x \alpha$

3. $(\alpha \to \exists x\beta) \leftrightarrow \exists x(\alpha \to \beta)$
4. $(\forall x\beta \to \alpha) \leftrightarrow \exists x(\beta \to \alpha)$
5. $(\alpha \to \forall x\beta) \leftrightarrow \forall x(\alpha \to \beta)$
6. $(\exists x\beta \to \alpha) \leftrightarrow \forall x(\beta \to \alpha)$
7. $(\forall x\beta \vee \alpha) \leftrightarrow \forall x(\beta \vee \alpha)$
8. $(\alpha \vee \forall x\beta) \leftrightarrow \forall x(\alpha \vee \beta)$
9. $(\alpha \vee \exists x\beta) \leftrightarrow \exists x(\alpha \vee \beta)$
10. $(\exists x\beta \vee \alpha) \leftrightarrow \exists x(\beta \vee \alpha)$
11. $(\forall x\beta \wedge \alpha) \leftrightarrow \forall x(\beta \wedge \alpha)$
12. $(\alpha \wedge \forall x\beta) \leftrightarrow \forall x(\alpha \wedge \beta)$
13. $(\alpha \wedge \exists x\beta) \leftrightarrow \exists x(\alpha \wedge \beta)$
14. $(\exists x\beta \wedge \alpha) \leftrightarrow \exists x(\beta \wedge \alpha)$
15. $(\forall x\alpha \wedge \forall x\beta) \leftrightarrow \forall x(\alpha \wedge \beta)$
16. $(\exists x\alpha \vee \exists x\beta) \leftrightarrow \exists x(\alpha \vee \beta)$

noción de forma prenexa

α está en forma prenexa si se expresa como

$$Q_i x_i \cdots Q_n x_n \beta \tag{D.1}$$

donde $Q_i \in \{\exists, \forall\}$, para todo $1 \leq i \leq n$ y en la escritura de β no aparece ningún cuantificador. Llamamos literal a cualquier fórmula que sea atómica o de la forma $\neg\alpha$, donde α es una fórmula atómica. En (D.1), β se denomina matriz de la fórmula. Una fórmula en forma prenexa está en *forma normal prenexa* si su matriz está expresada como conjunción de disyunciones de literales.

existencia de forma prenexa

Dada φ siempre es posible encontrar, de forma algorítmica, al menos una ψ en forma normal prenexa tal que

$$\vdash \varphi \leftrightarrow \psi$$

Apéndice E

Polinomio interpolatorio de Lagrange

El problema de interpolar tiene una sencilla expresión en el método de Lagrange. Es la contrapartida al método de Newton, idóneo en problemas en los que se añaden puntos de interpolación a los previamente considerados. Complementariamente el método de Lagrange muestra su valor en problemas en los que se mantienen el número de puntos de interpolación y sus respectivas abscisas, siendo las ordenadas de los mismos lo mutable.

Teorema E.0.1 (*de D'Alembert*)**.** *Cualquier polinomio no nulo de grado n con coeficientes en un cuerpo tiene a lo sumo n raíces distintas en dicho cuerpo.*

Demostración. Es un sencillo ejercicio de inducción. □

Teorema E.0.2. *Sean $n_0, \ldots, n_d$ elementos distintos de un cuerpo $\mathbf{K}$ en cantidad igual a $d+1$. Para todo $0 \leq i \leq d$ existe un polinomio $h_i(x) \in K[x]$ cumpliendo:*

1. $\deg h_i(x) = d$
2. *para todo $0 \leq j \leq d$, $h_i(n_j) = \delta_{ij}$, donde δ_{ij} es la delta de Kronecker*

Demostración. En efecto, consideremos para cada $0 \leq i \leq d$:

$$g_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{d} (x - n_j)$$

que es un polinomio de $K[x]$ de grado igual a d, cumpliendo que para todo $0 \leq j \leq d$, $g_i(n_j) = 0$ siempre que $j \neq i$. Dado que $n_i \neq n_j$ siempre que $i \neq j$ y dado que K es un dominio de integridad (por ser cuerpo), para todo $0 \leq i \leq d$ se tendrá que $g_i(n_i) \neq 0$ y en consecuencia existirá $g_i(n_i)^{-1}$. Definamos finalmente, para todo $0 \leq i \leq d$, $h_i(x)$ por la siguiente igualdad:

$$h_i(x) = g_i(x)(g_i(n_i))^{-1}$$

Entonces tenemos para todo $0 \leq i \leq d$ que $\deg(h_i(x)) = \deg g_i(x) = d$ y que:

$$h_i(n_j) = g_i(n_j)(g_i(n_i))^{-1} = \begin{cases} 0, & \text{si } j \neq i \\ 1, & \text{si } j = i \end{cases}$$

y en definitiva que:

$$h_i(n_j) = \delta_{ij}$$

como queríamos demostrar. □

Corolario E.0.3. *Sean $n_0, \ldots, n_d$ elementos distintos de un cuerpo $\mathbf{K}$ en cantidad igual a $d+1$. Para todo vector $\mathbf{s} = \langle s_0, \ldots, s_d \rangle$ de $\mathbf{K}^n$ existe un único polinomio $a_{\mathbf{s}}(x) \in K[c]$ tal que:*

1. $\deg a_{\mathbf{s}}(x) \leq d$.
2. *Para todo* $0 \leq i \leq d$, $a_{\mathbf{s}}(n_i) = s_i$.

Demostración. (**Existencia**) Sea $a_{\mathbf{s}}(x)$ el polinomio de $K[x]$ definido por la igualdad:

$$a_{\mathbf{s}}(x) = \sum_{i=0}^{d} s_i h_i(x),$$

donde, para todo $0 \leq i \leq d$, $h_i(x)$ es el polinomio hallado en la demostración del Teorema E.0.2. En virtud de lo que afirma dicho resultado, $\deg a_{\mathbf{s}}(x) \leq d$ y además, para todo $0 \leq i \leq d$, $a_{\mathbf{s}}(n_i) = s_i$.
(**Unidad**) Sea ahora $g(x)$ otro polinomio cumpliendo lo que $a_{\mathbf{s}}(x)$. El polinomio $c(x) = a_{\mathbf{s}}(x) - g(x)$ tiene grado menor o igual que d y $d+1$ raíces, por lo que necesariamente debe ser el polinomio nulo (cfr. *Teorema de D'Alembert*, E.0.1), es decir, $g(x) = a_{\mathbf{s}}(x)$. □

Ejemplo E.0.1. Calcule el polinomio $u(x) \in \mathbb{Z}_{11}[x]$ que interpola a:

n_k	0	2	5
s_k	3	9	4

Solución. Consideremos los polinomios interpoladores de Lagrange:

$$\begin{aligned}
h_0(x) &= (x-2)(x-5)((0-2)(0-5))^{-1} \\
&= 10^{-1}(x-2)(x-5) \\
&= (-1)^{-1}(x-2)(x-5) \\
&= -(x-2)(x-5) \\
&= -x^2 + 7x + 1 \\
h_1(x) &= (x-0)(x-5)((2-0)(2-5))^{-1} \\
&= x(x-5)(-6)^{-1} \\
&= 5^{-1}x(x-5) \\
&= (-2)(x^2 - 5x) \\
&= -2x^2 - x \\
h_2(x) &= (x-0)(x-2)((5-0)(5-2))^{-1} \\
&= x(x-2)(4)^{-1} \\
&= 3x(x-2) \\
&= 3(x^2 - 2x) \\
&= 3x^2 + 5x
\end{aligned}$$

y entonces:

$$\begin{aligned}
u(x) &= 3(-x^2 + 7x + 1) + 9(-2x^2 - x) + 4(3x^2 + 5x) \\
&= -3x^2 - x + 3 + 4x^2 + 2x + x^2 - 2x \\
&= (-3 + 4 + 1)x^2 + (-1 + 2 - 2)x + 3 \\
&= 2x^2 - x + 3
\end{aligned}$$

o sea, $u(x) = 2x^2 - x + 3$ o, si se quiere, $u(x) = 2x^2 + 10x + 3$. □

Índice alfabético

∨ , 100
∧, 100
índice, 20
ínfimo, 25
álgebra de Boole, 97, 105
átomo, 114

alternancia, 86
antisimietría, 97
asignación, 73
axioma de elección, 26
axioma de extension, 7

biyección, 16
buen orden, 100

cadena, 24
cláusula, 86, 92
    ampliación, 92
    tautológica, 92
    vacía, 92
    unit, 92
clase de equivalencia, 15
coátomo, 114
codominio, 14
complejidad, 86
complemento relativo, 11
condición, 8
condición atómica, 8
conjunto, 7, 92
    cerrado, 82
    finitamente satisfacible, 80
    insatisfacible, 79
    satisfacible, 79
    simplete, 92
conjunto bien ordenado, 25, 100
conjunto cociente, 15
conjunto de índices, 20
conjunto de partes, 12
conjunto de sucesores, 21
conjunto finito, 24
conjunto indexado, 20
conjunto infinito, 24
conjunto ordenado, 24, 97
conjunto potencia, 12
conjunto totalmente ordenado, 24, 97
conjunto transitivo, 22
conjuntos comparables, 23
consecuencia tautológica, 137
contradicción, 76
cota superior, 98
cota inferior, 98

delta de Kronecker, 143
diferencia, 11
diferencia simétrica, 12
disjuntos, 10
disyunto, 92
dominio, 14
dualidad, 108

elemento, 7
entero, 26
enunciado proposicional, 31
enunciados atómicos, 66
epimorfismo, 112
expresión, 65
    booleana, 119
    booleana equivalente, 121
    booleana igual, 121
    expansión mediante u, 121
extesión, 17

fórmula, 70, 71
    refutable, 76
    satisfacible, 76
    proposicional, 71
    complejidad de, 72
    tautológica, 76
fórmula proposicional, 31
fórmula válida, 76
fórmulas atómicas, 66
fórmulas equivalentes, 77
fórmulas lógicamente equivalentes, 77

factorial, 34
familia, 20
familia no vacía, 20
finitariedad, 85
forma
    normal conjuntiva, 92
    normal disyuntiva, 92
forma
    normal conjuntiva, 86
    normal conjuntiva a izquierdas, 86
función, 15
función biyectiva, 16
función compuesta, 18
función característica, 18
función de elección, 26
función inclusión, 17
función inyectiva, 16
función sobreyectiva, 16
función booleana, 106
función de conmutación, 106
función de ajuste, 47
función peso, 65
función sucesor de Peano, 29
funciones booleanas, 97

gráfica, 16

hipótesis de inducción, 32
homomorfismo, 112

idempotencia, 81
identidad, 17
igualdad, 7
imagen directa, 16
imagen inversa, 16
implicación semántica, 76
intersección, 10
intersección de una familia, 20
isomorfismo, 112

Kepler, J., 39

Lamé, G., 39
lema de Zorn, 26
lenguaje
    proposicional estándard, 71
    booleano, 119
    peso, 66
    proposicional, 65
    símbolos, 66
lenguaje proposicional
    de la f.n.c. , 91
lenguaje proposicional
    de la f.n.c. , 86
ley
    ex falso sequitur quodlibet, 131
    ex toto, 132
    tertium non datur, 132
    verum sequitur ad quodlibet, 129
    de *Frege* o autodistributiva, 130
    de contraposición
        ponendo ponens, 131
        tollendo tollens, 131
    de identidad, 129
    de *a fortiori*, 129
    de *Clavius*, 131
        débil, 131
    de *Dummet*, 130
    de *Duns Scoto*, 130
        débil, 130
    de *Meredith*, 130
    de *modus ponens*, 130–132
        generalizada, 131
    de *Peirce*, 130
    de *reductio ad absurdum*
        clásica o fuerte, 130
        intuicionista o minimal, 131
    de *Tanaka*, 130
    de conmutación de premisas, 129
    de doble negación
        clásica o fuerte, 130
        intuicionista o minimal, 130
    de exportación, 132
    de importación, 132
    de reducción de premisas, 130
    de silogismo
        débil, 129
        fuerte, 129
    del dilema, 131
    trivalencia del sist. BCK, 130
ley asociativa, 110
ley de contraposición
    ponendo tollens, 131
    tollendo ponens, 131
ley de De Morgan, 111
leyes de De Morgan, 11
literal, 120
    complementario, 92
    proposicional, 72, 92
    puro, 92
longitud, 65, 86
Lucas, F., 39

máximo, 25
mínimo, 25
maximal, 25, 99
maximo, 98
mayorante, 25
minimal, 25, 99
minimo, 98
minorante , 25
modular, 103
monoide, 65
monomorfismo, 112
monotonía, 81

número entero, 26
número natural, 21
números enteros, 26

orden buen, 25
orden producto, 25, 97
orden lexicográfico, 25, 97
orden total, 24, 97

palabra, 65
palabra equilibrada, 67
palabra significativa, 66
palabra vacía, 65
pareja ordenada, 13
partición, 15
paso base, 32
paso de inducción, 32
pertenencia, 7
Pisa, L. de, 39
postulados de Huntington, 106
postulados de Peano, 29
principio
    de inconsistencia, 132
    de lectura única, 119
    de no contradicción, 132
    del *modus tollendo tollens*, 132
    del tercio excluso, 132
principio de inducción, 34
principio de inducción finita, 29
principio de dualidad, 11
principio de lectura única, 71
producto cartesiano, 13
producto cartesiano de una familia, 20
proposición, 8, 70, 71
proposición atómica, 8
proposiciones atómicas, 66
proyección, 17
proyección canónica, 17

rango, 14
razón de oro, 46
recurrencia, 39
    conjunto fundamental de soluciones, 43
    ecuación característica, 41
    lineal homogénea, 41
    lineal no homogénea, 46
    matriz compañera, 42
    orden, 41
    polinomio característico, 41
    solución, 41
reflexividad, 97
regla
    de modus ponens, 83
    de resolución proposicional, 83
relación, 13
relación antisimétrica, 24
relación de equivalencia, 15
relación de orden, 24
relación reflexiva, 15
relación simétrica, 15
relación transitiva, 15
restricción, 17
retículo, 97, 100
retículo distributivo, 102
retículo complementado, 104
retículo de las particiones, 97

síbmolos de variable proposicional, 66
símbolos, 71, 119
segmento, 66
segmento inicial, 66
segmento final, 66
segmento propio, 66
segmentos disjuntos, 66
signos, 65
simplete, 10
subconjunto, 7
subconjunto propio, 7
subfórmula, 70
sucesión, 21
sucesión de Fibonacci, 34
sucesión significativa, 66
sucesión de Fibonacci, 51
sucesor, 21
suma booleana, 12
supremo, 25
supremo, ínfimo, 99

tautología, 76
teorema de inducción, 22

teorema de recursión, 33
torres de hanoi, 58
transitividad, 97

unión, 10
unión de una familia, 20

valoración, 73

Bibliografía

[1] Biggs, N.L. *Matemática Discreta*. Vicens Vives, 1994.

[2] Boolos, G.S., Burgess, J.P., and Jeffrey, R.C. *Computability and Logic*. Cambridge University Press, fourth edition, 2003.

[3] Burris, S.N. *Logic for Mathematics and Computer Science*. Prentice-Hall, 1998.

[4] Chang C. and Lee, R.C. *Symbolic Logic and Mechanical Theorem Proving*. Academic Press, 1973.

[5] Delahaye, J.P. *Formal Methods in Artificial Intelligence*. John Wiley & Sons, 1987.

[6] Deo, N. *Graph Theory with Applications to Engineering and Computer Science*. Prentice-Hall, 1974.

[7] García Miranda, J. *Lógica para Informáticos y otras herramientas matemáticas*. Editorial Técnica Avicam, 2017.

[8] Grimaldi, R.P. *Matemática Discreta y Combinatoria*. Addison-Wesley Publishing Company, 1998.

[9] Hill, F.J. and Peterson, G.R. *Teoría de Commutación y Diseño Lógico*. Limusa, 1993.

[10] Kwak, J.H. and Hong, S. *Linear Algebra*. Springer Science+Business Media, LLC, 1948.

[11] Lipschutz, S. and Lipson, M. *2000 problemas resueltos de Matemática Discreta*. McGraw Hill, 1998.

[12] Lloyd, J.W. *Foundations of Logic Programming (Symbolic Computation: Artificial Intelligence)*. Springer-Verlag, 1987.

[13] Loveland, D.W. *Automated Theorem Proving: A Logical Basis*, volume 6 of *Fundamental Studies in Computer Science*. North-Holland Publishing Company, 1978.

[14] Permingeat, N. and Glaude, D. *Álgebra de Boole: Teoría, Métodos de Cálculo y Aplicaciones*. Vicens Vives, 1995.

[15] Rosen, K. H. *Matemática Discreta y sus Aplicaciones*. McGraw Hill, 2003.

[16] Sterling, L. and Shapiro, E. . *The Art of Prolog : advanced programming techniques*. MIT Press, 1975.

[17] Veerarajan, T. *Matemática Discreta*. McGraw Hill, 2008.

[18] Yablonsky, S.V. *Introduction to Discrete Mathematics*. Mir, 1975.