



# 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](#)

24 de septiembre de 2017



Lecciones sobre matemática discreta by [F.M. García Olmedo](#) is licensed under a [Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 Unported License](#) Permissions beyond the scope of this license may be available at [F.M. García Olmedo](#).



# Índice general

<b>1. Nociones sobre Conjuntos</b>	<b>7</b>
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 $\omega$ en $Z$ . . . . .	27
<b>2. Inducción</b>	<b>29</b>
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
<b>3. Relaciones de Recurrencia</b>	<b>37</b>
3.1. Introducción. . . . .	37
3.2. Teoría de la Recurrencia Lineal Homogénea . . . . .	39
3.3. Teoría de la Recurrencia Lineal No Homogénea . . . . .	45
3.4. Ejemplos de Recurrencia Lineal Homogénea . . . . .	49
3.5. Ejemplos de Recurrencia Lineal No Homogénea . . . . .	55
3.6. Ejercicios . . . . .	61
<b>4. Lenguajes</b>	<b>65</b>
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

<b>5. Lógica Proposicional</b>	<b>71</b>
5.1. Lenguaje Proposicional . . . . .	71
5.2. Implicación Semántica . . . . .	73
5.3. Propiedades Básicas de la Implicación Semántica . . . . .	81
5.4. Forma Normal Conjuntiva . . . . .	86
<b>A. Alfabeto Griego</b>	<b>89</b>
<b>B. Prontuario de cálculo clásico proposicional y de primer orden</b>	<b>91</b>

# Índice de figuras

3.1. Elecciones de $u_n^{(p)}$ según $f(n)$ , si $r$ no es sol. de la ecuación característica. . . . .	58
5.1. Tablas para la interpretación semántica de los símbolos lógicos . . . . .	74



# 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 conjunto 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 usualmente 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.  $\square$

*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.  $\square$

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

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

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

¿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  $b$ .  $\square$

**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:  $\emptyset$ ,  $\{\emptyset\}$ ,  $\{\{\emptyset\}\}$ ,  $\{\{\{\emptyset\}\}\}$  y  $\{\emptyset, \{\emptyset\}\}$ .

## 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.**  $\bigcup \emptyset = \emptyset$  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.  $A \cup \emptyset = A$
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.  $A \cap \emptyset = \emptyset$
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  $A \cap B = \emptyset$ .

**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.  $(A \cap B) \cup C = A \cap (B \cup C)$  *si y sólo si*  $C \subseteq A$

## 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.  $\emptyset' = E$  y  $E' = \emptyset$
3.  $A \cap A' = \emptyset$  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*,  $A \setminus B = \emptyset$ .
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.  $A + \emptyset = A$  y  $A + A = \emptyset$
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.  $\mathcal{P}(\emptyset) = \{\emptyset\}$
2.  $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$
3.  $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

**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.  $\emptyset = \bigcap_{X \in \mathcal{P}(A)} X$
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:

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

**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  $\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$ , en otras palabras,  $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$ .

**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.  $A \times B \subseteq \mathcal{P}(\mathcal{P}(A \cup B))$ .

**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  $A = \emptyset$  o  $B = \emptyset$  entonces  $A \times B = \emptyset$
5. Si  $A \subseteq X$  y  $B \subseteq Y$ , entonces  $A \times B \subseteq X \times Y$  y recíprocamente (siempre que  $A \times B \neq \emptyset$  o  $A = B = \emptyset$ )

## 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  $\emptyset$  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 esta última relación se la representa frecuentemente con el símbolo  $\nabla(X)$  o simplemente  $\nabla$  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  $\Delta$ . 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:

- $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- 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*,  $\text{dom } R$ , y su *rango* o *codominio*,  $\text{ran } R$ . Estos conjuntos quedan definidos por las siguientes igualdades:

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

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

*Ejemplo 1.6.3.*

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

*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  $X \in \mathcal{C}$ ,  $X \neq \emptyset$ .
2. Para todo  $X, Y \in \mathcal{C}$ , si  $X \neq Y$  entonces  $X \cap Y = \emptyset$  (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 cociente* 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  $x A/\mathcal{C} y$  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 equivalencia*.

**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  $\text{dom } f = X$  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

$$f: X \longrightarrow Y$$

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 llamamos función.

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

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

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

definidas como sigue:

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

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 escriben  $f$  en lugar de  $f_*$  y  $f^{-1}$  en lugar de  $f^*$ . Nosotros no seguiremos aquí tal convenio.

**Teorema 1.8.1.** Sea  $f: X \longrightarrow Y$  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.  $A \subseteq f^*(f_*(A))$

**Teorema 1.8.2.** Sea  $f: X \longrightarrow Y$  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.  $f^*(f_*(C)) \subseteq C$

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

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

1.  $f$  es sobreyectiva



2. Para todo  $B \in \mathcal{P}(Y) \setminus \{\emptyset\}$ ,  $f^*(B) \neq \emptyset$
3. Para todo  $C \subseteq Y$ ,  $f_*(f^*(C)) = C$ .

**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  $A \subseteq X$ ,  $A = f^*(f_*(A))$ .

**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 *extensión* 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  $\chi_A$ , 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.  $\chi_{A^c} = 1 - \chi_A$ .
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  $\chi_A$  es una biyección.

**Ejercicio 1.8.2.** Demostrar que:

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

**Observación 1.8.9.** Si  $f: X \rightarrow Y$  es inyectiva entonces para todo  $y \in \text{ran } f$ ,  $f^{-1}(\{y\})$  es un conjunto con un elemento, a saber,  $\{x\}$ . En esta situación tiene sentido la siguiente definición.

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

**Definición 1.8.8.** Sean  $X, Y$  y  $Z$  conjuntos y  $f: X \rightarrow Y$  y  $g: W \rightarrow Z$  funciones tales que  $\text{ran } f \subseteq \text{dom } g$  entonces representamos por  $g \circ f$  a la función de  $X$  en  $Z$  definida como  $g \circ f(x) = g(f(x))$  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  $f: X \rightarrow Y$ ,  $g: Y \rightarrow Z$  y  $h: Z \rightarrow U$  tres aplicaciones. Entonces

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

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

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

**Definición 1.8.9.** Sea  $f: X \rightarrow Y$  una aplicación. Si  $g: Y \rightarrow X$  es tal que  $g \circ f = I_X$  entonces a  $g$  se le denomina *inversa a izquierda* de  $f$  o *sección*. Si existe  $h: Y \rightarrow X$  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  $f: X \rightarrow Y$  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  $f: X \rightarrow Y$  una función. Entonces son equivalentes las siguientes afirmaciones:

1.  $f$  es biyectiva
2. Existe  $g: Y \rightarrow X$  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  $f: \{a\} \rightarrow \{b, c\}$  definida por  $f(a) = b$  es inyectiva no sobreyectiva y sin embargo sólo tiene una inversa a izquierda, que es  $g: \{b, c\} \rightarrow \{a\}$  definida por  $f(b) = f(c) = a$ .

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

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

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

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

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

1.  $f \circ p_A = p_C \circ (f \times g)$
2.  $g \circ p_B = p_D \circ (f \times g)$

*Ejercicio 1.8.3.*

1. Sean  $f: A \rightarrow C$ ,  $g: B \rightarrow D$ ,  $h: C \rightarrow E$  y  $k: D \rightarrow F$ . 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  $f: X \rightarrow Y$  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  $f: X \rightarrow Y$  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  $f: X \rightarrow Y$  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  $f: X \rightarrow Y$  una aplicación. Si  $xRy$  implica  $f(x) = f(y)$ , entonces existe una única aplicación  $g: X/R \rightarrow Y$  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  $f: X \rightarrow Y$  una aplicación. Si  $\pi_{R_f}$  es la proyección canónica de  $X$  sobre  $X/R_f$  e  $i$  es la inclusión de  $\text{ran } f$  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  $x: I \rightarrow X$  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  $C$  es el rango de una familia. Para ello basta tomar como conjuntos de índices al propio conjunto  $C$ .
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 vacío 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.  $(\bigcup_{i \in I} A_i) \cap (\bigcup_{j \in J} B_j) = \bigcup_{(i,j) \in I \times J} (A_i \cap B_j)$
2. Si ambas familias son no vacías, entonces  $(\bigcap_{i \in I} A_i) \cup (\bigcap_{j \in J} B_j) = \bigcap_{(i,j) \in I \times J} (A_i \cup B_j)$

*Observación 1.9.3.* Usualmente se escribe  $\bigcup_{i,j}$  en lugar de  $\bigcup_{(i,j) \in I \times J}$ .

**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  $\emptyset$  por el símbolo 0. En realidad este convenio notacional es parte de otro más amplio. Por ejemplo:

1.  $0 = \emptyset$
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). *Existe 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  $\omega$  a la intersección de todos los conjuntos de sucesores incluidos en  $A$ . Por su parte  $\omega^*$  será la abreviatura de  $\omega \setminus \{0\}$ .

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

**Definición 1.10.4.** Un *número natural* es cualquier elemento de  $\omega$ .

**Definición 1.10.5.** Una *sucesión* es cualquier familia cuyo conjunto de índices es  $\omega$  o un elemento de  $\omega$ . 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  $\omega$  tiene las siguientes propiedades:*

P1)  $0 \in \omega$

P2) Si  $n \in \omega$ , entonces  $n^+ \in \omega$ .

P3) 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  $n \not\subseteq m$ .*

**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  $f: X \rightarrow X$ . Existe una función  $u: \omega \rightarrow X$  tal que  $u(0) = a$  y que para todo  $n \in \omega$ ,  $u(n^+) = f(u(n))$ .*

**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.  $\omega$  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  $f: \omega \rightarrow \omega$  definida como  $f(k) = k^+$ . Existe una aplicación  $s_m: \omega \rightarrow \omega$  tal que  $s_m(0) = m$  y  $s_m(n^+) = (s_m(n))^+$ .*

*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  $p_m: \omega \rightarrow \omega$  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  $e_m: \omega \rightarrow \omega$  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  $\omega$  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  $f: n \rightarrow E$  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.**  $\omega$  es infinito.

**Lema 1.12.11.** Si  $E$  es biyectivo con dos números naturales, entonces estos 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  $\text{dom } f \subseteq \text{dom } g$  y  $f(x) = g(x)$ , para todo  $x \in \text{dom } f$  —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.,  $(a \neq c \text{ y } a \leq_1 c)$  o  $(a = c \text{ y } b \leq_2 d)$ .

**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 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 esto 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  $f: I \rightarrow \bigcup_{i \in I} A_i$  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  $\boxminus$  como sigue:

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

*Observación 1.15.1.* Las respectivas definiciones de  $\boxplus$  y  $\boxminus$  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.  $\langle m_1 u_1 + n_1 v_1, m_1 v_1 + n_1 u_1 \rangle \sim \langle m_2 u_2 + n_2 v_2, m_2 v_2 + n_2 u_2 \rangle$

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

## 1.16. Inmersión de $\omega$ 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.  $j(nm) = j(n) \boxtimes j(m)$

**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.  $\boxtimes$ ).

*Ejercicio 1.16.2.* Demostrar que:

1.  $\boxplus$  y  $\boxtimes$  son asociativas y conmutativas
2.  $\boxtimes$  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<sup>1</sup> 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  $\omega$ . 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.

---

<sup>1</sup>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 pertenecer 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  $S = \emptyset$ . Ello concluye la demostración.  $\square$

*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<sup>2</sup>  $n$  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  $0 = \emptyset$ , 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  $J = \emptyset$  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,  $\{0, \dots, j_0 - 1\} \subseteq P$  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  $J = \emptyset$  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.  $\square$

*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  $\emptyset \subseteq P$ , por lo que en virtud de la condición (2.1) se debe cumplir  $\emptyset \in P$ , 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  $P = \omega$ .

---

<sup>2</sup>Según el modelo que tenemos de  $\omega$ , también representado como  $\omega$ ,  $0 = \emptyset$  y si  $n \neq 0$  entonces  $n = \{0, \dots, n-1\}$ .

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:

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

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  $P = \omega$ .  $\square$

**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  $A = \emptyset$ . Tenemos así una demostración de la afirmación contrarrecíproca del principio del buen orden, es decir, dicho principio es válido.  $\square$

**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**).  $\square$

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  $k \in \omega$  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  $Q$  pertenece  $s(k) = i + 1$  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  $i_0 \leq i$ .  $\square$

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

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

*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:

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

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

*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.  $\square$

**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  $i_0 \leq i$ .  $\square$

**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.  $\square$

## 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  $f: X \rightarrow X$  una función. Existe una única función  $u: \omega \rightarrow X$  tal que  $u(0) = a$  y que para todo  $n \in \omega$ ,  $u(n^+) = f(u(n))$ .*

*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 debería 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  $\text{dom } u = \omega$  y  $\text{ran } u \subseteq X$ . 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

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

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 que  $u$  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  $f : x \rightarrow x$  definida como  $f(n, m) = \langle nm, n^+ \rangle$ . El teorema afirma que existe una única función

$$u : \omega \rightarrow \omega \times \omega$$

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

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

$$u : \omega \rightarrow \omega \times \omega \times \omega$$

que cumple  $u(0) = \langle 0, 1, 0 \rangle$  y  $u(s(n)) = f(u(n))$ , para todo  $n \in \omega$ . Llamemos  $v$  a la composición  $\pi_1 \circ f$ , donde  $\pi_1$  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:

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

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:

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$$

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. Todo número natural mayor que 1 es divisible por al menos un número primo.
7. Usar el teorema de inducción para demostrar que  $3^n + 7^n - 2$  es divisible por 8, para  $n \geq 1$ .
8. Usar el teorema de inducción para demostrar que  $n^3 + 2n$  es divisible por 3, para  $n \geq 1$ .
9. 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.
10. 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.
11. 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.
12. Sea  $N$  un número natural y sea  $S$  un conjunto de números naturales menores que  $N$ . Demuestre que o  $S$  es vacío o  $S$  tiene máximo.
13. Demuestre que para todo número natural  $n$ ,  $8^n - 3^n$  es múltiplo de 5.
14. Demuestre que para todo número natural  $n$ ,  $3^{4n} - 1$  es múltiplo de 5.

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

16. Sea  $p$  la función dada por:

$$p(a, 1) = a,$$

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

Demuestre por inducción que  $p(a, b) = a \cdot b$ , para todo  $1 \leq a, b$ .

17. Sea  $e$  la función dada por:

$$e(a, 0) = 1,$$

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

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

18. Demuestre que para todo número natural  $n$ :

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

19. Demuestre que para para todo número natural  $n$  se cumple:

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

20. 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 cantidad de céntimos superior a 13.

21. 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:

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

22. 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:

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

## 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  $a_0, \dots, a_{n-1}$ . 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*:

$F_{n+2} = F_{n+1} + F_n$ ,  $n \geq 0$ ;  $F_0, F_1 = 1$ , 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 para 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,  $u_0, u_1, \dots, u_{n-1}$ , 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:

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

La sucesión  $\{x_n\}$  sugerida por:

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

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  $x_n = c \cdot a^n$ . Demostremos por inducción que esto es así. En efecto, (paso base) para  $n = 0$ ,  $x_0 = ca^0 \cdot 1 = c$ . 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:

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

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.  $\square$

*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:

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k}, \text{ para todo } n \geq k \quad (3.3)$$

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

$$p(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k \quad (3.4)$$

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

$$x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k = 0 \quad (3.5)$$

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  $\sum_{i=0}^k a_i x_{n-i} = 0$ , 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:

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

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 propios 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 recurrencia 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 recurrencia 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  $f(\{x_n\}) = \langle x_{k-1}, \dots, x_1, x_0 \rangle$ . Así definida,  $f$  es una aplicación lineal. Por otra parte,  $f$  es biyectiva puesto que dados unos valores iniciales  $x_{k-1}, \dots, x_1, x_0$ , 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*.

**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  $c_0, \dots, c_k$  escalares para todo  $0 \leq i \leq k$ . Si

$$\sum_{i=0}^k c_i n^i = 0 \quad (3.6)$$

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

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

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

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

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

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

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

donde  $\mathbf{c} = (c_0 \ c_1 \ \dots \ c_k)^t$ , es compatible determinado y no tiene más que la solución nula, es decir, para todo  $0 \leq i \leq k$  se cumple  $c_i = 0$ .  $\square$

**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  $r_1, \dots, r_t$
2. y para todo  $1 \leq i \leq t$ , la multiplicidad de  $r_i$  es  $m_i$  y  $1 \leq m_i$  (si  $A$  es diagonalizable,  $m_1 + \dots + m_t = k$ ).

Entonces:

$$\langle \{r_i^n\}, \{nr_i^n\}, \dots, \{n^{m_i-1}r_i^n\} : 1 \leq i \leq t \rangle$$

es un sistema fundamental del conjunto de soluciones.

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

$$p(x) = x^k - a_1x^{k-1} - a_2x^{k-2} - \dots - a_{k-1}x - a_k$$

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

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

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

$$\begin{aligned} P_1(x) &= x^{n-k}p(x) \\ &= x^n - a_1x^{n-1} - \dots - a_{k-1}x^{n-k+1} - a_kx^{n-k} \end{aligned}$$

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:

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

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  $\{r_i^n\}, \{nr_i^n\}, \dots, \{n^{m_i-1}r_i^n\}$  son  $m_i$  soluciones de la relación de recurrencia. Más aún, son linealmente independientes pues si

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

conlleva que para todo natural  $n$ :

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

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.  $\square$

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

- *su ecuación característica (ecuación 3.5) tiene  $t$  raíces distintas:  $r_1, \dots, r_t$ ,*
- *para todo  $1 \leq i \leq t$ , la multiplicidad de  $r_i$  es  $m_i$  y  $1 \leq m_i$ ,*
- *$m_1 + \dots + m_t = k$*
- *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  $\alpha_{ij}$ , tales que para todo natural  $n$ :*

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

**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:

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

$\square$

**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:

$$\mathbf{P} = [\mathbf{v}_1 \ \mathbf{v}_2] = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 1 & 1 \end{pmatrix} \quad \mathbf{P}^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -\frac{1-\sqrt{5}}{2} \\ -1 & \frac{1+\sqrt{5}}{2} \end{pmatrix}$$

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*.  $\square$

### 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:

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + f(n), \text{ para todo } n \geq k \quad (3.8)$$

donde  $a_1, \dots, a_k$  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:

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

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  $n$ .  $\square$

**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:

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

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:

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

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:

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

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:*

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

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:

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

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

$$sx_{n-1} - a_1sx_{n-2} - a_2sx_{n-3} - \cdots - a_ksx_{n-(k-1)} = q(n-1)s^{n-1}s = q(n-1)s^n \quad (3.13)$$

Restando de la **igualdad 3.12** la **igualdad 3.13** resulta:

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

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:

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

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:

$$(x^k - a_1 x^{k-1} - \cdots - a_k)(x - s)$$

□

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

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + q(n)s^n, \quad (3.15)$$

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 homogénea cuya ecuación característica es

$$(x^k - a_1 x^{k-1} - \cdots - a_k)(x - s)^{d+1} = 0$$

*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:

$$(x^k - a_1 x^{k-1} - \cdots - a_k)(x - s) = 0$$

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:

$$(x^k - a_1 x^{k-1} - \cdots - a_k)(x - s) = 0$$

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:

$$(x^k - a_1 x^{k-1} - \cdots - a_k)(x - s)(x - s)^d = 0$$

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

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

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + q(n)s^n, \quad (3.16)$$

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:

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

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:

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

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

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

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

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

y en caso negativo, la expresión es:

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

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

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

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:

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

y en todo caso

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



□

*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:  $r_1, \dots, r_k$ , la expresión 3.7 se concreta en:

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

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,  $F_n = \left(\frac{1+\sqrt{5}}{2}\right)^n$  y  $F_n = \left(\frac{1-\sqrt{5}}{2}\right)^n$  son soluciones; además, son linealmente independientes, pues una no es múltiplo de la otra. De este modo

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

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:

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

lo que nos lleva a:

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

por lo que la solución particular es para todo natural  $n$ :<sup>1</sup>

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

□

*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:

$$Re(z) = x \quad Im(z) = y$$

3. Para todo número complejo  $z$  existen un número real  $r_z$  y un ángulo  $\theta_z$ , expresado en radianes, tal que:

$$z = r_z(\cos \theta_z + i \sin \theta_z)$$

4. Dado un número complejo  $z$ ,

$$\begin{aligned} r_z &= |z| \\ \theta_z &= \begin{cases} 2 \arctan \frac{Im(z)}{Re(z)+|z|} & , \text{ si } z \notin \mathbb{R}^- \\ \pi & , \text{ si } z \in \mathbb{R}^- \end{cases} \end{aligned}$$

5. El *Teorema de DeMoivre* que dice que si  $z = r(\cos \theta + i \sin \theta)$  y  $n \in \mathbb{N}$  entonces:

$$z^n = r^n(\cos n\theta + i \sin n\theta)$$

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

---

<sup>1</sup>Observar que para  $n = 0$  aún tiene sentido  $2^0 + 0 \cdot 2^{-1}$  y es  $1 + 0 \cdot \frac{1}{2} = 1$ .

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

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

y sabemos que  $\arctan(1/\sqrt{3}) = \pi/6$ . Multiplicando 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:  $|z| = \sqrt{2}$ ,  $\operatorname{Re}(z) = 1$  e  $\operatorname{Im}(z) = 1$ . Se tiene lo siguiente:

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

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.  $\square$

**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  $u_{12} = 31250$ .  $\square$

**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 resolvemos usando la inducción. Se tiene:

$$\begin{aligned} x_0 &= 1 \\ x_1 &= 1 \cdot x_0 = 1 \\ x_2 &= 2x_1 = 2 \cdot 1 \\ x_3 &= 3x_2 = 3 \cdot 2 \cdot 1 \\ x_4 &= 4x_3 = 4 \cdot 3 \cdot 2 \cdot 1 \\ &\vdots \quad \quad \quad \vdots \end{aligned}$$

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

**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:

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

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

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  $f(n) = b_t n^t + b_{t-1} n^{t-1} + \dots + b_1 n + b_0$  estamos en el caso particular  $s = 1$  de  $f(n) = (b_t n^t + b_{t-1} n^{t-1} + \dots + b_1 n + b_0) s^n$ .
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  $x_n^{(p)} = c_2 n^2 + c_1 n + c_0$ .
2. Si  $f(n) = 5^n(3n^2 + 2n + 1)$ , entonces  $x_n^{(p)} = 5^n(c_2 n^2 + c_1 n + c_0)$ .
3. Si  $f(n) = 5^n$ , entonces  $x_n^{(p)} = c5^n$  (¿por qué?).
4. Si  $f(n) = 2^n(3n + 1)$ , entonces  $x_n^{(p)} = 2^n n(c_1 n + c_2)$  (¿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  $x_n^{(p)} = 3^n c n^2$ .
2. Si  $f(n) = 3^n(5n + 1)$ , entonces  $x_n^{(p)} = 3^n n^2(c_1 n + c_0)$ .
3. Si  $f(n) = 2^n(5n + 1)$ , entonces  $x_n^{(p)} = 2^n(c_1 n + c_0)$ .

**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 multiplicidad 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:

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

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  $x_n^{(h)} = c_1 1^n = c_1$ , 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  $x_n = 2^n - 1$ ,  $n \geq 0$ . □

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

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

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

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

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:

$$u_0 = 2,$$

$$u_1 = 2,$$

$$u_n = u_{n-2} + 2^n + (-1)^n, \text{ siempre que } n \geq 2.$$

*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  $\pm 1$ . 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:

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

$f(n)$	$u_n^{(p)}$ 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 positivo	$c_t n^t + c_{t-1} n^{t-1} + \cdots + c_0$
$cr^n$ , $r$ 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.

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:

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

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,

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

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:

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

y de aquí al siguiente sistema:

$$\begin{cases} c_1 + c_2 = \frac{2}{3} \\ c_2 - c_1 = -\frac{1}{6} \end{cases}$$

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

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

y entonces la solución es:

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

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:

$$x_n^{(h)} = c_1 + nc_2$$

$$x_n^{(p)} = c_3(-2)^n$$

En esta situación está claro que:

$$x_{n+2}^{(p)} = c_3(-2)^{n+2}$$

$$= 4c_3(-2)^n$$

$$x_{n+1}^{(p)} = c_3(-2)^{n+1}$$

$$= -2c_3(-2)^n$$

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:

$$0 = \frac{4}{9} + 0c_2 + c_1 \quad \Rightarrow c_1 = -\frac{4}{9}$$

$$1 = \frac{4}{9}(-2) + c_2 - \frac{4}{9} \quad \Rightarrow c_2 = \frac{7}{3}$$

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:

$$1 = \frac{4}{9} + 0c_2 + c_1 \quad \Rightarrow c_1 = -\frac{5}{9}$$

$$0 = \frac{4}{9}(-2) + c_2 - \frac{5}{9} \quad \Rightarrow c_2 = \frac{3}{9}$$

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 aritmética*). (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.  $r_2 = \sqrt{2\sqrt{2}}$  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:

$$u_{n+2} = -4u_n - 3u_n + 5(-2)^n$$

(sol.  $x_n = c_1(-3)^n + c_2(-1)^n - 5(-2)^n$ )

10. Resuelva la relación de recurrencia:

$$u_{n+2} = -4u_n - 3u_n + 6 \cos \frac{n\pi}{2} + 3 \sin \frac{n\pi}{2}$$

$$(\text{sol. } x_n = 2^n (c_1 \cos \frac{n\pi}{2} + c_2 \sin \frac{n\pi}{2}) + 2 \cos \frac{n\pi}{2} + \sin \frac{n\pi}{2})$$

11. Resuelva la relación de recurrencia:

$$u_{n+2} = -4u_n + 6 \cos \frac{n\pi}{2} + 3 \sin \frac{n\pi}{2}$$

$$(\text{sol. } x_n = 2^n (k_1 \cos \frac{n\pi}{2} + k_2 \sin \frac{n\pi}{2} + 2 \cos \frac{n\pi}{2} + \sin \frac{n\pi}{2})$$

12. Resuelva la relación de recurrencia:

$$u_{n+2} = 6u_{n+1} - 9u_n + 3^n$$

$$(\text{sol. } x_n = (c_1 + c_2 n + \frac{n^2}{18})3^n)$$

13. Resuelva la relación de recurrencia:

$$u_{n+3} = -5u_{n+2} - 8u_{n+1} - 4u_n = 2(-1)^n + (-2)^{n+3}$$

$$(\text{sol. } x_n = (1 - 2n)(-1)^n + (3 + 2n + n^2)(-2)^n)$$

14. Resuelva el siguiente problema de recurrencia:

$$u_n - 2u_{n-1} = (n + 5)3^n \quad (3.26)$$

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 (exactamente 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  $M = \langle M, \circ, e \rangle$  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  $L_0(S)$  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*  $\emptyset$  es el elemento neutro en  $L_0(S)$ . La *longitud* de  $A \in L_0(S)$ , en símbolos  $l(A)$ , 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  $\emptyset$  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  $l(AB) = l(A) + l(B)$ .

**Definición 4.1.3.** Sea  $S$  un conjunto no vacío y supongamos que hay dada una aplicación  $n: S \rightarrow \omega$ . Notaremos con el mismo símbolo a su única extensión homomórfica a  $L_0(S)$  en  $\omega$ .  $n$  es llamada *función peso*.

*Observación 4.1.3.* Se tiene que  $n(AB) = n(A) + n(B)$  y entonces:

$$n(A) = \begin{cases} 0 & , \text{ si } A = \emptyset \\ \sum_{i=0}^k n(s_i) & , \text{ si } A = \langle s_i \rangle_{0 \leq i \leq k} \end{cases}$$

*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*  $L$  es una terna  $\langle X, Cons, a \rangle$  donde:

- $X \neq \emptyset$ ; 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  $Cons \cap X = \emptyset$ .
- $a$  es una aplicación  $a: Cons \rightarrow \omega^*$ .
- $S(\mathbf{L}) = X \cup Cons$  es el conjunto de *símbolos* del lenguaje.
- $Exp(\mathbf{L})$  abreviará al conjunto  $L(S(\mathbf{L}))$ .
- El *peso* asociado al lenguaje  $\mathbf{L}$  es  $n: S(\mathbf{L}) \rightarrow \omega$  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,  $A' = \emptyset$  (resp.  $A'' = \emptyset$ ). Si  $l(A') = k$ , 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  $n: S \rightarrow \omega$  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  $n(A_i) = 0$
2. existen  $p \in \omega^*$ ,  $i_1, \dots, i_p < i$  y  $f \in S$  tales que  $n(f) = p$  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  $n: S \rightarrow \omega$  una función peso. Son equivalentes las siguientes afirmaciones:

1. Existe al menos una palabra significativa según  $n$  en  $L_0(S)$
2.  $n^*(\{0\}) \neq \emptyset$

*Demostración.* Sea  $A$  una palabra significativa según  $n$  en  $L_0(S)$ . 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  $n(A_0) = 0$ , por lo que  $n^*(\{0\}) \neq \emptyset$ . Recíprocamente, si  $n^*(\{0\}) \neq \emptyset$ , sea  $s \in S$  tal que  $n(s) = 0$ . 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.  $\square$

**Lema 4.2.2.** Sea  $n: S \rightarrow \omega$  una función peso. Si  $A_1, \dots, A_p$  son palabras significativas de  $L_0(S)$  respecto a  $n$  y  $f \in S$  tal que  $n(f) = p$ , 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  $n: S \rightarrow \omega$  una función peso. Una palabra  $A$  de  $L_0(S)$  es *equilibrada* respecto a  $n$  sii, por definición, cumple las siguientes propiedades:

1.  $l(A) = n(A) + 1$
2. para todo segmento inicial propio y no vacío  $C$  de  $A$  se cumple  $l(C) \leq n(C)$ .

*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  $l(C) \leq n(C)$ ” pues  $l(\emptyset) = 0 = n(\emptyset)$ .

*Observación 4.3.2.* En virtud de la condición 1) en la Definición 4.3.1 es evidente que si  $A$  es equilibrada entonces  $A \neq \emptyset$ .

**Teorema 4.3.1.** Sea  $n: S \rightarrow \omega$  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  $0 = n(A_0)$  (Definición 4.2.1);  $A_0$  es equilibrada porque  $l(A_0) = 1$  y  $n(A_0) = 0$ . Supongamos que  $0 < k$  y que el resultado está establecido para todo  $0 \leq j < k$ . Si  $n(A_k) = 0$ , 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  $n(f) = p$  y para 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:

$$\begin{aligned}
 l(A_k) &= 1 + \sum_{j=1}^p l(B_j) \\
 &= 1 + \sum_{j=1}^p (n(B_j) + 1) \\
 &= 1 + p + \sum_{j=1}^p n(B_j) \\
 &= 1 + n(A_k)
 \end{aligned}$$

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  $D = \emptyset$ , entonces  $C = f$  y  $l(C) = 1 \leq p = n(C)$ . Si  $D \neq \emptyset$  entonces  $D$  es un segmento inicial propio y no vacío de la palabra significativa  $B_1$ :

$$\begin{aligned}
 l(C) &= 1 + l(D) \\
 &\leq p + n(D) \\
 &= n(f) + n(D) \\
 &= n(fD) \\
 &= n(C)
 \end{aligned}$$

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:

$$\begin{aligned}
 l(C) &= 1 + \left( \sum_{j=1}^q l(B_j) \right) + l(D) \\
 &\leq 1 + \left( \sum_{j=1}^q n(B_j) + 1 \right) + n(D) \\
 &\leq p + \left( \sum_{j=1}^q n(B_j) \right) + n(D) \\
 &= n(C)
 \end{aligned}$$

□

El enunciado recíproco del **Teorema 4.3.1** es cierto. Para su demostración son necesarios algunos resultados previos.

**Lema 4.3.2.** *Sea  $n: S \rightarrow \omega$  una función peso y  $A$  una palabra de  $L(S)$  equilibrada según  $n$ . Para todo número natural  $k$  tal que  $0 \leq k < l(A)$ , 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  $0 < l(A)$  (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  $l(B) = k$  y  $l(C) = q$ ; así pues  $q = l(A) - k$  y por tanto  $0 < q$ . Para todo  $0 \leq i \leq q$ , sea  $C_i$  el segmento inicial de longitud  $i$  de  $C$ .<sup>1</sup> Sea

$$X = \{j \in \omega : 0 < j \leq q \text{ y para todo } 0 \leq h < j, l(C_h) \leq n(C_h)\}$$

Se tiene que  $X \neq \emptyset$ , pues  $0 = l(C_0) \leq n(C_0) = 0$ , es decir,  $1 \in X$ ; además  $X$  es finito (sus elementos no superan el valor  $q$ ). Si  $i = \max X$ , se cumple que  $l(C_{i-1}) \leq n(C_{i-1})$  y  $l(C_i) \geq n(C_i) + 1$ . 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:

$$\begin{aligned}
 n(C_i) + 1 &\leq l(C_i) \\
 &= l(C_{i-1}) + 1 \\
 &\leq n(C_{i-1}) + 1 \\
 &\leq n(C_i) + 1
 \end{aligned}$$

de lo que se deduce  $l(C_i) = n(C_i) + 1$ . 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  $n: S \rightarrow \omega$  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  $n(f) = p$ , siempre que  $1 < l(A)$ .

<sup>1</sup> Como  $B$  es un segmento inicial propio de  $A$  (recuérdese que  $k < l(A)$ ), se tiene:

$$l(C_q) = l(A) - l(B) \geq n(A) + 1 - n(B) = n(C_q) + 1$$

*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:

$$k(i) = \begin{cases} 1 & , \text{ si } i = 1 \\ 1 + \sum_{j < i} l(A_j) & , \text{ si } i > 1 \end{cases}$$

Por otra parte:

$$\begin{aligned} 1 + \sum_{i=1}^p l(A_i) &= l(A) \\ &= n(A) + 1 \\ &= n(f) + \left( \sum_{i=1}^p n(A_i) \right) + 1 \\ &= n(f) + \left( \sum_{i=1}^p (l(A_i) - 1) \right) + 1 \end{aligned}$$

de donde se deduce que  $n(f) = p$ . 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.  $\square$

*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  $n: S \rightarrow \omega$  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  $l(A)$ . Si  $l(A) = 1$ , 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  $1 < l(A)$  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  $n(f) = p$  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.  $\square$

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  $n: S \rightarrow \omega$  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  $l(A) = 1$ .
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  $n(f) = p$ , siempre que  $1 < l(A)$ .

## 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:

$$\begin{aligned}\Phi_0 &= X \\ \Phi_{i+1} &= \Phi_i \cup \{fA_1 \cdots A_p : f \in Cons \text{ y } n(f) = p \text{ y } A_1, \dots, A_p \in \Phi_i\}\end{aligned}$$

y finalmente:

$$P(\mathbf{L}) = \bigcup_{i=0}^{\infty} \Phi_i$$

**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  $\text{Exp}(\mathbf{L})$ . 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  $l(A)$ . Si  $l(A) = 1$ , por el [Corolario 4.3.5](#) sabemos que  $A \in S(\mathbf{L})$  y que  $n(A) = 0$ , por tanto  $A \in X = \Phi_0$ . Supongamos que  $1 < l(A)$  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  $1 \leq i \leq p$  se cumple que  $A_i$  es una palabra significativa según  $n$  y donde  $n(f) = p$ . Por la hipótesis de inducción, para todo  $1 \leq i \leq p$  existe  $k_i$  tal que  $A_i \in \Phi_{k_i}$ . Sea  $k = \max\{k_1, \dots, k_p\}$ ; se cumple entonces que para todo  $1 \leq i \leq p$ ,  $A_i \in \Phi_k$  y por tanto,  $A \in \Phi_{k+1}$ . En definitiva, hemos concluido 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](#).  $\square$

**Definición 4.4.3.** Sea  $\mathbf{L} = \langle X, Cons, a \rangle$  un lenguaje proposicional,  $f \in Cons$  tal que  $n(f) = p$  y  $\Gamma \subseteq \text{Exp}(\mathbf{L})$ .  $\Gamma$  es cerrado para  $f$  sii, por definición, para todo  $A_1, \dots, A_p \in \Gamma$ ,  $fA_1 \cdots A_p \in \Gamma$ .  $\Gamma$  es cerrado para  $Cons$  sii, por definición,  $\Gamma$  es cerrado para cada  $f \in Cons$ .

**Teorema 4.4.2.** Sea  $\mathbf{L} = \langle X, Cons, a \rangle$  un lenguaje proposicional. Entonces:

$$P(\mathbf{L}) = \bigcap \{\Gamma \subseteq \text{Exp}(\mathbf{L}) : X \subseteq \Gamma \text{ y } \Gamma \text{ es cerrado para } Cons\}$$

*Demostración.* Existe al menos un subconjunto de  $\text{Exp}(\mathbf{L})$  cerrado para  $Cons$  que contiene a  $X$ , a saber,  $P(\mathbf{L})$ . Por tanto  $\bigcap \{\Gamma \subseteq \text{Exp}(\mathbf{L}) : X \subseteq \Gamma \text{ y } \Gamma \text{ es cerrado para } Cons\}$  existe y es un subconjunto de  $P(\mathbf{L})$ . Recíprocamente, si  $\Gamma \subseteq \text{Exp}(\mathbf{L})$ ,  $X \subseteq \Gamma$  y  $\Gamma$  es cerrado para  $Cons$  entonces evidentemente contiene como subconjunto a  $P(\mathbf{L})$ . Así pues,  $P(\mathbf{L})$  es subconjunto de  $\bigcap \{\Gamma \subseteq \text{Exp}(\mathbf{L}) : X \subseteq \Gamma \text{ y } \Gamma \text{ es cerrado para } Cons\}$   $\square$

**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  $\text{sub}(A)$ , es por definición:

$$\text{sub}(A) = \begin{cases} \{A\}, & \text{si } A \in X, \\ \{A\} \cup (\bigcup_{i=1}^r \text{sub}(A_i)), & \text{si } n(f) = r \text{ y } A = fA_1 \cdots A_r \end{cases}$$

Sea  $f \in Cons$ , si  $n(f) = r$  entonces  $f \in A$  significa que existen  $A_1, \dots, A_r \in \text{sub}(A)$  tales que  $fA_1 \cdots A_r \in \text{sub}(A)$ .

## Capítulo 5

# Lógica Proposicional

### 5.1. Lenguaje Proposicional

**Definición 5.1.1.** Un *lenguaje proposicional standard* es un lenguaje proposicional  $\mathbf{L} = \langle X, Cons, a \rangle$  cumpliendo que:

- $X$  es infinito numerable. Sus elementos son representados con las primeras letras minúsculas del alfabeto latino, subindicándolas si fuese preciso:  $a, b, c, a_0, a_1, a_2$ , etc.
- $Cons = \{N, C\}$ .
- $a(N) = 1$  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.* Sea  $\mathbf{L}$  el lenguaje proposicional standard y consideremos la siguiente sucesión de conjuntos definida recursivamente:

$$\begin{aligned}\Phi_0 &= X \\ \Phi_{i+1} &= \Phi_i \cup \{C\alpha\beta : \alpha, \beta \in \Phi_i\} \cup \{N\alpha : \alpha \in \Phi_i\}\end{aligned}$$

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:

$$P(\mathbf{L}) = \bigcup_{i=0}^{\infty} \Phi_i$$

Por tanto, son *fórmulas proposicionales* del lenguaje proposicional:

- Cada uno de los símbolos de variable proposicional,
- la expresión  $N\alpha$ , siempre que  $\alpha$  sea fórmula proposicional y
- la expresión  $C\alpha\beta$ , siempre que  $\alpha$  y  $\beta$  sean fórmulas proposicionales.

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  $\Phi_0$  en el lenguaje proposicional standard.  $\square$

**Definición 5.1.2.** Para cualesquiera fórmulas  $\alpha$  y  $\beta$ , usaremos las siguientes representaciones:

- $(\neg\alpha)$  por  $N\alpha$ .
- $(\alpha \rightarrow \beta)$  por  $C\alpha\beta$ .
- $A\alpha\beta$  por  $CN\alpha\beta$ .
- $(\alpha \vee \beta)$  por  $((\neg\alpha) \rightarrow \beta)$ , es decir, por  $CN\alpha\beta$ .
- $K\alpha\beta$  por  $NC\alpha N\beta$ .
- $(\alpha \wedge \beta)$  por  $(\neg(\alpha \rightarrow (\neg\beta)))$ , es decir, por  $NC\alpha N\beta$ .
- $E\alpha\beta$  por  $NCC\alpha\beta NC\beta\alpha$ .
- $(\alpha \leftrightarrow \beta)$  por  $((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha))$ , 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.** Se llama *literal* a cualquier símbolo de variable  $a$  o a la forma  $N\alpha$ , para cualquier símbolo de variable  $a$ , y no hay otros literales que estos.

**Definición 5.1.4** ( $V(\varphi)$ ). Para cualquier fórmulas proposiconal  $\varphi$  definimos el conjunto de símbolos de variable que intervienen en  $\varphi$ , en símbolos  $V(\varphi)$ , como sigue:

$$V(\varphi) = \begin{cases} V(a) & , \text{ si } \varphi = a \in X \\ V(\alpha) & , \text{ si } \varphi = N\alpha \\ V(\alpha) \cup V(\beta) & , \text{ si } \varphi = C\alpha\beta \end{cases}$$

Si  $Y$  es un conjunto de fórmulas,  $V_*(Y)$  es, por definición, el conjunto:

$$\bigcup \{V(\varphi) : \varphi \in Y\}$$

**Definición 5.1.5** ( $\text{Com}(\varphi)$ ). Para cualquier fórmula proposiconal  $\varphi$  definimos la *complejidad* de  $\varphi$ , en símbolos  $\text{Com}(\varphi)$ , como sigue:

1.  $\text{Com}(a) = 0$ , para todo símbolo de variable  $a$ .
2.  $\text{Com}(N\alpha) = 1 + \text{Com}(\alpha)$ , siempre que  $\alpha$  sea fórmula proposiconal.
3.  $\text{Com}(C\alpha\beta) = 1 + \text{Com}(\alpha) + \text{Com}(\beta)$ , siempre que  $\alpha$  y  $\beta$  sean fórmulas proposiconales.



## 5.2. Implicación Semántica

**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.

*Observación 5.2.1.* 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:

- $v(\neg\alpha) = v(\alpha) + 1$
- $v(\alpha \rightarrow \beta) = v(\alpha)v(\beta) + v(\alpha) + 1$

y en consecuencia:

- $v(\alpha \vee \beta) = v(\alpha)v(\beta) + v(\alpha) + v(\beta)$
- $v(\alpha \wedge \beta) = v(\alpha)v(\beta)$
- $v(\alpha \leftrightarrow \beta) = v(\alpha) + v(\beta) + 1$

donde las sumas y multiplicaciones entre los elementos 0 y 1 que hemos considerado en la enumeración anterior son las que se consignan en la siguientes tablas:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

de donde destacamos que para todo valor  $x$  e  $y$  escogidos en  $\{0, 1\}$ :  $x + y = y + x$ ,  $xy = yx$ ,  $x + 0 = x$ ,  $x \cdot 1 = x$ ,  $x + x = 0$  y  $x^2 = x$ .

*Observación 5.2.2.* Obsérvese que de la **Definición 5.2.1** se desprenden las siguiente consecuencias sencillas:

- $v(\neg\alpha) = 1$  sii  $v(\alpha) = 0$
- $v(\alpha \rightarrow \beta) = 1$  sii ( $v(\alpha) = 0$  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 5.1**.

*Ejemplo 5.2.1.* Sea  $v$  cualquier asignación. Entonces:

1. Evaluación de  $\alpha \rightarrow (\beta \rightarrow \gamma)$ :

$$\begin{aligned}
 v(\alpha \rightarrow (\beta \rightarrow \gamma)) &= v(\alpha)v(\beta \rightarrow \gamma) + v(\alpha) + 1 \\
 &= v(\alpha)(v(\beta)v(\gamma) + v(\beta) + 1) + v(\alpha) + 1 \\
 &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta) + v(\alpha) + v(\alpha) + 1 \\
 &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta) + 1 \\
 &= v(\alpha)v(\beta)(v(\gamma) + 1) + 1
 \end{aligned}$$

2. Evaluación de  $(\alpha \wedge \beta) \rightarrow \gamma$ :

$$\begin{aligned}
 v((\alpha \wedge \beta) \rightarrow \gamma) &= v(\alpha \wedge \beta)v(\gamma) + v(\alpha \wedge \beta) + 1 \\
 &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta) + 1 &= v(\alpha)v(\beta)(v(\gamma) + 1) + 1
 \end{aligned}$$

*Observación 5.2.3.* Como muestra el **Ejemplo 5.2.1**, 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.

**Lema 5.2.1** (de relevancia). *Sea  $\varphi$  una fórmula proposicional y  $v, v'$  asignaciones de variables cualesquiera. Si*

$$v \upharpoonright V(\varphi) = v' \upharpoonright V(\varphi) \quad (5.1)$$

*entonces  $v(\varphi) = v'(\varphi)$ .*

*Demostración.* El razonamiento es por inducción sobre la complejidad de  $\varphi$ . Supongamos que  $n \geq 0$  y que (**hip. de inducción**) el resultado es cierto para toda fórmula de complejidad menor que  $n$ . Caben tres posibilidades:

- $\varphi = a$ , para cierto símbolo de variable  $a$ ; así pues  $V(a) = \{a\}$ . 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  $V(\varphi) = V(\alpha)$  y la **hipótesis 5.1** conlleva  $v \upharpoonright V(\alpha) = v' \upharpoonright V(\alpha)$ . Como  $\text{Com}(\alpha) < \text{Com}(\varphi)$ , 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  $V(\varphi) = V(\alpha) \cup V(\beta)$  y la **hipótesis 5.1** conlleva  $v \upharpoonright V(\alpha) = v' \upharpoonright V(\alpha)$  y  $v \upharpoonright V(\beta) = v' \upharpoonright V(\beta)$ . Dado que tanto  $\alpha$  como  $\beta$  tienen menor complejidad que  $\varphi$ , la hipótesis de

$\alpha$	$\neg\alpha$
0	1
1	0

(a) negación

$\alpha$	$\beta$	$\alpha \rightarrow \beta$
0	0	1
0	1	1
1	0	0
1	1	1

(b) implicación

$\alpha$	$\beta$	$\alpha \vee \beta$
0	0	0
0	1	1
1	0	1
1	1	1

(c) disyunción

$\alpha$	$\beta$	$\alpha \wedge \beta$
0	0	0
0	1	0
1	0	0
1	1	1

(d) conjunción

$\alpha$	$\beta$	$\alpha \leftrightarrow \beta$
0	0	1
0	1	0
1	0	0
1	1	1

(e) equivalencia

Figura 5.1: Tablas para la interpretación semántica de los símbolos lógicos

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  $\varphi$ .

□

**Definición 5.2.2.** Sea  $\varphi$  una fórmula del lenguaje proposicional. Entonces:

1.  $\varphi$  es una *fórmula satisfacible* sii, por def., existe (al menos) una valoración  $v$  tal que  $v(\varphi) = 1$ .
2.  $\varphi$  es una *fórmula refutable* sii, por def.,  $(\neg\varphi)$  es una fórmula satisfacible.
3.  $\varphi$  es una *fórmula tautológica, tautología o válida* sii, por def., para toda asignación  $v$  se cumple  $v(\varphi) = 1$ .
4.  $\varphi$  es una *contradicción* sii, por def.,  $(\neg\varphi)$  es una *tautología*.

*Observación 5.2.4.* Sea observado que:

- $\varphi$  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  $\varphi$  es satisfacible pero no tautología, entonces es también refutable.
- $\varphi$  es una *contradicción* sii para toda valoración  $v$  se cumple la igualdad  $v(\varphi) = 0$ .
- Si una fórmula  $\varphi$  es refutable pero no contradicción, entonces es también satisfacible.

*Ejemplo 5.2.2.* Ejemplos de tautologías son las siguientes fórmulas:

1.  $\alpha \rightarrow \alpha$  (*ley de identidad*); en efecto, sea cual sea  $v$ ,

$$\begin{aligned}
 v(\alpha \rightarrow \alpha) &= v(\alpha)v(\alpha) + v(\alpha) + 1 \\
 &= v(\alpha) + v(\alpha) + 1 \\
 &= 0 + 1 \\
 &= 1
 \end{aligned}$$

2.  $(\alpha \rightarrow \beta) \rightarrow ((\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma))$  (*ley de silogismo fuerte*); en efecto, para toda asignación de variables  $v$ :

$$v((\alpha \rightarrow \beta)v(\beta \rightarrow \gamma)) = v(\alpha)v(\beta) + v(\beta)v(\gamma) + v(\alpha) + v(\beta) + 1$$

y así:

$$\begin{aligned}
 v((\alpha \rightarrow \beta) \rightarrow ((\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma))) &= v(\alpha \rightarrow \beta)v(\beta \rightarrow \gamma)(v(\alpha \rightarrow \gamma) + 1) + 1 \\
 &= v(\alpha \rightarrow \beta)v(\beta \rightarrow \gamma)(v(\alpha)v(\gamma) + v(\alpha)) + 1 \\
 &= (v(\alpha)v(\beta) + v(\beta)v(\gamma) + v(\alpha) + v(\beta) + 1)(v(\alpha)v(\gamma) + v(\alpha)) \\
 &\quad + 1 \\
 &= v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\beta)v(\gamma) + v(\alpha)v(\gamma) + v(\alpha)v(\beta)v(\gamma) \\
 &\quad + v(\alpha)v(\gamma) \\
 &\quad + v(\alpha)v(\beta) + v(\alpha)v(\beta)v(\gamma) + v(\alpha) + v(\alpha)v(\beta) + v(\alpha) + 1 \\
 &= 1
 \end{aligned}$$

3.  $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\beta \rightarrow (\alpha \rightarrow \gamma))$  (*ley de conmutación de premisas o cambio del antecedente*)

4.  $(\beta \rightarrow \gamma) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$  (*ley de silogismo débil*)

5.  $\alpha \rightarrow (\beta \rightarrow \alpha)$  (*ley de "a fortiori"* (con mayor razón) o "*verum sequitur ad quodlibet*" (la verdad se sigue de cualquiera)); en efecto, según el **Ejemplo 5.2.1**, sea cual sea  $v$ ,

$$\begin{aligned}
 v(\alpha \rightarrow (\beta \rightarrow \alpha)) &= v(\alpha)v(\beta)v(\alpha) + v(\alpha)v(\beta) + 1 \\
 &= v(\alpha)v(\beta) + v(\alpha)v(\beta) + 1 \\
 &= 0 + 1 \\
 &= 1
 \end{aligned}$$

6.  $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$  (*ley de Frege o autodistributiva*)

7.  $\alpha \rightarrow ((\alpha \rightarrow \beta) \rightarrow \beta)$  (*ley de modus ponens generalizada*)

8.  $\alpha \rightarrow ((\alpha \rightarrow \beta) \rightarrow \beta)$

9.  $(\alpha \rightarrow (\alpha \rightarrow \beta)) \rightarrow (\alpha \rightarrow \beta)$  (*ley de reducción de premisas*)

10.  $((\alpha \rightarrow \beta) \rightarrow (\beta \rightarrow \alpha)) \rightarrow (\beta \rightarrow \alpha)$

11.  $((\alpha \rightarrow \beta) \rightarrow \gamma) \rightarrow (\delta \rightarrow ((\beta \rightarrow (\gamma \rightarrow \varepsilon)) \rightarrow (\beta \rightarrow \varepsilon)))$

12.  $\varepsilon \rightarrow ((\alpha \rightarrow \beta) \rightarrow ((\delta \rightarrow \alpha) \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma))$

13.  $((\alpha \rightarrow \beta) \rightarrow \gamma) \rightarrow (((\beta \rightarrow \alpha) \rightarrow \gamma) \rightarrow \gamma)$  (*ley de Dummet*)

14.  $((\alpha \rightarrow \beta) \rightarrow \beta) \rightarrow ((\beta \rightarrow \alpha) \rightarrow \alpha)$  (*ley de Tanaka*)

15.  $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$  (*ley de Peirce*)

16.  $((((\varphi \rightarrow \psi) \rightarrow (\neg \alpha \rightarrow \neg \beta)) \rightarrow \alpha) \rightarrow \gamma) \rightarrow ((\gamma \rightarrow \varphi) \rightarrow (\beta \rightarrow \varphi))$  (*ley de Meredith*)

17.  $((\alpha \rightarrow \gamma) \rightarrow \beta) \rightarrow (((\beta \rightarrow \alpha) \rightarrow \beta) \rightarrow \beta)$  (*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 5.2.3.*

1.  $\neg \neg \alpha \rightarrow \alpha$  (*ley de doble negación clásica o fuerte*)

2.  $\alpha \rightarrow \neg\neg\alpha$  (*ley de doble negación intuicionista o minimal*)
3.  $\neg\neg\neg\alpha \rightarrow \neg\alpha$  (*ley de Brouwer*)
4.  $\neg\alpha \rightarrow (\alpha \rightarrow \beta)$  (*ley de Duns Scoto*); en efecto, para toda asignación de variables:

$$\begin{aligned}
 v(\alpha \rightarrow (\neg\alpha \rightarrow \beta)) &= v(\alpha)v(\neg\alpha \rightarrow \beta) + v(\alpha) + 1 \\
 &= v(\alpha)(v(\neg\alpha)v(\beta) + v(\neg\alpha) + 1) + v(\alpha) + 1 \\
 &= v(\alpha)((v(\alpha) + 1)v(\beta) + v(\alpha) + 1 + 1) + v(\alpha) + 1 \\
 &= v(\alpha)(v(\alpha)v(\beta) + v(\beta) + v(\alpha)) + v(\alpha) + 1 \\
 &= v(\alpha)^2v(\beta) + v(\alpha)v(\beta) + v(\alpha)^2 + v(\alpha) + 1 \\
 &= v(\alpha)v(\beta) + v(\alpha)v(\beta) + v(\alpha) + v(\alpha) + 1 \\
 &= 0 + 0 + 1 \\
 &= 1
 \end{aligned}$$

5.  $\alpha \rightarrow (\neg\alpha \rightarrow \neg\beta)$  (*ley débil de Duns Scoto*)
6.  $(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$  (*ley de “reductio ad absurdum” clásica o fuerte*)
7.  $(\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \neg\alpha)$  (*ley de contraposición “tollendo tollens”*); en efecto, sea cual sea  $v$ ,

$$\begin{aligned}
 v((\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \neg\alpha)) &= v(\alpha \rightarrow \beta)v(\neg\beta \rightarrow \neg\alpha) + v(\alpha \rightarrow \beta) + 1 \\
 &= (v(\alpha)v(\beta) + v(\alpha) + 1)(v(\neg\beta)v(\neg\alpha) + v(\neg\beta) + 1) \\
 &\quad + (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\
 &= (v(\alpha)v(\beta) + v(\alpha) + 1)((v(\beta) + 1)(v(\alpha) + 1) + v(\beta) + 1 + 1) \\
 &\quad + (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\
 &= (v(\alpha)v(\beta) + v(\alpha) + 1)(v(\alpha)v(\beta) + v(\alpha) + v(\beta) + 1 + v(\beta)) \\
 &\quad + (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\
 &= (v(\alpha)v(\beta) + v(\alpha) + 1)(v(\alpha)v(\beta) + v(\alpha) + 1) \\
 &\quad + (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\
 &= (v(\alpha)v(\beta) + v(\alpha) + 1) + (v(\alpha)v(\beta) + v(\alpha) + 1) + 1 \\
 &= 1
 \end{aligned}$$

8.  $(\neg\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \alpha)$  (*ley de contraposición “ponendo ponens”*);
9.  $(\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \neg\alpha)$  (*ley de contraposición “ponendo tollens”*);
10.  $(\neg\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \alpha)$  (*ley de contraposición “tollendo ponens”*);
11.  $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha)$  (*ley “reductio ad absurdum” intuicionista o minimal*)
12.  $(\neg\alpha \rightarrow \alpha) \rightarrow \alpha$  (*ley de Clavius*); en efecto, sea  $v$  una asignación de variables cualquiera:

$$\begin{aligned}
 v((\neg\alpha \rightarrow \alpha) \rightarrow \alpha) &= v((\neg\alpha \rightarrow \alpha))v(\alpha) + v((\neg\alpha \rightarrow \alpha)) + 1 \\
 &= (v(\neg\alpha)v(\alpha) + v(\neg\alpha) + 1)v(\alpha) + (v(\neg\alpha)v(\alpha) + v(\neg\alpha) + 1)v(\alpha) + 1 \\
 &= (v(\neg\alpha)v(\alpha) + v(\alpha))v(\alpha) + v(\neg\alpha)v(\alpha) + v(\alpha) + 1 \\
 &= v(\neg\alpha)v(\alpha) + v(\alpha) + v(\neg\alpha)v(\alpha) + v(\alpha) + 1 \\
 &= 0 + 0 + 1 \\
 &= 1
 \end{aligned}$$

13.  $(\alpha \rightarrow \neg\alpha) \rightarrow \neg\alpha$  (*ley débil de Clavius*)
14.  $\neg(\alpha \rightarrow \alpha) \rightarrow \beta$  (*ley “ex falso sequitur quodlibet”* (de lo falso se sigue cualquier cosa))
15.  $\alpha \rightarrow (\neg\beta \rightarrow \neg(\alpha \rightarrow \beta))$
16.  $(\alpha \rightarrow \beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \beta)$  (*ley del dilema*)
17.  $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha)$
18.  $(\alpha \rightarrow \gamma) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \gamma))$  (*ley de modus ponens generalizada*)

*Ejemplo 5.2.4.*

1.  $(\alpha \wedge \beta) \rightarrow \alpha$
2.  $(\alpha \wedge \beta) \rightarrow \beta$
3.  $(\gamma \rightarrow \alpha) \rightarrow ((\gamma \rightarrow \beta) \rightarrow (\gamma \rightarrow (\alpha \wedge \beta)))$
4.  $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta))$
5.  $(\beta \wedge \alpha) \rightarrow (\alpha \wedge \beta)$
6.  $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \wedge \beta) \rightarrow \gamma)$  (*ley de importación*)
7.  $((\alpha \wedge \beta) \rightarrow \gamma) \rightarrow (\alpha \rightarrow (\beta \rightarrow \gamma))$  (*ley de exportación*)
8.  $(\alpha \rightarrow \beta) \rightarrow ((\alpha \wedge \gamma) \rightarrow (\beta \wedge \gamma))$
9.  $((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma)$  (*ley “ex toto” o transitividad de  $\rightarrow$* )
10.  $(\alpha \wedge (\alpha \rightarrow \beta)) \rightarrow \beta$  (*ley de “modus ponens”*)

*Ejemplo 5.2.5.*

1.  $\alpha \rightarrow (\alpha \vee \beta)$
2.  $\beta \rightarrow (\alpha \vee \beta)$
3.  $(\alpha \rightarrow \gamma) \rightarrow ((\beta \rightarrow \gamma) \rightarrow ((\alpha \vee \beta) \rightarrow \gamma))$
4.  $(\alpha \rightarrow (\beta \vee \gamma)) \rightarrow ((\alpha \rightarrow \beta) \vee (\alpha \rightarrow \gamma))$
5.  $(\alpha \rightarrow \beta) \vee (\beta \rightarrow \alpha)$
6.  $(\beta \vee \alpha) \rightarrow (\alpha \vee \beta)$
7.  $(\alpha \rightarrow \varphi) \rightarrow ((\beta \rightarrow \psi) \rightarrow ((\alpha \vee \beta) \rightarrow (\varphi \vee \psi)))$

*Ejemplo 5.2.6.*

1.  $\alpha \vee \neg\alpha$  (*ley “tertium non datur” o principio del tercio excluso*)
2.  $\neg(\alpha \rightarrow \neg\alpha)$  (*principio de no contradicción*)
3.  $(\alpha \wedge \neg\alpha) \rightarrow \beta$  (*principio de inconsistencia*)
4.  $(\neg\beta \wedge (\alpha \rightarrow \beta)) \rightarrow \neg\alpha$  (*principio del “modus tollendo tollens”*)
5.  $((\alpha \vee \beta) \wedge \neg\beta) \rightarrow \alpha$
6.  $((\alpha \vee \beta) \wedge \neg\alpha) \rightarrow \beta$

7.  $((\alpha \vee \beta) \wedge (\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma)) \rightarrow \gamma$
8.  $((\neg\alpha \vee \neg\beta) \wedge (\gamma \rightarrow \alpha) \wedge (\gamma \rightarrow \beta)) \rightarrow \neg\gamma$
9.  $((\alpha \vee \beta) \wedge (\alpha \rightarrow \varphi) \wedge (\beta \rightarrow \psi)) \rightarrow (\varphi \vee \psi)$
10.  $((\neg\alpha \vee \neg\beta) \wedge (\varphi \rightarrow \alpha) \wedge (\psi \rightarrow \beta)) \rightarrow (\neg\varphi \vee \neg\psi)$
11.  $\neg(\alpha \wedge \neg\alpha)$

**Definición 5.2.3.** Dado un conjunto de fórmulas  $\Gamma$  —posiblemente vacío— y una fórmula  $\varphi$  decimos que  $\Gamma$  *implica semánticamente* a  $\varphi$ , abreviadamente  $\Gamma \models \varphi$ , si para toda valoración  $v$  se tiene  $v(\varphi) = 1$  siempre que para toda fórmula  $\gamma$  de  $\Gamma$  valga la igualdad  $v(\gamma) = 1$ . Si  $\Gamma$  consta solamente de las fórmulas  $\gamma_1, \dots, \gamma_n$ , en lugar de  $\{\gamma_1, \dots, \gamma_n\} \models \varphi$  escribimos  $\gamma_1, \dots, \gamma_n \models \varphi$  y cuando  $\Gamma = \emptyset$  escribimos simplemente  $\models \varphi$  en lugar de  $\emptyset \models \varphi$ .

*Ejemplo 5.2.7.*

1. Para cualquier tautología  $\alpha$ ,  $\models \alpha$ . En particular, para todo símbolo de variable proposicional,  $a$ , se cumple  $\models a \rightarrow a$ .
2.  $\alpha, \alpha \rightarrow \beta \models \beta$ ; en efecto, sea  $v$  una asignación cualquiera a condición de que  $v(\alpha) = v(\alpha \rightarrow \beta) = 1$  y demosremos que para una tal  $v$  debe cumplirse  $v(\beta) = 1$ . Basta considerar las siguientes igualdades:

$$\begin{aligned}
 1 &= v(\alpha \rightarrow \beta) \\
 &= v(\alpha)v(\beta) + v(\alpha) + 1 \\
 &= 1 \cdot v(\beta) + 1 + 1 \\
 &= v(\beta) + 0 \\
 &= v(\beta)
 \end{aligned}$$

3.  $\alpha \rightarrow (\beta \rightarrow \gamma), \alpha \rightarrow \beta, \alpha \models \gamma$ ; en efecto, sea  $v$  una asignación cualquiera a condición de que  $v(\alpha \rightarrow (\beta \rightarrow \gamma)) = v(\alpha \rightarrow \beta) = v(\alpha) = 1$  y demosremos 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:

$$\begin{aligned}
 1 &= v(\alpha \rightarrow (\beta \rightarrow \gamma)) && \text{hipótesis} \\
 &= v(\alpha)v(\beta \rightarrow \gamma) + v(\alpha) + 1 \\
 &= 1 \cdot v(\beta \rightarrow \gamma) + 1 + 1 && \text{pues } v(\alpha) = 1 \\
 &= v(\beta \rightarrow \gamma) \\
 &= v(\gamma) && \text{pues } v(\beta) = 1
 \end{aligned}$$

4.  $\alpha \rightarrow \beta, \beta \rightarrow \gamma \models \alpha \rightarrow \gamma$
5.  $(\alpha \vee \beta) \wedge (\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma) \models \gamma$
6.  $(\neg\alpha \vee \neg\beta) \wedge (\gamma \rightarrow \alpha) \wedge (\gamma \rightarrow \beta) \models \neg\gamma$
7.  $(\alpha \vee \beta) \wedge (\alpha \rightarrow \varphi) \wedge (\beta \rightarrow \psi) \models \varphi \vee \psi$
8.  $(\neg\alpha \vee \neg\beta) \wedge (\varphi \rightarrow \alpha) \wedge (\psi \rightarrow \beta) \models \neg\varphi \vee \neg\psi$
9.  $a \vee b \not\models a$ ; 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.  $a \not\models a \wedge b$

**Definición 5.2.4.** Dos fórmula  $\alpha$  y  $\beta$  son *lógicamente equivalentes* o simplemente *equivalentes* si, y sólo si, por definición,  $\models \alpha \leftrightarrow \beta$ , es decir, sii  $\alpha \leftrightarrow \beta$  es una tautología. La frase “ $\alpha$  y  $\beta$  son lógicamente equivalentes” será abreviada ocasionalmente como  $\alpha \equiv \beta$ .

*Ejemplo 5.2.8.* Sean  $\alpha$ ,  $\beta$  y  $\gamma$  fórmulas. Cada *item* subsiguiente enumera fórmulas lógicamente equivalentes:

1.  $\alpha \rightarrow \beta, \neg(\alpha \wedge \neg\beta)$

2.  $\neg\alpha \rightarrow \beta, \alpha \vee \beta$

**Teorema 5.2.2.** Sean  $\alpha$  y  $\beta$  fórmulas de un lenguaje proposicional. Son equivalentes las siguientes afirmaciones:

1.  $\alpha$  y  $\beta$  son lógicamente equivalentes

2.  $\models \alpha \rightarrow \beta$  y  $\models \beta \rightarrow \alpha$

3.  $\alpha \models \beta$  y  $\beta \models \alpha$

4. Para toda asignación  $v$ ,  $v(\alpha) = v(\beta)$

*Demostración.* Supongamos que  $\alpha$  y  $\beta$  son lógicamente equivalentes, es decir, que para todo asignación  $v$  se cumple  $v(\alpha \leftrightarrow \beta)$ . o equivalentemente  $v(\alpha \rightarrow \beta) = v(\beta \rightarrow \alpha) = 1$ , es decir,  $\models \alpha \rightarrow \beta$  y  $\models \beta \rightarrow \alpha$ . Supongamos ahora que  $\models \alpha \rightarrow \beta$  y  $\models \beta \rightarrow \alpha$ . Sea  $v$  una asignación cualquiera tal que  $v(\alpha) = 1$ . Como en particular, según la hipótesis  $\models \alpha \rightarrow \beta$ , para esa  $v$  se cumple  $v(\alpha \rightarrow \beta) = 1$ , deducimos por (2) que  $v(\beta) = 1$ . Acabamos de demostrar que  $\alpha \models \beta$  y la demostración de  $\beta \models \alpha$  es similar. Supongamos ahora que  $\alpha \models \beta$  y  $\beta \models \alpha$  y tomemos una asignación  $v$  cualquiera. Caben dos posibilidades:

- $v(\alpha) = 1$ ; debido a la hipótesis  $\alpha \models \beta$ , debe cumplirse  $v(\beta) = 1$ .
- $v(\alpha) = 0$ ; por reducción al absurdo, dado que por hipótesis se cumple  $\beta \models \alpha$ , 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:

$$\begin{aligned} v(\alpha \rightarrow \beta) &= v(\alpha)v(\beta) + v(\alpha) + 1 \\ &= v(\alpha)^2 + v(\alpha) + 1 \\ &= v(\alpha) + v(\alpha) + 1 \\ &= 0 + 1 \\ &= 1 \end{aligned}$$

Análogamente tendremos que  $v(\beta \rightarrow \alpha) = 1$  y, por tanto,  $v(\alpha \leftrightarrow \beta) = 1$ . □

*Observación 5.2.5.* Es claro que si  $\alpha$  es una tautología y  $\alpha \models \beta$ , entonces  $\beta$  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 fórmulas 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).



**Definición 5.2.5.** Un conjunto  $\Gamma$  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  $\Gamma$  de fórmulas del lenguaje es *satisfacible* cuando, y sólo cuando, no es insatisfacible.

*Ejemplo 5.2.9.*

1. Para todo símbolo de variable proposicional  $a$ ,  $\{a, \neg a\}$  es insatisfacible.
2. Cualquier conjunto que contenga a  $\{a, \neg a\}$ , siendo  $a$  un símbolo de variable proposicional cualquiera, es insatisfacible.
3. El conjunto  $\emptyset$  es satisfacible pues si fuera insatisfacible, no sería vacío.

*Observación 5.2.6.* Sea observado que:

- Un conjunto  $\Gamma$  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  $\Gamma$  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.
- $\varphi$  es satisfacible sii  $\{\varphi\}$  es satisfacible.
- Según un *razonamiento por vacuidad*, el conjunto  $\emptyset$  es satisfacible.
- Si  $\Gamma$  es un conjunto de fórmulas proposicionales,  $\varphi \in \Gamma$  y  $\varphi$  es una tautología, entonces  $\Gamma$  es satisfacible sii  $\Gamma \setminus \{\varphi\}$  es satisfacible.
- Si  $\Gamma$  es un conjunto de fórmula,  $\varphi \in \Gamma$  y  $\varphi$  es una contradicción, entonces  $\Gamma$  es insatisfacible.

### 5.3. Propiedades Básicas de la Implicación Semántica

**Definición 5.3.1** (satisfacibilidad finita). Un conjunto  $\Gamma$  de fórmulas es *finitamente satisfacible* si, y sólo si, por definición, cualquier subconjunto finito  $\Gamma_f$  de  $\Gamma$  es satisfacible.

**Lema 5.3.1.** Sea  $\Gamma$  un conjunto finitamente satisfacible de fórmulas y sea  $\varphi$  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  $\Gamma_1$  y  $\Gamma_2$  de  $\Gamma$  tales que  $\Gamma_1 \cup \{\varphi\}$  y  $\Gamma_2 \cup \{\varphi\}$  son insatisfacibles. Supongamos que la asignación  $v$  satisficiera 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  $\Gamma$ . Así pues,  $\Gamma$  no podría ser finitamente satisfacible.  $\square$

**Teorema 5.3.2** (de Compacidad). Sea  $\Gamma$  un conjunto de fórmulas proposicionales. Son equivalentes las siguientes afirmaciones:

1.  $\Gamma$  es satisfacible.
2.  $\Gamma$  es finitamente satisfacible.

*Demostración.* Si  $\Gamma$  es satisfacible, también lo son sus subconjuntos y en particular sus subconjuntos finitos. Recíprocamente, supongamos que cada subconjunto finito de  $\Gamma$  es satisfacible. Consideremos los símbolos de variables proposicionales enumerados  $\langle a_i \rangle_{i=0}^{\infty}$  y consideremos la siguiente definición recursiva:

$$\begin{aligned}\Delta_0 &= \Gamma \\ \Delta_{i+1} &= \begin{cases} \Delta_i \cup \{a_i\} & , \text{ si es finitamente satisfacible,} \\ \Delta_i \cup \{\neg a_i\} & , \text{ en otro caso.} \end{cases}\end{aligned}$$

En virtud del **Lema 5.3.1**) sabemos que cada  $\Delta_i$  es finitamente satisfacible. Sea  $\Delta = \bigcup_i \Delta_i$ , del que sabemos lo siguiente:

1.  $\Gamma \subseteq \Delta$
2.  $\Delta$  es finitamente satisfacible; en efecto, sea  $\Delta_f$  un subconjunto finito de  $\Delta$ . Como  $\Delta_f$  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  $\Delta_j$  es finitamente satisfacible,  $\Delta_f$  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  $\Delta$  es finitamente satisfacible y si para cierto  $i$ ,  $a_i$  y  $\neg a_i$  perteneciese a  $\Delta$ ,  $\{a_i, \neg a_i\}$  sería un subconjunto finito de  $\Delta$  insatisfacible.

Consideremos ahora la asignación de variables  $v$  definida por la siguiente condición:

$$v(a_i) = \chi_{\Delta}(a_i)$$

y  $\tau$  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  $Y = \{\tau(a) : a \in V(\varphi)\}$ . Entonces, por la definición de  $\tau$  y  $v$  tenemos que:

- Si  $\lambda \in Y$ , entonces  $v(\lambda) = 1$ . En efecto, si  $\lambda \in Y$  es porque existe  $a \in V(\varphi)$  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  $a \in V(\varphi)$  tal que  $\lambda = \tau(a)$ ; pero  $\tau(a) \in \Delta$ , luego  $\lambda \in \Delta$ .
- $V(\varphi) = V_*(Y)$ . En efecto,

$$\begin{aligned}V_*(Y) &= \bigcup \{V(\lambda) : \lambda \in Y\} && \text{por definición} \\ &= \bigcup \{V(\tau(a)) : a \in V(\varphi)\} \\ &= \bigcup \{\{a\} : a \in V(\varphi)\} && \text{pues } V(\tau(a)) = \{a\} \\ &= V(\varphi)\end{aligned}$$

- Para todo  $\lambda \in Y$ ,  $v(\lambda) = 1$ . En efecto, para todo  $\lambda \in Y$  existe  $a \in V(\varphi)$  tal que  $\lambda = \tau(a)$ ; como para todo  $a \in V(\varphi)$ ,  $\tau(a) \in \Delta$  entonces se cumple que  $v(\lambda) = \chi_{\Delta}(\tau(a)) = 1$ .

Como  $V(\varphi)$  es finito,  $V(\varphi) \cup \{\varphi\}$  es un subconjunto finito de  $\Delta$ . Como  $\Delta$  es finitamente satisfacible,  $V(\varphi) \cup \{\varphi\}$  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  $\lambda$  de  $Y$ ,  $v'(\lambda) = 1$ . Así pues,  $v \upharpoonright V(\varphi) = v' \upharpoonright V(\varphi)$  y por el **Lema 5.2.1**, deducimos que  $v(\varphi) = v'(\varphi) = 1$ . Como  $\varphi$  era una fórmula de  $\Gamma$  fija, pero arbitraria, hemos demostrado que  $v$  satisface a  $\Gamma$ , como se quería.  $\square$

**Corolario 5.3.3.** Sea  $\Gamma$  un conjunto de fórmulas proposicionales. Son equivalentes las siguientes afirmaciones:

1.  $\Gamma$  es insatisfacible.
2. Existe un subconjunto finito de  $\Gamma$  que es insatisfacible.

**Definición 5.3.2.** Dado un conjunto de fórmulas  $\Gamma$  del lenguaje, sea  $\text{Con}(\Gamma)$  el conjunto de fórmulas  $\gamma$  tales que  $\Gamma \models \gamma$ .

*Ejemplo 5.3.1.*  $\text{Con}(\emptyset)$  es el conjunto de las tautologías y, por tanto, es no vacío.

**Lema 5.3.4.** Si  $\Gamma$  es insatisfacible entonces cualquier fórmula proposicional es elemento de  $\text{Con}(\Gamma)$ .

*Demostración.* Supongamos que  $\Gamma$  es insatisfacible y que  $\varphi$  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,  $\Gamma$  sería satisfacible, en contra de lo supuesto. Por tanto, no puede darse  $\Gamma \not\models \varphi$  y entonces  $\Gamma \models \varphi$ .  $\square$

**Teorema 5.3.5.** Para cualesquiera conjuntos de fórmula  $\Gamma$  y  $\Delta$  son ciertas las siguientes afirmaciones:

1.  $\Gamma \subseteq \text{Con}(\Gamma)$
2. Si  $\Gamma \subseteq \Delta$ , entonces  $\text{Con}(\Gamma) \subseteq \text{Con}(\Delta)$  (monotonía)
3.  $\text{Con}(\text{Con}(\Gamma)) \subseteq \text{Con}(\Gamma)$
4.  $\text{Con}(\emptyset) \subseteq \text{Con}(\Gamma)$
5.  $\text{Con}(\text{Con}(\Gamma)) = \text{Con}(\Gamma)$  (indempotencia)

*Demostración.* Si cualquiera de los conjuntos  $\Gamma$  o  $\Delta$  fuera insatisfacible, todas las afirmaciones son trivialmente ciertas por lo que sabemos del **Lema 5.3.4**. Supongamos entonces que ambos conjuntos  $\Gamma$  y  $\Delta$  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  $\Gamma \models \gamma$ , o sea,  $\Gamma \subseteq \text{Con}(\Gamma)$ . En cuanto a la **afirmación 2**, sea  $\gamma \in \text{Con}(\Gamma)$  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  $\Gamma \models \gamma$ , se tiene que  $v(\gamma) = 1$ . Hemos demostrado que si  $\gamma \in \text{Con}(\Gamma)$  entonces  $\Delta \models \gamma$ , es decir,  $\gamma \in \text{Con}(\Delta)$  o equivalentemente que  $\text{Con}(\Gamma) \subseteq \text{Con}(\Delta)$ . En cuanto a la **afirmación 3**, sea una cualquiera de las asignaciones  $v$  tales que  $v_*(\Gamma) \subseteq \{1\}$ ; para cualquier  $\varphi \in \text{Con}(\Gamma)$  se cumplirá, por tanto,  $v(\varphi) = 1$ . Tenemos entonces que  $v_*(\text{Con}(\Gamma)) \subseteq \{1\}$ , así si  $\gamma \in \text{Con}(\text{Con}(\Gamma))$  entonces  $v(\gamma) = 1$  y, por tanto,  $\gamma \in \text{Con}(\Gamma)$ . Hemos demostrado que  $\text{Con}(\text{Con}(\Gamma)) \subseteq \text{Con}(\Gamma)$ . La **afirmación 4** es consecuencia de **afirmación 2**. Para **afirmación 5**, tengamos en cuenta que por la **1**),  $\Gamma \subseteq \text{Con}(\Gamma)$  y entonces, por **2**),  $\text{Con}(\Gamma) \subseteq \text{Con}(\text{Con}(\Gamma))$  y la igualdad se tiene entonces en virtud de **3**).  $\square$

**Teorema 5.3.6.** Para cualesquiera fórmulas  $\alpha$ ,  $\beta$  y  $\gamma$  y conjunto de fórmulas  $\Gamma$ :

1. Si  $\Gamma \models \alpha$  y  $\Gamma \models \alpha \rightarrow \beta$ , entonces  $\Gamma \models \beta$  (regla del modus ponens)
2. Si  $\Gamma \models \alpha \vee \beta$  y  $\Gamma \models \neg\alpha \vee \gamma$  entonces  $\Gamma \models \beta \vee \gamma$  (regla de resolución en log. proposicional)

*Demostración.* Si  $\Gamma \models \alpha$  y  $\Gamma \models \alpha \rightarrow \beta$ , entonces  $\alpha, \alpha \rightarrow \beta \in \text{Con}(\Gamma)$ . Por **2**) del **Ejemplo 5.2.7** y la monotonicidad de  $\text{Con}$ , sabemos que  $\beta \in \text{Con}(\text{Con}(\Gamma))$ , es decir,  $\beta \in \text{Con}(\Gamma)$  o equivalentemente  $\Gamma \models \beta$ . Por otra parte,  $\alpha \vee \beta$  (resp.  $\neg\alpha \vee \gamma$ ) es lógicamente equivalente a  $\neg\alpha \rightarrow \beta$  (resp.  $\alpha \rightarrow \gamma$ ), por lo que  $\models (\alpha \vee \beta) \rightarrow (\neg\alpha \rightarrow \beta)$  (resp.  $\models (\neg\alpha \vee \gamma) \rightarrow (\alpha \rightarrow \gamma)$ ). Tenemos, pues,

1.  $\Gamma \models \alpha \vee \beta$

2.  $\models (\alpha \vee \beta) \rightarrow (\neg\alpha \rightarrow \beta)$
3.  $\Gamma \models \neg\alpha \vee \gamma$
4.  $\models (\neg\alpha \vee \gamma) \rightarrow (\alpha \rightarrow \gamma)$

Por esto, la regla del *modus ponens* y la monotonía, tenemos que  $\Gamma \models \neg\alpha \rightarrow \beta$  y  $\Gamma \models \alpha \rightarrow \gamma$ . Por 10) del Ejemplo 5.2.3 y la monotonía tenemos que  $\Gamma \models (\neg\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \alpha)$ , por lo que  $\Gamma \models \neg\beta \rightarrow \alpha$  y  $\Gamma \models \alpha \rightarrow \gamma$ . Por 2) del Ejemplo 5.2.2 sabemos que en particular,  $\models (\neg\beta \rightarrow \alpha) \rightarrow ((\alpha \rightarrow \gamma) \rightarrow (\neg\beta \rightarrow \gamma))$  por lo que  $\Gamma \models (\neg\beta \rightarrow \alpha) \rightarrow ((\alpha \rightarrow \gamma) \rightarrow (\neg\beta \rightarrow \gamma))$ . Aplicando dos veces la regla del *modus ponens* concluimos que  $\Gamma \models \neg\beta \rightarrow \gamma$ ; pero al ser lógicamente equivalentes las fórmulas  $\neg\beta \rightarrow \gamma$  y  $\beta \vee \gamma$ , lo que hemos demostrado es que  $\Gamma \models \beta \vee \gamma$ , como queríamos.  $\square$

**Teorema 5.3.7.** *Sea  $\Gamma$  un conjunto de fórmulas propicionales. Son equivalentes las siguientes afirmaciones:*

1.  $\Gamma$  es insatisfacible
2. Existe una fórmula  $\alpha$  tal que  $\Gamma \models \alpha$  y  $\Gamma \models \neg\alpha$ .
3. Para toda fórmula proposicional  $\beta$ ,  $\Gamma \models \beta$ .

*Demostración.* Supongamos que  $\Gamma$  es insatisfacible y sea  $\alpha$  el símbolo de variable  $a_0$ . Si  $\Gamma \not\models a_0$  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  $\Gamma$  no sería insatisfacible, en contra de lo supuesto. Por tanto,  $\Gamma \models a_0$  y un razonamiento análogo conduce a que  $\Gamma \models \neg a_0$ . Supongamos que existe una fórmula  $\alpha$  tal que  $\Gamma \models \alpha$  y  $\Gamma \models \neg\alpha$ . Sea  $\beta$  cualquier fórmula. Por 4) del Ejemplo 5.2.3, tenemos que  $\models \neg\alpha \rightarrow (\alpha \rightarrow \beta)$  y por monotonía que  $\Gamma \models \neg\alpha \rightarrow (\alpha \rightarrow \beta)$ . Aplicando dos veces la regla del *modus ponens* concluimos que  $\Gamma \models \beta$ . Finalmente, si para cualquier fórmula  $\beta$  se cumple  $\Gamma \models \beta$  entonces, en particular para  $\Gamma \models a_0 \wedge \neg a_0$ . 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,  $\Gamma$  es necesariamente insatisfacible.  $\square$

**Teorema 5.3.8** (de la deducción). *Sea  $\Gamma \cup \{\varphi, \psi\}$  un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1.  $\Gamma, \psi \models \varphi$
2.  $\Gamma \models \psi \rightarrow \varphi$

*Demostración.* Sea  $\Gamma \cup \{\varphi, \psi\}$  un conjunto de fórmulas. Si alguno de los conjunto  $\Gamma$  o  $\Gamma \cup \{\psi\}$  fuere insatisfacible, las dos afirmaciones son obviamente equivalentes (¿por qué?). Supongamos, pues, que ni  $\Gamma$  ni  $\Gamma \cup \{\psi\}$  son insatisfacibles. Ahora supongamos también que  $\Gamma, \psi \models \varphi$  y que  $v$  es una asignación de variables cualquiera cumpliendo  $v_*(\Gamma) \subseteq \{1\}$ . Para  $v$  caben dos posibilidades:

- $v(\psi) = 0$ ; entonces

$$\begin{aligned}
 v(\psi \rightarrow \varphi) &= v(\psi)v(\varphi) + v(\psi) + 1 \\
 &= 0v(\varphi) + 0 + 1 \\
 &= 0 + 0 + 1 \\
 &= 1
 \end{aligned}$$

- $v(\psi) = 1$ ; entonces  $v_*(\Gamma \cup \{\psi\}) \subseteq \{1\}$  (de hecho ambos conjuntos coinciden en este caso) y como estamos suponiendo que  $\Gamma, \psi \models \varphi$ , para  $v$  debe cumplirse que  $v(\varphi) = 1$  y así  $v(\psi \rightarrow \varphi) = 1$

como en cualquiera de los casos posibles hemos obtenido que  $v(\psi \rightarrow \varphi) = 1$ , entonces hemos demostrado que  $\Gamma \models \psi \rightarrow \varphi$ . Recíprocamente, supongamos que  $\Gamma \models \psi \rightarrow \varphi$  y sea  $v$  una asignación de variables tal que  $v_*(\Gamma \cup \{\psi\}) \subseteq_* \{1\}$ . Entonces  $v(\psi \rightarrow \varphi) = 1 = v(\psi)$ , de donde  $v(\varphi) = 1$ . Hemos concluido, pues, que  $\Gamma, \psi \models \varphi$ .  $\square$

**Corolario 5.3.9.** *Para cualesquiera fórmulas  $\gamma_1, \dots, \gamma_n, \varphi$  ( $2 \leq n$ ) son equivalentes las siguientes afirmaciones:*

1.  $\gamma_1, \dots, \gamma_n \models \varphi$
2.  $\gamma_1 \wedge \dots \wedge \gamma_n \models \varphi$
3.  $\models \gamma_1 \wedge \dots \wedge \gamma_n \rightarrow \varphi$

**Teorema 5.3.10.** *Sea  $\Gamma \cup \{\varphi\}$  un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1.  $\Gamma \models \varphi$
2.  $\Gamma \cup \{\neg\varphi\}$  es insatisfacible

**Corolario 5.3.11.** *Sea  $\Gamma \cup \{\varphi\}$  un conjunto de fórmulas proposicionales. Son equivalentes las siguientes afirmaciones:*

1.  $\Gamma \models \varphi$
2. Existe un subconjunto finito de  $\Gamma$ ,  $\Gamma_f$ , tal que  $\Gamma_f \models \varphi$ .

*Demostración.* Supongamos que  $\Gamma \models \varphi$ , entonces  $\Gamma \cup \{\neg\varphi\}$  es insatisfacible. Por el Corolario 5.3.3 sabemos que existe un subconjunto finito  $\Sigma_f$  de  $\Gamma \cup \{\neg\varphi\}$  que es insatisfacible. Sea  $\Gamma_f$  el conjunto  $\Sigma_f \setminus \{\neg\varphi\}$ , que es un subconjunto finito de  $\Gamma$ . Entonces,  $\Gamma_f \cup \{\neg\varphi\}$  es insatisfacible (¿por qué?). Según el Teorema 5.3.10, se tendrá que  $\Gamma_f \models \varphi$ . Recíprocamente, supongamos que  $\Gamma_f$  es un subconjunto finito de  $\Gamma$  y que  $\Gamma_f \models \varphi$ . Esto equivale a que  $\varphi \in \text{Con}(\Gamma_f)$ ; pero por 2) del Teorema 5.3.5 sabemos que  $\text{Con}(\Gamma_f) \subseteq \text{Con}(\Gamma)$  y por tanto  $\varphi \in \text{Con}(\Gamma)$ , o sea,  $\Gamma \models \varphi$ .  $\square$

**Corolario 5.3.12.** *Sean  $\Gamma$  un conjunto de fórmulas proposicionales. Entonces:*

$$\text{Con}(\Gamma) = \bigcup_{\substack{\Gamma_f \subseteq \Gamma \\ \Gamma_f \text{ finito}}} \text{Con}(\Gamma_f) \quad (\text{finitariedad})$$

**Teorema 5.3.13.** *Sea  $\Gamma \cup \{\psi, \varphi\}$  un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1.  $\Gamma, \psi \wedge \varphi \models \xi$
2.  $\Gamma, \psi, \varphi \models \xi$

**Corolario 5.3.14.** *Para cualesquiera fórmulas  $\gamma_1, \dots, \gamma_n, \varphi$  ( $2 \leq n$ ) son equivalentes las siguientes afirmaciones:*

1.  $\gamma_1, \dots, \gamma_n \models \varphi$
2.  $\{\gamma_1, \gamma_2, \dots, \gamma_n, \neg\varphi\}$  es insatisfacible
3.  $\gamma_1 \wedge \gamma_2 \wedge \dots \wedge \gamma_n \wedge \neg\varphi$  es insatisfacible

**Teorema 5.3.15.** *Sea  $\Gamma \cup \{\psi, \varphi\}$  un conjunto de fórmulas. Son equivalentes las siguientes afirmaciones:*

1.  $\Gamma \models \psi$  y  $\Gamma \models \varphi$
2.  $\Gamma \models \psi \wedge \varphi$

*Demostración.* Supongamos que  $\Gamma \models \psi$  y  $\Gamma \models \varphi$ . Por monotonía y al ser  $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta))$  una tautología para cualesquiera fórmulas  $\alpha$  y  $\beta$ , tenemos que:

$$\Gamma \models \psi \rightarrow (\varphi \rightarrow (\psi \wedge \varphi))$$

Por la primera suposición y el *modus ponens* deducimos que  $\Gamma \models \varphi \rightarrow (\psi \wedge \varphi)$ ; por la segunda suposición y el *modus ponens* deducimos finalmente que  $\Gamma \models \psi \wedge \varphi$ . Recíprocamente, supongamos que  $\Gamma \models \psi \wedge \varphi$ . Como  $(\alpha \wedge \beta) \rightarrow \alpha$  es una ley lógica para cualesquiera fórmulas  $\alpha$  y  $\beta$ , tenemos en particular que  $\Gamma \models (\psi \wedge \varphi) \rightarrow \psi$  y  $\Gamma \models (\psi \wedge \varphi) \rightarrow \varphi$ . Si  $\Gamma \models \psi \wedge \varphi$ , como suponemos por hipótesis, entonces  $\Gamma \models \psi$  y  $\Gamma \models \varphi$  por medio del *modus ponens*.  $\square$

**Teorema 5.3.16.** Sea  $\Gamma \cup \{\psi, \varphi, \xi\}$  un conjunto de fórmulas.

1. Si  $\Gamma, \psi \models \xi$  y  $\Gamma, \varphi \models \xi$ , entonces  $\Gamma, \psi \vee \varphi \models \xi$ .
2. Si  $\Gamma \models \varphi$ , entonces  $\Gamma \models \varphi \vee \psi$

*Demostración.* Supongamos que  $\Gamma, \psi \models \xi$  y  $\Gamma, \varphi \models \xi$ ; entonces, por el *teorema de la deducción* (cfr. [Teorema 5.3.8](#)),  $\Gamma \models \psi \rightarrow \xi$  y  $\Gamma \models \varphi \rightarrow \xi$ . Por [3](#)) del [Ejemplo 5.2.5](#) tenemos que para cualesquier fórmulas  $\alpha, \beta, \gamma$ ,  $\models (\alpha \rightarrow \gamma) \rightarrow ((\beta \rightarrow \gamma) \rightarrow ((\alpha \vee \beta) \rightarrow \gamma))$ . En particular y por la monotonía tenemos:

$$\Gamma \models (\psi \rightarrow \xi) \rightarrow ((\varphi \rightarrow \xi) \rightarrow ((\psi \vee \varphi) \rightarrow \xi))$$

Por *modus ponens* deducimos que  $\Gamma \models (\psi \vee \varphi) \rightarrow \xi$  o equivalentemente  $\Gamma, \psi \vee \varphi \models \xi$ . Supongamos ahora que  $\Gamma \models \varphi$ . Por [1](#)) del [Ejemplo 5.2.5](#) tenemos que para cualesquier fórmulas  $\alpha, \beta, \gamma$ ,  $\models \alpha \rightarrow (\alpha \vee \beta)$ . En particular y por la monotonía tenemos que  $\Gamma \models \varphi \rightarrow (\varphi \vee \psi)$  y por *modus ponens* deducimos que  $\Gamma \models \varphi \vee \psi$ .  $\square$

## 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* es un lenguaje proposicional  $\mathbf{L}_{\mathbf{KA}} = \langle X, Cons, a \rangle$  cumpliendo que:

- $X$  es numerable no finito. Sus elementos serán 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  $P(\mathbf{L})$  en lugar de  $P(\mathbf{L}_{\mathbf{KA}})$ .
2. Los elementos de  $X$  en  $\mathbf{L}_{\mathbf{KA}}$  serán precisados más tarde.

**Definición 5.4.2.** Sea  $\Delta$  un conjunto no vacío de fórmulas del lenguaje  $\mathbf{L}_{\mathbf{KA}}$ . Definimos los siguientes conjuntos:

- $A(\Delta) = \bigcap \{ \Gamma : \Delta \subseteq \Gamma \subseteq P(\mathbf{L}) \text{ y } \Gamma \text{ es cerrado bajo } A \}$
- $K(\Delta) = \bigcap \{ \Gamma : \Delta \subseteq \Gamma \subseteq P(\mathbf{L}) \text{ and } \Gamma \text{ is closed under } K \}$
- $\Xi_A(\Delta) = \bigcap \{ \Gamma : \Delta \subseteq \Gamma \subseteq P(\mathbf{L}) \text{ and } A\alpha\beta \in \Gamma \text{ whenever } \alpha \in \Gamma \text{ and } \beta \in \Delta \}$
- $\Xi_K(\Delta) = \bigcap \{ \Gamma : \Delta \subseteq \Gamma \subseteq P(\mathbf{L}) \text{ and } K\alpha\beta \in \Gamma \text{ whenever } \alpha \in \Gamma \text{ and } \beta \in \Delta \}$

**Definición 5.4.3.** Sea  $\alpha \in P(\mathbf{L}_{KA})$ . La fórmula  $\alpha$  es una *forma normal conjuntiva* (resp. *cláusula*) sii, por definición,  $\alpha \in K(A(X))$  (resp.  $\alpha \in \Xi_A(X)$ ). Por otra parte,  $\alpha$  es una *forma normal conjuntiva a izquierdas* cuando, y sólo cuando,  $\alpha \in \Xi_K(\Xi_A(X))$ . En lo que sigue abreviaremos  $\Xi_K(\Xi_A(X))$  por  $\text{lcnf}(X)$ .

Para tener una medida del “volumen” de una fórmula, introducimos las funciones de *complejidad* y *longitud*.

**Definición 5.4.4.** Para cualquier  $\alpha$  perteneciente a  $P(\mathbf{L}_{KA})$ , la *complejidad* de  $\alpha$ ,  $\text{comp}(\alpha)$ , es por definición:

$$\text{comp}(\alpha) = \begin{cases} 0, & \text{if } \alpha \in X, \\ 1 + \text{comp}(\varphi) + \text{comp}(\psi), & \text{if } \alpha = A\varphi\psi \text{ or } \alpha = K\varphi\psi. \end{cases}$$

y la *longitud* de  $\alpha$ ,  $\text{lg}(\alpha)$ , es por definición:

$$\text{lg}(\alpha) = \begin{cases} 0, & \text{if } \alpha \in X, \\ 1 + \max\{\text{lg}(\varphi), \text{lg}(\psi)\}, & \text{if } \alpha = A\varphi\psi \text{ or } \alpha = K\varphi\psi. \end{cases}$$

Nuestro objetivo ahora es, dada una fórmula  $\varphi$  de  $P(\mathbf{L}_{KA})$ , encontrar otra  $\varphi_{cnf}$  perteneciente a  $K(A(X))$  tal que ambas sean lógicamente equivalentes. Esto será la base del algoritmo y para ello lo primero es determinar cómo de alejada está  $\varphi$  de  $K(A(X))$ .

**Definición 5.4.5.** Sea  $\alpha$  cualquier fórmula perteneciente a  $P(\mathbf{L}_{KA})$ . La *alternancia* de  $\alpha$ ,  $\text{alt}(\alpha)$ , es por definición:

$$\text{alt}(\alpha) = \begin{cases} 0, & \text{si } K \notin \alpha; \\ \max\{\text{alt}(\varphi), \text{alt}(\psi)\}, & \text{si } \alpha = K\varphi\psi; \\ 1 + \max\{\text{alt}(\varphi), \text{alt}(\psi)\}, & \text{si } \alpha = A\varphi\psi \text{ y } K \in \alpha. \end{cases}$$

En el **Lema 5.4.1** caracterizamos qué significa “pertenecer al conjunto  $K(A(X))$ ” mediante la aplicación  $\text{alt}$ .

**Lema 5.4.1.** *Let  $\alpha \in P(\mathbf{L}_{KA})$ . Son equivalentes las siguientes afirmaciones:*

1.  $\text{alt}(\alpha) = 0$ .
2.  $\alpha \in K(A(X))$ .

*Demostración.* Sea  $\alpha$  una fórmula tal que  $\text{alt}(\alpha) = 0$ . Si  $K \notin \alpha$ , entonces  $\alpha \in A(X)$  y así  $\alpha \in K(A(X))$ . Si  $K \in \alpha$ , entonces  $\alpha = K\phi\psi$ , donde  $\text{alt}(\phi) = \text{alt}(\psi) = 0$ . Por hipótesis de inducción,  $\phi, \psi \in K(A(X))$  y entonces  $\alpha \in K(A(X))$ . El recíproco es de demostración inmediata a partir de la **Definición 5.4.5**.  $\square$

**Definición 5.4.6 (distributivity).** Consideremos las siguientes reglas compuestas sobre relaciones binarias entre fórmulas de  $P(\mathbf{L}_{KA})$ :

$$x_i \rightarrow_{dak} x_i \quad (5.2)$$

$$\frac{A\varphi\xi \rightarrow_{dak} \alpha \quad A\psi\xi \rightarrow_{dak} \beta}{AK\varphi\psi\xi \rightarrow_{dak} K\alpha\beta} \quad (5.3)$$

$$\frac{A\xi\varphi \rightarrow_{dak} \alpha \quad A\xi\psi \rightarrow_{dak} \beta}{A\xi K\varphi\psi \rightarrow_{dak} K\alpha\beta} \quad (5.4)$$

$$\frac{\varphi \rightarrow_{dak} \varphi' \quad \psi \rightarrow_{dak} \psi'}{A\varphi\psi \rightarrow_{dak} A\varphi'\psi'} \quad (5.5)$$

$$\frac{\varphi \rightarrow_{dak} \varphi' \quad \psi \rightarrow_{dak} \psi'}{K\varphi\psi \rightarrow_{dak} K\varphi'\psi'} \quad (5.6)$$

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

$$dak: P(\mathbf{L}_{KA}) \longrightarrow P(\mathbf{L}_{KA})$$

por

$$dak(\varphi) = \psi, \text{ siempre que } \varphi \rightarrow_{dak} \psi$$

*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.

El significado esencial del **Teorema 5.4.2** es que aplicando dak a una fórmula dada, digamos  $\varphi$ , el resultado está más cerca de  $K(A(X))$  que  $\varphi$ , ello según la “medida” alt.

**Teorema 5.4.2.** Sea  $\alpha$  una fórmula cualquiera de  $P(\mathbf{L}_{KA})$ . Entonces:

$$alt(dak(\alpha)) = \begin{cases} 0, & \text{si } \alpha \in K(A(X)); \\ alt(\alpha) - 1, & \text{en otro caso.} \end{cases}$$

*Demostración.* Para obtener  $dak(\alpha)$  debemos aplicar una de las cinco reglas dadas en la **Definición 5.4.6**. Así pues tenemos la siguiente casuística.

1.  $\alpha \in A(X)$ ; el resultado se obtiene por el **Lema 5.4.1**.
2.  $\alpha = A K \varphi \psi \xi$ ; de ser así,  $alt(\alpha) = 1 + \max\{alt(\varphi), alt(\psi), alt(\xi)\}$ . Moreover, by **Rule 5.3**,  $alt(dak(\alpha)) = \max\{alt(dak(A \varphi \xi)), alt(dak(A \psi \xi))\}$ . Assume that  $K \in A \varphi \xi$  and  $K \in A \psi \xi$ . Then the value of  $\max\{alt(dak(A \varphi \xi)), alt(dak(A \psi \xi))\}$  is  $\max\{alt(\varphi), alt(\psi), alt(\xi)\}$  and so  $alt(dak(\alpha)) = alt(\alpha) - 1$ . If  $K \notin A \varphi \xi$  or  $K \notin A \psi \xi$ , the proof is similar.
3.  $\alpha = A \varphi K \psi \xi$ . The proof is analogous to the previous case.
4.  $\alpha = A \varphi \psi$  and neither  $\varphi$  nor  $\psi$  begins with K, but  $K \in \alpha$ . Let us assume without loss of generality that  $alt(\varphi) \geq alt(\psi)$ . Then  $alt(\alpha) = 1 + alt(\varphi)$  and so  $alt(dak(\alpha)) = 1 + \max\{alt(dak(\varphi)), alt(dak(\psi))\} = 1 + alt(dak(\varphi)) = alt(\alpha) - 1$ .
5.  $\alpha = K \varphi \psi$ . The proof in this case is analogous to that given for the previous case. □



## Apéndice A

# Alfabeto Griego

Nombre	Mayúscula	Minúscula	Pronunciación	orden L <sup>A</sup> T <sub>E</sub> X
alfa	A	$\alpha$	a	\alpha
beta	B	$\beta$	b,v	\beta
gamma	$\Gamma$	$\gamma$	g	\gamma
delta	$\Delta$	$\delta$	d	\delta
epsilón	E	$\epsilon, \varepsilon$	e breve	\epsilon, \varepsilon
dseta	Z	$\zeta$	z,ds	\zeta
eta	H	$\eta$	e larga	\eta
theta	$\Theta$	$\theta, \vartheta$	th	\theta, \vartheta
yota	I	$\iota$	i	\iota
cappa	K	$\kappa$	k,c	\kappa
lambda	$\Lambda$	$\lambda$	l	\lambda
mu	M	$\mu$	m	\mu
nu	N	$\nu$	n	\nu
xi	$\Xi$	$\xi$	x suave	\xi
omicrón	O	o	o breve	o
pi	$\Pi$	$\pi$	p	\pi
ro	R	$\rho$	r	\rho
sigma	$\Sigma$	$\sigma, \varsigma$	s	\sigma, \varsigma
tau	T	$\tau$	t	\tau
upsilón	$\Upsilon$	$\upsilon$	y,u breve	\upsilon
fi	$\Phi$	$\phi, \varphi$	f,ph	\phi, \varphi
ji	C	$\chi$	j,x fuerte	\chi
psi	$\Psi$	$\psi$	ps,bs	\psi
omega	$\Omega$	$\omega$	o larga	\omega



## Apéndice B

# Prontuario de cálculo clásico proposicional y de primer orden

### definición de sustituir $x$ por $t$ en $\alpha$ ( $\alpha_t^x$ )

1. Si  $\alpha \in \text{Atom}(\mathbf{L})$ ,  $\alpha_t^x$  es la fórmula obtenida sustituyendo las ocurrencias de  $x$  en  $\alpha$  por el término  $t$ .
2.  $(\neg\alpha)_t^x$  es  $\neg(\alpha_t^x)$
3.  $(\alpha \rightarrow \beta)_t^x$  es  $(\alpha_t^x \rightarrow \beta_t^x)$
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 $\alpha$ ”

1. Si  $\alpha \in \text{Atom}(\mathbf{L})$ ,  $x$  es sustituible por  $t$  en  $\alpha$
2.  $x$  es sustituible por  $t$  en  $(\neg\alpha)$  si, y solamente si,  $x$  es sustituible por  $t$  en  $\alpha$
3.  $x$  es sustituible por  $t$  en  $(\alpha \rightarrow \beta)$  si, y solamente si,  $x$  es sustituible por  $t$  en  $\alpha$  y  $\beta$
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  $\alpha$ .

( $x$  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

$$\frac{\begin{array}{l} y \text{ sustituible por } z \text{ en } \alpha \\ z \text{ no ocurre libremente en } \alpha \end{array}}{(z \text{ es sustituible por } y \text{ en } \alpha_z^y) + (\alpha_z^y)^z = \alpha}$$

## algunas abreviaturas

abreviatura	fórmula
$\alpha \vee \beta$	$\neg\alpha \rightarrow \beta$
$\alpha \wedge \beta$	$\neg(\alpha \rightarrow \neg\beta)$
$\alpha \leftrightarrow \beta$	$(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$
$\exists x\alpha$	$\neg(\forall x\neg\alpha)$

## Axiomas

- A1)  $\alpha \rightarrow (\beta \rightarrow \alpha)$  (ley “*a fortiori*” o “*verum sequitur ad quodlibet*”)
- A2)  $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$  (ley autodistributiva o *de Frege*)
- A3)  $(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$  (ley “*reductio ad absurdum*” clásica o fuerte)
- A4)  $\forall x\alpha \rightarrow \alpha_t^x$ , siendo  $x$  sustituible por  $t$  en  $\alpha$ ;
- A5)  $\forall x(\alpha \rightarrow \beta) \rightarrow (\forall x\alpha \rightarrow \forall x\beta)$ ;
- A6)  $\alpha \rightarrow \forall x\alpha$ , donde  $x$  no ocurre libremente en  $\alpha$ .
- A7)  $x \approx x$ ;
- A8)  $x \approx y \rightarrow (\alpha \rightarrow \tilde{\alpha})$ , donde  $\alpha$  es cualquier fórmula atómica del lenguaje y  $\tilde{\alpha}$  es obtenida de  $\alpha$  reemplazando  $x$ , en cero o más (no necesariamente todos) lugares por  $y$ .

## modus ponens (único motor de inferencia)

$$\frac{\Gamma \vdash \varphi \rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$

## leyes implicativas

1.  $\alpha \rightarrow \alpha$  (ley de identidad)
2.  $(\alpha \rightarrow \beta) \rightarrow ((\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma))$  (ley fuerte del silogismo)
3.  $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\beta \rightarrow (\alpha \rightarrow \gamma))$  (ley de conmutación de premisas o cambio del antecedente)
4.  $(\beta \rightarrow \gamma) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$  (ley débil del silogismo)
5.  $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma))$  (ley de *Frege*)
6.  $\alpha \rightarrow ((\alpha \rightarrow \beta) \rightarrow \beta)$
7.  $(\alpha \rightarrow (\alpha \rightarrow \beta)) \rightarrow (\alpha \rightarrow \beta)$  (ley de reducción)
8.  $((\alpha \rightarrow \beta) \rightarrow (\beta \rightarrow \alpha)) \rightarrow (\beta \rightarrow \alpha)$
9.  $((\alpha \rightarrow \beta) \rightarrow \gamma) \rightarrow (\delta \rightarrow ((\beta \rightarrow (\gamma \rightarrow \varepsilon)) \rightarrow (\beta \rightarrow \varepsilon)))$
10.  $\varepsilon \rightarrow ((\alpha \rightarrow \beta) \rightarrow ((\delta \rightarrow \alpha) \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma))$
11.  $((\alpha \rightarrow \beta) \rightarrow \gamma) \rightarrow (((\beta \rightarrow \alpha) \rightarrow \gamma) \rightarrow \gamma)$  (ley de *Dummet*)
12.  $((\alpha \rightarrow \beta) \rightarrow \beta) \rightarrow ((\beta \rightarrow \alpha) \rightarrow \alpha)$  (ley de *Sales* o de *Tanaka*)
13.  $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$  (ley de *Peirce*)

14.  $((((\varphi \rightarrow \psi) \rightarrow (\neg\alpha \rightarrow \neg\beta)) \rightarrow \alpha) \rightarrow \gamma) \rightarrow ((\gamma \rightarrow \varphi) \rightarrow (\beta \rightarrow \varphi))$  (ley de *Meredith*)
15.  $((\alpha \rightarrow \gamma) \rightarrow \beta) \rightarrow (((\beta \rightarrow \alpha) \rightarrow \beta) \rightarrow \beta)$  (ley para la trivalencia del sistema BCK)

#### leyes implicativo-negativas

1.  $\neg\neg\alpha \rightarrow \alpha$  (ley de doble negación clásica o fuerte)
2.  $\alpha \rightarrow \neg\neg\alpha$  (ley de doble negación intuicionista o minimal)
3.  $\neg\neg\neg\alpha \rightarrow \neg\alpha$  (ley de *Brouwer*)
4.  $\neg\alpha \rightarrow (\alpha \rightarrow \beta)$  (ley de *Duns Scoto*)
5.  $\alpha \rightarrow (\neg\alpha \rightarrow \neg\beta)$  (ley débil de *Duns Scoto*)
6.  $(\neg\beta \rightarrow \neg\alpha) \rightarrow (\alpha \rightarrow \beta)$  (ley de contraposición *ponendo ponens* o fuerte)
7.  $(\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \neg\alpha)$  (ley de contraposición *tollendo tollens* o débil)
8.  $(\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \neg\alpha)$  (ley de contraposición *ponendo tollens*)
9.  $(\neg\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \alpha)$  (ley de contraposición *tollendo ponens*)
10.  $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha)$  (ley “*reductio ad absurdum*” intuicionista o minimal)
11.  $(\neg\alpha \rightarrow \alpha) \rightarrow \alpha$  (ley de *Clavius*)
12.  $(\alpha \rightarrow \neg\alpha) \rightarrow \neg\alpha$  (ley débil de *Clavius*)
13.  $\neg(\alpha \rightarrow \alpha) \rightarrow \beta$  (“*ex falso sequitur quodlibet*”)
14.  $\alpha \rightarrow (\neg\beta \rightarrow \neg(\alpha \rightarrow \beta))$
15.  $(\alpha \rightarrow \beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \beta)$  (ley del dilema)
16.  $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha)$
17.  $(\alpha \rightarrow \gamma) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \gamma))$  (ley de *modus ponens* generalizada)

#### algunos sistemas equivalentes

$$\begin{aligned} &\alpha \rightarrow (\beta \rightarrow \alpha) \\ &(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma)) \\ &(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha) \end{aligned}$$

$$\begin{aligned} &\alpha \rightarrow (\beta \rightarrow \alpha) \\ &(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma)) \\ &(\neg\beta \rightarrow \neg\alpha) \rightarrow (\alpha \rightarrow \beta) \end{aligned}$$

$$\begin{aligned} &(\alpha \rightarrow \beta) \rightarrow ((\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)) \\ &(\neg\alpha \rightarrow \alpha) \rightarrow \alpha \\ &\neg\alpha \rightarrow (\alpha \rightarrow \beta) \end{aligned}$$

$$(((\varphi \rightarrow \psi) \rightarrow (\neg\alpha \rightarrow \neg\beta)) \rightarrow \alpha) \rightarrow \gamma \rightarrow ((\gamma \rightarrow \varphi) \rightarrow (\beta \rightarrow \varphi))$$

**leyes implicativo-conjuntivas**

1.  $(\alpha \wedge \beta) \rightarrow \alpha$
2.  $(\alpha \wedge \beta) \rightarrow \beta$
3.  $(\gamma \rightarrow \alpha) \rightarrow ((\gamma \rightarrow \beta) \rightarrow (\gamma \rightarrow (\alpha \wedge \beta)))$
4.  $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta))$
5.  $(\beta \wedge \alpha) \rightarrow (\alpha \wedge \beta)$
6.  $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \wedge \beta) \rightarrow \gamma)$  (ley de importación)
7.  $((\alpha \wedge \beta) \rightarrow \gamma) \rightarrow (\alpha \rightarrow (\beta \rightarrow \gamma))$  (ley de exportación)
8.  $(\alpha \rightarrow \beta) \rightarrow ((\alpha \wedge \gamma) \rightarrow (\beta \wedge \gamma))$
9.  $((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma)$  (otra forma del silogismo llamada “*ex toto*” o transitividad de  $\rightarrow$ )
10.  $(\alpha \wedge (\alpha \rightarrow \beta)) \rightarrow \beta$  (“*modus ponendo ponens*”)

**leyes implicativo-disyuntivas**

1.  $\alpha \rightarrow (\alpha \vee \beta)$
2.  $\beta \rightarrow (\alpha \vee \beta)$
3.  $(\alpha \rightarrow \gamma) \rightarrow ((\beta \rightarrow \gamma) \rightarrow ((\alpha \vee \beta) \rightarrow \gamma))$
4.  $(\alpha \rightarrow (\beta \vee \gamma)) \rightarrow ((\alpha \rightarrow \beta) \vee (\alpha \rightarrow \gamma))$
5.  $(\alpha \rightarrow \beta) \vee (\beta \rightarrow \alpha)$
6.  $(\beta \vee \alpha) \rightarrow (\alpha \vee \beta)$
7.  $(\alpha \rightarrow \varphi) \rightarrow ((\beta \rightarrow \psi) \rightarrow ((\alpha \vee \beta) \rightarrow (\varphi \vee \psi)))$

**otras leyes tautológicas**

1.  $\alpha \vee \neg\alpha$  (“*tertium non datur*” o ley del tercio excluido)
2.  $\neg(\alpha \rightarrow \neg\alpha)$  (principio de no contradicción)
3.  $(\alpha \wedge \neg\alpha) \rightarrow \beta$  (principio de inconsistencia)
4.  $(\neg\beta \wedge (\alpha \rightarrow \beta)) \rightarrow \neg\alpha$  (“*modus tollendo tollens*”)
5.  $((\alpha \vee \beta) \wedge \neg\beta) \rightarrow \alpha$
6.  $((\alpha \vee \beta) \wedge \neg\alpha) \rightarrow \beta$
7.  $((\alpha \vee \beta) \wedge (\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma)) \rightarrow \gamma$
8.  $((\neg\alpha \vee \neg\beta) \wedge (\gamma \rightarrow \alpha) \wedge (\gamma \rightarrow \beta)) \rightarrow \neg\gamma$
9.  $((\alpha \vee \beta) \wedge (\alpha \rightarrow \varphi) \wedge (\beta \rightarrow \psi)) \rightarrow (\varphi \vee \psi)$
10.  $((\neg\alpha \vee \neg\beta) \wedge (\varphi \rightarrow \alpha) \wedge (\psi \rightarrow \beta)) \rightarrow (\neg\varphi \vee \neg\psi)$

---

**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  $\text{Ded}_t$**

$\Gamma \vdash_t \varphi$  ( $\varphi$  es *consecuencia tautológica* de  $\Gamma$ ) si existe una lista finita  $\langle \alpha_1, \dots, \alpha_n \rangle$  tal que  $\varphi = \alpha_n$  y para cada  $1 \leq i \leq n$  se cumple una de las siguientes condiciones:

1.  $\alpha_i$  es una instancia de alguno de los esquemas A1, A2 o A3
2. existen  $1 \leq j, k < i$  tales que  $\alpha_j = \alpha_k \rightarrow \alpha_i$

$$\text{Ded}_t(\Gamma) = \{\varphi : \Gamma \vdash_t \varphi\}$$

**noción de generalización de una fórmula**

$\varphi$  es *generalización* de  $\psi$  si  $\varphi = \psi$  o existen  $x_{i_0}, \dots, x_{i_n}$  tales que  $\varphi = \forall x_{i_0} \dots \forall x_{i_n} \psi$

**definición de  $\vdash_\Upsilon$  y  $\text{Ded}_\Upsilon$**

$\Gamma \vdash_\Upsilon \varphi$  ( $\varphi$  es *consecuencia tautológica* de  $\Gamma$ ) si existe una lista finita  $\langle \alpha_1, \dots, \alpha_n \rangle$  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  $\alpha_j = \alpha_k \rightarrow \alpha_i$

$$\text{Ded}_\Upsilon(\Gamma) = \{\varphi : \Gamma \vdash_\Upsilon \varphi\}$$

En nuestro curso  $\Upsilon$  es el conjunto de las generalizaciones de A1–A6 o A1–A7. Una tal lista  $\langle \alpha_1, \dots, \alpha_n \rangle$  recibe el nombre de  $\langle \Gamma, \Upsilon \rangle$ -prueba de  $\varphi$  o simplemente  $\Gamma$ -prueba de  $\varphi$ .

**propiedades elementales de  $\text{Ded}_t$  y  $\text{Ded}_\Upsilon$**

1.  $\Gamma \subseteq \text{Ded}_t(\Gamma)$
2. Si  $\Gamma \subseteq \Delta$  entonces  $\text{Ded}_t(\Gamma) \subseteq \text{Ded}_t(\Delta)$
3.  $\text{Ded}_t(\text{Ded}_t(\Gamma)) \subseteq \text{Ded}_t(\Gamma)$
4.  $\text{Ded}_t(\Gamma) = \bigcup_{\Phi \in \mathcal{P}_f(\Gamma)} \text{Ded}_t(\Phi)$
5.  $\text{Ded}_t(\Gamma) \subseteq \text{Ded}_\Upsilon(\Gamma)$  (acotación funcional)
6. Si  $\alpha, \alpha \rightarrow \beta \in \text{Ded}_\Upsilon(\Gamma)$ , entonces  $\beta \in \text{Ded}_\Upsilon(\Gamma)$  (ser cerrado por *modus ponens*)
7.  $\Gamma \subseteq \text{Ded}_\Upsilon(\Gamma)$  (acotación de los conjuntos de fórmulas por cerrados)
8. Si  $\Gamma \subseteq \Delta$  entonces  $\text{Ded}_\Upsilon(\Gamma) \subseteq \text{Ded}_\Upsilon(\Delta)$  (monotonía)
9.  $\text{Ded}_\Upsilon(\text{Ded}_\Upsilon(\Gamma)) \subseteq \text{Ded}_\Upsilon(\Gamma)$  (idempotencia)
10.  $\text{Ded}_\Upsilon(\Gamma) = \bigcup_{\Phi \in \mathcal{P}_f(\Gamma)} \text{Ded}_\Upsilon(\Phi)$  (finitariedad)

## algunas equivalencias elementales

fórmula	equivalente
$\neg\neg\alpha$	$\alpha$
$\neg(\alpha \vee \beta)$	$\neg\alpha \wedge \neg\beta$
$\neg(\alpha \wedge \beta)$	$\neg\alpha \vee \neg\beta$
$\neg\alpha \vee \beta$	$\alpha \rightarrow \beta$
$\neg(\alpha \wedge \neg\beta)$	$\alpha \rightarrow \beta$
$\alpha \vee (\beta \wedge \gamma)$	$(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
$\alpha \wedge (\beta \vee \gamma)$	$(\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
$\alpha \wedge (\neg\beta \vee \beta \vee \gamma)$	$\alpha$

regla de *modus ponens* generalizada

$$\frac{\neg\alpha \rightarrow \beta \quad \alpha \rightarrow \gamma}{\neg\beta \rightarrow \gamma}$$

regla de *resolución*

$$\frac{\alpha \vee \beta \quad \neg\alpha \vee \gamma}{\beta \vee \gamma}$$

## teorema de la deducción

$$\frac{\Gamma \vdash \varphi \rightarrow \psi}{\Gamma, \varphi \vdash \psi} \quad \text{y} \quad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}$$

## 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  $\Gamma$ -prueba en la que no sea usada ninguna 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**

$$\frac{\begin{array}{c} \Gamma \vdash \varphi_1 \\ \dots \\ \Gamma \vdash \varphi_n \\ \varphi_1, \dots, \varphi_n \vdash_t \psi \end{array}}{\Gamma \vdash \psi}$$



**reglas de contraposición**

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma, \neg\psi \vdash \neg\varphi} \quad \frac{\Gamma, \neg\varphi \vdash \psi}{\Gamma, \neg\psi \vdash \varphi}$$

$$\frac{\Gamma, \varphi \vdash \neg\psi}{\Gamma, \psi \vdash \neg\varphi} \quad \frac{\Gamma, \neg\varphi \vdash \neg\psi}{\Gamma, \psi \vdash \varphi}$$

**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**

$$\frac{\Gamma \vdash \alpha \rightarrow \beta \quad \Gamma \vdash \beta \rightarrow \gamma}{\Gamma \vdash \alpha \rightarrow \gamma}$$

**regla de isotonía**

$$\frac{\Gamma \vdash \alpha \rightarrow \beta}{\Gamma \vdash (\gamma \rightarrow \alpha) \rightarrow (\gamma \rightarrow \beta)}$$

**regla de antiisotonía**

$$\frac{\Gamma \vdash \alpha \rightarrow \beta}{\Gamma \vdash (\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)}$$

**negación de la flecha**

$$\frac{\Gamma \vdash \alpha \quad \Gamma \vdash \neg\beta}{\Gamma \vdash \neg(\alpha \rightarrow \beta)}$$

$$\frac{\Gamma \vdash \neg(\alpha \rightarrow \beta)}{\Gamma \vdash \alpha} \quad \frac{\Gamma \vdash \neg(\alpha \rightarrow \beta)}{\Gamma \vdash \neg\beta}$$

**regla A4**

$\vdash \forall x\varphi \rightarrow \varphi_t^x$ , si  $x$  es sustituible por  $t$  en  $\varphi$

**regla A4 especial**

$$\vdash \forall x\varphi \rightarrow \varphi$$

**regla E4**

$\vdash \varphi_t^x \rightarrow \exists x\varphi$ , si  $x$  es sustituible por  $t$  en  $\varphi$

**generalización de constantes**

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall y \varphi_y^c}, \text{ si } c \text{ no ocurre en } \Gamma$$

( $y$  no ocurre en  $\varphi$  y  $\Gamma \vdash \forall y \varphi_y^c$  está avalada por un  $\Gamma$ -prueba en la que no interviene  $c$ )

**regla C (versión 1)**

$$\frac{\Gamma \vdash \varphi_c^x}{\Gamma \vdash \forall x \varphi}, \text{ si } c \text{ no ocurre en } \Gamma \cup \{\varphi\}$$

( $\Gamma \vdash \forall x \varphi$  está avalada por un  $\Gamma$ -prueba en la que no interviene  $c$ )

**regla EI**

$$\frac{\Gamma, \varphi_c^x \vdash \psi}{\Gamma, \exists x \varphi \vdash \psi}, \text{ si } c \text{ no ocurre en } \Gamma \cup \{\varphi, \psi\}$$

( $\Gamma, \exists x \varphi \vdash \psi$  está avalada por un  $\Gamma$ -prueba en la que no interviene  $c$ )

**regla C (versión 2 incompleta)**

$$\frac{\begin{array}{l} \Gamma \vdash \exists x \varphi \\ \Gamma, \varphi_c^x \vdash \psi \end{array}}{\Gamma \vdash \psi} \quad \text{si } c \text{ no ocurre en } \Gamma \cup \{\varphi, \psi\}$$

(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)**

$$\frac{\begin{array}{l} \exists x \varphi \in \Gamma \\ \Gamma, \varphi_c^x \vdash \psi \end{array}}{\Gamma \vdash \psi} \quad \text{si } c \text{ no ocurre en } \Gamma \cup \{\psi\}$$

( $\Gamma \vdash \psi$  está avalada por un  $\Gamma$ -prueba en la que no interviene  $c$ )

**regla de extensión**

$$\frac{\varphi \vdash \psi}{\forall x \varphi \vdash \forall x \psi}$$

**definición de  $\exists! x \alpha$** 

$$\exists x \alpha \wedge \forall x \forall y (\alpha \wedge \alpha_y^x \rightarrow x \approx y)$$

( $y$  es el primer s. de variable diferente de  $x$  que no ocurre en  $\alpha$ )

1.  $\vdash \forall x \exists! y x \approx y$
2.  $\vdash \exists! x \alpha \leftrightarrow \exists x \forall y (\alpha_y^x \leftrightarrow x \approx y)$
3.  $\vdash \forall x (\alpha \leftrightarrow \beta) \rightarrow (\exists! x \alpha \leftrightarrow \exists! x \beta)$
4.  $\vdash \exists! x (\alpha \vee \beta) \rightarrow (\exists! x \alpha \vee \exists! x \beta)$
5.  $\vdash \exists! x \alpha \leftrightarrow \exists x (\alpha \wedge \forall y (\alpha_y^x \rightarrow y \approx x))$

( $y$  es el primer s. de variable diferente de  $x$  que no ocurre en  $\alpha$ )

### algunas leyes lógicas con cuantificadores y/o igualdad

1.  $\forall x\varphi \rightarrow \exists x\varphi$
2.  $\exists x\forall y\varphi \rightarrow \forall y\exists x\varphi$
3.  $\forall x\forall y(x \approx y \rightarrow y \approx x)$
4.  $x \approx y \rightarrow (\forall zp(x, z) \rightarrow \forall zp(y, z))$
5.  $\forall x\forall y\forall z\forall v(x \approx z \rightarrow (y \approx v \rightarrow f(x, y) \approx f(z, v)))$
6.  $t_k \approx u \rightarrow (r(t_1, \dots, t_k, \dots, t_n) \rightarrow r(t_1, \dots, u, \dots, t_n))$
7.  $\forall x(x \approx x)$
8.  $\forall x\forall y(x \approx y \rightarrow y \approx x)$
9.  $\forall x\forall y\forall z(x \approx y \rightarrow (y \approx z \rightarrow x \approx z))$
10.  $\forall x\forall y\forall z\forall v(x \approx z \rightarrow (y \approx v \rightarrow f(x, y) \approx f(z, v)))$
11.  $\forall x\forall y\forall z\forall v(x \approx z \rightarrow (y \approx v \rightarrow r(x, y) \approx r(z, v)))$
12.  $x \approx y \rightarrow (\varphi \rightarrow \tilde{\varphi})$ , donde  $\tilde{\varphi}$  es cualquier fórmula obtenida a partir de  $\varphi$  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  $\varphi$

### equivalencia-negación

$$\frac{\vdash \alpha \leftrightarrow \alpha'}{\vdash \neg\alpha \leftrightarrow \neg\alpha'}$$

### equivalencia-implicación

$$\frac{\vdash \alpha' \rightarrow \alpha \quad \vdash \beta \rightarrow \beta'}{\vdash (\alpha \rightarrow \beta) \rightarrow (\alpha' \rightarrow \beta')} \quad \frac{\vdash \alpha \leftrightarrow \alpha' \quad \vdash \beta \leftrightarrow \beta'}{\vdash (\alpha \rightarrow \beta) \leftrightarrow (\alpha' \rightarrow \beta')}$$

### lema de renombramiento de variables

$$\frac{\begin{array}{l} y \text{ sustituible por } z \text{ en } \beta \\ z \text{ no ocurre libremente en } \beta \\ \vdash \alpha \leftrightarrow \beta \end{array}}{\vdash \forall y\alpha \leftrightarrow \forall z(\beta)_z^y}$$

### existencia de variante alfabética

$$\frac{\begin{array}{l} y \text{ s. variable y } t \text{ término} \\ \varphi \text{ fórmula} \end{array}}{\begin{array}{l} \text{existe } \varphi' \text{ tal que} \\ x \text{ es sustit. por } t \text{ en } \varphi' + \vdash \varphi \leftrightarrow \varphi' \end{array}}$$

### 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 supuesto de que  $x$  no ocurra libremente en  $\alpha$ :

1.  $\alpha \leftrightarrow \forall x \alpha$
2.  $\alpha \leftrightarrow \exists x \alpha$
3.  $(\alpha \rightarrow \exists x \beta) \leftrightarrow \exists x (\alpha \rightarrow \beta)$
4.  $(\forall x \beta \rightarrow \alpha) \leftrightarrow \exists x (\beta \rightarrow \alpha)$
5.  $(\alpha \rightarrow \forall x \beta) \leftrightarrow \forall x (\alpha \rightarrow \beta)$
6.  $(\exists x \beta \rightarrow \alpha) \leftrightarrow \forall x (\beta \rightarrow \alpha)$
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

$\alpha$  está en forma prenexa si se expresa como

$$Q_i x_i \cdots Q_n x_n \beta \tag{B.1}$$

donde  $Q_i \in \{\exists, \forall\}$ , para todo  $1 \leq i \leq n$  y en la escritura de  $\beta$  no aparece ningún cuantificador. Llamamos literal a cualquier fórmula que sea atómica o de la forma  $\neg \alpha$ , donde  $\alpha$  es una fórmula atómica. En (B.1),  $\beta$  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  $\varphi$  siempre es posible encontrar, de forma algorítmica, al menos una  $\psi$  en forma normal prenexa tal que

$$\vdash \varphi \leftrightarrow \psi$$

# Índice alfabético

- índice, 20
- ínfimo, 25
  
- alternancia, 87
- asignación, 73
- axioma de elección, 26
- axioma de extensión, 7
  
- biyección, 16
  
- cadena, 24
- cláusula, 87
- clase de equivalencia, 15
- codominio, 14
- complejidad, 87
- complemento relativo, 11
- condición, 8
- condición atómica, 8
- conjunto, 7
  - finitamente satisfacible, 81
  - insatisfacible, 81
  - satisfacible, 81
- conjunto bien ordenado, 25
- 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
- conjunto potencia, 12
- conjunto totalmente ordenado, 24
- conjunto transitivo, 22
- conjuntos comparables, 23
- consecuencia tautológica, 95
- contradicción, 75
  
- diferencia, 11
- diferencia simétrica, 12
- disjuntos, 10
- dominio, 14
  
- elemento, 7
- entero, 26
- enunciado proposicional, 31
- enunciados atómicos, 66
- expresión, 65
- extensión, 17
  
- fórmula, 70, 71
  - refutable, 75
  - satisfacible, 75
  - proposicional, 71
  - complejidad de, 72
  - tautológica, 75
- fórmula proposicional, 31
- fórmula válida, 75
- fórmulas atómicas, 66
- fórmulas equivalentes, 80
- fórmulas lógicamente equivalentes, 80
- factorial, 34
- familia, 20
- familia no vacía, 20
- finitariedad, 85
- forma
  - normal conjuntiva, 87
  - normal conjuntiva a izquierdas, 87
- 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 de ajuste, 45
- función peso, 65
- función sucesor de Peano, 29
  
- gráfica, 16
  
- hipótesis de inducción, 32
  
- identidad, 17
- igualdad, 7

- imagen directa, 16
- imagen inversa, 16
- implicación semántica, 79
- indempotencia, 83
- intersección, 10
- intersección de una familia, 20
  
- Kepler, J., 37
  
- Lamé, G., 37
- lema de Zorn, 26
- lenguaje
  - proposicional standard, 71
  - propo, 86
  - peso, 66
  - proposicional, 65
  - símbolos, 66
- ley
  - ex falso sequitur quodlibet*, 78
  - ex toto*, 78
  - tertium non datur*, 78
  - verum sequitur ad quodlibet*, 76
  - de Frege o autodistributiva, 76
  - de contraposición
    - ponendo ponens*, 77
    - tollendo tollens*, 77
  - de identidad, 75
  - de *a fortiori*, 76
  - de Clavius, 77
    - débil, 78
  - de Dummet, 76
  - de Duns Scoto, 77
    - débil, 77
  - de Meredith, 76
  - de *modus ponens*, 76, 78
    - generalizada, 78
  - de Peirce, 76
  - de *reductio ad absurdum*
    - clásica o fuerte, 77
    - intuicionista o minimal, 77
  - de Tanaka, 76
  - de conmutación de premisas, 76
  - de doble negación
    - clásica o fuerte, 76
    - intuicionista o minimal, 77
  - de exportación, 78
  - de importación, 78
  - de reducción de premisas, 76
  - de silogismo
    - débil, 76
    - fuerte, 75
  - del dilema, 78
    - trivalencia del sist. BCK, 76
- ley de contraposición
  - ponendo tollens*, 77
  - tollendo ponens*, 77
- leyes de De Morgan, 11
- literal, 72
- longitud, 65, 87
- Lucas, F., 37
  
- máximo, 25
- mínimo, 25
- maximal, 25
- mayorante, 25
- minimal, 25
- minorante, 25
- monoide, 65
- monotonía, 83
  
- número entero, 26
- número natural, 21
- números enteros, 26
  
- orden buen, 25
- orden producto, 25
- orden lexicográfico, 25
- orden total, 24
  
- 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, 37
- postulados de Peano, 29
- principio
  - de inconsistencia, 78
  - de no contradicción, 78
  - del *modus tollendo tollens*, 78
  - del tercio excluso, 78
- 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, 44
- recurrencia, 37
  - conjunto fundamental de soluciones, 41
  - ecuación característica, 39
  - lineal homogénea, 39
  - lineal no homogénea, 45
  - matriz compañera, 40
  - orden, 39
  - polinomio característico, 39
  - solución, 39
- 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
  
- símbolos de variable proposicional, 66
- símbolos, 71
- 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, 50
- sucesor, 21
- suma booleana, 12
- supremo, 25
  
- tautología, 75
- teorema de inducción, 22
- teorema de recursión, 33
  
- torres de hanoi, 57
  
- 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.