

MATEMÁTICA DISCRETA

UTN – FRT

## **Capítulo 1. LÓGICA PROPOSICIONAL Y DE PRIMER ORDEN**

Proposiciones. Conectivos lógicos.

Operaciones proposicionales.

Tautología, Contradicciones y Contingencias.

Equivalencias y Leyes Lógicas. Expresiones duales.

Implicaciones lógicas. Razonamientos o argumentos.

Validez de un argumento. Principales Reglas de Inferencia.

Predicados. Cuantificadores.

Reglas de Inferencias de Generalización y Especificación.

MATERIAL EN TRAMITE DE ISBN



## Introducción

La lógica surge desde el momento en que el hombre al enfrentarse a la naturaleza empieza a observar, experimentar, deducir y razonar. En general se aplica en la tarea diaria, ya que cualquier trabajo que se realiza tiene un procedimiento lógico, por ejemplo; para imprimir un archivo en la pc una persona tiene que realizar cierto procedimiento lógico que permita realizar dicha tarea. Por ello, se dice que es una ciencia que estudia la forma del razonamiento, es una disciplina que por medio de reglas y técnicas determina si un argumento o razonamiento es válido o no.

Sin embargo, a veces nuestro razonamiento lógico es deficiente y puede dar lugar a errores. Por lo que se hace necesario percatarse de la existencia de algunas técnicas de la lógica e identificar las leyes fundamentales de las derivaciones lógicas para poder distinguir los razonamientos válidos de los no válidos.

Además, la Lógica se ha convertido en uno de los fundamentos matemáticos y es una base formal indispensable en todo informático. La formalización del conocimiento y la automatización de las formas de razonamiento son primordiales en muchas áreas de la Informática. La importancia de la Lógica en los diseños curriculares de las carreras que tienen que ver con la Informática va tomando cuerpo propio debido a sus aplicaciones en contextos específicos tales como la Programación, la Ingeniería del Software, el Diseño de Sistemas de Bases de Datos y la Inteligencia Artificial, entre otros.

También desempeña un papel central en muchas otras ciencias, y es ampliamente aplicada en la Filosofía, Matemática, Física y Ciencias Naturales, entre otras. En la Filosofía para determinar si un razonamiento es válido, ya que una frase puede tener diferentes interpretaciones, pues la Lógica permite saber el significado correcto. En las Ciencias Física y Naturales, para sacar conclusiones de experimentos, y en Matemática, por ejemplo, para demostrar teoremas e inferir resultados matemáticos, que luego puedan ser aplicados en investigaciones.

Además en Matemática, como en todas las áreas de conocimiento, es necesario

un correcto uso del lenguaje a los efectos de evitar toda ambigüedad que muchas veces se presenta en el lenguaje corriente, es decir, debe existir una absoluta claridad en el uso de los términos empleados, como así también en las definiciones de los nuevos conceptos. Por tal motivo es que la Matemática usa el llamado “lenguaje simbólico” mediante la utilización de una colección de significantes (símbolos) que cobran significado en el contexto comunicacional en el que se esté trabajando. En Lógica a los símbolos se los denomina proposiciones o conectivos lógicos que juntos pueden combinarse y manipularse de varias maneras. Estas manipulaciones corresponden al estudio de la Lógica o Cálculo Proposicional. Pero, ¿Qué es una proposición?

## 1.1 Proposición

### ☞ Definición

Una proposición es toda oración afirmativa completa de la cual se puede decir que es verdadera o falsa, pero no ambas.

### □ Ejemplos 1.1

Las siguientes oraciones son proposiciones:

“La subrutina S ha terminado”

“Einstein fue un físico teórico”

“La letra o tiene dos significados”

“Marcela ganó en la olimpiadas matemáticas”

“10 es número primo”

“Los elementos del lenguaje L son las palabras de L”

También son proposiciones todas las leyes científicas, las fórmulas y esquemas lógicos, los enunciados cerrados, las oraciones aseverativas y las fórmulas matemáticas.

No son proposiciones las opiniones, proverbios, refranes, modismos,

suposiciones o juicios de valor, a las oraciones interrogativas (las que formulan preguntas), las exhortativas o imperativas (las que indican mandato o prohibición), las desiderativas (las que expresan deseos); las exclamativas o admirativas (las que expresan sorpresa o admiración) y los enunciados abiertos (oraciones incompletas). En efecto, no son proposiciones porque ninguna de ellas afirma o niega algo y, por lo tanto, no son verdaderas ni falsas

### □ Ejemplos 1.2

Las siguientes expresiones lingüísticas no son proposiciones:

- a) “La concatenación de  $w$  con  $z$ ”
- b) “La raíz cúbica de una melodía es igual a un fantasma”
- c) “No hay mal que por bien no venga”
- d) “¿Qué es la Lógica?
- e) “¡Imprime ya!”
- f) “Me gustaría que prenda la computadora”
- g) “Prolog es bueno”
- h) “Quizás funcione la notebook”
- i) “El triángulo es inteligente”
- j) “Eduardo es un número racional”
- k) “Esta melodía es una caricia al alma”

### ⌚ Observaciones

- Un enunciado del tipo “ $x$  es un numero entero” no es proposición a pesar de ser una afirmación. No posee valor de verdad. Más adelante se verá este tipo de enunciados, donde pueden aparecer una o más variables sin su especificación.
- Hay oraciones distintas en cuanto a su formación pero que tienen el mismo

significado, ambas constituyen la misma proposición. Por ejemplo:

“El decano de la FRT-UTN visita al Rector de la UTN”

“El Rector de la UTN es visitado por el decano de la FRT-UTN”

## Notación

Se utilizan para designar proposiciones, o bien letras mayúsculas o bien letras minúsculas, pero en este texto se denotará a cada afirmación con letras minúsculas  $p, q, r, \dots$ . Estas letras son variables de enunciado, por lo que mientras no se le asigne una proposición en particular, puede representar a cualquiera. A  $p, q, r, \dots$  se las denomina *variables proposicionales*.

### 1.1.1 Valor de verdad

En lógica matemática, una variable proposicional es una variable discreta que puede ser verdadera o falsa.

A la cualidad de una proposición de ser verdadera o falsa, se la denomina valor de verdad y se indica:  $p = V$  si  $p$  es verdadera y  $p = F$  si  $p$  es falsa.

A “V” y “F”, que representan verdadero y falso, respectivamente, se los denomina *constantes proposicionales*.

Siguiendo la notación utilizadas en las ciencias de la computación, también se puede representar “verdadero” por el símbolo “1”, y “falso” por 0.

### □ Ejemplos 1.3

Sean las proposiciones

$p$ : “Ayer dejó de funcionar la PC”;

$q$ : “ $2 + 3 = 5$ ”;

$r$ : “3 es número primo”;

$s$ : “El rector de la UTN fue presidente de Argentina”

El valor de verdad de  $p$  dependerá del día, lugar o momento en que es

enunciada, pero una vez fijados estos el valor de verdad de  $p$  es único y el mismo para todos. Así podría ser la proposición “el 20 de julio de 1998 dejó de funcionar la PC en el Departamento de Sistema”.

El valor de verdad de  $q$  y  $r$  es verdadero, y el de  $s$  es falso, por lo tanto, los valores de verdad de  $q$ ,  $r$  y  $s$  son constantes:

$$q = 1 , \quad r = 0 \quad y \quad s = 0$$

### 1.1.2 Proposiciones Simples y Compuestas

#### Definición

Una proposición es simple, primitiva o atómica, cuando no hay manera de descomponerla en partes que sean a su vez también proposiciones y cuando no es negación de una afirmación. En caso de no ser proposición simple se dice proposición compuesta o molecular.

#### Ejemplos 1.4

a) Las siguientes oraciones son proposiciones simples:

- i) Sandra programa en C++
- ii) Los ordenadores de 64 bits tienen capacidad de hacer más en menos tiempo.
- iii) La lógica es distinta a la matemática.
- iv) Mi pc tiene poca memoria

Estas oraciones carecen del adverbio de la negación “no” o sus equivalentes, y no se la puede separar en dos proposiciones simples porque carecen de significados, quedarían oraciones abiertas, por lo tanto no son proposiciones.

- v) Euclides y Boole son condiscípulos.

En este caso también es una proposición simple pues no tiene el adverbio de la negación o sus equivalentes, y no se puede separar o descomponer en más de

una proposición, pues “Euclides es condiscípulo” y “Boole es condiscípulo” son oraciones que carecen de sentido, son proposiciones abiertas. En este caso la palabra “y” tiene carácter relacional.

**b)** Las siguientes oraciones son proposiciones compuestas:

- i) 3 no es par.
- ii) Prolog o C++ son lenguajes de programación.
- iii) La adición y la multiplicación de números naturales son asociativas.
- iv) Hace unos años se consideraba al computador como una gran ‘calculadora’, pero hoy se habla de sus logros intelectuales.
- v) Si la inferencia es inductiva entonces es una inferencia en términos de probabilidad.

La oración del apartado i) tiene el adverbio de la negación “no” por lo tanto no es una proposición simple. El resto de las proposiciones combinan proposiciones simples a través de palabras que funcionan como nexos, como: o, y, pero, etc., y se las pueden descomponer en dos proposiciones simples.

### Observaciones

- A partir de proposiciones simples o compuestas se pueden obtener otras proposiciones compuestas mediante el uso de conjunciones o expresiones que tienen el mismo significado y que reciben el nombre de “constantes lógicas”. Estas constantes son reemplazadas por símbolos llamados “conectivos lógicos” y cada uno de ellos dará origen a una “operación lógica”.
- El valor de verdad de las proposiciones compuestas, dependen de las proposiciones por las que están compuestas y de los conectivos.

## 1.2 Conectivos lógicos

Los conectivos lógicos (u operadores o conectores lógicos) además de enlazar o conectar proposiciones establecen determinadas operaciones entre ellas. Son de dos clases: binario y unario.

Los conectivos binarios tienen un doble alcance: hacia la izquierda y hacia la derecha, es decir afectan a dos variables.

La negación (representa el adverbio negativo “no”) es el operador unario y tiene un solo alcance: hacia la derecha, es decir afecta a una sola variable.

Se trabajará con los siguientes conectivos cuyo significado y operación asociada se detallan en la siguiente tabla.

| Conectivo         | Significado   | Operación asociada        |
|-------------------|---|---------------------------|
| $\neg$ , ~        | no, no es cierto, no ocurre                         | Negación                  |
| $\wedge$          | y, pero, también, a la vez, sin embargo, aunque,    | Conjunción                |
| $\vee$            | “o” con sentido incluyente                          | Disyunción inclusiva      |
| $\vee\!\vee$      | “o” con sentido excluyente<br>O bien ... o bien.... | Disyunción exclusiva      |
| $\rightarrow$     | si...entonces,<br>implica                           | Implicación o condicional |
| $\leftrightarrow$ | “si y sólo si” (sii)                                | Doble implicación         |

Tabla 1.1. Conectivos, significado y operación asociada.

Para definir las operaciones entre proposiciones, en el sentido que dadas una o dos proposiciones, cuyos valores de verdad se conocen, se trata de caracterizar la proposición resultante (proposición compuesta) a través de su valor de verdad.

### 1.2.1 Negación

#### Definición

Si  $p$  es una proposición cualquiera, la expresión simbólica  $\neg p$  es la negación de  $p$  y se lee “No  $p$ ”. La proposición compuesta  $\neg p$  toma el valor de verdad contrario al de  $p$ . Esto es, si  $p$  es verdadera,  $\neg p$  es falsa; y si  $p$  es falsa,  $\neg p$  es verdadera.

#### Observaciones

- Se trata de una operación unaria, pues a partir de una proposición se obtiene otra, que es su negación.
- $\neg p$ : también puede leerse como “No es cierto que  $p$ ”, “Es falso que  $p$ ”, “No es verdad que  $p$ ”, etc.
- Se debe ser cuidadoso al negar. Muchos errores se cometen con este concepto. Ejemplos: La negación de “La pizarra es blanca”, no es “La pizarra es negra” sino “La pizarra no es blanca”. La negación de “El cable de la impresora mide más de 170 cm” no es “El cable de la impresora mide menos de 170 cm” sino “El cable de la impresora mide a lo sumo de 170 cm”.

#### Ejemplos 1.5

Sea la proposición  $p$ : “100 es par”, luego su negación ( $\neg p$ ) podría expresarse como:

“100 no es par”

“No es cierto que 100 sea par”

“Es falso que 100 es par”

“100 es impar” (dados que sólo hay dos posibilidades en el conjunto numérico de los enteros, o son pares o son impares).

### 1.2.2 Conjunction o Producto Lógico

#### Definición

Conjunction de las proposiciones  $p$  y  $q$  es la proposición compuesta, que se denota simbólicamente,  $p \wedge q$  y se lee “ $p$  y  $q$ ”.

La proposición compuesta  $p \wedge q = V$  sólo si lo son las dos proposiciones componentes, es decir si  $p = V$  y  $q = V$ . Y es falsa en cualquier otro caso.

#### Observaciones

- Las proposiciones conjuntivas llevan la conjunction copulativa ‘y’, o sus expresiones equivalentes como ‘e’, ‘pero’, ‘aunque’, ‘aun’, ‘tanto...como...’, ‘ni...ni...’, ‘sin embargo’, ‘además’, etc.
- Se puede tener la conjunction de dos o más proposiciones:  $p \wedge q \wedge r \wedge s\dots$

#### Ejemplos 1.6

a) “3 es un número impar y 7 es un número primo”

Se trata de la conjunction de las proposiciones:

$p$ : 3 es un número impar;  $q$ : 7 es un número primo

por ser  $p = V$  y  $q = V$  (ambas verdaderas), la proposición compuesta  $p \wedge q = V$  (es verdadera)

b) “Ignacio juega futbol, rugby y vóley”

Se trata de la conjunction de las proposiciones

$p$ : Ignacio juega futbol;  $q$ : Ignacio juega rugby;  $r$ : Ignacio juega vóley

la proposición compuesta escrita en forma simbólica:  $p \wedge q \wedge r$ , y será F (falsa) si alguna proposición o todas son F.

### 1.2.3 Disyunción Inclusiva o Suma Lógica

#### Definición

Dadas dos proposiciones cualesquiera  $p$  y  $q$ , la expresión simbólica  $p \vee q$  denota la disyunción entre  $p$  y  $q$ , y se lee ‘ $p$  o  $q$ ’.

Esta “o” tiene sentido *incluyente*.

La proposición compuesta  $p \vee q$  es falsa (F) sólo en el caso en que las dos proposiciones componentes sean F, y será V en cualquier otro caso.

#### Observaciones

- $p \vee q$ : se lee a veces ‘ $p$  y/o  $q$ ’.
- Se puede tener disyunción entre dos o más proposiciones:  $p \vee q \vee r \vee s$

#### Ejemplo 1.7

“Hoy llueve o sale el sol”

Representa la disyunción de las proposiciones:

$p$ : Hoy llueve;  $r$ : Hoy sale el sol

El sentido de la disyunción “o” es incluyente, pues si en efecto hoy llovió a la mañana pero a la tarde puede o no salir el sol, en cualquier caso la proposición compuesta  $p \vee q = V$  (es verdadera)

### 1.2.4 Disyunción Excluyente o Diferencia Simétrica

#### Definición

Dadas dos proposiciones cualesquiera  $p, q$  la expresión simbólica  $p \Delta q$  denota la disyunción excluyente entre  $p$  y  $q$ , y se lee “ $p$  o  $q$ , pero no ambas”.

Esta “o” tiene sentido *excluyente*. No da la posibilidad que se den simultáneamente las dos proposiciones.

La proposición compuesta  $p \Delta q$  es V (verdadera) si una y sólo una de las proposiciones componentes es V.

### Observación

$p \vee q$ : se lee también como “O bien  $p$  o bien  $q$ ” o “O  $p$  o  $q$ ”

### Ejemplos 1.8

a) “El rector se elige por consulta popular o por una comisión del consejo”

Representa la disyunción de las proposiciones

$p$ : El rector se elige por consulta popular;  $r$ : El rector se elige por una comisión del consejo

El sentido de la disyunción “o” es excluyente, ya que  $p$  y  $r$  no pueden ser simultáneamente verdaderas. Luego, la proposición compuesta expresada simbólicamente es:  $p \vee r$ .

b) “O el número 2 es par o impar”

Representa la disyunción de las proposiciones

$r$ : el número 2 es par;  $t$ : el número 2 es impar

El sentido de la disyunción “o” es excluyente, pues las proposiciones  $r$  y  $t$  no pueden ser simultáneamente verdaderas. Simbólicamente la proposición compuesta se la expresa como:  $r \vee t$ , la cual será V (verdadera) si una de las proposiciones es verdadera y la otra falsa.

#### 1.2.5 Implicación o condicional

##### Definición

Dadas dos proposiciones cualesquiera  $p, q$  para expresar que cuando suceda  $p$  sucederá  $q$ , simbólicamente se escribe  $p \rightarrow q$  que se lee “Si  $p$  entonces  $q$ ”.

Se dice de  $p$  que es el *antecedente* y  $q$  el *consecuente* del condicional. La implicación sólo es falsa cuando el antecedente es V y el consecuente es F, y verdadera en cualquier otro caso.

### @@Observación

$p \rightarrow q$  tiene otras formas de expresarse en español como: “ $p$  solo si  $q$ ”, “ $p$  es suficiente para  $q$ ”, “ $q$  es necesario para  $p$ ”, “ $p$  implica  $q$ ”, “Si  $p$ ,  $q$ ”, “ $q$  si  $p$ ”, etc.

### □ Ejemplo 1.9

“Si 28 es par entonces es divisible por 2”, es una proposición compuesta del tipo  $p \rightarrow q$  donde  $p$ : “28 es par” y  $q$ : “28 es divisible por 2”.

La misma proposición también puede leerse: “28 es par solo si es divisible por 2”, “Es suficiente que 28 sea par para que sea divisible por 2”, “Es necesario que 28 sea divisible por 2 para que sea par”, “28 es par, implica que 28 es divisible por 2”, “Si 28 es par, es divisible por 2”, “Es divisible por 2 si 28 es par”,...

### 1.2.6 Bicondicional o doble implicación

#### ☒ Definición

Dadas dos proposiciones cualesquiera  $p$ ,  $q$  para expresar que cuando suceda  $p$  sucederá  $q$ , y cuando suceda  $q$  sucederá  $p$ , se escribe simbólicamente ' $p \leftrightarrow q$ ' y se lee ' $p$  si y solo si  $q$ '.

El bicondicional sólo es verdadero si ambas proposiciones tienen el mismo valor de verdad y falso en cualquier otro caso.

#### @@Observaciones

- $p \leftrightarrow q$  puede leerse también como: “ $p$  es necesario y suficiente para  $q$ ”  
(Abreviado se tiene: “ $p$  sii  $q$ ”)
- El bicondicional puede definirse como la conjunción de  $(p \rightarrow q)$  y  $(q \rightarrow p)$ .

### □ Ejemplo 1.10

“T es equilátero si y sólo si T es equiángulo”, es la doble implicación de las proposiciones,  $p$ : ‘T es equilátero’ y  $q$ : ‘T es equiángulo’, es decir simbólicamente la oración es:  $p \leftrightarrow q$

### Actividad 1.1

Indicar cuáles de las siguientes expresiones son proposiciones y en los casos afirmativos, clasificar en simple o compuesta, luego expresar simbólicamente

- i) "No es cierto que 8 es un número par"
- ii) "6 es múltiplo de 3"
- iii) "2 es un número par y  $2^3 = 6$ "
- iv) "7 es impar y trae suerte"
- v) "Si 10 es múltiplo de 2, entonces 10 es par"
- vi) "15 es impar si y solo si 15 es múltiplo de 3 o de 7"

#### 1.2.7 Tablas de verdad

##### Definición

Son tablas que reflejan el valor de verdad de una proposición compuesta para cada una de las posibilidades de valores de verdad de las proposiciones simples que la componen.

En las siguientes tablas se representa a la variable verdadera (V) con el símbolo 1, y a la falsa (F) con 0.

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

Tabla 1.2. Valores de verdad de la Negación.

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ | $p \leq q$ | $p \rightarrow q$ | $p \leftrightarrow q$ |
|-----|-----|--------------|------------|------------|-------------------|-----------------------|
| 0   | 0   | 0            | 0          | 0          | 1                 | 1                     |
| 0   | 1   | 0            | 1          | 1          | 1                 | 0                     |
| 1   | 0   | 0            | 1          | 1          | 0                 | 0                     |
| 1   | 1   | 1            | 1          | 0          | 1                 | 1                     |

Tabla 1.3. Valores de verdad de las Operaciones binarias.

## □ Ejemplos 1.11

Para entender las asignaciones de valores de verdad expresadas en cada renglón de las Tablas 1.2 y 1.3, se asigna a las proposiciones:

$p$ : “Luis circula en moto” y  $q$ : “Luis usa casco”; luego la interpretación coloquial de las expresiones simbólicas: ‘ $\neg p$ ’ , ‘ $p \wedge q$ ’ , ‘ $p \vee q$ ’ , ‘ $p \underline{\vee} q$ ’ , ‘ $p \rightarrow q$ ’ y ‘ $p \leftrightarrow q$ ’ son:

$\neg p$ : “Luis no circula en moto”,

$p \wedge q$ : “Luis circula en moto y usa casco”,

$p \vee q$ : “Luis circula en moto o usa casco”,

$p \underline{\vee} q$ : “O bien Luis circula en moto o bien usa casco”,

$p \rightarrow q$  : “Si Luis circula en moto entonces usa casco” ,

$p \leftrightarrow q$ : “Luis circula en moto si y solo si usa casco”

¿Cuál es el valor de verdad de cada una de ellas?

Para ello se analizan los valores de verdad observando las tablas anteriores:

- “Luis no circula en moto” tomará el valor de verdad contrario a “Luis circula en moto”
- “Luis circula en moto y usa casco” solo tomará el valor de verdad Verdadero cuando Luis haga las dos cosas
- “Luis circula en moto o usa casco” solo tomará el valor de verdad Falso cuando Luis no circule en moto ni use casco, o sea, cuando ambas proposiciones simples sean falsas.
- “Si Luis circula en moto entonces usa casco” será falsa solamente cuando Luis circule en moto sin casco (esta implicación es una ley, y Luis sólo será multado en este caso)
- “Luis circula en moto si y solo si usa casco” nos dice que ambas proposiciones se implican mutuamente. Solo será falsa cuando una sea verdadera y la otra falsa.

## Observaciones

- Las tablas de verdad de proposiciones compuestas con 'n' variables proposicionales tienen  $2^n$  renglones ya que los valores de verdad de cada una deben combinarse con los posibles valores de verdad de las otras.
- En la Figura 1.1 se representa, a través de un diagrama de árbol, todas las combinaciones posibles de los valores de verdad para tres variables proposicionales.

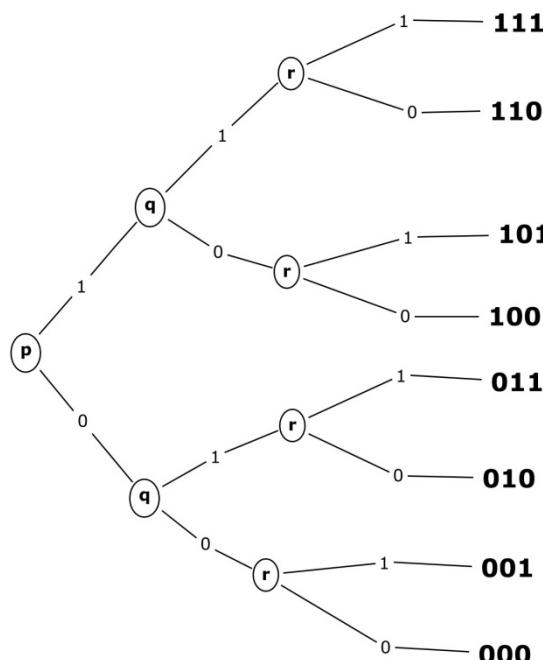


Fig.1.1. Valores de verdad para 3 proposiciones.

### Actividad 1. 2

- a) Confeccionar la tabla de verdad de  $q \wedge (\neg r \rightarrow p)$  y determinar en cuál renglón de la tabla toma el valor verdadero. Para esos casos dar los valores de las variables  $p$ ,  $q$  y  $r$  correspondientes.
- b) Sin realizar la tabla de verdad determinar los valores de verdad de las proposiciones interviniéntes sabiendo que:

- i)  $[p \wedge q \wedge r] = 1$
- ii)  $[(\neg p \vee F) \wedge q] = 1$
- iii)  $[(p \wedge q \wedge r) \rightarrow (s \vee t)] = 0$

### 1.3 Tautologías, Contradicciones y Contingencias

#### ◻ Definiciones

Se llama *tautología* a una proposición compuesta que es verdadera para todas las asignaciones de valores de verdad para sus proposiciones componentes. Si una proposición es falsa para todas las asignaciones se dice *contradicción* y cuando no es tautología ni contradicción se dice *contingencia*.

#### Notación

Con T y F se indica a cualquier tautología y a cualquier contradicción, respectivamente.

#### ◻ Ejemplos 1.12

Las expresiones  $p \vee V$  y  $p \vee \neg p$  son tautologías.

Son contradicciones las expresiones  $p \wedge F$ ,  $p \wedge \neg p$ .

Son contingencias las expresiones  $p \wedge V$ ,  $p \vee F$ ,  $p \wedge p$ ,  $p \vee q$ .

#### Actividad 1.3

Determinar si la siguiente proposición compuesta es tautología, contradicción o contingencia:  $[p \rightarrow (q \rightarrow r)] \leftrightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$

### 1.4 Conectivo Principal

#### ◻ Definición

Se llama conectivo principal al conectivo que da el valor de verdad final de la proposición compuesta

En una expresión lógica completamente entre paréntesis es claro quién es el conectivo principal.

### ◻ Ejemplos 1.13

¿Cuál es el conectivo principal (cp) en las siguientes expresiones lógicas?

$$\begin{array}{ccc} \neg(p \wedge q) & ; & (p \vee q) \wedge (s \rightarrow p) \\ \downarrow & & \downarrow \\ \text{cp} & & \text{cp} \end{array}$$

$$(p \rightarrow q) \rightarrow ((r \vee p) \wedge \neg q)$$

En una expresión sin paréntesis hay que respetar la REGLA DE PRIORIDAD.

La prioridad de mayor a menor está dada por el siguiente orden, (de izquierda a derecha):

$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

### Actividad 1.4

Determinar el conectivo principal en las siguientes afirmaciones

- a)  $p \vee q \wedge \neg r$
- b)  $\neg p \wedge q \rightarrow r$
- c)  $p \vee q \leftrightarrow r \wedge \neg s$

## 1.5 Equivalencias Lógicas

### ◻ Definición

Se dice que dos *expresiones lógicas* cualesquiera A y B, simples o compuestas, son lógicamente equivalentes y se denota  $A \Leftrightarrow B$  o  $A \equiv B$ , cuando ambas expresiones tienen los mismos valores de verdad para cada una de las combinaciones posibles de los valores de verdad de las proposiciones simples intervenientes.

Como *consecuencia* de esta definición se tiene que:

$A \Leftrightarrow B$  si A  $\rightarrow$  B es tautología

### ◻ Ejemplo 1.14

Si A =  $p \wedge q$  y B =  $q \wedge p$ , entonces A  $\equiv$  B

Las Equivalencias Lógicas más simples son la base del Algebra Proposicional y se denominan *Leyes Lógicas*. A continuación se da el listado de las principales leyes lógicas y éstas se pueden demostrar haciendo las correspondientes tablas de verdad.

### 1.5.1 Principales leyes lógicas

Las leyes lógicas son tautologías o formas lógicas verdaderas. Son fórmulas verdaderas independientemente de los valores que asumen sus variables proposicionales componentes.

Su estudio es tarea fundamental de la lógica de proposiciones, puesto que ellas constituyen un poderoso instrumento para el análisis de inferencias, que se verá más adelante.

Para cualquier  $p, q, r$  proposiciones simples, cualquier tautología T y cualquier contradicción F se cumple que:

|            |  |  |                       |
|------------|--|--|-----------------------|
| <b>1.</b>  | $\neg\neg p \Leftrightarrow p$                                       |  | Ley de Doble Negación |
| <b>2.</b>  | $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$                | $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$              | Leyes de De Morgan    |
| <b>3.</b>  | $p \vee q \Leftrightarrow q \vee p$                                  | $p \wedge q \Leftrightarrow q \wedge p$                            | Leyes conmutativas    |
| <b>4.</b>  | $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$                | $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$      | Leyes asociativas     |
| <b>5.</b>  | $(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$ | $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$ | Leyes distributivas   |
| <b>6.</b>  | $p \vee p \Leftrightarrow p$   | $p \wedge p \Leftrightarrow p$                                     | Leyes de Idempotencia |
| <b>7.</b>  | $p \vee F \Leftrightarrow p$   | $p \wedge T \Leftrightarrow p$                                     | Leyes de los Neutros  |
| <b>8.</b>  | $p \vee \neg p \Leftrightarrow T$                                    | $p \wedge \neg p \Leftrightarrow F$                                | Leyes de los Inversos |
| <b>9.</b>  | $p \vee T \Leftrightarrow T$   | $p \wedge F \Leftrightarrow F$                                     | Leyes de Dominación   |
| <b>10.</b> | $p \vee (p \wedge q) \Leftrightarrow p$                              | $p \wedge (p \vee q) \Leftrightarrow p$                            | Leyes de Absorción    |

Tabla 1.4. Principales Leyes Lógicas.

Existen otras equivalencias igualmente importantes que se usarán con mucha frecuencia tanto en el desarrollo de la teoría como en la práctica; ellas son:

|            |  |   |
|------------|--|---|
| <b>11.</b> | $p \vee q \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p)$                  | Ley de la disyunción excluyente             |
| <b>12.</b> | $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$                                | Ley asociativa de la disyunción excluyente  |
| <b>13.</b> | $p \rightarrow q \Leftrightarrow \neg p \vee q$                                      | Ley de la condicional                       |
| <b>14.</b> | $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$                          | Ley de la contrarecíproca de la condicional |
| <b>15.</b> | $\neg(p \rightarrow q) \Leftrightarrow p \wedge \neg q$                              | Ley de la negación de la condicional        |
| <b>16.</b> | $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$     | Ley de la bicondicional                     |
| <b>17.</b> | $\neg(p \leftrightarrow q) \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p)$ | Ley de la Negación de la bicondicional      |

Tabla 1.5. Leyes lógicas vinculadas a los conectivos  $\vee$ ,  $\rightarrow$  y  $\leftrightarrow$ .

### Actividad 1.5

Usando tablas de verdad demostrar:

- i) Una de las leyes distributivas;
- ii) Una de las leyes de absorción;
- iii) La ley de la contrarecíproca;
- iv) La ley de la negación de la condicional
- v) La ley asociativa de la disyunción excluyente

### ❖ Aplicaciones

#### +Circuitos digitales

La lógica proposicional también puede ser utilizada para diseñar circuitos digitales, que transformen secuencias de señales de 1s y 0s en otras secuencias de señales de 1s y 0s. Por ejemplo, un sumador.

## Compuertas

Un circuito digital se piensa abstractamente como una caja negra que establece una relación entre ciertas entradas y la salida:

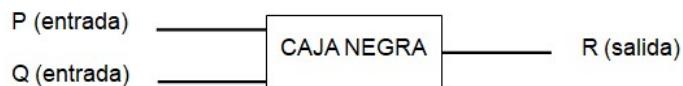


Fig.1.2. Representación circuito digital

La operación del circuito se halla completamente especificada al construir una tabla entrada/salida que liste todos los posibles valores de entrada con su respectivo valor de salida:

Una tabla entrada/salida se ve igual que una tabla de verdad. Probablemente entonces, los circuitos digitales puedan ser representados por oraciones de la lógica proposicional.

En los circuitos digitales se utilizan compuertas lógicas. En la siguiente tabla se observa los operadores, su símbolo y la expresión lógica que lo representa:

| Tipo de compuerta | Representación simbólica | Acción  |         |        |     |   |     |   |     |   |     |   |     |   |
|-------------------|--------------------------|---|---------|--------|-----|---|-----|---|-----|---|-----|---|-----|---|
| Sumadora OR       | p<br>q<br>r              | <table border="1"><thead><tr><th>Entrada</th><th>Salida</th></tr></thead><tbody><tr><td>p q</td><td>r</td></tr><tr><td>1 1</td><td>1</td></tr><tr><td>1 0</td><td>1</td></tr><tr><td>0 1</td><td>1</td></tr><tr><td>0 0</td><td>0</td></tr></tbody></table> | Entrada | Salida | p q | r | 1 1 | 1 | 1 0 | 1 | 0 1 | 1 | 0 0 | 0 |
| Entrada           | Salida                   |   |         |        |     |   |     |   |     |   |     |   |     |   |
| p q               | r                        |   |         |        |     |   |     |   |     |   |     |   |     |   |
| 1 1               | 1                        |   |         |        |     |   |     |   |     |   |     |   |     |   |
| 1 0               | 1                        |   |         |        |     |   |     |   |     |   |     |   |     |   |
| 0 1               | 1                        |   |         |        |     |   |     |   |     |   |     |   |     |   |
| 0 0               | 0                        |   |         |        |     |   |     |   |     |   |     |   |     |   |

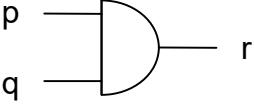
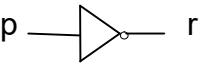
| Multiplicadora<br>AND |  | <table border="1"> <thead> <tr> <th>Entrada</th><th>Salida</th></tr> </thead> <tbody> <tr> <td>p      q</td><td>r</td></tr> <tr> <td>1      1</td><td>1</td></tr> <tr> <td>1      0</td><td>0</td></tr> <tr> <td>0      1</td><td>0</td></tr> <tr> <td>0      0</td><td>0</td></tr> </tbody> </table> | Entrada | Salida | p      q | r | 1      1 | 1 | 1      0 | 0 | 0      1 | 0 | 0      0 | 0 |
|-----------------------|---|---|---------|--------|----------|---|----------|---|----------|---|----------|---|----------|---|
| Entrada               | Salida  |   |         |        |          |   |          |   |          |   |          |   |          |   |
| p      q              | r   |   |         |        |          |   |          |   |          |   |          |   |          |   |
| 1      1              | 1   |   |         |        |          |   |          |   |          |   |          |   |          |   |
| 1      0              | 0   |   |         |        |          |   |          |   |          |   |          |   |          |   |
| 0      1              | 0   |   |         |        |          |   |          |   |          |   |          |   |          |   |
| 0      0              | 0   |   |         |        |          |   |          |   |          |   |          |   |          |   |
| Inversora<br>NOT      |  | <table border="1"> <thead> <tr> <th>Entrada</th><th>Salida</th></tr> </thead> <tbody> <tr> <td>p</td><td>r</td></tr> <tr> <td>1</td><td>0</td></tr> <tr> <td>0</td><td>1</td></tr> </tbody> </table>  | Entrada | Salida | p        | r | 1        | 0 | 0        | 1 |          |   |          |   |
| Entrada               | Salida  |   |         |        |          |   |          |   |          |   |          |   |          |   |
| p                     | r   |   |         |        |          |   |          |   |          |   |          |   |          |   |
| 1                     | 0   |   |         |        |          |   |          |   |          |   |          |   |          |   |
| 0                     | 1   |   |         |        |          |   |          |   |          |   |          |   |          |   |

Tabla 1.6. Compuertas Lógicas.

La aplicación más directa de las compuertas lógicas es la combinación entre dos o más de ellas para formar circuitos lógicos que responden a salidas más complejas (funciones booleanas).

La operación más básica en una computadora como el presionar una tecla del teclado hará que se realicen una serie de operaciones lógicas binarias en microsegundos, esto para poder desplegar el valor de la tecla presionada en la pantalla. Esto es posible gracias a la infinidad de compuertas lógicas que se encuentran dentro del microprocesador de la computadora.

## Circuitos lógicos

Para interpretar el funcionamiento de las máquinas de calcular, se interpretará a las operaciones lógicas mediante circuitos eléctricos. Cada proposición está representada por una llave o interruptor, tal que si la proposición es verdadera deja pasar corriente y si es falsa la corta. La verdad de la proposición compuesta se interpreta como el pasaje de corriente de un terminal  $T_1$  a  $T_2$ , o bien el encendido de una lámpara.

## Negación

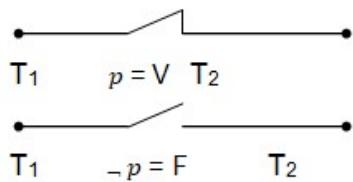


Fig. 1.3. Circuito de la Negación.

## Conjunción

El *circuito lógico* de la conjunción se interpreta mediante un circuito en serie.

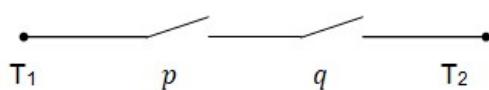


Fig. 1.4. Circuito de la conjunción.

$$p = F ; q = F, \quad p \wedge q = F$$

Únicamente llegará corriente de  $T_1$  a  $T_2$ , si las dos proposiciones son V.

## Disyunción Inclusiva

El *circuito lógico* correspondiente se interpreta mediante un circuito en paralelo.

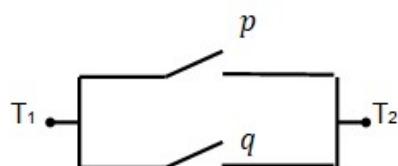


Fig.1.5. Circuito de la disyunción inclusiva.

## Disyunción excluyente

El *circuito lógico* correspondiente a esta operación se hace en base al de las operaciones anteriores, pues decir “ $p$  o  $q$ ” (sentido excluyente) se quiere significar que “se cumple  $p$  y no se cumple  $q$ , o bien no se cumple  $p$  y se cumple  $q$ ”.

En símbolos:

$$p \vee q \text{ es equivalente a } (p \wedge \neg q) \vee (\neg p \wedge q)$$

En consecuencia el circuito lógico será:

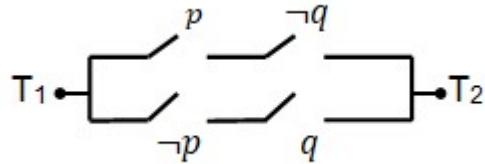


Fig.1.6. Circuito de la disyunción excluyente

#### ⦿ Observación

Cuando se habla de disyunción se refiere a la disyunción con sentido incluyente.

#### Condicional y Bicondicional

Para el *circuito lógico* se tiene en cuenta la siguiente equivalencia. Al decir: “si  $p$  entonces  $q$ ” se está diciendo “no es posible que, se cumpla  $p$  y no se cumpla  $q$ ”, o lo que es lo mismo: “no se cumple  $p$  o se cumple  $q$ ”

Se verifica con tablas de verdad la equivalencia mencionada:

| $p$ | $\neg p$ | $q$ | $\neg q$ | $p \rightarrow q$ | $p \wedge \neg q$ | $\neg(p \wedge \neg q)$ | $\neg p \vee q$ |
|-----|----------|-----|----------|-------------------|-------------------|-------------------------|-----------------|
| V   | F        | V   | F        | V                 | F                 | V                       | V               |
| V   | F        | F   | V        | F                 | V                 | F                       | F               |
| F   | V        | V   | F        | V                 | F                 | V                       | V               |
| F   | V        | F   | V        | V                 | F                 | V                       | V               |

Tabla 1.7. Equivalencias del Condicional.

Como las columnas remarcadas son iguales, las expresiones son equivalentes, por lo tanto al circuito lógico se lo realiza en base a la tercera columna. Como es una disyunción corresponde un circuito en paralelo. Y como el bicondicional es una conjunción de condicionales ambos circuitos quedan a cargo del lector.

### 1.5.2 Expresiones lógicas duales

Observe en la Tabla 1.4 que a menos de la ley de la doble negación el resto de las leyes vienen de a pares, las propiedades valen tanto para la disyunción como para la conjunción. Esto se expresa en el siguiente concepto.

 **Definición:** Sea A una expresión lógica tal que no contiene condicionales ni bicondicionales. Se llama expresión lógica dual de A, que se denota  $A^d$ , a la expresión que se obtiene de A al reemplazar cada ocurrencia de  $\wedge$  por  $\vee$ , y viceversa y cada ocurrencia de T por F, y viceversa.

#### □ Ejemplos 1.15

Las siguientes expresiones son duales:

a)  $\neg(p \vee q)$  y  $\neg(p \wedge q)$

b)  $(p \vee q) \wedge r$  y  $(p \wedge q) \vee r$

¿Por qué es importante el conocimiento de las expresiones duales?. La respuesta está en la siguiente propiedad:

#### Propiedad de las expresiones duales

Sean A y B dos expresiones lógicas y sean  $A^d$  y  $B^d$  sus correspondientes duales. Se tiene que  $A \Leftrightarrow B$  si y solo si  $A^d \Leftrightarrow B^d$

Esto significa que si se demuestra la equivalencia entre A y B, no hará falta probar la equivalencia entre sus expresiones duales.

#### Uso de las leyes lógicas en la manipulación de las expresiones lógicas

Las leyes lógicas se usan: i) para demostrar otras equivalencias, donde

intervienen muchas variables proposicionales, pues realizar la tabla de verdad es muy tedioso por el número de combinaciones posibles de los valores de verdad de las mismas; ii) para encontrar frases que transmitan el mismo mensaje y, por supuesto, conserven el valor de verdad; esto es: frases equivalentes; y iii) para demostrar la validez de un razonamiento, concepto que se verá más adelante.

### Actividad 1.6

a) Sin realizar tablas de verdad, demostrar las siguientes equivalencias lógicas usando leyes lógicas. Luego escribir la expresión dual, si es que existe.

i)  $(\neg p \wedge \neg q \wedge \neg r) \wedge (p \vee q \vee r) \Leftrightarrow F$

ii)  $[(p \rightarrow q) \wedge (p \rightarrow r)] \Leftrightarrow [p \rightarrow (q \wedge r)]$

iii)  $\neg ((r \vee p) \wedge \neg p) \Leftrightarrow \neg r \vee p$

b) Llenar la línea de puntos con una frase equivalente, y justificar su respuesta:

i) No es cierto que no estudié  $\Leftrightarrow \dots$

ii) No estudie inglés ni Francés  $\Leftrightarrow \dots$

iii) No es cierto que, comeré chocolates o caramelos  $\Leftrightarrow \dots$

iv) No es cierto que, si cobro el dinero viajare al sur  $\Leftrightarrow \dots$

c) Negar las siguientes expresiones usando las equivalencias correspondientes.

Escribir simbólicamente a ambas expresiones

i) Aprobaré Algebra y Discreta.

ii) Si la universidad brinda becas de estudio, podré estudiar.

### 1.6 Implicación Lógica

#### Definición

Sean A y B dos expresiones lógicas. Se dice que A implica lógicamente a B si y solo si cada vez que A es verdadera, B también lo es. Se denota:  $A \Rightarrow B$

Como consecuencia de esta definición se tiene que:

$A \Rightarrow B$  si y solo si  $A \rightarrow B$  es tautología.

### □ Ejemplo 1.16

Observar los 3° y 4° renglones de la Tabla 1.8, cada vez que el antecedente ( $p$ ) es verdadero, el consecuente ( $p \vee q$ ) también lo es, razón por la cual se puede escribir que  $p \Rightarrow p \vee q$

| $p$ | $q$ | $p \vee q$ | $p \rightarrow p \vee q$ |
|-----|-----|------------|--------------------------|
| 0   | 0   | 0          | 1                        |
| 0   | 1   | 1          | 1                        |
| 1   | 0   | 1          | 1                        |
| 1   | 1   | 1          | 1                        |

Tabla 1.8. Valores de verdad de  $p \rightarrow p \vee q$ .

### Actividad 1.7

Demostrar y analizar el mensaje que transmite cada implicación lógica. Dar un ejemplo coloquial donde se vea su aplicación:

- $[(p \rightarrow q) \wedge \neg q] \Rightarrow \neg p$
- $[(p \rightarrow q) \wedge (q \rightarrow r)] \Rightarrow (p \rightarrow r)$

#### 1.6.1 Razonamientos o Argumentos

**Definición:** Un razonamiento o argumento es toda expresión lógica cuya estructura es del tipo  $(p_1, p_2, \dots, p_n) \rightarrow q$  donde  $p_1, p_2, \dots, p_n$  (premisas) y  $q$  (conclusión) son proposiciones cualesquiera.

Otra forma de notación es en formato vertical:

$$\begin{array}{c} p_1 \\ p_2 \\ \vdots \\ \underline{p_n} \\ \therefore q \end{array}$$

Se lee: “ $p_1, p_2, \dots, p_n$ , por lo tanto  $q$ ”

### □ Ejemplo 1.17

Dado el siguiente argumento:

*“Esta noche viene Luis. Si viene Luis entonces voy al cine. Por lo tanto, esta noche llueve”*

Se tienen dos premisas,

$p_1$ : *Esta noche viene Luis* , y  $p_2$ : *Si viene Luis entonces voy al cine.*

La conclusión  $q$ : *esta noche llueve.*

¿Qué se puede observar de este argumento? ¿La conclusión “esta noche llueve” se deduce de las premisas dadas?

La respuesta es No, porque hay dos clases de argumentos, los válidos (los coherentes, los que tienen sentido) y los no válidos.

### 1.6.2 Validez de un argumento

#### ☞ Definición

Se dice que un argumento es válido cuando la conclusión se infiera (se deduzca) de las premisas. Esto es, cuando la conclusión sea verdadera cada vez que las premisas lo sean.

Por lo tanto una vía para establecer la validez de un argumento es demostrar que la proposición  $(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$  es una tautología. Esto es, debe suceder que  $(p_1 \wedge p_2 \wedge \dots \wedge p_n) \Rightarrow q$  , luego todas las implicaciones lógicas nos brindan razonamientos válidos.

#### ☞ Observación

No hace falta hacer toda la tabla de verdad de  $(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$  , sólo se necesita analizar el/los casos donde las premisas  $p_1 \wedge p_2 \wedge \dots \wedge p_n$  sean verdaderas y se debe constatar que la conclusión  $q$  es verdadera también.

## 1.7 Reglas de Inferencia

La idea de inferencia se puede expresar de la manera siguiente: de premisas verdaderas se obtienen sólo conclusiones que son verdaderas. Es decir, si las premisas son verdaderas, entonces las conclusiones que se derivan o se infieren de ellas lógicamente, han de ser verdaderas.

### Definición

Al conjunto de razonamientos válidos, se les llama Reglas de Inferencia.

Las reglas de inferencia que rigen el uso de los términos de enlace son muy simples. Ellas son:

### 1.7.1 Modus Ponens (MP)

La regla de inferencia llamada *modus ponendo ponens* (generalmente llamada simplemente *modus ponens*) permite demostrar ‘q’ a partir de  $p \rightarrow q$  y  $p$ .

$$\begin{array}{c} p \rightarrow q \\ \hline p \\ \therefore q \end{array}$$

La misma regla se aplica tanto si el antecedente es una proposición simple o compuesta, y tanto si el consecuente es una proposición simple o compuesta.

### Ejemplos 1.18

a) Sea el siguiente argumento:

“Si Silvio estudia ISI, entonces cursará Matemática Discreta. Silvio estudia ISI. Luego, Silvio cursará Matemática Discreta.”

Considerando  $p$ : “Silvio estudia ISI”,  $q$ : “Silvio cursará Matemática Discreta”.

Su forma simbólica es

$$p \rightarrow q$$

$$\begin{array}{c} p \\ \hline \therefore q \end{array}$$

b) Sea el siguiente argumento:

“Si Juan José no aprueba Matemática I, no cursará Matemática II. Juan José no aprueba Matemática I. Por consiguiente, Juan José no cursará Matemática II.”

Su forma simbólica es

$$\neg p \rightarrow \neg q$$

$$\frac{\neg p}{\neg q}$$

$$\therefore \neg q$$

Siendo

$p$ : “Juan José aprueba Matemática I” y  $q$ : “Juan José cursará Matemática II”

c) En todos los ejemplos que se dan a continuación se aplica el *modus ponens*:

i)  $p$

$$\frac{p \rightarrow \neg q}{\therefore \neg q}$$

ii)  $\neg p \rightarrow q$

$$\frac{\neg p}{\therefore q}$$

iii)  $p \wedge q \rightarrow r$

$$\frac{p \wedge q}{\therefore r}$$

iv)  $p$

$$\frac{p \rightarrow q \wedge r}{\therefore q \wedge r}$$

En cada uno de los ejemplos, la regla *modus ponens* permite pasar de dos premisas a la conclusión. Decir que la conclusión es consecuencia lógica de las premisas, o sea, que siempre que las premisas sean ciertas, la conclusión es también cierta.

El nombre *modus ponendo ponens* se puede explicar de la siguiente manera: esta regla de inferencia es el método (*modus*), que afirma (*ponens*) el consecuente, afirmando (*ponendo*) el antecedente.

### 1.7.2 Modus Tollens (MT)

La regla de inferencia que tiene el nombre latino *modus tollendo tollens* se aplica también a las proposiciones condicionales. Pero en este caso, negando (*tollendo*) el consecuente, se puede negar (*tollens*) el antecedente de la condicional.

$$p \rightarrow q$$

$$\underline{\neg q}$$

$$\therefore \neg p$$

La misma regla se aplica tanto si el antecedente es una proposición simple o compuesta, y tanto si el consecuente es una proposición simple o compuesta.

### □ Ejemplos 1.11

a) La deducción siguiente es un ejemplo del uso del modus tollens.

“Si tiene luz propia, entonces el astro es una estrella. El astro no es una estrella. Por tanto no tiene luz propia.”

Se simbolizará al argumento de la siguiente manera:

sea  $p$ : “Tiene luz propia” y  $q$ : “El astro es una estrella”

$$p \rightarrow q$$

$$\underline{\neg q}$$

$$\therefore \neg p$$

b) “Si la memoria de la pc es la correcta, el análisis de la base de dato se podrá realizar. No se pudo realizar el análisis de la base de dato. Luego, la memoria de la pc no es la correcta.”

Sean  $p$ : La memoria de la pc es correcta;  $r$ : El análisis de la base de dato se puede realizar

$$p \rightarrow r$$

$$\underline{\neg r} .$$

$\therefore \neg p$  que coincide con la estructura válida del Modus Tollens.

c) En los ejemplos siguientes, se usa la regla modus tollendo tollens que permite pasar de dos premisas (una de las premisas es una condicional, y la otra premisa niega el consecuente), a una conclusión que niega el antecedente.

|                                    |                            |                                 |                                      |
|------------------------------------|----------------------------|---------------------------------|--------------------------------------|
| i) $q$                             | ii) $\neg p \rightarrow q$ | iii) $p \wedge q \rightarrow r$ | iv) $\neg(q \vee r)$                 |
| $\underline{p \rightarrow \neg q}$ | $\underline{\neg q}$       | $\underline{\neg r}$            | $\underline{p \rightarrow q \vee r}$ |
| $\therefore \neg p$                | $\therefore p$             | $\therefore \neg(p \wedge q)$   | $\therefore \neg p$                  |

### 1.7.3 Adición disyuntiva

La regla o *ley de adición* expresa el hecho que si se tiene una proposición que es cierta, entonces la disyunción de aquella proposición y otra cualquiera “ha de ser también cierta”.

Si se da la proposición  $p$ , entonces la proposición  $p \vee q$  es consecuencia de  $p$ .

Una justificación es recordar el significado de la disyunción:  $p \vee q$  indica que por lo menos una de las dos proposiciones ligadas por el término de enlace «o» ha de ser cierta. Además sólo una ha de ser necesariamente cierta. Puesto que se ha dado  $p$  como proposición cierta, se sabe que  $p \vee q$  ha de ser una proposición cierta; y esto es precisamente lo que se entiende por una conclusión lógica válida.

En forma simbólica la *regla de adición* quedaría:

$$\begin{array}{ccc} \underline{p} & \text{ó} & \underline{p} \\ \therefore p \vee q & & \therefore q \vee p \end{array}$$

#### □ Ejemplos 1.12

a) Con ejemplos en lenguaje ordinario se ve lo obvia que es esta regla.

Si, como premisa cierta, se tiene que:

“Daniela aprobó el parcial de Matemática Discreta”

Entonces se puede concluir que las siguientes proposiciones deben ser ciertas:

“Daniela aprobó el parcial de Matemática Discreta o el parcial de Análisis”.

“Daniela aprobó el parcial de Matemática Discreta o el final de Algebra”.

“Daniela aprobó el parcial de Matemática Discreta o el parcial de Análisis”, y así hay infinitos ejemplos.

En todos estos ejemplos una parte es cierta y esto es todo lo que se necesita para que una disyunción sea cierta.

En forma simbólica, si se tiene la proposición  $p$ , se puede concluir:

$p \vee q$ , o  $p \vee r$ , o  $s \vee p$ , o  $t \vee p$ , y así sucesivamente.

**b)** Otros ejemplos de la ley de adición son:

i)  $\underline{q}$

$\therefore q \vee r$

ii)  $\underline{\neg r}$

$\therefore p \vee \neg r$

iii)  $\underline{p \wedge \neg q}$

$\therefore (p \wedge \neg q) \vee r$

iv)  $\underline{\neg p}$

$\therefore \neg p \vee \neg q$

#### Observación

De  $p$  se puede deducir  $p \vee q$ , o se puede deducir  $q \vee p$  por la comutatividad de la conjunción.

#### 1.7.4 Combinación conjuntiva

Se suponen dadas dos proposiciones verdaderas como premisas, entonces se podrían juntar en una proposición simple utilizando el término de enlace «y» y se tendría una proposición verdadera.

La regla que permite pasar de las dos premisas a la conclusión se denomina regla de combinación conjuntiva o de adjunción.

Si ambas premisas son ciertas, entonces la conclusión tendría que ser cierta. De manera simbólica se puede ilustrar la regla así:

$$\begin{array}{c} p \\ \underline{q} \\ \therefore p \wedge q \end{array}$$

$$\begin{array}{c} p \\ \underline{q} \\ \therefore q \wedge p \end{array}$$

El orden de las premisas es indiferente, y también porque en la conjunción se puede alterar el orden.

### □ Ejemplos 1.13

a) Dadas dos proposiciones como premisas,

$p$ : “El número atómico del hidrógeno es 1”,

$q$ : “El número atómico del helio es 2.”

La conclusión podría ser: o bien “El número atómico del hidrógeno es 1 y del helio es 2”, o bien “El número atómico del helio es 2 y del hidrógeno es 1”

b) En los siguientes ejemplos, se dan varios argumentos en los que se utiliza la regla de combinación o adjunción.

|    |                                  |     |                                   |      |   |     |                                      |
|----|----------------------------------|-----|-----------------------------------|------|---|-----|--------------------------------------|
| i) | $q \wedge r$                     | ii) | $\neg p$                          | iii) | $p \wedge q$                            | iv) | $\neg(q \vee r)$                     |
|    | $\underline{p \wedge q}$         |     | $\underline{\neg q}$              |      | $\underline{\neg r}$                    |     | $\underline{p}$                      |
|    | $\therefore p \wedge q \wedge r$ |     | $\therefore \neg p \wedge \neg q$ |      | $\therefore (p \wedge q \wedge \neg r)$ |     | $\therefore \neg(q \vee r) \wedge p$ |

#### 1.7.5 Simplificación de la conjunción

La regla que permite pasar de una conjunción a cualquiera de las dos proposiciones que están unidas por ‘ $\wedge$ ’ se denomina *regla de simplificación*.

Esta regla es opuesta a la anterior (combinación). En forma simbólica la regla de simplificación es:

$$\begin{array}{ccc} \underline{p \wedge q} & \text{ó} & \underline{p \wedge q} \\ \therefore p & & \therefore q \end{array}$$

## □ Ejemplos 1.14

a) Si se tiene una premisa que dice:

“El número 2 es par y primo”

De esta premisa se pueden deducir dos proposiciones. Una conclusión es:

“El número 2 es par”.

La otra conclusión es:

“El número 2 es primo”.

Si la premisa es cierta, cada una de las conclusiones es también es cierta.

b) Otros ejemplos del uso de la regla de simplificación son:

$$\begin{array}{llll} \text{i)} & \underline{(p \vee q) \wedge r} & \text{ii)} & \underline{(p \vee q) \wedge r} \\ & \therefore r & & \therefore (p \vee q) \\ & & \text{iii)} & \underline{\neg p \wedge \neg q} \\ & & \therefore \neg p & \\ & & & \text{iv)} \quad \underline{\neg p \wedge \neg q} \\ & & & \therefore \neg q \end{array}$$

### ⦿ Observación

La regla de simplificación *no se puede* aplicar a  $p \wedge q \rightarrow r$ , cuyo significado es:  $(p \wedge q) \rightarrow r$  (por la regla de prioridad); pero se puede aplicar a  $p \wedge (q \rightarrow r)$ , obteniendo como conclusión  $p \wedge q \rightarrow r$ .

### 1.7.6 Silogismo hipotético (SH)

A partir de dos fórmulas condicionales, donde el consecuente de la primera es el antecedente de la segunda, se obtiene una condicional formada por el antecedente de la primera y el consecuente de la segunda.

En forma simbólica:

$$p \rightarrow q$$

$$\underline{q \rightarrow r}$$

$$\therefore p \rightarrow r$$

## □ Ejemplos 1.15

a) “3 es mayor que 2 si 4 es mayor que 3. Además 4 es mayor que 2 si 3 es mayor que 2 . Luego, si 4 es mayor que 3 entonces 4 es mayor que 2.”

Forma lógica:

$p_1$ : Si 4 es mayor que 3, entonces 3 es mayor que 2.

$p_2$ : Si 3 es mayor que 2 , entonces 4 es mayor que 2

$q$ : Si 4 es mayor que 3 entonces 4 es mayor que 2

Por lo tanto se tiene un razonamiento (con dos premisas y su conclusión) del tipo “  $p_1, p_2$  por lo tanto  $q$ ”.

Fórmula: para identificar si un razonamiento es válido es necesario analizar cada premisa y conclusión, ver las proposiciones simples que la componen y así deducir la relación que las vincula.

Para ello, sean:

$p$ : “4 es mayor que 3”;  $q$ : “3 es mayor que 2”, y  $r$ : “4 es mayor que 2”

$$(p_1) p \rightarrow q$$

$$(p_2) q \rightarrow r$$

$\therefore p \rightarrow r$  (Conclusión), fórmula que coincide con la estructura válida del Silogismo Hipotético.

b) Los siguientes argumentos, reflejan la regla del silogismo hipotético, obsérvese que algunos de los antecedentes y consecuentes son proposiciones compuestas. La forma, sin embargo, es la misma.

i)

$$\neg p \rightarrow \neg q$$

$$\underline{\neg q \rightarrow \neg r}$$

$$\therefore \neg p \rightarrow \neg r$$

ii)

$$\neg p \rightarrow q \vee r$$

$$\underline{q \vee r \rightarrow \neg t}$$

$$\therefore \neg p \rightarrow \neg t$$

iii)

$$s \rightarrow t$$

$$\underline{t \rightarrow r \vee q}$$

$$\therefore s \rightarrow r \vee q$$

iv)

$$(q \vee r) \rightarrow s$$

$$\underline{s \rightarrow p}$$

$$\therefore (q \vee r) \rightarrow p$$

### 1.7.7 Silogismo disyuntivo (SD)

Esta regla dice que negando (*tollendo*) un miembro de una disyunción se afirma (*ponens*) el otro miembro. De allí que también se la denomina *modus tollendo ponens*.

Simbólicamente, el silogismo disyuntivo se puede expresar:

De la premisa:  $p \vee q$

y la premisa:  $\neg p$

se puede concluir:  $\therefore q$

o

De la premisa:  $p \vee q$

y la premisa:  $\neg q$

se puede concluir:  $\therefore p$

#### □ Ejemplos 1.16

a) Si se tiene como premisa 1, la disyunción: “Esta sustancia contiene hidrógeno o contiene oxígeno”; la premisa 2 dice: “Esta sustancia no contiene hidrógeno”. Luego, por medio del SD se puede concluir: “Esta sustancia contiene hidrógeno”.

Para aclarar la *forma* de esta inferencia, se puede simbolizar considerando las proposiciones:

$p$ : “Esta sustancia contiene hidrógeno” y  $q$ : “Esta sustancia contiene oxígeno”

La demostración de la conclusión es:

$p \vee q$  (premisa 1)

$\neg p$  (premisa 2)

$\therefore q$  (conclusión)

El SD no está limitado a proposiciones simples. Igual que los otros tipos de proposiciones, la disyunción tiene lugar entre proposiciones compuestas de igual

manera que entre proposiciones simples.

|                    |                     |                            |                          |
|--------------------|---------------------|----------------------------|--------------------------|
| i) $q \vee \neg r$ | ii) $\neg p \vee t$ | iii) $(p \wedge q) \vee s$ | iv) $\neg q \vee \neg r$ |
| $\frac{}{r}$       | $\frac{}{\neg t}$   | $\frac{}{\neg s}$          | $\frac{}{\neg(\neg q)}$  |
| $\therefore q$     | $\therefore \neg p$ | $\therefore (p \wedge q)$  | $\therefore \neg r$      |

### Observaciones

En el SD una premisa es contraria a uno de los alcances de la disyunción. La conclusión afirma precisamente la otra parte. No importa cuál sea el miembro (o alcance) negado, el derecho o el izquierdo. La disyunción dice que por lo menos un miembro se cumple; por lo tanto, si se encuentra que uno de los miembros *no* se cumple, se sabe que el otro ha de cumplirse.

### Actividad 1.8

Escribir una conclusión que se deduzca de las premisas que se dan en cada caso, justificando su respuesta:

- a) Estudio inglés y francés. Por lo tanto,.....
- b) Si el banco depositara el dinero, pagaré. El banco depositó el dinero. Por lo tanto, .....
- c) Si el banco depositara el dinero, pagaré. Pero no pague. Por consiguiente,.....
- d) Si el banco depositara el dinero, pagaré. Si pagara, cancelaría la deuda. Por lo tanto, .....

### 1.8 Tipos de demostraciones para validar un razonamiento

Una importante aplicación de los conceptos de consecuencias y equivalencias lógicas y de las reglas de inferencia se encuentra cuando en Matemática se necesita demostrar teoremas, que son básicamente una implicación lógica del tipo  $p \Rightarrow q$ , donde  $p$  es la hipótesis (datos o premisas) y  $q$  es la tesis (o conclusión).

En todo teorema  $p \Rightarrow q$  se requiere que el condicional sea tautológico.

Los métodos de demostración usuales en Matemática se clasifican en directos e indirectos.

### 1.8.1 Método directo

Es el método de demostración más empleado en Matemática y que consiste en demostrar la verdad de una conclusión o tesis, dadas unas premisas o hipótesis, que son verdaderas.

En la tabla de verdad de la implicación (Tabla 1.9), en los 3º y 4º renglones se puede concluir que bajo el supuesto de que  $p$  sea verdadera (1) la única condición para que la implicación sea verdadera es que  $q$  sea verdadera.

| $p$ | $q$ | $p \rightarrow q$ |
|-----|-----|-------------------|
| 0   | 0   | 1                 |
| 0   | 1   | 1                 |
| 1   | 0   | 0                 |
| 1   | 1   | 1                 |

Tabla 1.9. Casos donde  $p = 1$ .

En el caso de la demostración de la validez de un razonamiento  $p_1, p_2, \dots, p_n \rightarrow q$ , por este método, se usan reglas de inferencia o leyes lógicas para demostrar que la conclusión se infiere o se deduce de las premisas.

Se puede utilizar el formalismo de la deducción Natural o *Derivación Formal* para describir los pasos dados en la demostración y la justificación de cada uno de ellos.

### Procedimiento de deducción

1. Se determina cuáles son las premisas y se escribe cada premisa en una línea numerada, comenzando en 1.
2. Se determina cuál es la conclusión, y se deja aparte, que es lo que se quiere demostrar.
3. Se aplican leyes lógicas o reglas de inferencia sobre las premisas de la cual se derivan nuevas líneas, que se deben seguir numerando a

continuación de la última premisa.

4. El proceso termina cuando se llega a una línea que contiene lo que se quiere demostrar.

### □ Ejemplos 1.17

- a) Para demostrar la validez del siguiente argumento:

$$p, p \rightarrow q, \neg r \rightarrow \neg q, s \vee \neg r \Rightarrow s$$

Es aconsejable seguir el siguiente formato, que se denomina *Derivación formal*.

- |                                |   |
|--------------------------------|---|
| 1) $p$                         | premisa                                 |
| 2) $p \rightarrow q$           | premisa                                 |
| 3) $\neg r \rightarrow \neg q$ | premisa                                 |
| 4) $s \vee \neg r$             | premisa                                 |
| 5) $q$                         | 1 y 2 MP (modus ponens)                 |
| 6) $\neg(\neg r)$              | 3 y 5 MT (modus tollens)                |
| 7) $r$                         | 6 DN (doble negación)                   |
| 8) $s$                         | 4 y 7 SD, ( lo que se quería demostrar) |

Luego el argumento es válido.

- b) Para demostrar que el siguiente razonamiento es válido:

$$\begin{array}{c} \neg p \rightarrow q \\ \neg p \vee r \\ \hline \neg q \rightarrow r \end{array}$$

Se utiliza la derivación formal:

- 1)  $\neg p \rightarrow q$  ----- premisa (hipótesis) 1
- 2)  $\neg p \vee r$  ----- premisa (hipótesis) 2
- 3)  $p \rightarrow r$  ----- (2) Ley del condicional
- 4)  $\neg q \rightarrow p$  ----- (1) Contrarecíproca y DN
- 5)  $\neg q \rightarrow r$  ----- (4 y 3) S. H. ( a demostrar)

### ⦿ Observación

Para la aplicación de las reglas lógicas se puede utilizar una o más premisas y

las veces que sean necesarias siempre y cuando se usen las reglas adecuadamente. Deben de operarse con todas las premisas.

### Actividad 1.9

Utilizar las reglas de inferencia y/o las leyes lógicas para determinar la validez de los siguientes razonamientos.

a)  $p \rightarrow q$

$$\begin{array}{c} p \rightarrow \neg q \\ \hline \therefore \neg p \end{array}$$

b)  $p \rightarrow q \vee r$

$$\begin{array}{c} p \rightarrow \neg q \\ \hline \begin{array}{c} p \\ \hline \therefore \neg r \end{array} \end{array}$$

Muchas veces es difícil o imposible realizar una demostración directa de un razonamiento. En tales casos se puede intentar otras estrategias incorporando la negación de la conclusión, lo cual resultaría en un método de **demostración indirecta**.

#### 1.8.2 Métodos Indirectos

##### i) Método por contraposición o contrarecíproco

Las demostraciones por contraposición están basadas en la equivalencia lógica del contrarecíproco, la cual dice que:  $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

Es decir, se toma  $\neg q$  como válida y se debe deducir  $\neg p$ . Y a partir de allí, lo que se hace es construir una demostración directa de  $\neg q \rightarrow \neg p$ .

Cuando se tiene:  $p_1, p_2, \dots, p_n \rightarrow q$ , análogamente se supone que la conclusión  $q$  es falsa.

Para que la implicación  $p_1 \wedge p_2 \wedge \dots \wedge p_n \rightarrow q$  sea verdadera, si su consecuente es falso, debe ser también falso el antecedente. Para ello basta que con la suposición hecha, alguna de las premisas resulte falsa.

## Procedimiento de deducción

1. Suponer que la conclusión es falsa.
2. Analizar los valores de verdad de las proposiciones que componen las premisas. Se debe trabajar bajo la suposición de que las premisas son verdaderas; hasta que resultan todas verdaderas o hasta que una de ellas (premisa) resulte forzosamente falsa. Si resultan todas las premisas verdaderas el razonamiento no es válido mientras que si alguna premisa es falsa, el razonamiento es válido.

### □ Ejemplos 1.18

- a) Para establecer la validez del siguiente razonamiento, con el método contrarecíproco:

“Si 1Gb es mejor que nada, se comprará un ordenador nuevo. No se compra un ordenador nuevo. Luego, no es cierto que 1Gb sea mejor que nada”

Se consideran las siguientes proposiciones:

$p$  : 1Gb es mejor que nada

$r$  : se comprará un ordenador nuevo

Expresado simbólicamente, el razonamiento, quedaría:

$$p_1: p \rightarrow r$$

$$p_2: \underline{\neg r}$$

$$\therefore \neg p$$

Suponiendo que la conclusión ( $\neg p$ ) es falsa,  $p$  es verdadera.

En  $p_1$ , el antecedente ( $p$ ) es verdadero, entonces el consecuente ( $r$ ) también es verdadero así  $p_1$  resulte verdadera; y por lo tanto  $p_2$  ( $\neg r$ ) es falsa. Lo cual indica que este razonamiento es válido puesto que se tiene una premisa falsa.

b) Si el razonamiento fuera el siguiente:

$$p_1: p \rightarrow r$$

$$p_2: \underline{\neg p}$$

$$\therefore r$$

utilizando el método contrarecíproco, se tendría que suponer que  $r$  es falso y comenzar por el análisis de  $p_1$ . Como el consecuente ( $r$ ) es falso, el antecedente ( $p$ ) debe ser falso, así  $p_1$  es verdadera. Analizando  $p_2$ ; como  $p$  es falso  $\neg p$  es verdadera. Por lo tanto el razonamiento no es válido ya que la conclusión es falsa y todas las premisas son verdaderas.

## ii) Método por Reducción al Absurdo (o contradicción)

Recordando la regla de inferencia vista anteriormente:

$$p \rightarrow F$$

$$\therefore \neg p$$

Es decir, si la suposición de que  $p$  sea verdadera lleva a una contradicción ( $F$ ), entonces  $p$  debe ser falsa y por lo tanto  $\neg p$  debe ser verdadera.

Aplicado a razonamientos con más de una premisa, para demostrar que  $p_1, p_2, \dots, p_n \rightarrow q$  por este método, también se debe llegar a una contradicción el suponer que se dan simultáneamente todas las premisas y no la conclusión.

$$(p_1, p_2, \dots, p_n) \wedge (\neg q) \rightarrow F$$

## Procedimiento de deducción

1. Suponer que la conclusión es falsa.
2. Utilizar las hipótesis como premisas adicionales para producir una contradicción de la forma  $(r \wedge \neg r)$ , para alguna proposición  $r$ .
3. Una vez en presencia de la contradicción se concluye que el razonamiento es válido pues estaría probado que suponer que cuando sean verdaderas las premisas es posible que sea falsa la conclusión es una contradicción.

### □ Ejemplo 1.19

Para demostrar que el siguiente razonamiento es válido por este método:

$$\neg p \rightarrow q$$

$$\neg p \vee r$$

$$\neg q \rightarrow r$$

Se utiliza derivación formal:

1.  $\neg p \rightarrow q$  . . . . . premisa 1
2.  $\neg p \vee r$  . . . . . premisa 2
3.  $\neg(\neg q \rightarrow r)$  . . . . . Se supone que la conclusión no es verdadera
4.  $\neg q \wedge \neg r$  . . . . . Negación de la implicación en 3
5.  $\neg q$  . . . . . Simplificación conjuntiva en 4
6.  $\neg r$  . . . . . Simplificación conjuntiva en 4
7.  $p$  . . . . . MT con 1. y 5
8.  $\neg p$  . . . . . SD con 2. y 6
9. F . . . . . Adición conjuntiva con 7 y 8
10.  $\neg q \rightarrow r$  . . . . . Queda probada la conclusión por el Método de Contradicción

### ❖ Aplicación

Un algoritmo (y por extensión un programa de ordenador) se lo puede ver como una deducción en la cual nuestras premisas son los parámetros de entrada y la conclusión que se quiere deducir son los datos de salida; las reglas que se pueden utilizar serán el conjunto de instrucciones que proporciona el lenguaje.

La idea básica y motivacional es observar a "la computación como una forma de deducción".

En la tabla 1.10 se presenta una comparación entre los pasos lógicos y los computacionales:

| Deducción                                   | Computación                            |
|---|--|
| Premisas                                    | valores de entrada                     |
| Conclusión                                  | valores de salida                      |
| reglas básicas                              | conjunto de instrucciones del lenguaje |
| fórmulas de las líneas de derivación        | traza del programa                     |
| justificaciones de las líneas de derivación | líneas (instrucciones) del programa    |
| reglas de derivación                        | procedimientos                         |
| subdeducciones                              | modularización                         |

Tabla 1.10. Comparación deducción vs computación.

### □ Ejemplo 1.20

El siguiente programa tiene como entrada números reales, realiza los cálculos necesarios y devuelve el valor promedio de los datos ingresados:

#### Proceso Promedio

```

Escribir "Ingrese la cantidad de datos:"

Leer n

acum<-0

Para i<-1 Hasta n Hacer
    Escribir "Ingrese el dato ",i,":"
    Leer dato
    acum<-acum+dato
FinPara

prom<-acum/n

Escribir "El promedio es: ",prom

FinProceso

```

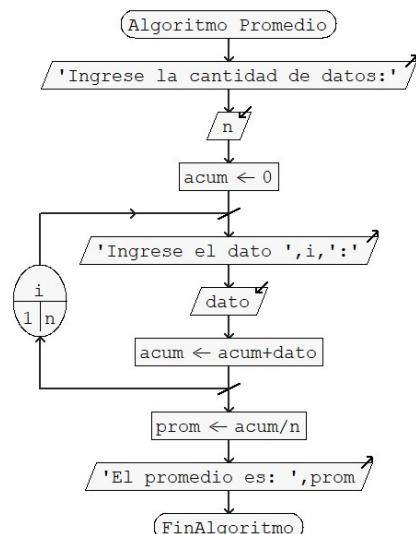


Fig. 1.7 Diagrama de Flujo realizado con el software PSeint.

## 1.9 Lógica de Predicados de Primer Orden

### 1.9.1 Predicados

#### Definición

Se denomina predicado o función proposicional a toda frase declarativa que no es una proposición pero que contiene una o más variables, que cuando se reemplazan por valores de un universo dado se convierte en proposición.

**Notación:** Se denotan con  $p(x)$ ,  $q(x)$ , etc. También pueden estar conectados, por ejemplo:  $p(x) \rightarrow q(x)$ ;  $p(x) \vee q(x)$ , etc.

Las opciones permisibles de reemplazo, o Universo de Discurso o Dominio ( $U$ ), \* $\{$ son todos aquellos valores de la/s variables para los cuales el predicado tiene sentido. Una vez que se particulariza los predicados automáticamente se puede decir verdadero o falso, esto es, se convierten en proposición.

#### Ejemplo 1.21

Sean los predicados

$p(x)$ : “El numero  $x$  es par” ;  $q(x)$ : “El numero  $x$  es divisible por 4”.

Las opciones de reemplazo en este ejemplo son todos los números enteros, es decir que  $U=\mathbb{Z}$ .

Luego  $p(3)$ : “El número 3 es par” es falso; o sea que  $p(3)=0$ ;  $p(2) = 1$ , pues “El número 1 es divisible por 4” es verdadero.

Además, se puede combinar los predicados  $p(x)$  y  $q(x)$  a través de los conectivos lógicos vistos:

$p(x) \rightarrow q(x)$ : “ Si  $x$  es par entonces es divisible por 4”

$[p(8) \rightarrow q(8)] = 1$  y también  $[p(2) \rightarrow q(2)] = 0$

$p(x) \vee \neg q(x)$ : “El numero  $x$  es par o no es divisible por 4”

$[p(6) \vee \neg q(6)] = 1$ .

### Actividad 1.10

Dados los siguientes predicados,

$p(x)$ : “ $x$  cursa Algebra”,  $q(x)$ : “ $x$  regularizó Análisis Matemático I” y  $r(x)$ : “ $x$  es estudiante de la UTN”,

a) Interpretar en forma coloquial las siguientes expresiones simbólicas:

i)  $\neg(p(\text{Juan}) \wedge q(\text{Juan}))$       ii)  $r(\text{Juan}) \rightarrow (p(\text{Juan}) \vee q(\text{Juan}))$

b) Suponer que es verdadero que Juan curse Algebra pero no regularizó Análisis Matemático I, siendo alumno de la UTN, y encontrar el valor de verdad de las expresiones lógicas.

### 1.9.2 Cuantificadores

Si a un predicado se le antepone una frase que exprese como mensaje la frecuencia de ocurrencia de los mismos, automáticamente se convierte en proposición.

#### □ Ejemplos 1.22

Sea el predicado  $p(x)$ : “ $x$  asiste a las clases de M. Discreta”, con universo de discurso a los estudiantes de 1º año de ISI de la FRT, queda cuantificado si se dice:

“Todos los estudiantes asisten a las clases de M. Discreta” o

“Algún estudiante asiste a las clases de M. Discreta”.

“Alguien asiste a las clases de M. Discreta”

Las palabras *todos* y *algún (alguien)* cuantifican al predicado y de las nuevas frases formadas ya se puede dar el valor de verdad por lo que se dice que ellas son proposiciones.

A estas palabras, las que cuantifican un predicado se las denomina cuantificadores. Hay de dos tipos: cuantificador universal y cuantificador existencial.

## Notación

“Para algún  $x$  (del dominio), se cumple o tiene la propiedad  $p(x)$ ” se representa “ $\exists x, p(x)$ ”

“Para todos los  $x$  (del dominio), se cumple o tiene la propiedad  $p(x)$ ” se representa “ $\forall x, p(x)$ ”

Los valores de verdad en cada caso se analizan según la siguiente tabla:

| Frase             | Cuando es verdadera?   | Cuando es falsa?   |
|-------------------|--|--|
| $\exists x, p(x)$ | Para al menos un $a$ del universo, tal que <b><math>p(a)</math> es verdadero</b> | Para cada $a$ del universo, <b><math>p(a)</math> es falso</b>        |
| $\forall x, p(x)$ | Para cada $a$ del universo, <b><math>p(a)</math> es verdadero</b>                | Para al menos un $a$ del universo, <b><math>p(a)</math> es falso</b> |

Tabla 1.11. Valores de verdad de los cuantificadores.

### □ Ejemplo 1.23

Las palabras que cuantifican universalmente, son: “Todo/s”, “Para todo/s”, “Cualquier”, “Para cualquier”, “Un”, etc

‘Todos los alumnos aprobaron el evaluativo’

‘Cualquier persona razona’

‘Todo número real elevado al cuadrado es no negativo’

### □ Ejemplo 1.24

Las palabras que cuantifican existencialmente, son: “Algún/os”, “Para algún/os”, “Hay”, “Existe/n”, etc.

‘Hay números primos que son pares’

‘Algún matemático es filósofo’

‘Existe algún software que caduca’

Las palabras "ningún", "ninguno", "nada", "nadie" corresponden también a enunciados universales con negaciones, pero de una manera distinta a las proposiciones anteriores. La proposición "ninguno es ingeniero" no equivale a la proposición "no todos son ingenieros" sino a la expresión "para todo x, x no es ingeniero" que se simboliza " $\forall x, \neg p(x)$ ", con  $p(x)$ : x es ingeniero".

Las proposiciones existenciales pueden estar negadas, como se vio anteriormente, por ejemplo "no es cierto que hay números mayores que 1" la cual se simboliza como:  $\neg \exists x, p(x)$  donde  $p(x)$ : "x es mayor que 1". Análogamente a lo que ocurre con los cuantificadores universales, las proposiciones existenciales pueden tener negaciones internas como "alguien no aprobó el parcial", la cual se simboliza como:  $\exists x, \neg q(x)$ , donde  $q(x)$ : "x aprobó el parcial".

### □ Ejemplos 1.25

En el universo de los números enteros, considere las siguientes afirmaciones:

"Todos los pares son divisible en 2";

"Algunos pares no son primos";

"Algunos que son divisibles en 2 no son primos".

Si  $p(x)$ : x es par;  $q(x)$ : x es divisible en 2;  $r(x)$ : x es primo, a las afirmaciones anteriores se las puede representar como:

$$\forall x, p(x) \rightarrow q(x)$$

$$\exists x, p(x) \wedge \neg r(x)$$

$$\exists x, q(x) \wedge \neg r(x)$$

### @@Observaciones

- Si un cuantificador es usado sobre una variable x, entonces se dice que la variable x aparece cuantificada o ligada en la expresión (fórmula).
- Para que una fórmula tenga un valor de verdad entonces todas sus variables deben estar ligadas. Por ejemplo: el valor de verdad de  $\exists x, x + y = 1$

depende del valor que tome y.

### Actividad 1.11

a) Dar el valor de verdad de las siguientes expresiones lógicas. Considerar que el Dominio es el conjunto de los Números Reales

$$\text{i) } \forall x, x > 0 \quad \text{ii) } \exists x, 3x - 5 = 0$$

b) Dar el valor de verdad de las expresiones anteriores considerando ahora que el Dominio es el conjunto de los Números Naturales.

### 1.9.3 Predicados equivalentes

#### Definición

Sean  $p(x)$  y  $q(x)$  predicados definidos en el mismo universo. Se dice que  $p(x)$  y  $q(x)$  son equivalentes, y se escribe " $\forall x [p(x) \Leftrightarrow q(x)]$ " cuando la Bicondicional  $p(a) \leftrightarrow q(a)$  es verdadera para cada reemplazo  $a$  del universo dado.

#### Ejemplo 1.26

En el universo  $U = \mathbb{R}$ , sean  $p(x)$ : " $|x| < 3$ " y  $q(x)$ : " $-3 < x < 3$ ", observar que si  $a$  es un real cualquiera se tendrá que  $p(a) \leftrightarrow q(a)$  es verdadera para cada  $a$ . Entonces se podrá escribir que " $\forall x [|x| < 3 \Leftrightarrow -3 < x < 3]$ " y se dirá que los predicados  $|x| < 3$  y  $-3 < x < 3$  son equivalentes.

### 1.9.4 Implicación entre predicados

#### Definición

Sean  $p(x)$  y  $q(x)$  predicados definidos en el mismo universo. Si la implicación  $p(a) \rightarrow q(a)$  es verdadera para cada valor  $a$  del universo se dice que  $p(x)$  implica lógicamente a  $q(x)$  y se denota  $\forall x [p(x) \Rightarrow q(x)]$ .

### ◻ Ejemplo 1.27

En el universo de los números reales sean  $p(x)$ : “ $|x| > 3$ ”  $\wedge$   $q(x)$ : “ $x > 3$ ”.

Si ‘ $a$ ’ es un número real cualquiera,  $q(a) \rightarrow p(a)$  será verdadero mientras que  $p(a) \rightarrow q(a)$  será falso. Por lo tanto no se cumple que:  $\forall x [p(x) \Leftrightarrow q(x)]$ , sino que lo que se cumple es:  $\forall x [q(x) \Rightarrow p(x)]$ .

### Actividad 1.12

En el universo de todos los cuadriláteros considerar los siguientes predicados:

$c(x)$ : “ $x$  es cuadrado”

$t(x)$ : “ $x$  es trapecio isósceles”

$a(x)$ : “ $x$  tiene dos pares de ángulos internos iguales”

$r(x)$  : “ $x$  tiene cuatro ángulos rectos”

$l(x)$ : “ $x$  tiene cuatro lados iguales”

a) Traducir cada una de las siguientes proposiciones en una frase en español (lenguaje coloquial), y determinar si la proposición dada es verdadera o falsa

i)  $\forall x [r(x) \rightarrow c(x)]$       ii)  $\forall x [t(x) \rightarrow a(x)]$

iii)  $\forall x [c(x) \leftrightarrow l(x)]$       iv)  $\forall x [c(x) \leftrightarrow (r(x) \wedge l(x))]$

b) Dados los resultados del apartado a) concluir cuales son los predicados equivalentes o cuáles son implicaciones de otros.

### 1.9.5 Negación de Cuantificadores

#### Propiedad

En el cálculo cuantificacional, se dan las siguientes equivalencias:

$$\neg \forall x, p(x) \Leftrightarrow \exists x, \neg p(x)$$

$$\neg \exists x, p(x) \Leftrightarrow \forall x, \neg p(x)$$

Según lo anterior, se tiene que la negación de una proposición universal (o existencial) es equivalente a la afirmación de un cuantificador existencial (o universal) cuya función proposicional es la negación de la primera.

### □ Ejemplos 1.28

Considerando el universo de discurso el conjunto de los números enteros:

- i) La proposición “Hay números pares” expresada en forma simbólica es:  $\exists x, p(x)$  donde  $p(x)$ : “ $x$  es par”, su negación es  $\forall x, \neg p(x)$  que en forma coloquial o verbal seria: “Todos los números no son pares”.
- ii) La proposición “Todos los números son primos” expresada en forma simbólica sería:  $\forall x, q(x)$  donde  $q(x)$ :  $x$  es primo. Su negación es:  $\exists x, \neg q(x)$  que en forma coloquial seria: “Hay números que no son primos”.

### Actividad 1.13

Escribir las siguientes proposiciones en forma simbólica y encontrar su negación en forma simbólica y verbal, especificando en cada caso el universo de discurso.

- a) Al menos un número entero es par
- b) Si  $x$  es cualquier número par, entonces  $x$  no es divisible por 5
- c) Existe al menos un racional que es entero

En Matemática la complejidad en las demostraciones de teoremas (que son proposiciones verdaderas pero que necesitan ser demostradas, o razonamientos válidos que hay que justificar) varía enormemente.

Anteriormente se vio métodos directos e indirectos de demostración. Existe otro método sencillo, pero que no siempre posible de aplicar, es el llamado **Método exhaustivo**, el cual propone que si debe demostrarse que  $p(x)$  es verdadero para todo  $x$ , se debe examinar el valor de verdad de  $p(x)$  para cada valor de  $x$  del universo de discurso.

### □ Ejemplo 1.29

Suponiendo que en el Universo de los números pares entre 2 y 10, se debe probar la siguiente propiedad: “Todos los números pares entre 2 y 10 pueden expresarse como cuadrado perfecto o como la suma de a lo sumo tres cuadrados perfectos.”

Siendo el Universo  $U = \{2, 4, 6, 8, 10\}$  finito, es factible tomar cada valor y ver el cumplimiento de  $p(x)$  para cada  $x$

$2 = 1 + 1$  ,  $4 = 4$  ,  $6 = 4 + 1 + 1$  ,  $8 = 4 + 4$  ,  $10 = 9 + 1$  , con lo cual se tiene que  $p(x)$  es verdadera en  $U$ .

Frente a una situación en la que el universo es grande pero dentro del alcance de un computador, se podría escribir un programa que verifique todos los casos.

Un gran número de proposiciones y teoremas matemáticos tratan de universos que no se prestan al método exhaustivo, para ello se presentan las siguientes reglas que ayudan a la demostración de enunciados cuantificados.

#### 1.9.6 Reglas de Inferencias

- **Generalización universal (G.U.)**

“Si se demuestra que un predicado  $p(x)$  es verdadero cuando  $x$  se reemplaza por cualquier elemento  $c$  elegido en forma arbitraria de nuestro universo, entonces la proposición cuantificada universalmente es verdadera”

$$\frac{p(c) \quad \text{para un } c \text{ arbitrario}}{\forall x, p(x)}$$

### □ Ejemplo 1.30

Para demostrar que  $\forall x \in R, x^2 \geq 0$ , se parte de un número real cualquiera. Sea  $a \in R$ , entonces se cumple que  $a^2 = a \cdot a \geq 0$  por definición de potencia y por regla de los signos. Entonces, dado que  $a$  es un número real cualquiera, se puede generalizar y decir que  $x^2 \geq 0$  para todo  $\forall x \in R$ .

- **Particularización Universal (P.U.)**

“Si un predicado es verdadero para todos los reemplazos de los miembros de un universo dado, entonces ese predicado es verdadero para cada miembro específico”

$$\forall x, p(x)$$

$$p(c)$$

□ **Ejemplo 1.31**

Se cumple que  $|x| \geq 0, \forall x \in R$ .

Entonces para  $x = -1$  se cumple que  $|-1| > 0$

Estos conceptos ayudan a demostrar razonamientos donde están involucrados cuantificadores.

□ **Ejemplo 1.32**

Para establecer si el siguiente argumento es válido

a)

Todos los ingenieros caminan mucho.

El Sr Beltrán es ingeniero.

∴ El Sr Beltrán camina mucho

Se consideran los siguientes predicados:

$p(x)$ : “ $x$  es ingeniero”,

$q(x)$ : “ $x$  camina mucho” definidos en el universo de todas las personas.

Sea Beltrán un individuo del universo de discurso. Entonces el razonamiento puede expresarse simbólicamente del siguiente modo:

$$\forall x [p(x) \rightarrow q(x)]$$

$p(Beltran)$ .

∴  $q(Beltran)$

Se utiliza la derivación formal (método directo) y las reglas de inferencia que se vio en el cálculo proposicional:

1.  $\forall x [p(x) \rightarrow q(x)]$  Premisa
2.  $p(\text{Beltran})$  Premisa
3.  $p(\text{Beltran}) \rightarrow q(\text{Beltran})$  1. P.U.
4.  $q(\text{Beltran})$  2 y 3 M.P (Modus Ponens)

Por lo tanto el razonamiento es válido.

b) En el siguiente razonamiento:

Todos los enteros son racionales

El número  $\pi$  no es racional

$\therefore$  El número  $\pi$  no es entero

Sean  $p(x)$ : "x es entero" y  $q(x)$ : "x es racional" definidos en el universo de los números reales. Sea  $\pi$  un valor de dicho universo. Entonces el razonamiento puede expresarse simbólicamente del siguiente modo:

$$\forall x [p(x) \rightarrow q(x)]$$

$$\underline{\neg q(\pi)}.$$

$$\therefore \neg p(\pi)$$

Derivación formal:

1.  $\forall x [p(x) \rightarrow q(x)]$  Premisa
2.  $\neg q(\pi)$  Premisa
3.  $p(\pi) \rightarrow q(\pi)$  1. P.U.
4.  $\neg p(\pi)$  3 y 2 M.T (Modus Tollens)

Por lo tanto el razonamiento es válido.

### Actividad 1.14

Especificando el universo adecuado, establecer si los siguientes argumentos son válidos

- a) Si  $n$  es múltiplo de 4 entonces  $n$  es par  
10 es par.  
 $\therefore 10$  es múltiplo de 4
- b) Todo polígono cerrado de cuatro lados es un cuadrilátero  
Un cuadrilátero es tal que la suma de sus ángulos interiores es  $360^\circ$   
 $\therefore$  Cada polígono cerrado de cuatro lados es tal que la suma de sus ángulos interiores es  $360^\circ$ .

## ❖ Aplicaciones

En los lenguajes de programación, aparecen estructuras de decisión del tipo “Si...., entonces” En este contexto, el condicional “si  $p$  entonces  $q$ ” significa que se ejecutará  $q$  únicamente en caso de que  $p$  sea verdadera. Si  $p$  es falsa, el control pasa a la siguiente instrucción del programa.

Por ejemplo si se quiere determinar, para cada segmento de programa contenido en los apartados siguientes, el número de veces que se ejecuta la *sentencia*  $x := x + 1$

- 1)  $z := 1$   
*Si  $z < 2$  ó  $z > 0$  entonces*  
 $x := x + 1$   
*de lo contrario*  
 $x := x + 2$

*En este caso, sean  $p(z): z < 2$  ,  $q(z): z > 0$*

Otra forma de escribir el segmento de programa propuesto sería

- $z := 1$   
*Si  $p(z) \vee q(z)$  es verdadero entonces*  
 $x := x + 1$   
*Si  $p(z) \vee q(z)$  es falso entonces*  
 $x := x + 2$

Como el valor de  $z$  es 1, ambos predicados se convierten en proposiciones verdaderas, por lo tanto  $p(z) \vee q(z)$  es verdadero y la sentencia  $x := x + 1$  se

ejecuta una vez.

La programación de este segmento, con el lenguaje propio de PSeint, tendrá la siguiente codificación y diagrama de Flujo respectivo:

*Proceso Aplicación1*

```
Z<-1 ;  
Si (Z < 2 | Z>0) Entonces  
    X<-X+1  
    Escribir ("Se ejecuto  
    X<-X+1")  
    SiNo  
        X<-X+2  
        Escribir ("Se ejecuto  
        X<-X+2")  
    Fin Si  
FinProceso
```

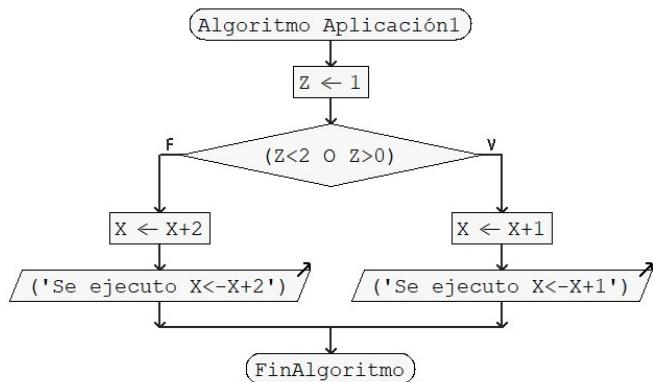


Fig. 1.8. Diagrama de Flujo Aplicación 1.

2)  $z := 2$

Si ( $z < 0$  y  $z > 1$ ) ó  $z = 3$  entonces

$x := x + 1$

de lo contrario

$x := x + 2$

Sean  $p(z): z < 0$ ,  $q(z): z > 1$  y  $r(z): z = 3$

Otra forma de escribir el segmento de programa propuesto sería

$z := 2$

Si  $[p(z) \wedge q(z)] \vee r(z)$  es verdadero entonces

$x := x + 1$

Si  $[p(z) \wedge q(z)] \vee r(z)$  es falso entonces

$x := x + 2$

Pues bien, para que  $[p(z) \wedge q(z)] \vee r(z)$  sea una proposición verdadera, bastará

con que lo sea una de las dos. Como el valor de  $y$  es 2,  $r(z)$  será una proposición falsa, de aquí que tenga que ser verdad la conjunción  $p(z) \wedge q(z)$  para lo cual tendrán que ser  $p$  y  $q$  ambas verdaderas, lo cual es imposible ya que cuando  $p(z)$  sea verdad,  $q(z)$  será falsa y viceversa.

Consecuentemente, la sentencia  $x := x + 1$  no se ejecuta ninguna vez.

La programación de este segmento, con el lenguaje propio de PSeint, tendrá la siguiente codificación y diagrama de Flujo respectivo:

#### *Algoritmo Aplicación2*

```

 $Z \leftarrow 2$ 
Si ( $(Z < 0 \text{ Y } Z > 1) \text{ O } Z > 3$ ) Entonces
     $X \leftarrow X + 1$ 
    Escribir ('Se ejecuto  $X \leftarrow X + 1$ ')
SiNo
     $X \leftarrow X + 2$ 
    Escribir ('Se ejecuto  $X \leftarrow X + 2$ ')
FinSi
FinAlgoritmo

```

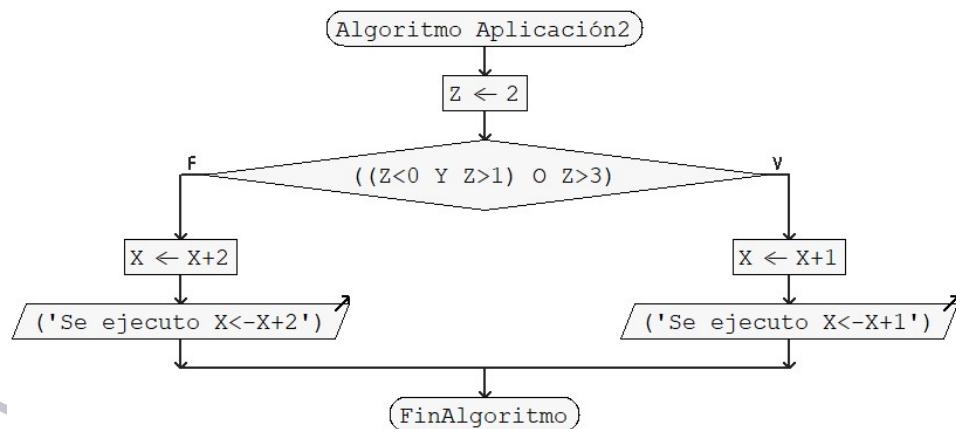


Fig. 1.9. Diagrama de Flujo Aplicación 2.

3)  $z := 1$

Hacer mientras  $z < 3$

Comienzo

$x := x + 1$

$z := z + 1$

Fin

Para esta situación, sea  $p(z)$ :  $z < 3$ . Entonces, el segmento de programa propuesto será

```
z := 1
Hacer mientras p(z) sea verdad
Comienzo
  x := x + 1
  z := y + 1
Fin
```

El predicado  $p(z)$  será una proposición verdadera para aquellos valores de  $z$  que sean estrictamente menores que 3 y dado que el valor inicial de  $z$  es 1 y aumenta en una unidad ( $z := z + 1$ ) cada vez que se ejecutan las sentencias entre comienzo y fin, la sentencia  $x := x + 1$  se ejecutará dos veces.

La programación de este segmento con el lenguaje propio de PSeint se tendrá la siguiente codificación y diagrama de Flujo respectivo:

*Algoritmo Aplicación3*

```
Z <- 1
Mientras z<3 Hacer
  x<-x+1
  z<-z+1
  Escribir ('Se ejecuto X<-X+1')
Fin Mientras
```

*FinAlgoritmo*

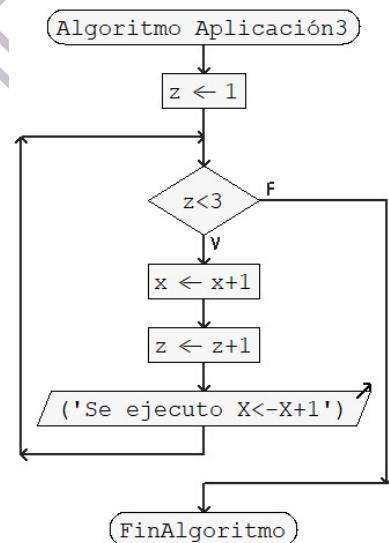


Fig. 1.10. Diagrama de Flujo Aplicación 3.

MATEMÁTICA DISCRETA

UTN – FRT

## Capítulo 2. CONJUNTOS Y RELACIONES

Conjuntos y Elementos.

Inclusión de conjuntos. Subconjuntos.

Operaciones con conjuntos.

Algebra de conjuntos. Dualidad.

Partición de un conjunto.

Relación. Función.

Matrices y Digrafos.

Relación de Equivalencia.

Conjunto Cociente.

Relación de Orden.

Diagrama de Hasse



## Introducción

El concepto de conjunto es de fundamental importancia en las matemáticas modernas. La mayoría de los matemáticos creen que es posible expresar todas las matemáticas en el lenguaje de la teoría de conjuntos. Éstos fueron estudiados formalmente por primera vez por George Cantor (1845-1918). Despues de que la teoría de conjuntos se estableciera como un área bien definida de las matemáticas, aparecieron contradicciones o paradojas en la misma. Para eliminarlas, se desarrollaron aproximaciones más sofisticadas que las que hizo Cantor. Un tratamiento introductorio de la teoría de conjuntos se ocupa, generalmente, de la Teoría Elemental, la cual es bastante similar al trabajo original de Cantor.

Nuestro interés en los conjuntos se debe tanto al papel que representan en las matemáticas como a su utilidad en la modelización e investigación de problemas en la informática. La Teoría de Conjuntos junto a la Teoría de Lógica es la base de las Ciencias para la Computación ya que sirve de fundamento del Álgebra Booleana, de los Lenguajes, de los Autómatas, de las relaciones entre Bases de Datos, de los Grafos, de las Redes y de los Árboles, entre otros temas.

### 2.1 Conjuntos y Elementos

#### Definición

Un conjunto es cualquier colección de objetos que pueda tratarse como una entidad. A cada objeto de la colección se lo denomina elemento o miembro del conjunto.

#### Notación

A los conjuntos se los designa con letras mayúsculas y a sus elementos con letras minúsculas. La afirmación “el elemento ‘ $a$ ’ pertenece al conjunto  $A$ ” se escribe:  $a \in A$  y la negación de este hecho,  $\neg(a \in A)$ , se escribe:  $a \notin A$

La definición de un conjunto no debe ser ambigua en el sentido de que pueda decidirse cuando un objeto particular pertenece, o no, a un conjunto.

Se pueden expresar los conjuntos por extensión o por comprensión.

### 2.1.1 Determinación por Extensión

#### ☞ Definición

Un conjunto está definido por extensión cuando se especifican todos los elementos que forman el mismo.

#### □ Ejemplos 2.1

Los siguientes conjuntos están definidos por extensión.

a) El conjunto de las vocales del alfabeto.

$$A = \{a, e, i, o, u\}$$

b) El conjunto formado por los números enteros pares no negativos y menores que diez.

$$B = \{0, 2, 4, 6, 8\}$$

#### ☞ Observación

- Los conjuntos se indican como una lista encerrada entre llaves pero separados por comas, sin importar el orden y sin repetir.

Los elementos de un conjunto infinito no pueden especificarse de una forma explícita; consecuentemente, se necesita una forma alternativa de describir tales conjuntos implícitamente.

### 2.1.2 Determinación por Comprensión

#### ☞ Definición

Se dice que un conjunto está definido por comprensión cuando se especifica una propiedad que caracteriza a todos los elementos del mismo.

Esta propiedad o especificación implícita, se hace a menudo mediante un

predicado con una variable libre. El conjunto estará determinado por aquellos elementos del universo (U) que hacen del predicado una proposición verdadera. De aquí que si  $p(x)$  es un predicado en  $x$ , la notación  $A = \{x : p(x)\}$  denota al conjunto A formado por los elementos  $a \in U$  para los cuales  $p(a)$  es verdadero.

### □ Ejemplos 2.2

Los siguientes conjuntos:

- a) El conjunto de los enteros mayores que diez.
- b) El conjunto de los enteros pares.
- c) El conjunto  $\{1, 2, 3, 4, 5\}$

definidos por comprensión serían, respectivamente:

- a)  $A = \{x / x \in \mathbb{Z} \wedge x > 10\}$
- b)  $B = \{x / x \in \mathbb{Z} \wedge x = 2k, \text{ con } k \in \mathbb{Z}\}$
- c)  $C = \{x / x \in \mathbb{Z} \wedge 1 \leq x \leq 5\}$

## 2.2 Conjuntos finitos e infinitos

### ▢ Definición

Un conjunto A se dice finito si tiene ' $n$ ' elementos distintos donde  $n \in \mathbb{N}_0$ .

Se dice que ' $n$ ' es el cardinal, o sea el número de elementos de A y se lo indica:

$$|A| = n.$$

### ▢ Ejemplo 2.3

Si  $A = \{x / x \text{ es una letra del abecedario}\}$ , entonces  $|A|=27$

### ▢ Definición

Un Conjunto se dice infinito si no es finito.

Los conjuntos infinitos se clasifican en numerables y no numerables. Son numerables cuando entre dos elementos cualesquiera hay una cantidad finita de elementos. Caso contrario se dicen infinitos no numerables

A los *Conjuntos Finitos o Infinitos Numerables* se les llama *Conjuntos Discretos* y son el objeto de estudio de Matemática Discreta.

A veces tanto en conjuntos finitos demasiado grandes como en conjuntos infinitos, se utiliza puntos suspensivos “...” (elipsis matemática) para caracterizar a los elementos de un conjunto.

#### Ejemplos 2.4

El conjunto de los números enteros del 1 al 100,

$$C = \{1, 2, 3, \dots, 100\}$$

o el conjunto de los enteros pares no negativos,

$$D = \{0, 2, 4, 6, \dots\}$$

Algunos conjuntos aparecerán muy frecuentemente a lo largo del texto y se usan símbolos especiales para designarlos.

$\mathbb{Z}$ : Conjunto de los números enteros

$\mathbb{N} = \mathbb{Z}^+$ : Conjunto de los números naturales o enteros positivos.

$\mathbb{N}_0^+$ : Conjunto de los enteros no negativos.

$\mathbb{Q}$  : Conjunto de los números racionales.

$\mathbb{R}$ : Conjunto de los números reales.

Todos son conjuntos infinitos, pero  $\mathbb{N}$  y  $\mathbb{Z}$  son numerables, mientras que  $\mathbb{R}$  y  $\mathbb{Q}$  son no numerables.

## 2.3 Conjuntos especiales: Vacío, Unitario, Universal

### Definiciones

a) Un conjunto se dice vacío si no tiene elementos.

Su cardinal es 0 y se representa  $\emptyset$  o por {}.

b) Un conjunto se dice Unitario si tiene exactamente un elemento.

Su cardinal es 1.

c) Al conjunto que contiene todos los elementos del tema de referencia se le llama Conjunto Universal y se denota con la letra U.

### Ejemplos 2.5

Para cada uno de los conjuntos siguientes, se elige un conjunto universal y un predicado apropiados para definirlo.

a) El conjunto de los enteros entre 0 y 1.

$$A = \{x \in \mathbb{Z} : 0 < x < 1\} = \{\} = \emptyset$$

b) El conjunto de los enteros positivos impares.

$$B = \{x \in \mathbb{Z}^+ : x = 2k + 1, k \in \mathbb{Z}^+\}$$

c) El conjunto de los múltiplos de 10 entre 15 y 25

$$C = \{x \in \mathbb{Z} : x = 10k, k \in \mathbb{Z} \wedge 15 < x < 25\} = \{20\}$$

### Actividad 2.1

¿Cuál de los siguientes conjuntos es vacío? ¿Cuál es unitario? ¿Cuál puede considerarse el universo adecuado para los tres conjuntos?. Representar gráficamente

$$A = \{x \in \mathbb{N} / x - 3 = 5\}$$

$$B = \{x \in \mathbb{R} / x^2 = 5\}$$

$$C = \{x \in \mathbb{N} / x \text{ es par y } x^2 \text{ es impar}\}$$

## 2.4 Igualdad de Conjuntos

### Definición

Se dice que dos conjuntos A y B son iguales si, y solo si tienen los mismos elementos. Es decir, cada elemento del conjunto A es un elemento de B y cada elemento de B es un elemento de A.

Su expresión formal en notación lógica es:

$$A = B \Leftrightarrow \forall x [(x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)]$$

O bien,

$$A = B \Leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$$

### Observación

- Si dos conjuntos tienen los mismos elementos, ambos son iguales, independientemente de como estén definidos.

### Ejemplos 2.6

Dados los siguientes conjuntos, en el Universo de los Números Enteros ( $\mathbb{Z}$ ), se analizará cuáles son iguales.

$$A = \{x / x \text{ es par y } x^2 \text{ es impar}\}$$

$$B = \{x / \exists y, y \in \mathbb{Z} \wedge x = 2y\}$$

$$C = \{1, 2, 3\}$$

$$D = \{0, 2, -2, 3, -3, 4, -4, \dots\}$$

$$E = \{2x / x \in \mathbb{Z}\}$$

$$F = \{3, 2, 1\}$$

$$G = \{x / x^3 - 6x^2 - 7x - 6 = 0\}$$

Un camino para determinar si poseen los mismos elementos, es expresar a cada conjunto por extensión, si es que no lo estuviera ya.

Sea  $x$  cualquier número entero,

- En el conjunto A, no existe un elemento  $x$  que pertenezca a él, ya que la proposición  $x$  es par  $\wedge$   $x^2$  es impar es falsa para todo  $x$ , o dicho de otra forma no existe un número par cuyo cuadrado sea impar y por lo tanto  $A = \emptyset$ .

- Para el conjunto B, se tiene que  $x \in B \Leftrightarrow \exists y / y \in \mathbb{Z} \wedge x = 2y \Leftrightarrow x \text{ es par}$ , luego  $B = \{x \in \mathbb{Z} / x \text{ es par}\} = \{\dots, -4, -2, 0, 2, 4, \dots\}$
- En el conjunto C, un elemento  $x \in C \Leftrightarrow x = 1 \vee x = 2 \vee x = 3$ .
- En el conjunto E  $= \{0, 2, -2, 4, -4, 6, -6, \dots\} = \{x \in \mathbb{Z} / x \text{ es par}\}$
- En el conjunto F, un elemento  $x \in F \Leftrightarrow x = 1 \vee x = 2 \vee x = 3$
- En el conjunto G,  $x \in G \Leftrightarrow x^3 - 6x^2 - 7x - 6 = 0$ , pero en esta ecuación no existe ningún número entero que la satisfaga, por lo tanto,  $G = \emptyset$ , es el conjunto vacío.

De todo lo anterior, se sigue que los pares de conjuntos que son iguales son:

$A = G$ ;  $B = E$  y  $C = F$ ; y que el conjunto D no es igual a ninguno de los otros.

## 2.5 Conjuntos Disjuntos

### Definición

Se dice que A y B son disjuntos si y solo si A y B no tienen elementos en común.

## 2.6 Diagramas de Venn

Una representación gráfica para los conjuntos son los diagramas de Venn. El conjunto universal se representa por el interior de un rectángulo y todos los demás conjuntos se representan por regiones cerradas incluidos en el mismo.

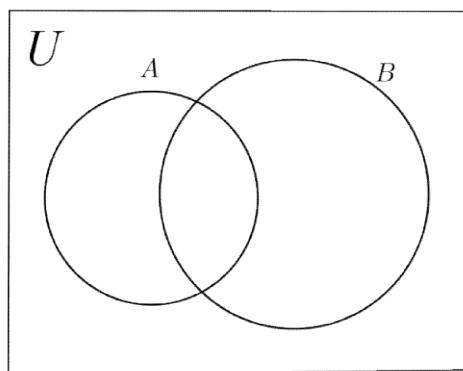


Fig. 2.1. Diagrama de Venn para dos subconjuntos de U

## Observaciones

- En un diagrama de Venn los conjuntos disjuntos pueden representarse en regiones separadas por completo.
- Conjuntos Distintos no es lo mismo que Conjuntos Disjuntos.

## Ejemplo 2.7

¿Qué se puede decir de los siguientes conjuntos? ¿son distintos o son disjuntos?

$$A = \{1, 2\}; \quad B = \{1, 3\}$$

Para ello se analizará los elementos que tienen cada uno.

Ya que  $2 \in A$  y  $2 \notin B$ ,  $3 \in B$  y  $3 \notin A$  se puede decir que A y B son distintos. Además A y B no son conjuntos disjuntos porque tienen a 1 como elemento en común.

## Actividad 2.2

- Dar una condición necesaria y suficiente para que dos conjuntos sean distintos. *Sugerencia*  $\neg(A = B)$
- Si se tiene el universo  $U = \{x / x \text{ es alumno de la UTN-FRT}\}$  y los subconjuntos A, B y C definidos como sigue:

$$A = \{x \in U / x \text{ tiene al menos 20 años}\},$$

$$B = \{x \in U / x \text{ trabaja}\},$$

$$C = \{x \in U / x \text{ tiene al menos un hijo}\}$$

Responder y justificar a la vez:

- Luis trabaja?
- Juan tiene hijos y trabaja?
- Maxi es alumno de la FRT?
- Maxi es un alumno de la FRT menor de 20 años?

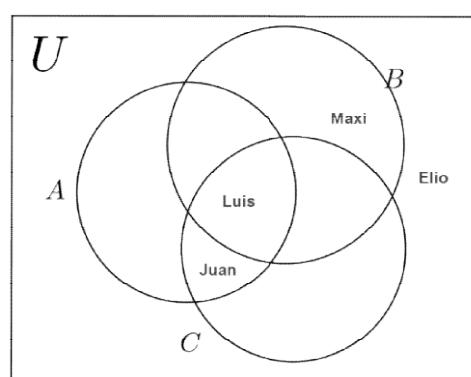


Fig. 2.2. Diagrama de Venn.

iv) Quienes tienen al menos 20 años y tienen hijos?

v) Quienes trabajan y no tienen hijos?

### Actividad 2.3

Sea el Universo de los Números Naturales y sean los conjuntos A y B que se dan en cada apartado, analizar si son disjuntos

a)  $A = \{x \in \mathbb{N} / x \text{ es par}\}$  y  $B = \{x \in \mathbb{N} / x \text{ es impar}\}$

b)  $A = \{x \in \mathbb{N} / 2x \text{ es par}\}$  y  $B = \{x \in \mathbb{N} / x \text{ es impar}\}$

## 2.7 Inclusión de conjuntos. Subconjuntos

### ☞ Definición

Sean A y B dos conjuntos. Se dice que A está incluido en B o que es un subconjunto de B, y se lo denota  $A \subseteq B$ , si cada elemento de A es un elemento de B, es decir,

$$A \subseteq B \Leftrightarrow \forall x, (x \in A \Rightarrow x \in B)$$

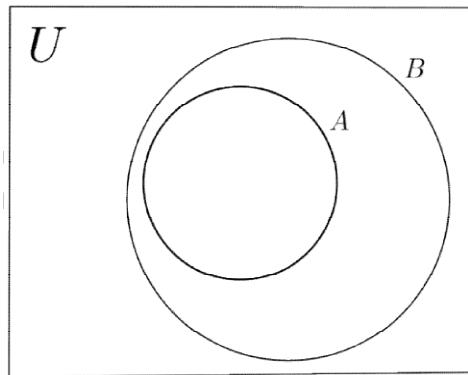


Fig.2.3.Inclusión.

### ☞ Observaciones

- También se dice que A está incluido en B o que B contiene a A, en cuyo caso se denota  $B \supseteq A$ .
- El símbolo  $\subseteq$  se llama “Símbolo de inclusión amplia”. Si en particular A es

subconjunto de B y B existen elementos que no pertenecen a A, se dice que A es subconjunto propio de B y se escribe  $A \subset B$ . El símbolo  $\subset$  se llama “símbolo de inclusión estricta”.

### □ Ejemplo 2.8

Para probar que el conjunto  $A = \{x \in \mathbb{R} / x^2 - 3x + 2 = 0\}$  es subconjunto del conjunto  $B = \{1, 2, 4\}$ , se toma un elemento cualquiera de  $\mathbb{R}$ . Sea  $a \in A$ , luego este elemento debe verificar la ecuación:  $a^2 - 3a + 2 = 0 \Leftrightarrow a = 2 \vee a = 1 \Rightarrow a \in B$

Por consiguiente:  $\forall x (x \in A \Rightarrow x \in B)$  y según la definición anterior,  $A \subseteq B$ .

### □ Ejemplo 2.9

Una condición necesaria y suficiente para que un conjunto A no esté contenido en otro conjunto B es que exista, al menos, un elemento en A que no esté en B.

$$\begin{aligned} A \not\subseteq B &\Leftrightarrow \neg(A \subseteq B) \Leftrightarrow \neg[\forall x, (x \in A \Rightarrow x \in B)] \\ &\Leftrightarrow \exists x, [\neg(x \in A \Rightarrow x \in B)] \\ &\Leftrightarrow \exists x, (x \in A \wedge x \notin B) \end{aligned}$$

### □ Ejemplo 2.10

¿Es  $B = \{1, 2, 4\}$  un subconjunto de  $A = \{x \in \mathbb{R}: x^2 - 3x + 2 = 0\}$ ?

Observar que  $4 \in B$  y, sin embargo,  $4^2 - 3 \cdot 4 + 2 \neq 0$ , luego  $4 \notin A$ , es decir, hay un elemento en B que no está en A, por lo tanto,  $B \not\subseteq A$ .

## Propiedades de la Inclusión

1) Si A es un conjunto cualquiera, se cumple que

- $\emptyset \subseteq A$  El vacío es subconjunto de cualquier conjunto
- $A \subseteq A$  Todo conjunto es subconjunto de sí mismo
- $A \subseteq U$  Todo conjunto es subconjunto del conjunto Universal

## Demostraciones

1a) (por contradicción)

Suponer por el contrario:  $\emptyset \not\subseteq A$ . Entonces, debe existir un elemento en  $\emptyset$  que no pertenece a A. Contradicción!!...  $\emptyset$  no tiene elementos.

Esta contradicción fue una consecuencia de haber supuesto que  $\emptyset \not\subseteq A$ .

Por lo tanto se concluye que  $\emptyset \subseteq A$

### 1b) (directa)

Es evidente por definición, que el conjunto A es un subconjunto de A si y solo si la implicación ( $x \in A \rightarrow x \in A$ ) es verdadera para cada x de A, y esto es verdad  $\therefore A \subseteq A$ , lo que se puede afirmar que “Todo elemento de A, pertenece a A”.

### 1c) (trivial)

Se basa en la definición de conjunto universal que permite afirmar que la proposición  $\forall x, x \in U$  es una tautología, es decir es siempre verdadera.

El conjunto A es un subconjunto de U si, y sólo si la implicación  $x \in A \rightarrow x \in U$  es verdadera para cada x de U. Pero  $x \in U$  es verdad para todos los x, luego la implicación también es verdad independientemente de que  $x \in A$  sea verdadero o falso. Como x es un elemento arbitrario de U, se sigue que:

$$\forall x, (x \in A \rightarrow x \in U) \text{ es verdad y, por lo tanto, } A \subseteq U.$$

## 2) Caracterización de la Igualdad.

Sean A, B y C son conjuntos cualesquiera de un universal arbitrario U. Entonces:

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

### Demostración

i) Primera parte, se demuestra que si  $A = B \Rightarrow A \subseteq B \wedge B \subseteq A$

En efecto, sea  $A = B$ , entonces por el axioma de extensión, cada elemento de A es un elemento de B luego, por definición de subconjunto,  $A \subseteq B$ .

Así pues, si  $A = B$ , entonces  $A \subseteq B$  (1)

Utilizando los mismos argumentos, aunque intercambiando los papeles de A y B, se tiene que si  $A = B$ , entonces  $B \subseteq A$  (2). De aquí que por (1) y (2):

$(A = B \Rightarrow A \subseteq B) \wedge (A = B \Rightarrow B \subseteq A)$  lo cual equivale a

$$A = B \Rightarrow A \subseteq B \wedge B \subseteq A \text{ (I)}$$

ii) Segunda parte, se demuestra: que  $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$

En efecto,  $(A \subseteq B) \wedge (B \subseteq A) \Rightarrow [(\forall x, (x \in A \rightarrow x \in B)] \wedge [(\forall x, (x \in B \rightarrow x \in A)]$   
consecuentemente, por el axioma de extensión  $\Rightarrow A = B$

$$\text{Es decir } (A \subseteq B) \wedge (B \subseteq A) \Rightarrow A = B \text{ (II)}$$

Luego de (I) y (II),  $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$  a lo que se quería llegar.

### 3) Transitividad de la Inclusión

Sean A, B y C son conjuntos cualesquiera de un universal arbitrario U.

Si  $A \subseteq B \wedge B \subseteq C$ , entonces  $A \subseteq C$ .

#### Demostración

Sea x un elemento arbitrario del universal U.

De  $A \subseteq B$ , se sigue que  $x \in A \rightarrow x \in B$

De  $B \subseteq C$ , se sigue que  $x \in B \rightarrow x \in C$

De la transitividad de la implicación lógica se sigue que  $x \in A \rightarrow x \in C$  y al ser x arbitrario, se tiene:

$$\forall x, (x \in A \rightarrow x \in C) \text{ por lo tanto } A \subseteq C.$$

#### Actividad 2.4

En cada caso colocar el símbolo que corresponda:  $\subseteq$  o  $\supseteq$

i)  $\mathbb{N} \dots \mathbb{Z}$

ii)  $\{ x \in \mathbb{Z} / x \text{ es par} \} \dots \{ x \in \mathbb{Z} / (x - 2).(x + 4) = 0 \}$

iii)  $\{ x / x \text{ es una vocal} \} \dots \{ a, e, i, o, u \}$

### ⌚ Observaciones

- Los conjuntos también pueden ser objetos, pueden ser elementos de otros conjuntos, por ejemplo el conjunto  $A = \{\{1, 2\}, \{1, 3\}, \{2\}, \{3\}\}$  tiene cuatro elementos que son los conjuntos  $\{1, 2\}$ ,  $\{1, 3\}$ ,  $\{2\}$  y  $\{3\}$ .
- Si  $A$  es un conjunto, entonces  $\{A\}$  es un conjunto con un único elemento  $A$ , sin importar cuantos elementos tenga  $A$ .
- De la misma forma  $\{\emptyset\}$  es un conjunto con un elemento, el conjunto  $\emptyset$ , mientras que  $\emptyset$  no contiene elementos, así que  $\emptyset$  y  $\{\emptyset\}$  son conjuntos distintos. Se tiene que  $\emptyset \in \{\emptyset\}$  e incluso  $\emptyset \subseteq \{\emptyset\}$ , pero  $\emptyset \neq \{\emptyset\}$ .

### ◻ Ejemplo 2.11

¿Cuál es la diferencia entre los conjuntos  $\{a\}$  y  $\{\{a\}\}$  y entre los conjuntos  $\emptyset$ ,  $\{\emptyset\}$  y  $\{\emptyset, \{\emptyset\}\}$ ?

- $\{a\}$  es un conjunto cuyo único elemento es  $a$ .
- $\{\{a\}\}$  es un conjunto cuyo único elemento es el conjunto  $\{a\}$ .
- $\emptyset$  es el conjunto vacío, el cual no tiene elementos.
- $\{\emptyset\}$  es el conjunto con un único elemento que es el  $\emptyset$ .
- $\{\emptyset, \{\emptyset\}\}$  es el conjunto con dos elementos, el  $\emptyset$  y el  $\{\emptyset\}$ .

## 2.8 Conjunto Potencia de un conjunto finito

### Ἑ Definición

Dado un conjunto  $A$ , el Conjunto Potencia de  $A$  es la colección de todos los subconjuntos de  $A$ , y se denota por  $P(A)$ .

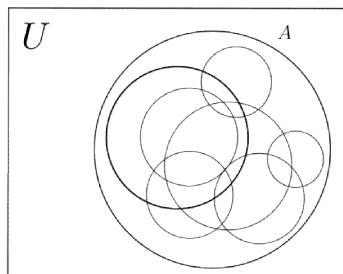


Fig. 2.4. Potencia de  $A$ .

### 👁 Observaciones

- De acuerdo a la definición, si  $X$  es un conjunto cualquiera del universo arbitrario  $U$ , entonces

$$X \in P(A) \Leftrightarrow X \subseteq A$$

- El conjunto Potencia del conjunto  $\emptyset$  es  $P(\emptyset) = \{ \emptyset \}$ , un conjunto unitario.
- El conjunto Potencia del conjunto  $\{\emptyset\}$  es  $P(\{\emptyset\}) = \{ \emptyset, \{ \emptyset \} \}$  un conjunto con dos elementos.

### ◻ Ejemplo 2.12

¿Cuantos elementos tiene  $P(A)$ , si  $A = \{a, b\}$ ?

De la propiedad de la inclusión, se sigue que el conjunto vacío,  $\emptyset$  es uno de sus elementos. Por otra parte,  $a \in A$  y  $b \in A$  luego por la definición de inclusión  $\{a\}$ ,  $\{b\}$  y  $\{a, b\}$  son subconjuntos de  $\{a, b\} = A$ . Consecuentemente, el conjunto propuesto tiene cuatro subconjuntos distintos y por lo tanto  $P(A) = \{\emptyset, \{a\}, \{b\}, A\}$

### ◻ Ejemplo 2.13

Análogamente, se tiene que si  $A = \{1, 2, 3\}$ , entonces,

$$P(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, A \}$$

En general, si  $|A| = n$ , los elementos de  $P(A)$  son: el  $\emptyset$  (conjunto con 0 elementos); todos los conjuntos unitarios; todos los conjuntos formados por dos elementos; todos los conjuntos formados por tres elementos, y así sucesivamente el conjunto formado por  $n$  elementos que es  $A$ .

### 💳 Cardinal del Conjunto Potencia

Si  $|A| = n$  con  $n \neq 0$ , entonces  $P(A)$  es un conjunto finito y es tal que  $|P(A)| = 2^n$

En efecto, sea  $X$  un elemento arbitrario de  $P(A)$ . Para cada  $a \in A$ , hay dos opciones  $a \in X \vee a \notin X$ ; como hay  $n$  elementos en  $A$ , habrá

$$\overbrace{2 \cdot 2 \cdot 2 \cdots \cdots \cdots 2}^{n \text{ veces}} = 2^n$$

diferentes conjuntos X. Es decir,  $P(A)$  tiene  $2^n$  elementos

### Actividad 2.5

Sea el conjunto finito  $A = \{u, v, x, y\}$ . Calcular  $|A|$  y  $|P(A)|$  y expresar por extensión  $P(A)$ . Además decir cuántos elementos de  $P(A)$  tienen cardinal 0, cardinal 1, cardinal 2, cardinal 3 y cuantos de cardinal 4.

A continuación se verán las operaciones con conjuntos que permiten obtener nuevos conjuntos, partiendo de conjuntos ya conocidos. A y B serán conjuntos cualquiera de un universal arbitrario U.

## 2.9 Álgebra de Conjuntos: Operaciones

### 2.9.1 Unión

#### Definición

La unión de dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a A o a B. Se denota  $A \cup B$ .

$$A \cup B = \{x \in U / x \in A \vee x \in B\}$$

La disyunción ‘ $\vee$ ’ se utiliza en el sentido inclusivo, es decir, significa “y/o”.

Generalizando para tres conjuntos  $A \cup B \cup C = \{x \in U / x \in A \vee x \in B \vee x \in C\}$

Las regiones sombreadas representan a las operaciones indicadas en cada pie de los diagramas de Venn.

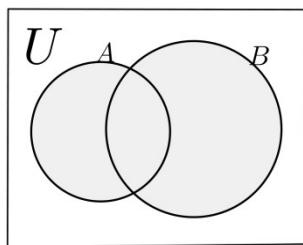


Fig.2.5.  $A \cup B$ .

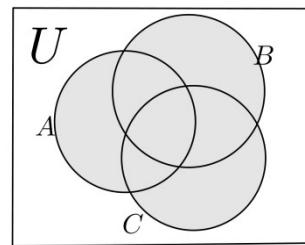


Fig.2.6.  $A \cup B \cup C$ .

## 2.9.2 Intersección

### Definición

La Intersección de dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a ambos conjuntos a la vez. Se denota  $A \cap B$ .

$$A \cap B = \{x / x \in A \wedge x \in B\}.$$

Si A y B no tienen elementos en común, es decir si  $A \cap B = \emptyset$ , entonces se dice que A y B son conjuntos disjuntos.

Generalizando para tres conjuntos  $A \cap B \cap C = \{x / x \in A \wedge x \in B \wedge x \in C\}$

Las regiones sombreadas representan a las operaciones indicadas en cada pie de los diagramas de Venn.

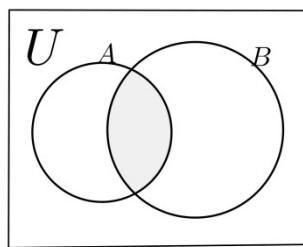


Fig. 2.7.  $A \cap B$ .

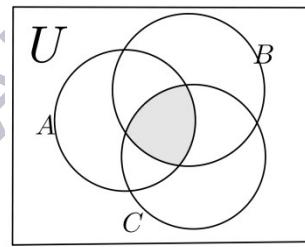


Fig. 2.8.  $A \cap B \cap C$ .

## 2.9.3 Diferencia

### Definición

La diferencia entre dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a A y no pertenecen a B. Se nota por  $A - B$ , y se lee “A menos B”.

$$A - B = \{x \in U / x \in A \wedge x \notin B\}$$

De la misma manera se define  $B - A$  como:

$$B - A = \{x \in U / x \in B \wedge x \notin A\}$$

### 👁 Observaciones

- $A - B = A$  y  $B - A = B$  si y solo si  $A \cap B = \emptyset$
- $A - B - C = \{ x \in U / x \in A \wedge x \notin B \wedge x \notin C \}$
- Las regiones sombreadas representan a las operaciones indicadas en cada pie de los diagramas de Venn

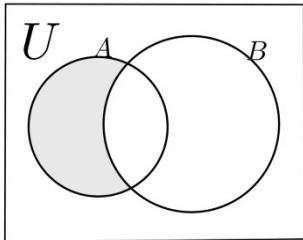


Fig. 2.9.  $A - B$ .

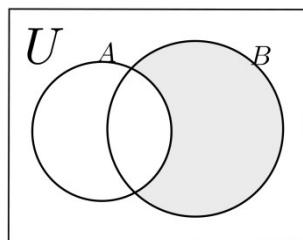


Fig. 2.10.  $B - A$ .

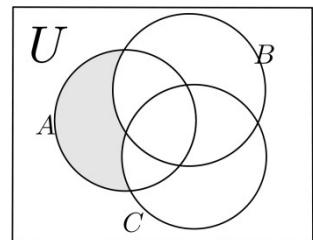


Fig. 2.11.  $A - B - C$ .

### 2.9.4 Complemento

#### Ἑ Definición

El complemento de un conjunto  $A$  es el conjunto formado por todos los elementos del universal que no pertenecen a  $A$ . Se denota  $A'$ .

$$A' = \{ x \in U / x \notin A \}$$

### Ἑ Observaciones

- Dado que  $A \subseteq U$ , la diferencia  $U - A$  es el complemento de  $A$ .

Las regiones sombreadas representan a las operaciones indicadas en cada pie de los diagramas de Venn.

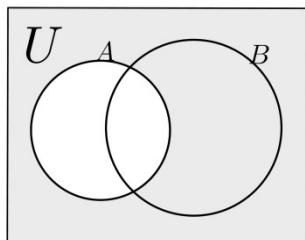


Fig. 2.12.  $A'$ .

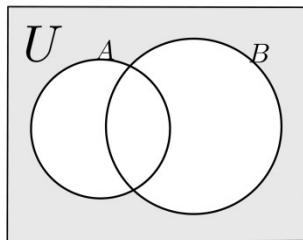


Fig. 2.13.  $(A \cup B)'$ .

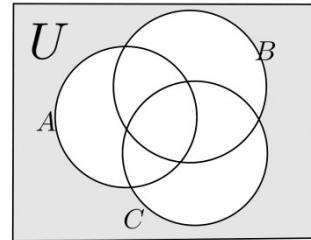


Fig. 2.14.  $(A \cup B \cup C)'$ .

## 2.9.5 Diferencia simétrica

### Definición

La diferencia simétrica entre dos conjuntos A y B es el conjunto de todos los elementos que pertenecen a A o a B, pero no a ambos. Se denota  $A \oplus B$ .

$$A \oplus B = \{x / x \in A \vee x \in B\} = (A - B) \cup (B - A)$$

### Observaciones

- $A \oplus B \oplus C = (A - B - C) \cup (B - A - C) \cup (C - A - B) \cup (A \cap B \cap C)$
- Las regiones sombreadas representan a las operaciones indicadas en cada pie de los diagramas de Venn

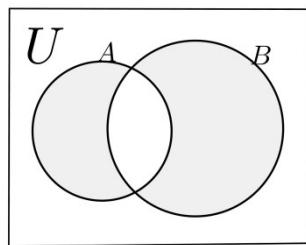


Fig.2.15.  $A \oplus B$ .

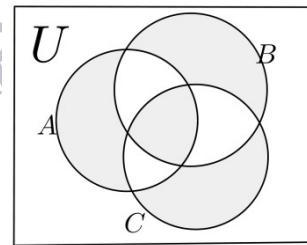


Fig.2.16.  $A \oplus B \oplus C$ .

### Ejemplos 2.14

Sean los conjuntos:

$$A = \{n \in \mathbb{Z}^+: n < 9\}; B = \{n \in \mathbb{Z}^+: n \text{ es par y } n \leq 16\}; C = \{n \in \mathbb{Z}^+: n \text{ es impar y } n < 15\}$$

Los elementos de los siguientes conjuntos:  $A \cup B$ ;  $A \cap B$ ;  $A'$ ;  $B'$ ;  $C'$ ;  $A - B$ ;  $B - A$ ;  $A \oplus B$ ;  $B \cap C$ ;  $A - C$ , se los determinan expresando por extensión a A, B y C, y aplicando la definición.

$$A = \{n \in \mathbb{Z}^+: n < 9\} = \{1, 2, 3, 4, 5, 6, 7, 8\};$$

$$B = \{n \in \mathbb{Z}^+: n \text{ es par y } n \leq 16\} = \{2, 4, 6, 8, 10, 12, 14, 16\}$$

$$C = \{n \in \mathbb{Z}^+: n \text{ es impar y } n < 15\} = \{1, 3, 5, 7, 9, 11, 13\}.$$

Luego

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\} \cup \{2, 4, 6, 8, 10, 12, 14, 16\}$$

$$= \{1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16\}$$

$$A \cap B = \{1, 2, 3, 4, 5, 6, 7, 8\} \cap \{2, 4, 6, 8, 10, 12, 14, 16\} = \{2, 4, 6, 8\}$$

$$A' = \{n \in \mathbb{Z}^+: n \notin A\} = \{n \in \mathbb{Z}^+: n \geq 9\} = \{9, 10, 11, 12, 13, 14, 15, 16, \dots\}$$

$$B' = \{n \in \mathbb{Z}^+: n \notin B\} = \{n \in \mathbb{Z}^+: \neg(n \in B)\} = \{n \in \mathbb{Z}^+: \neg[n \text{ es par} \wedge (n \leq 16)]\}$$

$$= \{n \in \mathbb{Z}^+: (n \text{ es impar}) \vee (n > 16)\}$$

$$= \{1, 3, 5, 7, 9, 11, 13, 15, 17, \dots\} \cup \{17, 18, 19, 20, 21, 22, \dots\}$$

$$= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 18, 19, 20, 21, 22, \dots\}$$

$$C' = \{n \in \mathbb{Z}^+: n \notin C\} = \{n \in \mathbb{Z}^+: \neg(n \in C)\} = \{n \in \mathbb{Z}^+: \neg(n \text{ es impar} \wedge n < 15)\}$$

$$= \{n \in \mathbb{Z}^+: (n \text{ es par}) \vee (n \geq 15)\} =$$

$$= \{2, 4, 6, 8, 10, 12, 14, 16\} \cup \{15, 16, 17, 18, 19, 20, 21, 22, \dots\}$$

$$= \{2, 4, 6, 8, 10, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, \dots\}$$

$$A - B = \{n \in \mathbb{Z}^+: n \in A \wedge n \notin B\} = \{n \in \mathbb{Z}^+: n \in A \wedge n \in B'\} =$$

$$= \{1, 2, 3, 4, 5, 6, 7, 8\} \cap \{1, 3, 5, 7, 9, 11, 13, 15, 17, 18, 19, \dots\}$$

$$= \{1, 3, 7\}$$

$$B - A = \{n \in \mathbb{Z}^+: n \in B \wedge n \notin A\} =$$

$$= \{2, 4, 6, 8, 10, 12, 14, 16\} \cap \{9, 10, 11, 12, 13, 14, 15, 16, \dots\} = \{14, 16\}$$

$$A \oplus B = (A - B) \cup (B - A)$$

$$= \{1, 3, 7\} \cup \{14, 16\} = \{1, 3, 7, 14, 16\}$$

$$B \cap C = \{n \in \mathbb{Z}^+: n \text{ es par y } n \leq 16\} \cap \{n \in \mathbb{Z}^+: n \text{ es impar y } n < 15\}$$

$$= \{2, 4, 6, 8, 10, 12, 14, 16\} \cap \{1, 3, 5, 7, 9, 11, 13\} = \emptyset$$

$$A - C = \{n \in \mathbb{Z}^+: n \in A \wedge n \notin C\} = \{n \in \mathbb{Z}^+: n \in A \wedge n \in C'\} =$$

$$= \{1, 2, 3, 4, 5, 6, 7, 8\} \cap \{2, 4, 6, 8, 10, 12, 14, 15, 16, 17, 18, 19, \dots\} = \emptyset$$

### □ Ejemplos 2.15

Sean A y B subconjuntos arbitrarios de un conjunto arbitrario universal U. Entonces, se puede demostrar las siguientes relaciones entre las operaciones y los conjuntos operandos.

a)  $B - A \subseteq B$

Se toma un elemento arbitrario x de U:

$$x \in B - A \Leftrightarrow x \in B \wedge x \notin A \text{ (definición de diferencia)}$$

$$\Rightarrow x \in B \text{ (ley de simplificación)}$$

Luego,

$$\forall x, [x \in (B - A) \Rightarrow x \in B] \text{ consecuentemente } B - A \subseteq B.$$

b)  $A \subseteq A \cup B$

Sea x un elemento arbitrario de U:

$$x \in A \Rightarrow x \in A \vee x \in B \text{ (ley de adición disyuntiva)}$$

$$\Leftrightarrow x \in (A \cup B) \text{ (definición de unión)}$$

Luego,

$$\forall x, [x \in A \Rightarrow x \in (A \cup B)] \text{ consecuentemente } A \subseteq A \cup B$$

c)  $A \cap B \subseteq B$

Sea  $x$  un elemento arbitrario de  $U$ :

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B \text{ (definición de intersección)}$$

$$\Rightarrow x \in B \text{ (simplificación)}$$

Luego,

$$\forall x, [x \in (A \cap B) \Rightarrow x \in B] \text{ consecuentemente } A \cap B \subseteq B.$$

### Actividad 2.6

a) Observar el diagrama de Venn y responder con Verdadero o Falso, justificando su respuesta:

i)  $b \in (A \cap B' \cap C')$

ii)  $a \in (A \cup B) - C$

iii)  $B = \{e\}$

iv)  $d \notin (A \cup B \cup C)$

v)  $cc \in A'$

vi)  $h \in (A' \cap B' \cap C')$

vii)  $f \in (A - B)$

viii)  $g \in (C - A - B)$

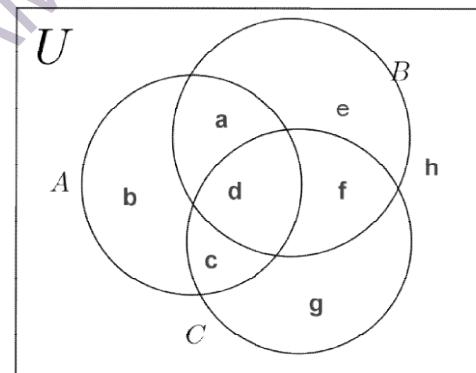


Fig.2.17. Actividad 2.6.

b) Realizar las siguientes operaciones y sombrear en la gráfica la zona correspondiente a cada apartado

i)  $A \cap B' \cap C'$

ii)  $(A \cap B) \cup C$

iii)  $A' \cap B' \cap C'$

iv)  $(C \cup B) - A$

## 2.10 Leyes del Álgebra de Conjuntos

Bajo las operaciones definidas anteriormente, los conjuntos satisfacen varias leyes o identidades conocidas también como propiedades de las operaciones entre conjuntos.

### 2.10.1 Leyes de Idempotencia

Dado cualquier conjunto A en un universal arbitrario U cualesquiera de un universo arbitrario U, se cumple que:

$$\text{i) } A \cup A = A$$

$$\text{ii) } A \cap A = A$$

#### Demostración

1i) Sea  $x$  un elemento arbitrario de U. Entonces,

$$x \in (A \cup A) \Leftrightarrow x \in A \vee x \in A \quad (\text{Definición de unión})$$

$$\Leftrightarrow x \in A \quad (\text{Idempotencia de } \vee)$$

De la arbitrariedad de  $x$  se sigue que

$$\forall x, [x \in (A \cup A) \Leftrightarrow x \in A]$$

De aquí que  $A \cup A = A$

1ii) Análogamente se prueba que  $A \cap A = A$ .

### 2.10.2 Leyes Comutativas

Dados dos conjuntos A y B de un universo arbitrario U, se verifica:

$$\text{i) } A \cup B = B \cup A$$

$$\text{ii) } A \cap B = B \cap A$$

#### Demostración

2i) Sea  $x$  un elemento arbitrario de U. Entonces,

$$x \in (A \cup B) \Leftrightarrow x \in A \vee x \in B \quad (\text{Definición de unión})$$

$$\Leftrightarrow x \in B \vee x \in A \quad (\text{Comutatividad de } \vee)$$

$$\Leftrightarrow x \in (B \cup A) \quad (\text{Definición de unión})$$

Como  $x$  es cualquiera de  $U$ , se sigue que

$$\forall x, [x \in (A \cup B) \Leftrightarrow x \in B \cup A]$$

Por lo tanto,  $A \cup B = B \cup A$

**2ii)** De forma similar se demuestra que  $A \cap B = B \cap A$ .

### 2.10.3 Leyes Asociativas

Dados tres conjuntos  $A, B$  y  $C$  de un universo arbitrario  $U$ , se verifica:

$$i) A \cup (B \cup C) = (A \cup B) \cup C$$

$$ii) A \cap (B \cap C) = (A \cap B) \cap C$$

#### Demostración

**3i)** Sea  $x$  un elemento arbitrario de  $U$ . Entonces,

$$x \in A \cup (B \cup C) \Leftrightarrow x \in A \vee [x \in (B \cup C)] \quad (\text{Definición de unión})$$

$$\Leftrightarrow x \in A \vee (x \in B \vee x \in C) \quad (\text{Definición de unión})$$

$$\Leftrightarrow (x \in A \vee x \in B) \vee x \in C \quad (\text{Asociatividad de } \vee)$$

$$\Leftrightarrow x \in (A \cup B) \vee x \in C \quad (\text{Definición de unión})$$

$$\Leftrightarrow x \in (A \cup B) \cup C \quad (\text{Definición de unión})$$

De la arbitrariedad de  $x$  se sigue que

$$\forall x, [x \in (A \cup (B \cup C)) \Leftrightarrow x \in ((A \cup B) \cup C)]$$

De aquí que  $A \cup (B \cup C) = (A \cup B) \cup C$

**3ii)** Análogamente se prueba que:  $A \cap (B \cap C) = (A \cap B) \cap C$

### 2.10.4 Leyes Distributivas

Dados tres conjuntos  $A, B$ , y  $C$  de un universo arbitrario  $U$ , se verifica:

$$i) A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad ii) A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

## Demostración

4i) Sea  $x$  un elemento arbitrario de  $U$ . Entonces,

$$\begin{aligned}x \in A \cup (B \cap C) &\Leftrightarrow x \in A \vee [x \in (B \cap C)] && (\text{Definición de unión}) \\&\Leftrightarrow x \in A \vee (x \in B \wedge x \in C) && (\text{Definición de intersección}) \\&\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) && (\text{Distributividad}) \\&\Leftrightarrow x \in (A \cup B) \wedge x \in (A \cup C) && (\text{Definición de unión}) \\&\Leftrightarrow x \in (A \cup B) \cap (A \cup C) && (\text{Definición de intersección})\end{aligned}$$

Al ser  $x$  cualquier elemento de  $U$ , se sigue que

$$\forall x, [x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)]$$

Queda probado entonces que:  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

4ii) Análogamente se prueba que:  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ .

## 2.10.5 Leyes de Absorción

Dados dos conjuntos  $A$  y  $B$  de un universo arbitrario  $U$ , se verifica:

$$\text{i)} A \cup (A \cap B) = A \quad \text{ii)} A \cap (A \cup B) = A$$

## Demostración

5i) Sea  $x$  un elemento arbitrario de  $U$ . Entonces,

$$\begin{aligned}x \in A \cup (A \cap B) &\Leftrightarrow x \in A \vee [x \in (A \cap B)] && (\text{Definición de unión}) \\&\Leftrightarrow x \in A \vee (x \in A \wedge x \in B) && (\text{Definición de intersección}) \\&\Leftrightarrow x \in A && (\text{Absorción})\end{aligned}$$

Al ser  $x$  cualquier elemento de  $U$ , se sigue que

$$\forall x, [x \in A \cup (A \cap B) \Leftrightarrow x \in A]$$

Consecuentemente:  $A \cup (A \cap B) = A$

**5ii)** Análogamente se prueba la expresión dual:  $A \cap (A \cup B) = A$

### 2.10.6 Leyes de los Complementos

Dado un conjunto cualquiera  $A$  de un universal arbitrario  $U$ , se verifica:

$$\text{i)} A \cup A' = U$$

$$\text{ii)} A \cap A' = \emptyset$$

#### Demostración

**6i)** Sea  $x$  un elemento arbitrario de  $U$ . Entonces,

$$x \in (A \cup A') \Leftrightarrow x \in A \vee x \in A' \quad (\text{Definición de unión})$$

$$\Leftrightarrow x \in A \vee x \notin A \quad (\text{Complementario})$$

$$\Leftrightarrow x \in A \vee \neg(x \in A) \quad (\text{Negación})$$

$$\Leftrightarrow x \in U \quad (\text{Tautología})$$

Luego,  $\forall x, [x \in (A \cup A') \Leftrightarrow x \in U]$ . Por lo tanto,  $A \cup A' = U$

**6ii)** En efecto,

$$A \cap A' = \{x \in U : x \in A \wedge x \in A'\} = \{x \in U : x \in A \wedge x \notin A\} = \emptyset$$

### 2.10.7 Ley de Involución o Involutiva

Dado un conjunto cualquier  $A$  de un universal  $U$ , se verifica:

$$(A')' = A$$

#### Demostración

Por definición de complemento se tiene que:

$$A' = \{x \in U : \neg(x \in A)\}$$

$$\text{Luego } (A')' = \{x \in U : \neg[\neg(x \in A)]\} \quad (\text{Doble Negación})$$

$$\text{Por lo tanto } (A')' = \{x \in U : x \in A\} = A$$

$$\text{En consecuencia } (A')' = A$$

## 2.10.8 Leyes de De Morgan

Dados dos conjuntos A y B en un universal U, se verifica:

$$\text{i) } (A \cup B)' = A' \cap B' \quad \text{ii) } (A \cap B)' = A' \cup B'$$

### Demostración

8i) Sea x un elemento arbitrario de U. Entonces,

$$\begin{aligned} x \in (A \cup B)' &\Leftrightarrow x \notin (A \cup B) && (\text{Def. de complementario}) \\ &\Leftrightarrow \neg[x \in (A \cup B)] && (\text{Negación}) \\ &\Leftrightarrow \neg[(x \in A) \vee (x \in B)] && (\text{Def. de unión}) \\ &\Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) && (\text{De Morgan para } \vee) \\ &\Leftrightarrow x \notin A \wedge x \notin B && (\text{Negación}) \\ &\Leftrightarrow x \in A' \wedge x \in B' && (\text{Definición de complementario}) \\ &\Leftrightarrow x \in A' \cap B' && (\text{Definición de intersección}) \end{aligned}$$

Al ser x cualquier elemento de U, se sigue que

$$\forall x, [x \in (A \cup B)' \Leftrightarrow x \in (A' \cap B')]. \text{ Luego } (A \cup B)' = A' \cap B'.$$

8ii) Análogamente se prueba que:  $(A \cap B)' = A' \cup B'$ .

## 2.10.9 Leyes de los elementos neutros

Dado un conjunto cualquier A de un universal U, se verifica:

$$\text{i) } A \cup \emptyset = A \quad \text{ii) } A \cap U = A$$

### Demostración

9i) Sea x un elemento arbitrario de U. Entonces,

$$\begin{aligned} x \in A \cup \emptyset &\Leftrightarrow (x \in A) \vee (x \in \emptyset) && (\text{definición de unión}) \\ &\Leftrightarrow x \in A && (x \in \emptyset \text{ es falso siempre}) \end{aligned}$$

Luego,  $\forall x, [x \in (A \cup \emptyset) \Leftrightarrow x \in A]$ . De aquí que  $A \cup \emptyset = A$ .

**9ii)** En forma análoga se demuestra:  $A \cap U = A$ .

### 2.10.10 Leyes de Dominación

Dado un conjunto cualquier  $A$  de un universal  $U$ , se verifica:

$$\text{i) } A \cap \emptyset = \emptyset$$

$$\text{ii) } A \cup U = U$$

#### Demostración

**10i)** Sea  $x$  un elemento arbitrario de  $U$ . Entonces,

$$x \in A \cap \emptyset \Leftrightarrow (x \in A) \wedge (x \in \emptyset) \quad (\text{definición de intersección})$$

$$\Leftrightarrow x \in \emptyset \quad (x \in \emptyset \text{ es falso siempre})$$

Luego,  $A \cap \emptyset = \emptyset$

**10ii)** En forma análoga se demuestra que:  $A \cup U = U$

#### Observaciones

- Existe una dualidad entre las leyes que utilizan la intersección y la unión, y las que utilizan el vacío y el universal. Es decir que al intercambiar las operaciones de unión por intersección, o intercambiar el  $\emptyset$  por el  $U$ , y viceversa, se obtiene otra expresión (o ley), que se llama su expresión dual.

### Actividad 2.7

Demostrar las siguientes propiedades:

a)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

b)  $(A \cap B)' = A' \cup B'$

c)  $A - B = A \cap B'$

d)  $A \oplus B = (A \cap B') \cup (B \cap A')$

e)  $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

f)  $A \oplus B \oplus C = (A \cap B' \cap C') \cup (B \cap A' \cap C') \cup (C \cap A' \cap B') \cup (A \cap B \cap C)$

## 2.11 Partición de un conjunto

### Definición

Sea  $A$  un conjunto cualquiera y sean:  $A_1, A_2, A_3, \dots, A_k$  subconjuntos no vacíos de  $A$ . Se dice que el conjunto  $\{A_1, A_2, A_3, \dots, A_k\}$  es una partición de  $A$  si y sólo si se cumplen las siguientes condiciones:

- 1) La unión de todos los subconjuntos arroja como resultado a  $A$ :

$$A_1 \cup A_2 \cup A_3 \cup \dots \cup A_k = A$$

- 2) Todo par de subconjuntos son disjuntos:

$$A_i \cap A_j = \emptyset \quad , \quad \forall i \neq j$$

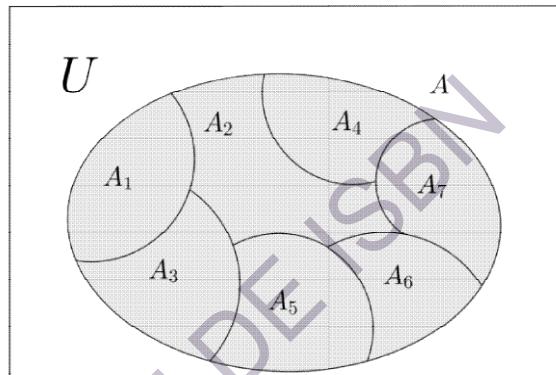


Fig. 2.18. Conjunto  $A$  particionado en siete subconjuntos.

### Ejemplo 2.16

Sea  $\mathbb{Z}$  el conjunto de los enteros. Si  $\mathbb{P} = \{x: x \text{ es par}\}$  e  $\mathbb{I} = \{x: x \text{ es impar}\}$ , se tiene que  $\{\mathbb{P}, \mathbb{I}\}$  es una partición de  $\mathbb{Z}$ , pues:  $\mathbb{P} \cap \mathbb{I} = \emptyset$  y  $\mathbb{P} \cup \mathbb{I} = \mathbb{Z}$ .

### Actividad 2.8

Sea  $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Determinar si las siguientes son particiones de  $A$ . Graficar los casos afirmativos.

- a)  $\{\{0, 1, 2, 3\}, \{3, 4, 5, 6\}, \{6, 7, 8, 9\}\}$
- b)  $\{\{0, 1, 2, 3\}, \{4, 5, 6\}, \{7\}, \{8, 9\}\}$
- c)  $\{\{x \in A / x \text{ es par}\}, \{x \in A / x \text{ es impar}\}\}$

## 2.12 Producto Cartesiano

### Definición

Dada una colección arbitraria de conjuntos  $A_1, A_2, \dots, A_n$ , el producto cartesiano de los mismos, y que se expresa como  $A_1 \times A_2 \times \dots \times A_n$ , es el conjunto formado por todas las  $n$ -úplas ordenadas  $(a_1, a_2, a_3, \dots, a_n)$ , donde  $a_i \in A_i$ ,  $1 \leq i \leq n$ . Es decir,

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, a_3, \dots, a_n), a_i \in A_i, 1 \leq i \leq n\}$$

En el caso de dos conjuntos  $A$  y  $B$ , se tiene:  $A \times B = \{(a, b) / a \in A \wedge b \in B\}$

El concepto de par ordenado es fundamental en Matemática. Nombrar un par ordenado significa dar dos elementos, uno de los cuales se identifica como primer elemento del par y el otro como segundo elemento del par.

Se usan pares ordenados de números reales para definir números complejos, para indicar las componentes de un vector en el plano, para asociar a cada punto del plano un par ordenado de números reales o al escribir la solución de los sistemas de dos ecuaciones con dos incógnitas, entre otros.

Si  $A = B$ ;  $A \times A = \{(a, b) / a \in A \wedge b \in A\}$  y se lo denota  $A^2$ .

Su extensión a ' $n$ ' conjuntos se define como

$$\overbrace{A \times A \times \dots \times A}^{n \text{ veces}} = \{(a_1, a_2, a_3, \dots, a_n), a_i \in A, 1 \leq i \leq n\} = A^n$$

### Observación

- El producto cartesiano:  $A \times \emptyset = \emptyset$ . En efecto, si  $A \times \emptyset$  no fuese vacío entonces existiría, al menos, un par  $(a, b) \in A \times \emptyset$  de aquí, por definición,  $a \in A \wedge b \in \emptyset$ , lo cual es imposible.

### Ejemplo 2.17

Sea el conjunto  $\mathbb{R}$  de los números reales, el producto cartesiano  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$  es el

conjunto de todos los pares ordenados de números reales.

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) / x, y \in \mathbb{R}\}$$

Cada punto P representa un par ordenado  $(x, y)$  de números reales y viceversa.

A  $\mathbb{R}^2$  se le llama usualmente PLANO CARTESIANO.

### ☞ Teorema

Si A y B son conjuntos finitos tal que  $|A| = n$  y  $|B| = m$ , entonces  $|A \times B| = n \cdot m$

### □ Ejemplo 2.18

Sean los conjuntos  $A = \{x \in \mathbb{Z} : 4 < x < 9\}$  y  $B = \{x \in \mathbb{Z} : -8 < x \leq -6\}$ .

Para determinar los elementos de  $A \times B$ , primero se determina por extensión los conjuntos A y B:

$$A = \{x \in \mathbb{Z} : 4 < x < 9\} = \{5, 6, 7, 8\}; \text{ luego } |A| = 4$$

$$B = \{x \in \mathbb{Z} : -8 < x \leq -6\} = \{-7, -6\}; \text{ luego } |B| = 2.$$

$$\text{Entonces: } A \times B = \{(5, -7); (5, -6), (6, -7); (6, -6), (7, -7); (7, -6), (8, -7); (8, -6)\}$$

$$\text{Y el cardinal de este conjunto es: } |A \times B| = |A| \cdot |B| = 4 \cdot 2 = 8$$

### Actividad 2.9

Sean  $A = \{1, 2, 3\}$  y  $B = \{a, b\}$ . Contestar Verdadero o Falso, y justificar la respuesta:

i)  $A \subseteq (A \times B)$

ii)  $(A \times B) - A = B$

iii)  $(1, 3) \in A \times A \wedge (3, 1) \in A \times A$

iv)  $|B \times B| = 4$

## 2.13 Relaciones entre conjuntos

Existen algunas estructuras básicas que pueden representarse a través de la relación entre elementos de conjuntos.

Las relaciones tienen una importancia fundamental tanto en la teoría como en las aplicaciones a la informática.

Una estructura de datos como una lista, una matriz o un árbol, se usan para representar conjuntos de elementos junto con una relación entre los mismos.

Las relaciones que son parte de un modelo matemático están a menudo implícitamente representadas por relaciones en una estructura de datos.

Aplicaciones numéricas, recuperación de información y problemas de redes son otros ejemplos donde las relaciones ocurren como parte de la descripción del problema, y la manipulación de éstas son importantes en la resolución de procedimientos. También juegan un importante papel en la teoría de computación, incluyendo estructuras de programas y análisis de algoritmos.

Anteriormente, se trabajó con relaciones importantes entre proposiciones: la implicación y la equivalencia; y la relación de subconjunto para conjuntos.

En la vida diaria existen relaciones entre elementos, entre conjuntos y entre elementos y conjuntos. Hay relaciones de parentesco, de amistad, de paisaje, etc., entre personas; relaciones diplomáticas, económicas, etc., entre países; entre números, relaciones como “mayor que” o “menor o igual que” etc.

### Definición

Sean los conjuntos  $A_1, A_2, \dots, A_n$ . Una relación  $R$  sobre  $A_1 \times A_2 \times \dots \times A_n$  es cualquier subconjunto de este producto cartesiano, es decir,

$$R \subseteq A_1 \times A_2 \times \dots \times A_n$$

Si  $R = \emptyset$ , se llama a  $R$  relación vacía

Si  $R = A_1 \times A_2 \times \dots \times A_n$ , se llama a  $R$  la relación universal.

Si  $A_i = A$ ,  $\forall i = 1, 2, \dots, n$ , entonces  $R$  es una relación  $n$ -aria sobre  $A$ .

Si  $n = 2$ , se dice que  $R$  es una relación binaria y si  $n = 3$ , una relación ternaria.

### 2.13.1 Relaciones binarias

La clase más importante de relaciones es la de las relaciones binarias, debido a que este tipo de relaciones son las más frecuentes en las aplicaciones.

En general el término “relación” denota una relación binaria, en otro caso se especificará con términos tales como “ternaria” o “ $n$ -aria”.

#### Definición

Sean  $A$  y  $B$  dos conjuntos no vacíos. Una relación  $R$  binaria de  $A$  en  $B$  es cualquier subconjunto del producto cartesiano  $A \times B$ . Simbólicamente:

$$R \subseteq (A \times B) \quad \text{o} \quad R : A \rightarrow B$$

#### Notación:

Dado que  $R$  es un conjunto de pares ordenados, si  $(a, b)$  forma parte de la relación se denota

$$(a, b) \in R \quad \text{o} \quad a R b$$

En cualquiera de los casos se tiene que  $a$  está relacionado con  $b$ .

#### Caso particular:

Si  $A = B$ ,  $R$  es una relación definida en  $A$  y se expresa

$$R \subseteq (A \times A) \quad \text{o} \quad R : A \rightarrow A$$

#### Ejemplos 2.19

a) Sea  $R$  la relación “mayor que” definida en el conjunto  $\mathbb{Z}$  de los números enteros. Se tiene que  $8 > -2$  para indicar que el par  $(8, -2) \in R$  y el par  $(-2, 8) \notin R$  porque  $-2$  no es mayor que  $8$ .

b) Cuando un compilador traduce un programa informático construye una tabla de símbolos que contiene los nombres de los símbolos presentes en el programa, los atributos asociados a cada nombre y las sentencias de programa en las que están presentes cada uno de los nombres. Así pues, si  $S$  es el

conjunto de los símbolos, A es el conjunto de los posibles atributos y P es el conjunto de las sentencias de programa, entonces la tabla de símbolos incluye información representada por las relaciones binarias de  $S \rightarrow A$  y de  $S \rightarrow P$ .

c) Sea  $A = \{a, b, c\}$  y  $R = \{(a, a); (a, b), (a, c), (c, c)\}$  una relación en A, ya que es un subconjunto de  $A \times A$ .

Con respecto a esta relación se tiene que:  $a R a$ ;  $a R b$ ;  $b R c$ , y  $c R c$ .

### 2.13.2 Dominio e Imagen

#### Definición

El dominio de una relación R es el conjunto formado por los primeros elementos de los pares ordenados de R.

La imagen de R es el conjunto formado por los segundos elementos de los pares ordenados de R.

Es decir, si  $R: A \rightarrow B$ , entonces:

$$\text{Dom}(R) = \{x \in A / \exists y \in B \wedge (x, y) \in R\}$$

$$\text{Img}(R) = \{y \in B / \exists x \in A \wedge (x, y) \in R\}$$

Así en el Ejemplo (2.19 c), el  $\text{Dom}(R) = \{a, c\}$  y la  $\text{Img}(R) = \{a, b, c\}$ .

### 2.13.3 Conjunto Relativo de un elemento

#### Definición

Sea  $R: A \rightarrow B$  y sea  $a \in A$ . Se define conjunto relativo de  $a$ , que se denotará  $R(a)$ , al conjunto de elementos de B que están relacionados con  $a$ . Simbólicamente:  $R(a) = \{y \in B / (a, y) \in R\}$

También se dice que  $R(a)$  es el conjunto imagen de  $a$  por medio de R.

## □ Ejemplo 2.20

Sean los conjuntos  $A = \{2, 4, 6\}$  y  $B = \{12, 16, 18, 19\}$ , los elementos de la relación  $R \subseteq A \times B$ , donde

$$x R y \Leftrightarrow x \text{ divide a } y$$

Luego los elementos de  $R$  son:  $R = \{(2, 12), (2, 16), (2, 18), (4, 12), (4, 16)\}$

Y, por ejemplo, el conjunto relativo de 4, es:

$$R(4) = \{y \in B / (4, y) \in R\} = \{12, 16\}.$$

### 2.13.4 Función

Las funciones son un tipo especial de relaciones binarias. Una función puede tomarse como una relación de entrada-salida; es decir, para cada entrada o argumento, una función produce una salida o valor. Las funciones son la base de muchas herramientas matemáticas, y muchos de nuestros conocimientos en informática pueden ser codificados convenientemente describiendo las propiedades de cierto tipo de funciones.

#### ☒ Definición

Sean  $A$  y  $B$  dos conjuntos no vacíos. Una función  $f$  de  $A$  en  $B$  es una relación de  $A$  en  $B$ , en la que para cada  $a \in A$ , existe un único elemento  $b \in B / (a, b) \in f$ .

#### Notación

$$f: A \rightarrow B$$

Es decir, una función  $f$  de  $A$  en  $B$  es una relación de  $A$  en  $B$  con las dos características especiales siguientes.

i)  $\text{Dom } f = A$  (condición de existencia)

$\forall a \in A, \exists b \in B: f(a) = b$ , o sea, para cada elemento de  $A$  ha de encontrarse un elemento  $b$  en  $B$  tal que  $f(a) = b$

ii)  $(a, y) \in f \wedge (a, z) \in f \Rightarrow y = z$  (condición de unicidad)

Es decir si  $f(a) = y \wedge f(a) = z$ , entonces  $y = z$

## ⌚ Observaciones

- Si  $(a, b) \in f$  se tiene  $f(a) = b$  y se dice que  $b$  es la imagen de  $a$  mediante  $f$ .
- Una relación de  $A \rightarrow B$  no es función si existen elementos en  $A$  que no se correspondan con los elementos de  $B$ . O bien, porque exista algún elemento en  $A$  que tenga dos imágenes, es decir que haya dos pares ordenados en  $R$  con la misma primera componente.
- Las funciones reciben también el nombre de aplicaciones o transformaciones, ya que desde un punto de vista geométrico, se pueden considerar como reglas que asignan a cada elemento  $a \in A$ , el único elemento  $f(a) \in B$ .

## ▣ Ejemplos 2.21

Sean los conjuntos  $A = \{1, 3, 5\}$  y  $B = \{a, b, c, d\}$ , y las relaciones siguientes:

- i)  $R_1 = \{(3, a); (5, a)\}$       ii)  $R_2 = \{(3, a); (3, b), (5, b), (5, c)\}$   
iii)  $R_3 = \{(1, a), (3, a); (5, a)\}$       iv)  $R_4 = \{(1, a), (3, b); (5, a)\}$

Se analizará cada una para ver si son funciones de  $A$  en  $B$ .

i)  $R_1$  no es función ya que  $\text{Dom}(R_1) = \{3, 5\} \neq A$ .

Hay un elemento de  $A$ , el 1, que no es primer elemento de los pares de la relación, es decir a 1 no le corresponde ningún elemento del conjunto  $B$ .

ii)  $R_2$  no es función ya que contiene los pares ordenados  $(3, a)$  y  $(3, b)$ , es decir, el 3 tiene dos imágenes distintas, a y b, lo cual no cumple la segunda condición de la definición de relación.

iii)  $R_3$  si es función, dado que,  $f: A \rightarrow B$  tal que  $f(x) = a, \forall x \in A$ . Su  $\text{Img}(f) = \{a\}$ .

iv)  $R_4 = \{(1, a), (3, b); (5, a)\}$ , si es función dado que  $f: A \rightarrow B$  y tal que

$f(1) = a, f(3) = b, f(5) = a$ , luego  $\text{Dom}(f) = A$ .

Además no hay dos pares ordenados con la misma primera componente. Su  $\text{Img}(f) = \{a, b\}$

### Actividad 2.10

a) Si  $A = \{1, 2, 3, 4, 5\}$  y  $B = \{0, 1, 2, 3, 4, 5\}$ , expresar por extensión las siguientes relaciones de  $A$  en  $B$ :

$$R_1 = \{(x, y) / |x - y| = 1\}$$

$$R_2 = \{(x, y) / x = y + 1\}$$

b) Si  $A = \{1, 2, 3, 4, 5\}$ , expresar por comprensión las siguientes relaciones definidas en  $A$ :

$$R_3 = \{(1,2), (1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5), (4,5)\}$$

$$R_4 = \{(1,1), (2,4)\}$$

$$R_5 = \{(1,1), (2,2), (3,3), (4,4), (5,5)\}$$

c) Dar dominio e imagen de cada una y también el conjunto relativo a 2

d) ¿Cuál de las relaciones es función?

### 2.14 Matriz de una Relación Binaria

Una de las formas de representar una relación entre dos conjuntos finitos, es a través de su matriz booleana.

#### Definición

Una matriz booleana es una matriz (arreglo rectangular de números dispuestos en  $m$  reglones horizontales y  $n$  columnas verticales), cuyas componentes o entradas son exclusivamente ceros '0' o unos '1'.

Es decir, dados  $m, n \in \mathbb{N}$ , la matriz booleana  $A = (a_{ij})$  de orden  $mxn$  es aquella matriz, tal que su elemento genérico:  $a_{ij} \in \{0, 1\}$ , con  $1 \leq i \leq m, 1 \leq j \leq n$

Se emplean para representar estructuras discretas (representación de relaciones en programas informáticos, modelos de redes de comunicación y sistemas de transporte).

### □ Ejemplo 2.22

Matrices booleanas de tamaño 3x3 y de 3x2

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

#### 2.14.1 Operaciones con matrices booleanas

Las operaciones que se pueden realizar entre matrices booleanas son tres: unión, conjunción y producto booleano. Sin embargo, estas operaciones no pueden realizarse sobre dos matrices cualesquiera, sino que deben cumplir ciertas condiciones para poder llevarse a cabo. En particular, en el caso de la unión y la conjunción, las matrices que intervienen en la operación deben tener el mismo tamaño, y en el caso del producto booleano, las matrices deben ser conformables para el producto de matrices.

##### a) Unión / Disyunción

###### ▢ Definición

Sean  $A = (a_{ij})$  y  $B = (b_{ij})$  matrices booleanas del mismo orden ( $mxn$ ), la unión/disyunción de  $A$  y  $B$ , es la matriz booleana  $C$  (de orden  $mxn$ ) que se denota  $C = A \vee B$ , y tal que

$$c_{ij} = \begin{cases} 1 & \text{si y solo si } a_{ij} = 1 \vee b_{ij} = 1 \\ 0 & \text{en otro caso} \end{cases}$$

También se denomina a  $C$  como matriz suma lógica

### □ Ejemplo 2.23

Si  $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$  y  $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ , la matriz suma lógica de A y B, es

$$C = A \vee B = \begin{pmatrix} 1 \vee 1 & 1 \vee 0 & 0 \vee 1 \\ 0 \vee 1 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 1 \vee 1 & 1 \vee 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

### b) Intersección/conjunción

#### ☒ Definición

Sean  $A = (a_{ij})$  y  $B = (b_{ij})$  matrices booleanas del mismo orden ( $m \times n$ ), la conjunción/intersección de A y B, es la matriz booleana C (de orden  $m \times n$ ) que se deno como  $C = A \wedge B$ , y tal que

$$c_{ij} = \begin{cases} 1 & \text{si y solo si } a_{ij} = b_{ij} = 1 \\ 0 & \text{en otro caso} \end{cases}$$

También se denomina a C como matriz producto lógico.

### □ Ejemplo 2.24

Si  $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$  y  $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ , la matriz producto lógico de A y B, es

$$C = A \wedge B = \begin{pmatrix} 1 \wedge 1 & 1 \wedge 0 & 0 \wedge 1 \\ 0 \wedge 1 & 1 \wedge 0 & 0 \wedge 0 \\ 0 \wedge 0 & 1 \wedge 1 & 1 \wedge 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

### c) Producto booleano

#### ☒ Definición

Sean  $A = (a_{ij})$  y  $B = (b_{ij})$  dos matrices booleanas tales que A es de orden  $m \times r$  y B es de orden  $r \times n$ , la *matriz producto booleano* entre A y B es la matriz

booleana C de orden  $m \times n$ , que se denota como  $C = A \odot B$ , y tal que:

$$c_{ij} = \begin{cases} 1 & \text{si y solo si } \exists k / a_{ik} = 1 \wedge b_{kj} = 1 \\ 0 & \text{en otro caso} \end{cases}$$

### Observaciones

- El producto booleano es idéntico a la multiplicación matricial ordinaria en donde se operan filas de la primera matriz con columnas de la segunda matriz interviniente y tal que
  - La adición es sustituida por  $\vee$ , y
  - La multiplicación es sustituida por  $\wedge$ .

### Ejemplo 2.25

Si  $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$  y  $B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ , el producto booleano de A y B es la matriz:

$$C = A \odot B = \begin{pmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

### d) Dominación

#### Definición

Sean las matrices  $A = (a_{ij})$  y  $B = (b_{ij})$  del mismo orden, se dice que A domina a B y se escribe  $A \geq B$ , si y sólo si  $a_{ij} \geq b_{ij} \quad \forall i, j$ .

### ◻ Ejemplo 2.26

La matriz  $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$  domina a la matriz  $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Pues  $\forall i, j: a_{ij} \geq b_{ij}$

### Actividad 2.11

Dadas las matrices

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

- Calcular  $A \vee B$ ,  $A \wedge B$ ,  $A \odot B$  y  $B \odot A$
- Responder : A domina a B , B domina a A?

Desde ahora y hasta el final del capítulo se trabajarán con las relaciones definidas en un conjunto, o sea las del tipo  $R : A \rightarrow A$ .

#### 2.14.2 Matriz de adyacencia de una Relación

##### ❖ Definición

Sea  $A$  un conjunto finito y sea  $R$  una relación definida en  $A$ . Se define matriz de adyacencia de  $R$  y se denota  $M_R$ , a la matriz cuyo elemento genérico  $m_{ij}$  está dado por

$$M_R = (m_{ij}) : m_{ij} = \begin{cases} 1 & \text{si } (a_i, a_j) \in R \\ 0 & \text{si } (a_i, a_j) \notin R \end{cases}$$

##### ❖ Observación

- $M_R$  es una matriz booleana de orden  $n$ , y de la definición se deduce que la matriz es cuadrada.

### Teorema

Toda relación definida en un conjunto finito tiene representación matricial booleana y recíprocamente toda matriz booleana representa una relación binaria.

### Ejemplo 2.27

Sea  $A = \{1, 2, 4\}$ , si se define la relación  $R$  mediante la expresión:

$$a R b \Leftrightarrow b \text{ es múltiplo de } a, \quad \forall a \in A.$$

La relación vendrá dada por el conjunto

$$R = \{(1,1), (1,2), (1,2), (1,4), (2,2), (2,4), (4,4)\}$$

Y la matriz de la relación  $R$ , es:  $M_R = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

### Observación

- $M_R$  es la matriz de una relación de  $A \rightarrow A$ , cada fila se corresponde con un elemento de  $A$  y cada columna con un elemento de  $A$ . Para calcular el dominio de  $R$  bastará ver en qué filas hay, al menos, un uno y para calcular la imagen bastará con ver en qué columnas hay, al menos, un uno. En el Ejemplo 2.27, el  $\text{Dom}(R) = \{1, 2, 4\}$  y la  $\text{Img}(R) = \{1, 2, 4\}$ .

Existe otra forma de representar una relación cuando es de un conjunto en sí mismo, es decir, cuando la relación es binaria.

## 2.15 Dígrafo

### Definición

Un dígrafo o grafo dirigido es un par ordenado  $D = (A, R)$  donde  $A$  es un conjunto finito y  $R$  es una relación binaria definida sobre  $A$ .

A los elementos de  $A$  se los denominan nodos o vértices y a los elementos de  $R$  se los denominan arcos o aristas del dígrafo  $D$ .

### 2.15.1 Representación gráfica de un Dígrafo

- 1) A los elementos del conjunto A los se los representa arbitrariamente en el plano por medio de puntos, círculos, etc. los cuáles serán los vértices o nodos del dígrafo.
- 2) A los pares ordenados de la relación R se los representará por medio de flechas en el plano uniendo los vértices, de tal modo que si  $(x, y) \in R$  entonces se dibujará una flecha que va desde  $x$  hacia  $y$ . Estas serán las aristas o arcos del dígrafo. El primer elemento del par “ $x$ ” se denomina vértice inicial y al segundo elemento del par “ $y$ ”, vértice final de la arista  $(x, y)$ .
- 3) Si  $(x, x) \in R$  entonces se dibujará una flecha de  $x$  a  $x$ . Se le llamará bucle o lazo.

#### □ Ejemplo 2.28

En la Figura 2.19, se tiene una representación gráfica del dígrafo  $D = (A, R)$ , siendo  $A = \{1, 2, 3, 4\}$  y  $R = \{(1,2); (1, 3), (2,1), (2,3), (3,4), (4,3)\}$ .

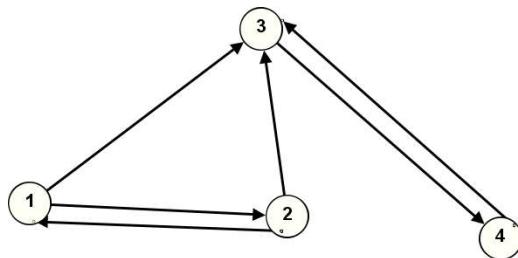


Fig. 2.19.  $D=(A,R)$

#### @@ Observaciones

- Un grafo dirigido caracteriza a una relación, es decir, conociendo la relación se conoce el dígrafo y conociendo el dígrafo, puede establecerse la relación.
- Si  $D$  es el dígrafo de una relación en un conjunto finito  $A$ , entonces el dominio y la imagen de  $R$  están formados por los puntos que son, respectivamente, extremo inicial y final de algún arco.
- Posteriormente, cuando se estudie el tema de Grafos y Árboles se representará a

los dígrafos por medio de la notación  $D = (V, A, \varphi)$  donde  $V$  representa al conjunto de vértices,  $A$  al conjunto de aristas y  $\varphi$  una función, llamada de incidencia dirigida, que representa  $\varphi: A \rightarrow (V \times V)$ .

### Actividad 2.12

Encontrar la matriz y el digrafo de las relaciones definidas en  $A = \{1, 2, 3, 4\}$

$$R_1 = \{(x, y) / x - y = 1\}$$

$$R_2 = \{(x, y) / x = -y\}$$

$$R_3 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$$

$$R_4 = \{(1, 2), (2, 4), (2, 1), (4, 2)\}$$

### 2.16 Composición de Relaciones

#### Definición

Sean  $R_1$  y  $R_2$  relaciones en el conjunto  $A$ , la composición de  $R_1$  seguida de  $R_2$ , y que se denota  $R_2 \circ R_1$ , es la relación definida por:

$$R_2 \circ R_1 = \{(x, y) / \exists z \in A \text{ tal que } (x, z) \in R_1 \wedge (z, y) \in R_2\}$$

#### Ejemplos 2.29

Sean las relaciones  $R_1$  y  $R_2$  definidas en  $A = \{1, 2, 3, 4, 5\}$  por medio de

$$R_1 = \{(1, 2), (1, 3), (2, 4), (3, 5), (5, 1), (4, 4)\}$$

$$R_2 = \{(1, 4), (3, 5), (4, 1), (4, 3), (5, 2)\}$$

Entonces se tiene que

$$R_2 \circ R_1 = \{(x, y) / \exists z \in A \text{ tal que } (x, z) \in R_1 \wedge (z, y) \in R_2\}$$

$$= \{(1, 5), (2, 1), (2, 3), (3, 2), (5, 4), (4, 1), (4, 3)\}$$

$$R_1 \circ R_2 = \{(x, y) / \exists z \in A \text{ tal que } (x, z) \in R_2 \wedge (z, y) \in R_1\}$$

$$= \{(1, 4), (3, 1), (4, 2), (4, 3), (4, 5), (5, 4)\}$$

### Observación

La composición de relaciones NO es commutativa.

### Actividad 2.13

Sean las relaciones  $R_1$  y  $R_2$  definidas en  $A = \{1, 2, 3, 4, 5, 6\}$  por medio de

$$R_1 = \{(1, 1), (1, 3), (1, 2), (2, 4), (3, 5), (4, 5), (5, 2), (6, 6)\}$$

$$R_2 = \{(1, 4), (2, 3), (2, 6), (3, 6), (4, 1), (5, 3), (6, 2)\}$$

Expresar por extensión a las nuevas relaciones  $R_2 \circ R_1$  y  $R_1 \circ R_2$ , y confeccionar los correspondientes dígrafos.

### Teorema sobre la matriz de una composición de relaciones

Sea  $A$  un conjunto finito y sean  $R_1$  y  $R_2$  relaciones definidas en  $A$  con sus respectivas matrices de Adyacencia  $M_{R_1}$  y  $M_{R_2}$ . Entonces para la composición  $R_2 \circ R_1$  la matriz de adyacencia  $M_{R_2 \circ R_1}$  es el producto booleano entre las matrices  $M_{R_1}$  y  $M_{R_2}$ . Es decir:  $M_{R_2 \circ R_1} = M_{R_1} \odot M_{R_2}$

### Actividad 2.14

Considerando  $R_1$  y  $R_2$  definidas en la Actividad 2.13, encontrar las matrices de las nuevas relaciones en cada apartado realizando los correspondientes productos:

- i)  $R_2 \circ R_1$
- ii)  $R_1 \circ R_2$
- iii)  $R_1 \circ R_1$
- iv)  $R_2 \circ R_2$

## 2.17 Relaciones Compuestas

### Definición

Sea  $A$  finito y sea  $R: A \rightarrow A$ . Se define  $R^n$  como la composición de  $R$  por si misma  $n$  veces. Esto es

$$R^n = R \circ R \circ \dots \circ R$$

Expresado de otro modo se tiene que:

$$R^n = \{ (x, y) / \exists z_1, z_2, \dots, z_{n-1} \in A, \text{ tal que } (x, z_1), (z_1, z_2), \dots, (z_{n-1}, y) \in R \}.$$

### Teorema

Sea  $A$  un conjunto finito y sea  $R: A \rightarrow A$ .

La matriz de adyacencia de la relación  $R^n$  se obtiene como el producto booleano de la matriz de  $R$  por si misma 'n' veces. Esto es:

$$M_{R^n} = \overbrace{M_R \odot M_R \odot \dots \odot M_R}^{n \text{ veces}}$$

### Actividad 2.15

Si  $A = \{1, 2, 3, 4\}$  y sea  $R$  dada por la Figura 2.20

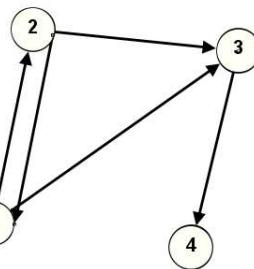


Fig. 2.20 . Digrafo de  $R$ .

Demostrar que los digrafos de las relaciones  $R^2$ ,  $R^3$  y  $R^4$  son los siguientes, respectivamente:

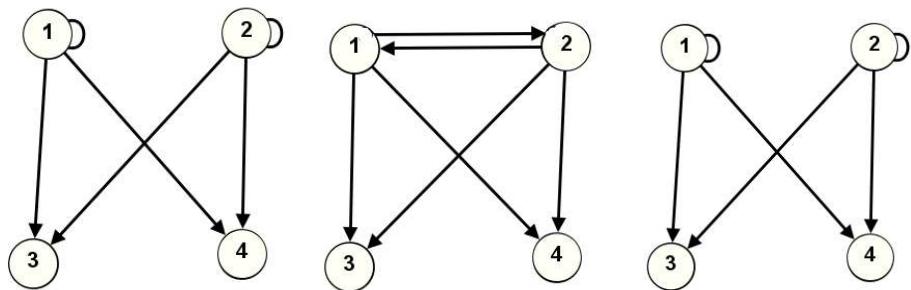


Fig. 2.21. Digrafos de  $R^2$ ,  $R^3$  y  $R^4$ .

## 2.17.1 Trayectorias en Digrafos

### Definición

La sucesión “ $x, z_1, z_2, \dots, z_{n-1}, y$ ” que se obtiene de  $R^n$ , se denomina trayectoria de  $x$  a  $y$ , cuya longitud es  $n$  dado que los vértices  $x$  e  $y$  están conectados por medio de  $n$  aristas.

Cada par  $(x, y)$  que pertenece a estas nuevas relaciones  $R^2, R^3$  y  $R^4, \dots, R^n$  debe cumplir la condición de que existan  $n-1$  elementos (aristas) que los conecten.

## 2.18 Propiedades de las Relaciones Binarias

Sea  $A$  un conjunto y sea  $R: A \rightarrow A$  una relación binaria.  $R$  puede gozar de ciertas propiedades las cuales se presentan a continuación:

### 2.18.1 Reflexividad

#### Definición

Una relación binaria  $R$  sobre un conjunto  $A$  se dice que es reflexiva, cuando cada elemento de  $A$  está relacionado consigo mismo. Es decir,

$$R \text{ es Reflexiva} \Leftrightarrow \forall x \in A, (x, x) \in R$$

Si se niega ambos miembros, se tiene:

$$R \text{ no es Reflexiva} \Leftrightarrow \exists x \in A, (x, x) \notin R$$

Consecuentemente, si se puede encontrar, al menos, un elemento ‘ $x$ ’ en el conjunto  $A$  que no esté relacionado consigo mismo, la relación  $R$  no es reflexiva.

Cuando  $\forall x \in A, (x, x) \notin R$ , se dice que la relación  **$R$  es Arreflexiva**.

#### Observaciones

- Esta propiedad se refleja en un digrafo, cuando todos los vértices tienen lazos (ciclos de longitud 1) en cada uno de los vértices.
- La matriz de una relación reflexiva, se caracteriza por tener todos los elementos

de su diagonal principal iguales a uno. Es decir,  $M_R = (m_{ij})$ , entonces

$$R \text{ es reflexiva} \Leftrightarrow m_{ii} = 1, \forall i \quad y \quad R \text{ no es reflexiva} \Leftrightarrow \exists i: m_{ii} = 0$$

- La propiedad ‘no reflexiva’ se refleja en un dígrafo, cuando algunos de los vértices no tienen lazos.
- La matriz de una relación arreflexiva, se caracteriza por tener todos los elementos de su diagonal principal iguales a cero. Es decir,  $M_R = (m_{ij})$ , entonces

$$R \text{ es arreflexiva} \Leftrightarrow m_{ii} = 0, \forall i$$

## 2.18.2 Simetría

### Definición

Una relación binaria  $R$  sobre un conjunto  $A$  es simétrica si cada vez que  $x$  está relacionado con  $y$  se sigue que  $y$  está relacionado con  $x$ . Es decir,

$$R \text{ es Simétrica} \Leftrightarrow \forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$$

Negando ambos miembros, se tiene:

$$\neg(R \text{ es Simétrica}) \Leftrightarrow \exists x, y \in A: \neg[(x, y) \in R \vee (y, x) \in R] \text{ es decir}$$

$$R \text{ es no simétrica} \Leftrightarrow \exists x, y \in A : (x, y) \in R \wedge (y, x) \notin R$$

O sea, si hay dos elementos ‘ $x$ ’ e ‘ $y$ ’ en  $A$  tales que ‘ $x$ ’ esté relacionado con ‘ $y$ ’ pero ‘ $y$ ’ no lo esté con ‘ $x$ ’, entonces  $R$  es *no simétrica*.

### Observaciones

- Si  $G$  es el dígrafo de una relación simétrica, entonces entre cada dos vértices distintos de  $G$  existen dos aristas con distintos sentidos, o no existe ninguna.
- La matriz  $M_R = (m_{ij})$  de una relación simétrica, satisface la propiedad de que todo par de elementos colocados simétricamente respecto de la diagonal principal son iguales. Luego entonces

$$R \text{ es simétrica} \Leftrightarrow \forall i, j, m_{ij} = m_{ji}$$

$$\text{y } R \text{ es no simétrica} \Leftrightarrow \exists i, j \text{ tales que } m_{ij} \neq m_{ji}.$$

### 2.18.3 Asimetría

#### Definición

Una relación binaria  $R$  definida en un conjunto  $A$  se dice que es asimétrica si cada vez que  $x$  está relacionado con  $y$  se sigue que  $y$  no está relacionado con  $x$ . Es decir,

$$R \text{ es Asimétrica} \Leftrightarrow \forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \notin R$$

#### Observaciones

- Otra forma de expresar esta definición es:

$$R \text{ es Asimétrica} \Leftrightarrow \forall x, y \in A, (x, y) \in R \vee (y, x) \notin R$$

- Si  $G$  es el dígrafo de una relación asimétrica, entonces entre cada dos vértices distintos de  $G$ , existe un arco o no existe ninguno, además no existen los lazos en relaciones asimétricas.
- La matriz  $M_R = (m_{ij})$  de una relación asimétrica, satisface la propiedad de que si  $i = j$ ,  $m_{ij} = 0$ , y si  $m_{ij} = 1$  entonces  $m_{ji} = 0$ ,  $\forall i \neq j$ .

### 2.18.4 Antisimetría

#### Definición

Una relación binaria  $R$  definida en  $A$  se dice antisimétrica si cada vez que  $x$  está relacionado con  $y$  e  $y$  está relacionado con  $x$ , entonces  $x = y$ . Es decir,

$$R \text{ es Antisimétrica} \Leftrightarrow \forall x, y \in A, (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$$

#### Observaciones

- Otra forma de expresar la definición de antisimetría es:

$$R \text{ es Antisimétrica} \Leftrightarrow \forall x, y \in A, [x \neq y \Rightarrow (x, y) \notin R \vee (y, x) \notin R]$$

- Es decir, si  $G$  es el dígrafo de una relación antisimétrica, entonces entre cada dos vértice distintos de  $A$ , existe un arco o no existe ninguno, permitiendo los bucles.
- La matriz  $M_R = (m_{ij})$  de una relación antisimétrica, satisface la propiedad de que:

$$\text{Si } \exists i \text{ tal que } m_{ii} = 1 \text{ y } \forall i \neq j, m_{ij} = 0 \vee m_{ji} = 0.$$

## 2.18.5 Transitividad

### Definición

Se dice que una relación  $R$  definida en un conjunto  $A$  es transitiva, si cada vez que  $x$  está relacionado con  $y$  e  $y$  está relacionado con  $z$ , entonces  $x$  está relacionado con  $z$ .

Es decir,

$$\begin{aligned} R \text{ es transitiva} &\Leftrightarrow \forall x, y, z \in A, [(x R y \wedge y R z) \Rightarrow x R z] \\ &\Leftrightarrow \forall x, y, z \in A, (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R \end{aligned}$$

Negando los dos miembros de la equivalencia anterior, se tiene

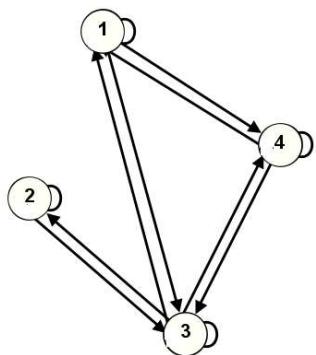
$$R \text{ es no transitiva} \Leftrightarrow \exists x, y, z \in A: (x, y) \in R \wedge (y, z) \in R \wedge (x, z) \notin R$$

### Observaciones

- Si  $D$  es el dígrafo de una relación transitiva y existen arcos desde  $x$  hasta  $y$ , y desde  $y$  hasta  $z$ , entonces existirá un arco desde  $x$  hasta  $z$ . En otras palabras, si existe una trayectoria de longitud 2 entre  $x$  y  $z$  entonces debe existir la trayectoria de longitud 1 entre ellos. Y se debe probar que esto se verifica para **todas** las ternas posibles.
- Es posible caracterizar la relación transitiva por su matriz  $M_R$  y  $M_{R^2}$ . Dado que la relación  $R^2$  representa a las trayectorias de longitud 2 presentes en  $R$ . Es decir, se tendrá que  $R$  es transitiva si y solo si la matriz de  $R$  domina a la matriz de  $R^2$ , o sea,  $R$  es una relación transitiva si y solo si  $M_R \geq M_{R^2}$ .

### Ejemplo 2.30

Sea la relación  $R$ , definida en el conjunto  $A = \{1, 2, 3, 4\}$  cuyo digrafo es la Figura 2.22. Se observa que:



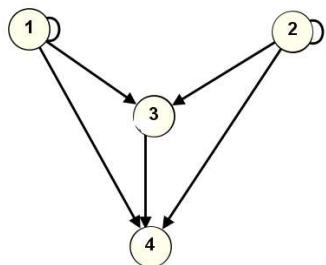
- i) R es reflexiva, porque todos los vértices están relacionados consigo mismo,
- ii) R es simétrica porque entre dos vértices distintos de G existen dos aristas con distintos sentidos, o ninguna.
- iii) R no es transitiva porque  $1 \text{ R } 3$  y  $3 \text{ R } 2$  pero  $(1, 2) \notin R$ .

Fig.2.22. Digrafo de R.

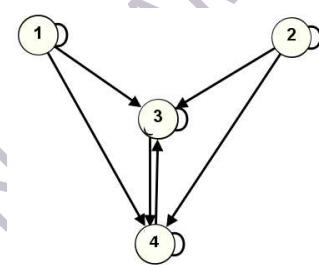
### Actividad 2.16

Dadas las relaciones  $R_1$ ,  $R_2$  y  $R_3$  por sus digrafos  $D_1$ ,  $D_2$  y  $D_3$ , determinar las propiedades que satisfacen cada una.

$D_1$



$D_2$



$D_3$

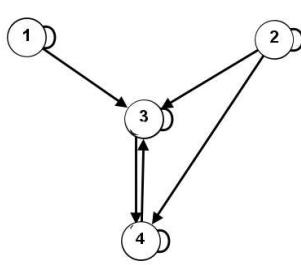


Fig.2.23. Digrafos de  $R_1$ ,  $R_2$  y  $R_3$ .

## 2.19 Relaciones de Equivalencia

Este tipo de relaciones binarias juegan un papel importante en todas las ciencias porque permiten clasificar los elementos del conjunto en el que están definidas.

Muchas veces se tratará a los elementos de un conjunto más por sus propiedades que como objetos individuales. En tales situaciones, se podrá ignorar todas las propiedades que no sean de interés y tratar elementos diferentes como “equivalentes” o indistinguibles, a menos que puedan diferenciarse utilizando únicamente las propiedades que interesen.

La noción de “equivalencia” tiene tres características o propiedades importantes que son la base para una clase importante de relaciones binarias sobre un conjunto.

### Definición

Sea  $R$  una relación definida en  $A$ . Se dice que  $R$  es una Relación de Equivalencia si y solo si se cumplen las siguientes propiedades:

- Propiedad *Reflexiva*:  $\forall x \in A, (x, x) \in R$
- Propiedad *Simétrica*:  $\forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$
- Propiedad *Transitiva*:  $\forall x, y, z \in A, (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

### Ejemplo 2.31

Sea  $A = \{1, 2, 3, 4\}$  y  $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 3), (3, 3), (4, 4)\}$ .

Para investigar si  $R$  es de equivalencia, se analiza:

#### i) Reflexividad

En efecto,  $(1, 1) \in R$ ,  $(2, 2) \in R$ ,  $(3, 3) \in R$  y  $(4, 4) \in R$ ; luego,

$\forall x (x \in A \Rightarrow x R x)$ , es decir,  $R$  es reflexiva.

#### ii) Simetría.

En efecto,  $(1, 2) \in R$  y  $(2, 1) \in R$

$(3, 4) \in R$  y  $(4, 3) \in R$

Luego se cumple que  $\forall x, y \in A [(x, y) \in R \Rightarrow (y, x) \in R]$ ,  $R$  es simétrica.

### iii) Transitividad

Se deben tomar todas las ternas posibles. En efecto,

$$(1, 1) \in R \text{ y } (1, 2) \in R \Rightarrow (1, 2) \in R$$

$$(1, 2) \in R \text{ y } (2, 1) \in R \Rightarrow (1, 1) \in R$$

$$(1, 2) \in R \text{ y } (2, 2) \in R \Rightarrow (1, 2) \in R$$

$$(2, 1) \in R \text{ y } (1, 1) \in R \Rightarrow (2, 1) \in R$$

$$(2, 1) \in R \text{ y } (1, 2) \in R \Rightarrow (2, 2) \in R$$

$$(2, 2) \in R \text{ y } (2, 1) \in R \Rightarrow (2, 1) \in R$$

$$(3, 4) \in R \text{ y } (4, 4) \in R \Rightarrow (3, 4) \in R$$

$$(3, 3) \in R \text{ y } (3, 4) \in R \Rightarrow (3, 4) \in R$$

$$(4, 3) \in R \text{ y } (3, 3) \in R \Rightarrow (4, 3) \in R$$

$$(4, 4) \in R \text{ y } (4, 3) \in R \Rightarrow (4, 3) \in R \quad \text{luego,}$$

$\forall x, y, z \in A \ [ (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R]$  y la relación es, por tanto, transitiva.

#### Observaciones

- Para la simetría no se toman pares ordenados donde  $x = y$  pues en esos casos esta propiedad siempre se cumple, esto es  $(x, x) \in R \rightarrow (x, x) \in R$
- Si  $R$  tuviera más elementos para comparar la transitividad, sería muy tedioso el análisis, y es probable que no se consideraran todas las ternas posibles. En estos casos es conveniente trabajar comparar las matrices  $M_R$  y  $M_{R^2}$  pues:  $R$  es una relación transitiva  $\Leftrightarrow M_R \geq M_{R^2}$ .

Continuando con el Ejemplo 2.31 se tiene que:

$$M_R = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \text{ entonces:}$$

$$M_{R^2} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = M_R,$$

Éste es un caso particular, pues no siempre se da la igualdad.

Luego se verifica que  $M_R \geq M_{R^2}$ , por lo tanto R es transitiva.

### Actividad 2.17

Demostrar que la relación R, definida en el conjunto {1, 2, 3, 4, 5}, y dada por el digrafo de la Figura 2.24 es de equivalencia

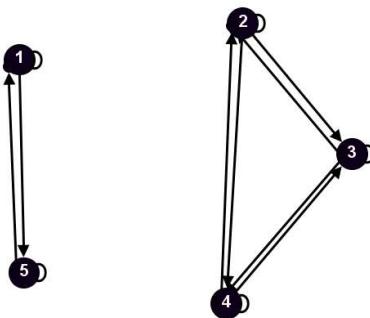


Fig.2.24. Digrafo de R.

### □ Ejemplos 2.32

- a) La relación universal sobre cualquier conjunto A es una relación de equivalencia.
- b) La relación vacía  $\emptyset$  es una relación de equivalencia sobre el conjunto vacío  $\emptyset$
- c) La relación de igualdad sobre cualquier conjunto es una relación de equivalencia.

### 2.19.1 Dígrafo asociado a una Relación de Equivalencia

El dígrafo asociado a una relación de equivalencia  $R$ , tiene algunas características que lo distinguen.

- Como  $R$  es reflexiva, cada vértice tiene un lazo o bucle.
- La simetría implica que si existe un arco desde  $a$  hasta  $b$ , también existe un arco desde  $b$  hasta  $a$ .
- La transitividad implica que si existe un camino de longitud dos desde  $a$  hasta  $b$ , entonces existe un arco desde  $a$  hasta  $b$ .

Consecuentemente, cada una de las componentes del dígrafo de una relación de equivalencia es tal que cada vértice está relacionado con el resto (dígrafo completo).

### 2.19.2 Clase de equivalencia de un elemento

#### Definición

Sea  $R$  una relación de equivalencia definida en  $A$ . Para cada elemento  $a \in A$ , se denomina clase de equivalencia del elemento  $a$ , al conjunto formado por todos los elementos de  $A$  que estén relacionados con él, o sea al conjunto relativo de  $a$  definido por la relación  $R$ . Simbólicamente se denota con  $[a]$ .

Entonces  $[a] = R(a) = \{x \in A / (a, x) \in R\}$

#### Ejemplo 2.33

Sea  $A = \{a, b, c, d\}$  y  $R$  definida en  $A$  mediante el conjunto

$$R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (c, d), (d, c), (d, d)\}$$

En la Figura 2.25 se observa su dígrafo, por lo tanto las clases de equivalencia de cada elemento son:

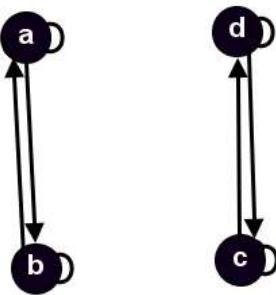


Fig.2.25. Digrafo  $G=(A, R)$ .

$$[a] = \{x \in A : x R a\} = \{a, b\}; \quad [b] = \{x \in A : x R b\} = \{a, b\}$$

$$[c] = \{x \in A : x R c\} = \{c, d\}; \quad [d] = \{x \in A : x R d\} = \{c, d\}$$

Nótese que existen solo dos clases de equivalencias distintas

### Teorema

Sea  $R$  una relación de equivalencia en  $A$ , y sean  $a, b \in A$ . Entonces

$$(a, b) \in R \Leftrightarrow [a] = [b]$$

Es decir, si hay una relación de equivalencia en  $A$  entonces dos elementos estarán relacionados si y solo si sus clases de equivalencia son iguales.

### 2.19.3 Conjunto Cociente de una Relación de Equivalencia

#### Definición

El Conjunto Cociente es el conjunto formado por todas las clases de equivalencia distintas generadas por una Relación de Equivalencia  $R$  en un conjunto  $A$ .

Se denota  $A/R$  indicando así que es el conjunto  $A$  partido (o particionado) por la relación de equivalencia  $R$ .

#### Ejemplo 2.34

En el Ejemplo 2.33, las clases de equivalencias de la relación  $R$  definida en

$A = \{a, b, c, d\}$ , son:

$$[a] = [b] = \{a, b\}$$

$$[c] = [d] = \{c, d\}$$

Luego, el conjunto cociente  $A/R$  estará definido por:

$$A/R = \{[a]; [c]\} = \{\{a, b\}; \{c, d\}\}$$

### □ Ejemplo 2.35

En el conjunto  $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  se considera la relación

$$a R b \Leftrightarrow (a - b) \text{ es múltiplo de } 3$$

Se puede probar que es de equivalencia y por lo tanto encontrar las clases de equivalencia y el conjunto cociente. Pues:

Se tiene que  $(a - b)$  es múltiplo de 3  $\Leftrightarrow a - b = 3k; k \in \mathbb{Z}$ ; luego la relación puede escribirse en la forma

$$a R b \Leftrightarrow a - b = 3k; k \in \mathbb{Z}$$

El análisis es el siguiente:

i) ¿Es  $R$  Reflexiva? Para cada elemento ' $a$ ' de  $A$  se verifica que

$$a - a = 0$$

lo cual puede escribirse en la forma

$$a - a = 3 \rightarrow 3 \cdot 0; 0 \in \mathbb{Z}; \text{ luego } (a, a) \in R, \text{ es decir: } a R a.$$

ii) ¿Es  $R$  Simétrica? Si  $a$  y  $b$  son dos elementos cualesquiera de  $A$  tales que:  $a R b$ , entonces

$$a - b = 3k; k \in \mathbb{Z}$$

de aquí que:  $b - a = 3(-k); (-k) \in \mathbb{Z}$ ; y por tanto,  $b R a$ .

iii) ¿Es  $R$  Transitiva? Se debe probar que:

Si  $a R b$  y  $b R c$ , entonces  $a R c$ ,  $\forall a, b, c \in A$

$$a - b = 3k_1; k_1 \in \mathbb{Z} \quad y \quad b - c = 3k_2; k_2 \in \mathbb{Z}$$

sumando miembro a miembro ambas ecuaciones, se tiene que

$$a - c = 3(k_1 + k_2); \quad k_1 + k_2 \in \mathbb{Z} \Rightarrow a R c.$$

Queda demostrado que  $R$  es de equivalencia.

Para determinar las clases de equivalencia, se considera un ' $a$ ' cualquiera de  $A$ , entonces:

$$\begin{aligned} x \in [a] &\Leftrightarrow x R a \\ &\Leftrightarrow x - a = 3k; \quad k \in \mathbb{Z} \\ &\Leftrightarrow x = a + 3k; \quad k \in \mathbb{Z}; \quad \text{luego} \\ [a] &= \{x : x = a + 3k; \quad k \in \mathbb{Z}\}. \end{aligned}$$

Así pues,

$$[0] = \{x : x = 3k; \quad k \in \mathbb{Z}\} = \{0, 3, 6, 9\}$$

$$[1] = \{x : x = 1 + 3k; \quad k \in \mathbb{Z}\} = \{1, 4, 7\}$$

$$[2] = \{x : x = 2 + 3k; \quad k \in \mathbb{Z}\} = \{2, 5, 8\}$$

El conjunto cociente será, por tanto,

$$A/R = \{\{0, 3, 6, 9\}, \{1, 4, 7\}, \{2, 5, 8\}\}$$

### ☞ Teorema: Conjunto Cociente de una Relación de Equivalencia

Sea  $R$  una relación de equivalencia definida en  $A$ . Entonces  $R$  determina una partición en  $A$ , la cual es el conjunto cociente  $A/R$  y recíprocamente toda partición sobre  $A$  determina una relación de equivalencia  $R$  en  $A$ .

### □ Ejemplo 2.36

Sea  $A = \{1, 3, 3, 4\}$ , y  $\{\{1, 2, 3\}, \{4\}\}$  una partición de  $A$ .

Teniendo en cuenta que las clases de equivalencia son los subconjuntos de la partición, se tiene:

$$[1] = \{1, 2, 3\} \quad \text{y} \quad [4] = \{4\}$$

A partir de la definición de clases de equivalencia y de que R ha de ser de equivalencia, se tiene:

[1] = {1,2,3}, luego  $(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2)$  y  $(3,3) \in R$

[4] = {4}, luego  $(4,4) \in R$ , de aquí que:

$R = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}$  es la relación de equivalencia correspondiente en A.

### □ Ejemplos 2.37

a) Para averiguar si la relación R cuya matriz  $M_R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$  se da es una relación de equivalencia sobre el conjunto  $A = \{a, b, c\}$ , se analizan las siguientes condiciones:

i) ¿Es R Reflexiva?

En efecto lo es, ya que  $m_{ii} = 1 \forall i$ , o sea todos los elementos de la diagonal principal son unos, lo cual significa que

$$\forall x (x \in A \rightarrow x R x)$$

ii) ¿Es R Simétrica?

También lo es, ya que  $m_{ij} = m_{ji} \forall i, j$ , lo cual significa que

$$\forall x, y \in A (x R y \rightarrow y R x)$$

iii) ¿Es R Transitiva? Dado que  $M_R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

Se sigue que

$$M_{R^2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = M_R \therefore M_R \geq M_{R^2}, \text{ luego } R \text{ es}$$

transitiva, lo cual significa que:  $\forall x, y, z \in A (x R y \wedge y R z \Rightarrow x R z)$

Luego R es de equivalencia.

b) Si la matriz de una relación  $M_R = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$  está definida sobre el

conjunto  $A = \{a, b, c, d\}$ , la relación que la define no es de equivalencia ya que  $m_{13} = 1$  y  $m_{31} = 0$ , lo cual significa que la relación propuesta no es simétrica, por lo tanto  $R$  no es de equivalencia.

### Actividad 2.18

Encontrar  $A/R$  donde  $R$  está definida en  $A = \{1, 2, 3, 4, 5\}$  de la Actividad 2.17.

Realizar un diagrama de Venn de la partición generada.

## 2.20 Relaciones de Orden

Pueden definirse dos tipos de relaciones de orden parcial: orden amplio y orden estricto.

Cualesquiera sean los casos, una relación de orden permite ordenar los elementos de un conjunto, permite compararlos; a diferencia de una relación de equivalencia que permite marcar características similares entre elementos de un conjunto.

La palabra parcial que acompaña a orden se refiere a que puede haber elementos no comparables, concepto que se describirá luego de las siguientes definiciones.

### Definición

Sea  $R$  una relación binaria definida en  $A$ . Se dice que  $R$  es una relación de orden amplio, si y solo si se cumplen las siguientes propiedades:

$R$  es *Reflexiva*:  $\forall x \in A, (x, x) \in R$

$R$  es *Antisimétrica*:  $\forall x, y \in A, (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$

$R$  es *Transitiva*:  $\forall x, y, z \in A, (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

## Definición

Sea  $R$  una relación binaria definida en  $A$ . Se dice que  $R$  es una relación de orden estricto si y solo si se cumplen las siguientes propiedades:

$R$  es Arreflexiva:  $\forall x \in A, (x, x) \notin R$

$R$  es Asimétrica:  $\forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \notin R$

$R$  es Transitiva:  $\forall x, y, z \in A, (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

## Ejemplos 2.38

i) Ejemplos de orden parcial amplio, por incluir la Igualdad, se tiene como ejemplos: el *orden alfabético* puesto que una palabra puede ser igual a otra, el *orden de contenencia o inclusión* ( $\subseteq$ ) de conjuntos donde un conjunto está contenido en sí mismo, el *orden de divisibilidad* definido en los números naturales, donde cada número es divisible por sí mismo.

Además la relación idéntica es una relación de orden parcial; y la relación vacía en un conjunto vacío es un orden parcial.

ii) Ejemplos de orden estricto se tiene: el *orden cronológico lineal* presente en las competencias deportivas, en la sucesión de eventos históricos de una familia, una sociedad o un país, donde no hay manera de establecer la simultaneidad real de dos eventos; en el *orden definido por las magnitudes*, presente en las ordenaciones por estatura (creciente o decreciente) de algunas personas, en general ordenaciones por longitud, área, volumen, o cualquier otra magnitud; el *orden definido por la distancia* entre dos o más puntos de algún espacio, como por ejemplo se ordenan los planetas por su distancia media al sol; que como en el caso anterior, no hay exactitud experimental que permita establecer la igualdad de dos magnitudes o de dos distancias; el *orden definido en los conjuntos numéricos* como números reales, racionales y enteros a partir de un conjunto de números positivos.

Además en un conjunto con dos elementos  $A = \{0, 1\}$ , las siguientes relaciones

son órdenes estrictos.

$$R_0 = \emptyset$$

$$R_1 = \{(0, 1)\}$$

$$R_2 = \{(1, 0)\}$$

### 2.20.1 Conjuntos parcialmente ordenados

#### Definición

Se denomina Conjunto Parcialmente Ordenado (CPO) a todo par  $(A, R)$  formado por un conjunto  $A \neq \emptyset$  y una relación  $R$  de orden parcial definida en  $A$ .

#### Ejemplos 2.39

- i) El par  $(A, R)$ , donde  $A = \{a, b, c\}$  y  $R = \{(a, a), (b, b), (c, c), (a, c), (b, c)\}$  es un CPO.

Habitualmente se designan a las relaciones de orden con el símbolo  $\leq$ .

Sea  $(A, \leq)$  un CPO. En lugar de  $(x, y) \in R$  se escribe  $(x, y) \in \leq$ , o sea  $x \leq y$ .

Si  $x \leq y$  se dice que, “ $x$  precede a  $y$ ” o que “ $x$  es menor o igual que  $y$ ”.

Si  $(A, \leq)$  un CPO, se representa con “ $\geq$ ” a la relación opuesta de “ $\leq$ ”, y es tal que  $(A, \geq)$  es el CPO dual de  $(A, \leq)$ .

Es claro que “ $x \geq y$ ” si y sólo si “ $y \leq x$ ”.

Si  $x \geq y$ , se dice que “ $x$  sucede a  $y$ ” o que “ $x$  es mayor o igual que  $y$ ”.

- ii) Sea el CPO  $(A, \leq)$ , donde  $A = \{1, 2, 3, 4\}$ , y  $\leq$  tal que:

$$\leq = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}.$$

Entonces se tiene que:

$$1 \leq 1, 1 \leq 2, 1 \leq 3, 1 \leq 4,$$

$$2 \leq 2, 2 \leq 3, 2 \leq 4, 3 \leq 3, 3 \leq 4 \text{ y } 4 \leq 4.$$

### Actividad 2.19

Sea la relación definida en  $A = \{a, b, c, d\}$  por el digrafo que se muestra, demostrar que  $A$  es un CPO.

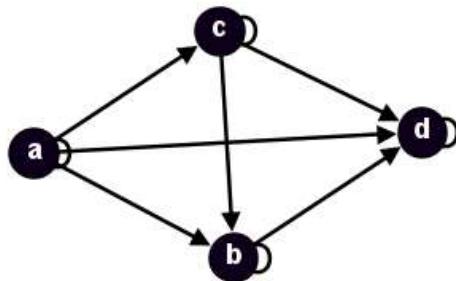


Fig.2.26. Digrafo  $G=(A, \leq)$ .

### 2.20.2 Elementos comparables en un conjunto ordenado

#### Definición

Sea  $(A, \leq)$  un conjunto ordenado. Los elementos  $x$  e  $y$  se dicen comparables si y solo si  $x \leq y$  o  $y \leq x$

De este concepto se desprende la razón para llamarse orden parcial, ya que puede haber elementos que no sean comparables.

Si todos los elementos son comparables el orden se llama *lineal* o *total* y en ese caso se dice que el conjunto  $A$  es una *cadena*.

### Actividad 2.20

Determinar si existen elementos no comparables en la relación de orden dada en la Actividad 2.19

### 2.20.3 Diagrama de Hasse

#### Definición

Se denomina Diagrama de Hasse a una gráfica que se realiza simplificando el digrafo de las relaciones de orden finito mediante el siguiente procedimiento:

Paso 1. Se eliminan los lazos o bucles, si el orden es amplio .

Paso 2. Se eliminan las aristas que son consecuencias de la transitividad.

Paso 3. Se orientan las aristas que quedan, luego de la simplificación, hacia arriba e incluso se puede eliminar las orientaciones de las flechas.

### □ Ejemplos 2.40

i) Sea  $(A, \leq_1)$  un CPO y tal que  $A = \{a, b, c, d\}$  con la relación de orden  $\leq_1$  dada por:

$$a \leq_1 a, a \leq_1 b, a \leq_1 c, a \leq_1 d, b \leq_1 b, b \leq_1 c, b \leq_1 d, c \leq_1 c, c \leq_1 d, d \leq_1 d.$$

Entonces su diagrama de Hasse es



Fig.2.27. Diagrama de Hasse de  $(A, \leq_1)$ .

ii) Sea  $(A, \leq_2)$  un CPO, tal que  $A = \{a, b, c, d, e\}$  y la relación  $\leq_2$  dada por:

$$\leq_2 = \{(a,a), (a,b), (b,b), (c,d), (d,d), (a,c), (c,c), (a,d), (a,e), (b,d), (d,e), (b,e), (e,e), (c,e)\}.$$

Para confeccionar el diagrama de Hasse es conveniente enlistar los pares que satisfacen el orden estricto ( $<_2$ ) y a partir de él detectar cuáles son los sucesores inmediatos de cada elemento.

Ellos son:

- |                                  |                                 |
|----------------------------------|---------------------------------|
| $(a, b), (a, c), (a, d), (a, e)$ | se lee b, c, d y e siguen a 'a' |
| $(b, d), (b, e)$                 | se lee d y e siguen a 'b'       |
| $(c, d), (c, e)$                 | se lee d y e siguen a 'c'       |
| $(d, e)$                         | se lee e sigue a 'd'            |

Entonces su diagrama de Hasse es:

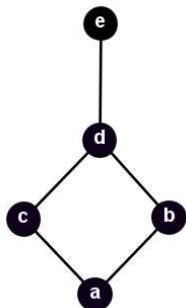


Fig.2.28. Diagrama de Hasse de  $(A, \leq_2)$ .

- iii) En el conjunto ordenado,  $A = \{a, b, c\}$ , donde se define la relación de orden dada por su matriz:

$$M_R = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Nótese que la relación de orden es estricta, Luego el diagrama de Hasse es:



Fig.2.29. Diagrama de Hasse de  $(A, R)$ .

### Actividad 2.21

Encontrar el diagrama de Hasse de la Actividad 2.20.

#### 2.20.4 Elementos extremos de una Relación de Orden

##### Definición

Sea  $(A, \leq)$  un conjunto ordenado. Sean  $a$  y  $b$  elementos de  $A$ .

Se dice que  $a$  es el elemento *máximo* si y solo si  $x \leq a, \forall x \in A$

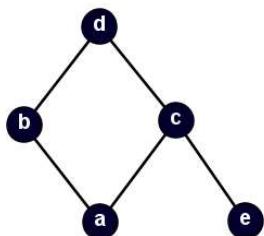
Se dice que  $b$  es el elemento *mínimo* si y solo si  $b \leq x, \forall x \in A$

## □ Ejemplos 2.41

a) En los diagramas de Hasse del Ejemplo 2.40

- i) (Figura 2.27) ‘a’ es el máximo y ‘d’ el elemento mínimo
- ii) (Figura 2.28) ‘e’ es el elemento máximo y ‘a’ es el mínimo.

b) El Diagrama de Hasse del dígrafo correspondiente a la Actividad 2.21 está representado en la Figura 2.30.



‘d’ es el máximo, pero no existe elemento *mínimo*, pues ‘a’ no puede ser elemento mínimo porque ‘e’ no es mayor o igual que ‘a’; ni ‘e’ puede ser el mínimo porque ‘a’ no sucede a ‘e’.

Fig.2.30. Diagrama de Hasse  
de Actividad 2.21.

### Actividad 2.22

Dadas las siguientes relaciones  $\leq_1$  y  $\leq_2$  definidas en  $A = \{1, 2, 3, 4, 5\}$  por medio de los Dígrafos de las Figuras 2.31 y 2.32, se pide:

- a) Demostrar que  $(A, \leq_1)$  y  $(A, \leq_2)$  son CPO.
- b) Dibujar sus correspondientes diagramas de Hasse.
- c) Encontrar sus elementos extremos, si es que existen.

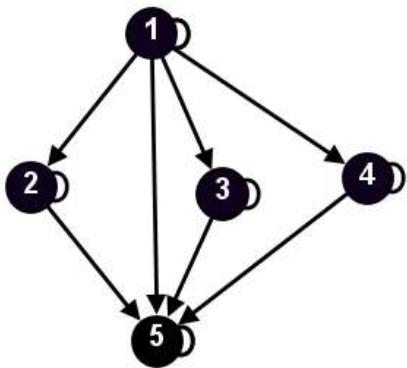


Fig. 2.31. Digrafo de  $(A, \leq_1)$ .

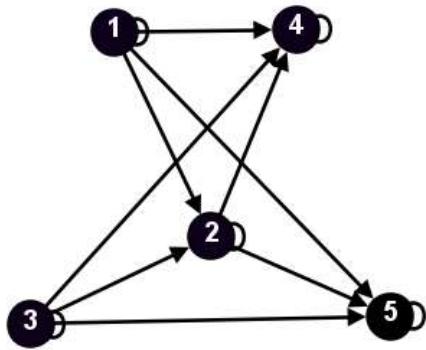


Fig. 2.32. Digrafo de  $(A, \leq_2)$ .

MATERIAL EN TRAMITE DE ISB.V

## Capítulo 3. TEORIA DE NUMEROS ENTEROS

**El conjunto de los Números Enteros.**

**División en  $\mathbb{Z}$ .**

**Números Primos y Compuestos.**

**Teorema Fundamental de la Aritmética**

**Máximo Común Divisor.**

**Números Coprimos.**

**Mínimo Común Múltiplo.**

**Ecuaciones diofánticas.**

**Congruencia en  $\mathbb{Z}$ .**



## Introducción

La parte de la Matemática Discreta que trata de los números enteros y sus propiedades recibe el nombre de Teoría de Números. Esta teoría ocupa una posición central entre la Aritmética, el Álgebra y la Geometría, y su primer edificador como ciencia fue C.F. Gauss (1777-1855), considerado “el principio de las matemáticas”.

En el conjunto de los números naturales la ecuación:  $a + x = b$ , tiene solución en  $\mathbb{N}$ , cuando  $b > a$ , pues la solución está dada por  $x = b - a$ . Es decir,  $x$  pertenece a  $\mathbb{N}$  cuando el minuendo es mayor que el sustraendo, caso contrario la solución no es un número natural. Para salvar este inconveniente y que la diferencia entre dos elementos de un conjunto sea resultado otro elemento del mismo conjunto (ley de cierre) se debe ampliar el campo numérico  $\mathbb{N}$  y se crea un nuevo conjunto, el de los números enteros, que se lo simboliza con  $\mathbb{Z}$  y que contiene a los  $\mathbb{N}$ . Por ello se dice que  $\mathbb{Z}$  es una extensión de  $\mathbb{N}$ ,  $\mathbb{N} \subset \mathbb{Z}$ .

En computación el conjunto de los Números Enteros tiene un amplio espectro de aplicaciones: criptografía, comercio electrónico, transmisión y almacenamiento de datos, etc. pues por seguridad informática se necesita enviar mensajes que no puedan ser comprendidos por otros que no sea el destinatario y para ello se necesita manejar la aritmética modular que se define con elementos de  $\mathbb{Z}$ , la teoría de los enteros no negativos y en particular la de los números primos y coprimos.

### 3.1 El conjunto de los Números Enteros

#### Definición

El conjunto de los Números Enteros ( $\mathbb{Z}$ ) se define como la unión de los Números Naturales ( $\mathbb{N}$ ), el cero (0) y los opuestos de los naturales.

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-x / x \in \mathbb{N}\}$$

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Con  $\mathbb{Z}^+$  se representa al conjunto de los enteros positivos, que son los números

naturales; esto es:  $\mathbb{Z}^+ = \{1, 2, 3, \dots\} = \mathbb{N}$

### ⦿ Observación

El número entero 0 no tiene signo, no es ni positivo ni negativo.

El conjunto de los números enteros,  $\mathbb{Z}$ , goza de una serie de propiedades que se pueden dividir en dos tipos:

- *Aritméticas*: tienen en cuenta las propiedades de las operaciones adición (+) y multiplicación (.)
- *De orden*: se deducen de la relación ' $\leq$ ' usual .

#### 3.1.1 Propiedades de las operaciones adición y multiplicación en $\mathbb{Z}$

En  $\mathbb{Z}$  se definen las operaciones de adición: '+' y multiplicación: '·' ya conocidas en la escuela primaria, las cuales  $\forall x, y, z \in \mathbb{Z}$  cumplen las siguientes propiedades

1. Leyes de composición internas

$$x + y \in \mathbb{Z} \quad x \cdot y \in \mathbb{Z}$$

También se dice que la adición y multiplicación son operaciones cerradas en  $\mathbb{Z}$

2. Leyes asociativas:

$$(x + y) + z = x + (y + z) \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

3. Leyes commutativas:

$$x + y = y + x \quad x \cdot y = y \cdot x$$

4. Leyes de existencia del neutro '0' y de la unidad '1':

$$\exists 0 \in \mathbb{Z} / x + 0 = 0 + x = x; \quad \exists 1 \in \mathbb{Z} / x \cdot 1 = 1 \cdot x = x$$

5. Ley de existencia del opuesto:

$$\exists (-x) \in \mathbb{Z} / x + (-x) = (-x) + x = 0$$

6. Ley Distributiva de la multiplicación respecto de la adición:

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad (y + z) \cdot x = y \cdot x + z \cdot x$$

7. Propiedad cancelativa:

$$\text{Si } x \neq 0 \wedge x \cdot y = x \cdot z, \text{ entonces } y = z$$

### ⦿ Observación

La mayoría de las leyes dadas anteriormente cumplen con la propiedad de dualidad.

## La relación de orden en $\mathbb{Z}$

### Definición

$$x \leq y \text{ si y solo si } \exists k \in \mathbb{N} / y = x + k$$

La relación ' $\leq$ ' es una relación de orden en el conjunto  $\mathbb{Z}$  de los números enteros, la cual cumple además con las siguientes propiedades:

1. Propiedad Reflexiva:  $\forall x \in \mathbb{Z}, x \leq x$
2. Propiedad antisimétrica:  $x \leq y \wedge y \leq x \Rightarrow x = y, \forall x, y \in \mathbb{Z}$
3. Propiedad transitiva:  $x \leq y \wedge y \leq z \Rightarrow x \leq z, \forall x, y, z \in \mathbb{Z}$

Además:

4. Si  $x, y \in \mathbb{Z}, x \leq y \wedge z \in \mathbb{Z}$ , entonces  $x + z \leq y + z$
5. Si  $x, y \in \mathbb{Z}, x \leq y \wedge 0 \leq z$ , entonces  $x.z \leq y.z$
6. Si  $x, y \in \mathbb{Z}, x \leq y \wedge z \leq 0$ , entonces  $x.z \geq y.z$

Todas estas propiedades no sólo se verifican en  $\mathbb{Z}$ , también se cumplen para los números racionales  $\mathbb{Q}$  y reales  $\mathbb{R}$ . Pero:

*¿Qué es, entonces, lo que diferencia a los números enteros del resto de números?*

La diferencia radica en una propiedad que se conoce como *Principio o Axioma del buen orden*.

Antes de enunciarlo, se verá algunas definiciones.

## Definiciones

Sea  $X \subset \mathbb{Z}$  un subconjunto de números enteros. Se dice que  $c \in \mathbb{Z}$  es una cota inferior del conjunto  $X$ , si  $c \leq x, \forall x \in X$ . Luego  $X$  es un conjunto acotado inferiormente.

Si además,  $c \in X$  recibe el nombre de primer elemento (o mínimo).

Análogamente, se dice que  $d \in \mathbb{Z}$  es una cota superior del conjunto  $X$  si  $x \leq d, \forall x \in X$ . Luego  $X$  es un conjunto acotado superiormente.

Si además,  $d \in X$  recibe el nombre de último elemento (o máximo).

## Ejemplos 3.1

a) El conjunto  $\{-17, -15, -5, 5, 15, 19, 100\}$  tiene cotas inferiores y superiores. Por ejemplo  $(-20), (-22), (-30)$  son cotas inferiores, pero  $(-17)$  es la mayor de las cotas inferiores y de hecho pertenece al conjunto. Luego  $(-17)$  es el elemento mínimo del conjunto dado.

Cotas superiores del conjunto dado podrían ser:  $100, 101, 102, \dots, 170, \dots$ , pero  $100$  es la mínima cota superior y pertenece al conjunto, luego el elemento máximo de este conjunto es  $100$ .

b) Algunos conjuntos no tienen cotas inferiores, por ejemplo el conjunto de los enteros negativos ( $\mathbb{Z}^-$ ), o no tienen cotas superiores como sería el caso de  $\mathbb{Z}^+$ .

c) El conjunto de números racionales  $\{1/n; n \in \mathbb{N}\} \subseteq \mathbb{Q}$  tiene cotas inferiores pero no tiene mínimo.

En efecto, basta con darse cuenta que  $0$  es la mejor cota inferior, pero no está en el conjunto. Es decir, este conjunto no tiene primer elemento o mínimo.

Esto proporciona una justificación de la idea intuitiva de los números enteros como un conjunto de puntos regularmente espaciados en una recta que se

extiende infinitamente en ambas direcciones. En particular, dice que no se puede acercar a un entero más y más sin llegar a él. El hecho de que haya huecos entre los enteros lleva a decir que  $\mathbb{Z}$  es un conjunto discreto y es esta propiedad la que da el nombre a la *Matemática Discreta*.

### Principio del buen Orden

“Todo subconjunto no vacío de  $\mathbb{Z}$  acotado inferiormente (superiormente) posee un primer (último) elemento”

Lo relevante del principio del buen orden no es sólo el hecho de que distingue el conjunto  $\mathbb{Z}$  de otros conjuntos de números, sino que resulta de gran utilidad desde el punto de vista matemático. Este principio fundamenta distintas técnicas básicas, como la demostración por inducción que se verá más adelante.

## 3.2 División en $\mathbb{Z}$

Si  $a$  y  $b$  son números enteros positivos, con  $a > b > 0$ , entonces existen dos enteros,  $q$  y  $r$ , únicos, tales que  $a = bq + r$ , con  $0 \leq r < b$ .

A los números  $a$ ,  $b$ ,  $q$  y  $r$  se les suele llamar, respectivamente, dividendo, divisor, cociente y resto.

¿Pero qué pasa con esta operación cuando  $a$  y  $b$  son  $\mathbb{Z}$ ?

### Definición

Si  $a, b \in \mathbb{Z}$  y  $b \neq 0$ , existen  $q, r \in \mathbb{Z}$ , únicos, tales que:

$$a = b \cdot q + r \text{ con } 0 \leq r < |b|.$$

Donde  $a$  es el dividendo,  $b$  es el divisor,  $q$  el cociente y  $r$  es el resto.

### Observación

Si  $a, b \in \mathbb{Z}^+$ , el algoritmo de la división corresponde a la división usual.

### Ejemplos 3.2

1. Sean  $a = 25$  y  $b = 3$ .

El mayor múltiplo de 3 menor o igual que 25 es  $3 \cdot 8$ , luego tomando  $q = 8$  y  $r = 25 - 3 \cdot 8 = 1$ , se tiene que  $25 = 3 \cdot 8 + 1$ , con  $0 \leq 1 < 3$ .

2. Sean  $a = 3$  y  $b = 25$ .

El mayor múltiplo de 25 menor o igual que 3 es  $25 \cdot 0$ , luego si  $q = 0$  y  $r = 3 - 25 \cdot 0 = 3$ , se sigue que  $3 = 25 \cdot 0 + 3$ , con  $0 \leq 3 < 25$

3. Sean  $a = -25$  y  $b = 3$ .

El mayor múltiplo de 3 menor o igual que (-25) es  $3 \cdot (-9)$ , luego se tiene:

$q = -9$  y  $r = -25 - 3(-9) = 2$ , luego se sigue que:  $-25 = 3(-9) + 2$ , con  $0 \leq 2 < 3$ .

4. Sean  $a = 61$  y  $b = -7$ .

El mayor múltiplo de (-7) menor o igual que 61 es  $(-7)(-8)$ , así pues si  $q = -8$  y  $r = 61 - (-7)(-8) = 61 - 56 = 5$ , se tiene que  $61 = (-7)(-8) + 5$ , con  $0 \leq 5 < |-7| = 7$ .

5. Sean  $a = 7$  y  $b = -61$ .

El mayor múltiplo de (-61) menor o igual que 7 es  $(-61) \cdot 0$ , por tanto si  $q = 0$  y  $r = 7 - (-61) \cdot 0 = 7$ , resulta

$7 = (-61) \cdot 0 + 7$ , con  $0 \leq 7 < |-61| = 61$ .

6. Sean  $a = -21$  y  $b = -15$ .

El mayor múltiplo de (-15) menor o igual que (-21) es  $(-15)(-2)$ . Si  $q = -2$  y  $r = -21 - (-15)(-2) = 9$ , resulta  $-21 = (-15)(-2) + 9$ , con  $0 \leq 9 < |-15| = 15$ .

### 3.2.1 Operadores binarios *div* y *mod*

*div* y *mod* son dos operadores matemáticos, que se usan en Programación, que permiten tomar el residuo o resto, y el divisor de una operación. Son parte de la división de dos números enteros.

#### El operador *div*

##### ☞ Definición

Es la parte entera de la división, es decir el cociente entero de dos enteros.

#### □ Ejemplos 3.3

- a)  $4 \text{ div } 2 = 2$ ;
- b)  $(-4) \text{ div } 2 = -2$ ;
- c)  $79 \text{ div } 8 = 9$ .

#### El operador *mod*

##### ☞ Definición

Es el residuo o resto de la división entre dos enteros.

#### □ Ejemplos 3.4

- 1) a)  $4 \text{ mod } 2 = 0$  y  $(-4) \text{ mod } 2 = 0$   
b)  $79 \text{ mod } 8 = 7$  y  $-79 \text{ mod } 8 = 1$
- 2) Si  $x = 7$ , e  $y = 11$ , al evaluar:  $(x + y)\text{mod } 7 + (3 * x) \text{ div } y$

Se reemplazan los valores:

$$\begin{aligned}(x + y)\text{mod } 7 + (3 * x) \text{ div } y &= (7 + 11)\text{mod } 7 + (3 * 7) \text{ div } 11 = \\ &= 17 \text{ mod } 7 + 21 \text{ div } 11 \\ &= 3 + 1 = 4\end{aligned}$$

## ❖ Aplicación

¿Cuándo se utilizan estos operadores?

Se los usa cuando se quiere saber si un número es *divisible* entre otro, cuantas *partes enteras* tiene una división, para saber si un número es *múltiplo* o *submúltiplo* de otros; para *descomponer* un numero en unidades, decenas, centenas y otros casos más.

### □ Ejemplo 3.5

Para hacer un programa que capture un número de tres cifras y lo descomponga en unidades, decenas y centenas, éste debe indicar cuantas unidades hay, cuantas decenas y cuantas centenas.

Así para el número 785, el programa tiene que devolver 7 centenas, 8 decenas y 5 unidades como resultado. Si se aplican los operadores *div* y *mod*, se puede hacer el siguiente análisis:

- $785 \bmod 10 = 5$ , por lo tanto ya se tiene la cantidad de unidades (que se puede comprobar haciendo la división manual).
- $785 \bmod 10 = 78$ , aquí se puede aplicar  $(785 \bmod 10) \bmod 10$  que es como decir  $78 \bmod 10$ , que resulta ser 8 por lo tanto, se obtiene las decenas.
- $785 \bmod 100 = 7$ , con esta operación se obtiene las centenas.

## 👁 Observaciones

- Con estos nuevos conceptos, se puede decir que:
  - $x$  es cualquier entero par si y solo si  $x \bmod 2 = 0$
  - $x$  es cualquier entero impar si y solo si  $x \bmod 2 = 1$

### Actividad 3.1

i) Decir Verdadero o Falso, y justificar la respuesta:

$$a) (-25) \text{ div } 5 = -5 \text{ y } (-25) \text{ mod } 5 = 0$$

$$b) (-735) \text{ div } (-31) = 24 \text{ y } (-735) \text{ mod } (-31) = 9$$

ii) Si  $a = 3$ ,  $b = 10$ , y  $c = 5$ , evaluar  $(c^a) \text{ mod } 9 + (b + 2^{a-1}) / ((7 * c) \text{ div } a)$

### 3.3 Divisibilidad: Divisores y múltiplos

La divisibilidad en  $\mathbb{Z}$  es la base de la Teoría de Números que es una sólida estructura desarrollada por los matemáticos desde la antigüedad, caracterizada por posibilitar la aplicación de la capacidad creadora. Su fuerza radica en la facilidad de plantear problemas de todo tipo de complejidad.

El conjunto  $\mathbb{Z}$  no es cerrado respecto de la división, esto significa que la división de dos enteros no siempre es otro entero. Pero existen infinitos casos de división exacta. Por ejemplo 3 divide a 6, ya que  $6 \text{ div } 3 = 0$ .

#### Definición

Sean  $a, b \in \mathbb{Z}$  con  $a \neq 0$  se dice que ' $a$  divide  $b$ ' si existe un entero  $n$  tal que  $b = a \cdot n$ . Se denota:  $a|b$ .

Simbólicamente:  $a|b \Leftrightarrow \exists n \in \mathbb{Z} \text{ tal que } b = a \cdot n$

Expresiones equivalentes a ' $a$  divide  $b$ ' son:

$a$  "es un factor de"  $b$

$a$  "es un divisor de"  $b$

$b$  "es múltiplo de"  $a$

$b$  "es divisible por"  $a$

Negando ambos miembros de la equivalencia anterior, en virtud de la equivalencia lógica entre una proposición y su contrarrecíproca, se tiene:

$$a \nmid b \Leftrightarrow b \neq a \cdot n; \forall n \in \mathbb{Z}$$

Es decir,  $a$  no divide a  $b$  (y se simboliza  $a \nmid b$ ) si  $b \neq a \cdot n$  para cualquier entero. Dicho de otra forma,  $b$  no es múltiplo de  $a$ .

Los múltiplos de un número entero son los números enteros que resultan de multiplicar ese número por otros números enteros. Se dice que un número es múltiplo de otro si le contiene un número entero de veces.

### Observación

- Sean  $x, y, z \in \mathbb{Z} - \{0\}$ , del producto ' $x \cdot y = z$ ', se puede tener dos divisiones exactas ' $z \text{ div } x$ ' y ' $z \text{ div } y$ ' que es exactamente lo mismo decir que  $z$  es múltiplo de  $x$  e  $y$ , o que  $x$  e  $y$  son divisores de  $z$ .
- Para obtener múltiplos de cualquier número se debe multiplicar dicho número por un entero cualquiera.
- Todo número entero tiene infinitos múltiplos, excepto el 0, que tiene sólo uno (él mismo).
- Todo entero es múltiplo de sí mismo y de la unidad (el 1).
- Los múltiplos de 2 reciben el nombre de números pares ( $2k; k \in \mathbb{Z}$ ); los restantes son los números impares.

### Ejemplos 3.6

- i.  $3|6$  pues existe  $2 \in \mathbb{Z}$  que verifica  $6 = 3 \cdot 2$ . Por lo cual  $3|6$ .
- ii.  $(-4)|12$  pues existe  $(-3) \in \mathbb{Z}$  que verifica  $12 = (-4) \cdot (-3)$ . Por lo cual  $(-4)$  es un divisor o submúltiplo de  $12$ .
- iii. 5 divide a 35, pues existe  $(-7) \in \mathbb{Z}$  que verifica  $(-35) = 5 \cdot (-7)$ . Por lo tanto se tiene que:  $(-35)$  es múltiplo de 5 o de  $(-7)$ , o que el 5 es un divisor de  $(-35)$ .
- iv. Para demostrar que  $n^2 + 3n$  es divisible por 2, basta ver que  $n^2 + 3n$  se puede factorizar y escribir como:  $n^2 + 3n = n(n + 3)$ .

Si  $n$  es par, entonces el número resultante es divisible por 2. Si  $n$  es impar, entonces  $n + 3$  tiene que ser par y, por lo tanto, de nuevo el número resultante es divisible por 2.

### Observación

- Si  $a \neq 0$  y  $b = 0$  se dice que  $a|0$  porque existe  $n = 0$  tal que  $0 = a \cdot 0$ . De lo que se deduce que todo entero no nulo es divisor de cero y que 0 es múltiplo de todo entero no nulo.

## Algoritmo para determinar si un número divide a otro en lenguaje de Pseint

### Algoritmo Divisibilidad

```

Escribir ("Para determinar si a|b");
Escribir ("Ingresar el valor de a");
Leer a
Escribir ("Ingresar el valor de b");
Leer b
r <- b MOD a
Si r=0 Entonces
    Escribir a " divide a " b ;
SiNo
    Escribir a " no divide a " b ;
Fin Si
FinAlgoritmo

```

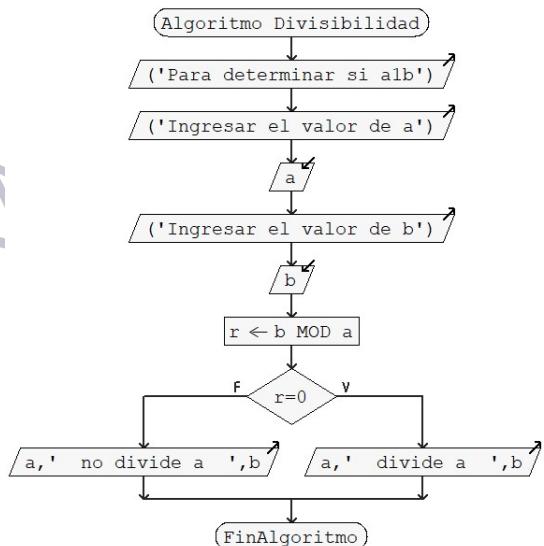


Fig. 3.1. Algoritmo de Divisibilidad

### 3.3.1 Propiedades de la divisibilidad

1. Todo número entero  $a$  no nulo posee los siguientes divisores:  $1, -1, a, -a$ .

### Demostración

Sea  $a \in \mathbb{Z} - \{0\}$ ,

- $1|a$  pues  $\exists a \in \mathbb{Z} / a = 1 \cdot a$
- $(-1)|a$  pues  $\exists (-a) \in \mathbb{Z} / a = (-a)(-1)$

- $a|a$  pues  $\exists 1 \in \mathbb{Z} / a = a \cdot 1$
- $(-a)|a$  pues  $\exists (-1) \in \mathbb{Z} / a = (-a)(-1)$

**2.** La divisibilidad goza de la propiedad *reflexiva*, pues:

$$a|a, \forall a \in \mathbb{Z} - \{0\} \text{ ( } a \text{ entero no nulo)}$$

**3.** La divisibilidad goza de la propiedad de *antisimetría*.

$$\text{Si } a|b \wedge b|a \Rightarrow a = \pm b, \forall a, b \in \mathbb{Z} - \{0\}$$

**Demostración** (método directo)

Sean  $a, b \in \mathbb{Z} - \{0\}$ , por hipótesis:

- $a|b$  entonces  $\exists k_1 \in \mathbb{Z} / b = a \cdot k_1 \quad (1)$
- $b|a$  entonces  $\exists k_2 \in \mathbb{Z} / a = b \cdot k_2 \quad (2)$

Sustituyendo (1) en (2) se tiene  $a = (a \cdot k_1) \cdot k_2 \Rightarrow a = a \cdot (k_1 \cdot k_2)$ , para que esta igualdad se cumpla debe ocurrir que  $(k_1 \cdot k_2) = 1$  y como  $k_1, k_2 \in \mathbb{Z}$  se tiene que las únicas posibilidades son:

$$k_1 = k_2 = 1 \vee k_1 = k_2 = (-1).$$

De allí que, reemplazando en (1) o en (2) se tiene  $a = \pm b$

#### ☞ Observación

En particular si  $a, b \in \mathbb{Z}^+$  se tendrá que  $k_1, k_2 \in \mathbb{Z}^+$  y por lo tanto la única posibilidad será  $k_1 = k_2 = 1$ . De allí que  $a = b$ .

**4.** La divisibilidad goza de la propiedad *transitiva*

$$\text{Si } a, b \in \mathbb{Z} - \{0\}, a|b \wedge b|c \Rightarrow a|c$$

**Demostración** (método directo)

Por hipótesis, se tiene que:

- $a|b$  entonces  $b = a \cdot k_1$ , para algún  $k_1 \in \mathbb{Z} \quad (1)$

-  $b|c$  entonces  $c = b \cdot k_2$ , para algún  $k_2 \in \mathbb{Z}$  (2)

Si se reemplaza (1) en (2), se tiene que:  $c = (a \cdot k_1) \cdot k_2 \Rightarrow c = a \cdot (k_1 \cdot k_2)$

Como  $(k_1 \cdot k_2) \in \mathbb{Z}$ , se tiene que  $k_1 \cdot k_2 = k$ , con  $k \in \mathbb{Z}$  tal que  $c = a \cdot k$ , luego se concluye que  $a|c$ .

**5. Si  $a|b \Rightarrow a|(b \cdot x)$  donde  $a \neq 0$  y  $\forall x \in \mathbb{Z}$**

En palabras, si 'a' divide a 'b' entonces 'a' divide a todos los múltiplos de 'b'

### Demostración

Sean  $a, b, x \in \mathbb{Z}$ . Si  $a|b$  entonces  $b = a \cdot k$  (3), para algún  $k \in \mathbb{Z}$

Multiplicando miembro a miembro (3) por  $x$  se tendrá:  $b \cdot x = (a \cdot k) \cdot x$

Como el producto es asociativo se puede escribir:  $b \cdot x = a \cdot (k \cdot x)$

Al ser  $(k \cdot x) \in \mathbb{Z}$  se concluye que ' $a| (b \cdot x)$ '

**6. Si  $a|b$  y  $a|c \Rightarrow a|(b \cdot x + c \cdot y)$  donde  $a \neq 0$  y  $\forall x, y \in \mathbb{Z}$**

En palabras la propiedad 6, dice que: si  $a$  divide a  $b$  y  $a$  divide a  $c$  entonces  $a$  divide a toda combinación lineal de  $b$  y  $c$ .

### Demostración

Sean  $a, b, c \in \mathbb{Z}$ , con  $a \neq 0$

Por hipótesis  $a|b$ , luego por la propiedad 5,

$$a|(b \cdot x), \forall x \in \mathbb{Z}, \therefore (\text{por lo tanto}) \quad b \cdot x = a \cdot k_1, \text{ para algún } k_1 \in \mathbb{Z} \quad (1)$$

Análogamente,  $a|c$ , luego por la propiedad 5,

$$a|(c \cdot y), \forall y \in \mathbb{Z}, \therefore c \cdot y = a \cdot k_2, \text{ para algún } k_2 \in \mathbb{Z} \quad (2)$$

Se desea determinar un entero  $k$  tal que  $b \cdot x + c \cdot y = a \cdot k$ , para ello sumando (1) y (2), miembro a miembro, se tiene:  $b \cdot x + c \cdot y = a \cdot k_1 + a \cdot k_2 \quad (3)$

Sacando factor común en (3)  $b \cdot x + c \cdot y = a \cdot (k_1 + k_2)$  y como  $k_1 + k_2 = k \in \mathbb{Z}$  se concluye que:  $a|(b \cdot x + c \cdot y), \forall x, y \in \mathbb{Z}$

### □ Ejemplos 3.7

1) Se quiere demostrar que si  $a$  divide a dos enteros ( $b$  y  $c$ ) cualesquiera, entonces divide a su suma y a su diferencia. Para ello, como  $a|b$  y  $a|c \Rightarrow a|p.b + q.c \quad \forall p, q \in \mathbb{Z}$  (x prop.6)

$\Rightarrow a|b + c$  (Tomando  $p = q = 1$ ) y  $a|b - c$  (Tomando  $p = 1$  y  $q = -1$ )

2) Divisores de (-18) son 1, (-1), 18 y (-18); además como

$(-18) = 2 \cdot (-9) = (-2) \cdot 9 = (-2) \cdot 3 \cdot 3 = 3 \cdot (-6) = (-3) \cdot 6$  luego los números 2, (-9), 3 y (-6) son también divisores de (-18).

3) Del ejemplo anterior se observa que  $3|9$  y  $9|(-18)$  luego  $3|(-18)$

### Actividad 3.2

Indicar si las siguientes afirmaciones son Verdaderas o Falsas, justificando su respuesta:

- i)  $(-3)|33 \wedge 33|11$
- ii)  $a|6 \wedge 6|a \rightarrow a = 6, \text{ con } a \in \mathbb{Z} \text{ y } a \neq 0$
- iii)  $a|b \wedge c|b \rightarrow (a \cdot c)|b, \text{ con } a, b, c \in \mathbb{Z} \text{ y } a, c \neq 0$
- iv)  $3|(6x - 9y), \quad \forall x, y \in \mathbb{Z}$
- v)  $8|(16x - 4y), \quad \forall x, y \in \mathbb{Z}$
- vi)  $\exists x, y \in \mathbb{Z} \text{ tales que } 2x + 5y = 1$
- vii)  $\exists x, y, z \in \mathbb{Z} \text{ tales que } 12x + 8y + 20z = 105$

### 3.4 Números Primos y Compuestos

#### ▢ Definición

Un entero positivo  $p > 1$  es un número primo si y solo si sus únicos divisores son  $\pm 1$  y  $\pm p$

Todos los demás enteros positivos mayores que 1 que no son primos se llaman compuestos

Los primeros veinte números primos son:

|    |    |    |    |    |
|----|----|----|----|----|
| 2  | 3  | 5  | 7  | 11 |
| 13 | 17 | 19 | 23 | 29 |
| 31 | 37 | 41 | 43 | 47 |
| 53 | 59 | 61 | 67 | 71 |

Fig. 3.2. Primeros Números Primos.

### Observaciones

- El número 1 no es primo ni compuesto. No es primo porque no tiene dos divisores positivos distintos. No es compuesto porque no tiene otros divisores distintos de la unidad y sí mismo.
- El número 2 es el único par primo.

¿Por qué son importantes los números primos?

Pues cumplen muchas propiedades que no cumplen los números compuestos (los que no son primos).

Los números 1, -1, 0 no son primos pero tampoco compuestos, son casos particulares.

### Propiedades de los números primos

- a) Si  $n \in \mathbb{Z}^+$  y  $n$  es un número compuesto, entonces existe al menos un número primo  $p$  tal que  $p|n$ .
- b) Sea  $p \in \mathbb{Z}^+$ . Si  $p$  es primo y  $p|(a \cdot b)$  entonces  $p|a$  o  $p|b$ .

### Demostración (por contradicción)

a) Se supone por el contrario, que existe un número  $n$  compuesto que no tiene divisores primos. Se define al conjunto de estos números:  $S = \{n \in \mathbb{Z}^+ / n \text{ es un número compuesto y no tiene divisores primos}\}$ . Por lo dicho anteriormente  $S \neq \emptyset$  y por el principio del Buen Orden,  $S$  posee un mínimo, el cual se llamará ' $m$ '. Como ' $m$ '  $\in S$ , el elemento  $m$  es compuesto y no tiene divisores primos, por lo que es posible escribir a ' $m$ ' como ' $m = m_1 \cdot m_2$ ', donde ambos  $m_i$  son menores que ' $m$ '.

Como  $m_1 \notin S$  porque ' $m$ ' es el mínimo de  $S$ , se deduce que  $m_1$  es primo o tiene divisores primos. Cualquiera sea el caso, existe un primo  $p$  tal que  $p|m_1$  y esto contradice la suposición. Luego  $S = \emptyset$  y se concluye que todo número compuesto admite al menos un divisor que es un número primo.

### □ Ejemplos 3.8

El siguiente condicional:

$$\text{Si } n | a \cdot b \Rightarrow n|a \vee n|b, \text{ para } n, a, b \in \mathbb{Z} \text{ es Falso.}$$

Pues  $8|4 \cdot 10$  pero no es cierto que  $(8|4 \vee 8|10)$ .

En cambio, si se tiene como dato que el número ' $n$ ' es primo, por la propiedad anterior (b) el condicional dado sería verdadero.

### ➲ Teorema: El legado de Euclides

“Existen infinitos números primos”

### Demostración (método de reducción al absurdo)

Se supone que no es cierto el enunciado del teorema, entonces hay únicamente un número finito de números naturales primos, sean éstos  $p_1, p_2, \dots, p_t$ . El número  $q = p_1 \cdot p_2 \dots p_t + 1$  da resto 1 al dividirlo por todos los primos conocidos. Se tiene pues un número distinto de 0 y 1 que no es un producto de números primos, lo que es una contradicción. Luego existen infinitos primos.

### Actividad 3.3

a) Dar al menos un primo que divide a cada uno de los siguientes números compuestos:

i) 27      ii) 35      iii) 121      iv) 1002

b) Buscar en la web a los números primos entre 1000 y 1100.

### Teorema Fundamental de la Aritmética

Si  $n \in \mathbb{Z}, n > 1$ , entonces  $n$  es primo o puede escribirse de manera única en la forma:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}.$$

donde los  $p_i$  son números primos distintos tal que y los  $a_i \in \mathbb{Z}^+$

### Ejemplo 3.9

La descomposición en factores primos de 30, 64 y 48 son:

$$30 = 2 \cdot 3 \cdot 5 \quad 64 = 2^6 \quad 48 = 2^4 \cdot 3$$

### Algoritmo para la determinación de números primos

Sea  $n$  entero mayor que 1,  $n$  es primo si ningún primo  $p$  tal que  $p \leq \sqrt{n}$ , lo divide.

Paso 1: Verifique si  $n$  es 2. Si lo es,  $n$  es primo. Si no es, prosiga con el paso 2.

Paso 2: Verifique si  $2 | n$ . Si es afirmativo,  $n$  no es primo; de lo contrario, prosiga al paso 3.

Paso 3: Calcule mayor entero  $k$  menor a  $\sqrt{n}$ . Luego siga con el paso 4.

Paso 4: Verifique si  $D | n$ , donde  $D$  es cualquier número primo, tal que  $1 < D \leq K$ . Si algún  $D$  es tal que  $D | n$ , entonces  $n$  no es primo; de lo contrario,  $n$  es primo.

### □ Ejemplo 3.10

Para determinar si 113 es primo, se aplica el algoritmo:

- 1) 113 no es 2, entonces sigo con el paso 2
- 2) 113 no es par, entonces sigo con el paso 3
- 3) Calculo el mayor entero k cercano a  $\sqrt{113}$ . Se tiene k=10
- 4) Tomo como elementos de D a los primos tales que  $1 < D \leq 10$  y se calcula si  $D|113$ 
  - i) Para  $D=3$ , se tiene que 3 no divide a 113
  - ii) Para  $D = 5$ , se tiene que 5 no divide a 113
  - iii) Para  $D = 7$ , se tiene que 7 no divide a 113

Fin

Resultado: 113 es primo

### ☒ Algoritmo para determinar Números Primos en lenguaje Pseint

En el siguiente algoritmo, por razones de simplicidad, los valores de D tomados son números impares, no solo números primos

*Proceso Números Primos*

*Escribir 'Ingrese el número N:';*

*Leer N;*

*Si N=2 Entonces*

*Escribir N, " es Primo";*

*Sino*

*resto <- N MOD 2;*

*Si resto=0 Entonces*

*Escribir N, " no es Primo";*

*Sino*

*k<-TRUNC(RC(N));*

*C<-3;*

*MULTIPL<-VERDADERO;*

```

Mientras C<=K Hacer
    resto <- C MOD 2;
    Si resto<>0 Entonces
        MULT <- N MOD C;
        Si MULT=0 Entonces
            MULTIPL<-FALSO;
        FinSi
    FinSi
    C<-C+2;
FinMientras
Si MULTIPL Entonces
    Escribir N, " es Primo";
Sino
    Escribir N, " NO es Primo";
FinSi
FinSi
FinProceso

```

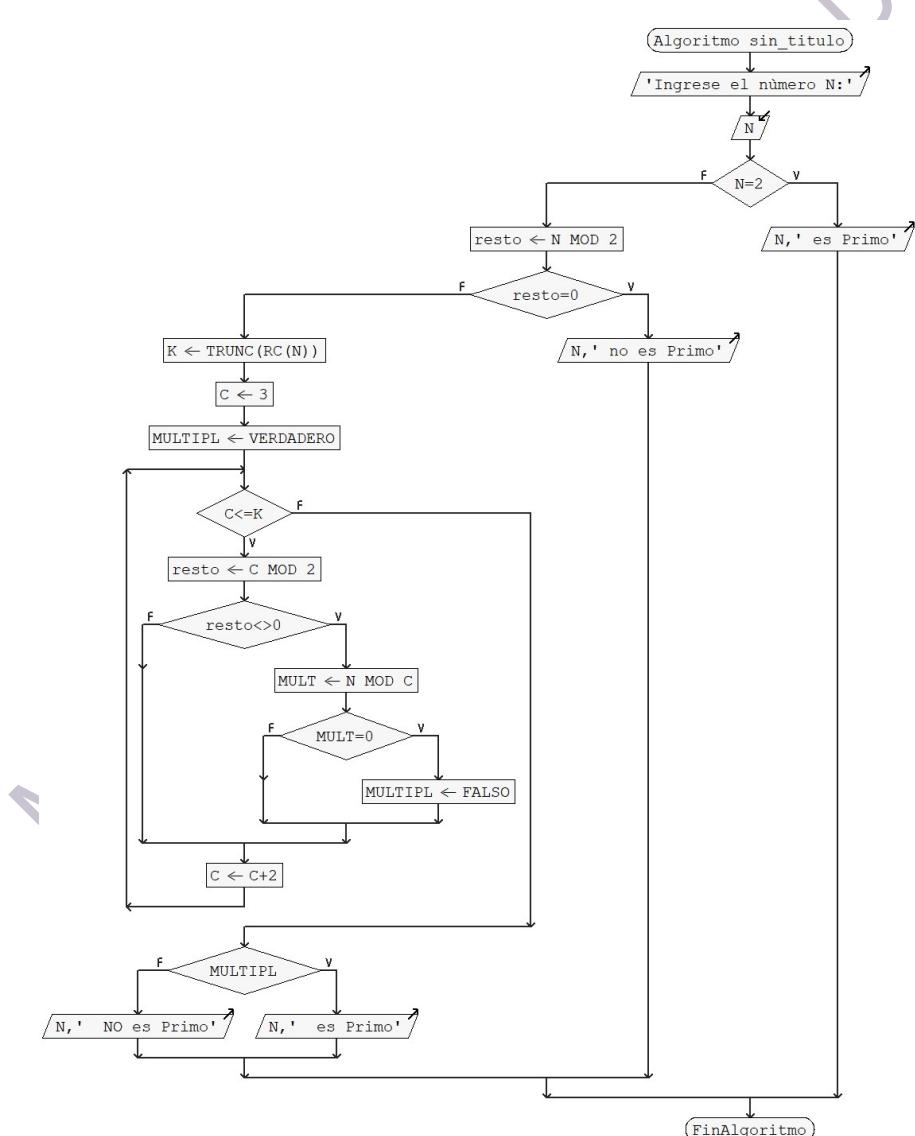


Fig. 3.3. Algoritmo Números Primos.

### Actividad 3.4

- Determinar si los siguientes números son primos: 2317 y 2437.
- En caso de que alguno de los números del apartado a) sea un número compuesto, expresarlo como producto de factores primos.

### 3.5 Máximo Común Divisor

#### Definición

Sean  $a, b \in \mathbb{Z}$  no ambos nulos; se dice que  $d \in \mathbb{Z}^+$  es el máximo común divisor de  $a$  y  $b$ , y se denota  $d = mcd(a, b)$ , si y sólo si:

- $d|a \wedge d|b$
- $\forall c \in \mathbb{Z}, c|a \wedge c|b \Rightarrow c|d$

#### Observaciones

- En la definición 1) que  $d|a \wedge d|b$  significa que  $d$  es divisor común de  $a$  y  $b$ ; y en 2) que  $d$  es el mayor común divisor de  $a$  y  $b$ .
- Sea  $D_a$  al conjunto de divisores de  $a$  y  $D_b$  el conjunto de divisores de  $b$ . Estos conjuntos no son vacíos pues al menos  $1 \in D_a$  y  $1 \in D_b$ . El máximo común divisor común de  $a$  y  $b$  es el más grande entero positivo del conjunto  $D_a \cap D_b$ .

#### Ejemplos 3.11

i)  $mcd(12, 30) = 6$ , pues

$$D_{12} = \{1, 2, 3, 4, 6, 12\} \text{ y } D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\},$$

$D_{12} \cap D_{30} = \{1, 2, 3, 6\}$ , luego  $6 = mcd(12, 30)$  por ser el mayor entero positivo del conjunto.

ii)  $mcd(13, 15) = 1$ , pues,

$$D_{13} = \{1, 13\} \text{ y } D_{15} = \{1, 15\}, \text{ y } D_{13} \cap D_{15} = \{1\}, \text{ luego } mcd(13, 15) = 1.$$

iii) Los números 12 y 36 tienen varios divisores comunes, ellos son 1, 2, 3, 4,

6 y 12 siendo el este último el mayor , por lo tanto ,  $mcd(12,36) = 12$ .

### Propiedades del Máximo Común Divisor

Sean  $a, b \in \mathbb{Z}$  no simultáneamente nulos. Se verifica que:

- i)  $mcd(a, b) = mcd(b, a)$
- ii)  $mcd(a, 0) = |a|$
- iii)  $mcd(a, b) = mcd(|a|, |b|)$
- iv)  $mcd(a, k \cdot a) = |a|, \forall k \in \mathbb{Z}$
- v)  $mcd(a, b) = mcd(b, r)$  siendo  $r = a \bmod b$
- vi)  $mcd(n \cdot a, n \cdot b) = n \cdot mcd(a, b), \text{ para } n \in \mathbb{Z}^+$

### Demostraciones

- i) Sea  $d = mcd(a, b)$  , entonces  $d$  verifica que  $d|a$  y  $d|b$  y si  $c|a$  y  $c|b$  entonces  $c|d$  . Teniendo en cuenta que la conjunción es conmutativa se tiene  $d|b$  y  $d|a$  y si  $c|b$  y  $c|a$  entonces  $c|d$ . De donde  $d = mcd(b, a)$
- ii) Si  $a > 0$  entonces  $|a| = a$  y como  $a|a$  y  $a|0$  . Se concluye que  $|a|$ , que es  $a$  , es divisor común de  $a$  y  $0$ . Para analizar que es el mayor divisor común: se toma un entero positivo  $c$  tal que  $c|a$  y  $c|0$  , por lo tanto  $c||a|$  , de allí que  $|a| = mcd(a, 0)$   
Si  $a < 0$  entonces  $|a| = -a$  y como  $-a|a$  y  $-a|0$  . Se concluye que  $|a|$ , que es  $(-a)$  , es divisor común de  $a$  y  $0$ . Para analizar que es el mayor divisor común: se toma un entero positivo  $c$  tal que  $c|a$  y  $c|0$  , por lo tanto  $c|-a$  y siendo  $-a = |a|$  se concluye que  $|a| = mcd(a, 0)$
- iii) Sea  $d = mcd(a, b)$  , entonces  $d|a$  y  $d|b$  y si  $c|a$  y  $c|b$  entonces  $c|d$ . Como  $d|a$  entonces  $d|-a$

Entonces  $d \mid -a$  y  $d \mid b$ , esto es  $d$  es divisor común de  $-a$  y  $b$ .

Además todo entero  $c$  tal que  $c \mid -a$  y  $c \mid b$  verifica también que  $c \mid a$  y  $c \mid b$ , luego  $c \mid d$  ya que  $d = \text{mcd}(a, b)$ . Entonces  $d = \text{mcd}(-a, b)$

iv) Si  $a \geq 0$  y  $b \geq 0$  entonces  $|a| = a$  y  $|b| = b$ , luego se verifica que

$$\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$$

Si  $a < 0$  y  $b \geq 0$  entonces  $|a| = -a$  y  $|b| = b$ , luego por iii) se verifica  $\text{mcd}(a, b) = \text{mcd}(-a, b) = \text{mcd}(|a|, |b|)$ . Análogamente se cumple para  $a \geq 0$  y  $b < 0$

Si  $a < 0$  y  $b < 0$  entonces  $|a| = -a$  y  $|b| = -b$ , luego se tendrá que  $\text{mcd}(|a|, |b|) = \text{mcd}(-a, -b) = \text{mcd}(-a, b) = \text{mcd}(a, b)$

v) Cualquiera sea  $a, |a| \mid a$  y  $|a| \mid k.a$  con lo que se dice que  $|a|$  es un divisor común entre  $a$  y  $k.a$ .

Si  $c$  es cualquier otro entero tal que  $c \mid a$  y  $c \mid k.a$  entonces  $c < |a|$  ya que el mayor divisor de  $a$  es  $|a|$ . Entonces  $\text{mcd}(a, k.a) = |a|$ .

vi) Sea  $d = \text{mcd}(a, b)$ , mostrar que  $d = \text{mcd}(b, r)$ , es probar que  $d \mid b$  y  $d \mid r$  y que si  $c \mid b$  y  $c \mid r$  entonces  $c \mid d$ . Como  $a = b.q + r$  y  $d \mid a$  y  $d \mid b$  por ser el máximo común divisor entre ellos entonces se tiene que  $d \mid (a - b.q)$  y por lo tanto  $d \mid r$ . Además si  $c \mid b$  y  $c \mid r$  entonces  $c \mid (b.q + r)$  y por lo tanto  $c \mid a$ . Pero como  $d$  es el máximo común divisor de  $a$  y  $b$  entonces  $c \mid d$

### ☞ Teorema: Identidad de Bezout

Si  $d = \text{mcd}(a, b)$  entonces  $d$  puede expresarse como combinación lineal de  $a$  y  $b$  de infinitas maneras. Esto es, existen infinitos enteros  $x, y$  tales que cumplen la siguiente igualdad  $d = a.x + b.y$

Este teorema sirve para demostrar el siguiente corolario:

Dos enteros  $a$  y  $b$  son coprimos (o primos relativos) si y solo si existen enteros  $x$ ,  $y$  tales que:  $ax + by = 1$ .

### □ Ejemplos 3.12

- a) Como  $1 = 3.8541 + (-2).12811$  entonces  $mcd(8541, 12811) = 1$
- b) Dos enteros consecutivos siempre son coprimos, es decir,  $mcd(x, x+1) = 1$ , ya que:  $1.(x+1) + (-1).x = 1$

### Actividad 3.5

Responder Verdadero o Falso, y justificar la respuesta:

- i)  $mcd(10, 25) = 5 \wedge mcd(-10, -25) = -5$
- ii)  $mcd(-5, 5.k) = 5, \forall k \in \mathbb{Z}$
- iii)  $mcd(115, 113) = mcd(113, 2) = mcd(2, 1) = 1$
- iv) 1 es combinación lineal de 2 y 3
- v) 3 es combinación lineal de 12 y 15
- vi)  $mcd(55, 135) = 5 \cdot mcd(11, 27) = 5 \cdot mcd(11, 6)$

### ☞ Algoritmo de Euclides para el cálculo de mcd

Este algoritmo propone calcular el mcd en base a solo divisiones lo cual hace que el cálculo, ya sea si quiere hacerse de manera manual o de manera computacional, sea más eficiente. Consiste en tomar los dos números enteros, no nulos  $a$  y  $b$ , ordenarlos de mayor a menor y hacer divisiones sucesivas de la siguiente forma:

Sean  $a, b \in \mathbb{Z}^+$

- 1) Si  $a = b$  entonces  $mcd(a, b) = a = b$
- 2) Si  $a > b$  y  $b|a$  entonces  $mcd(a, b) = b$

3) Si  $a > b$  y  $b \nmid a$  entonces se divide  $a$  por  $b$  obteniendo un resto  $r_1$  (por el algoritmo de la división)

$$a = b \cdot q_1 + r_1, \quad 0 \leq r_1 < b$$

Por propiedad resulta que  $\text{mcd}(a, b) = \text{mcd}(b, r_1)$

3.1) Si  $r_1 \mid b$  entonces  $\text{mcd}(a, b) = \text{mcd}(b, r_1) = r_1$

3.2) Si  $r_1 \nmid b$ , se divide  $b$  por  $r_1$ , obteniendo un resto  $r_2$ , entonces por el algoritmo de la división se tiene

$$b = r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1$$

Al igual que antes se tiene que  $\text{mcd}(b, r_1) = \text{mcd}(r_1, r_2)$

3.2.1) Si  $r_2 \mid r_1$  entonces  $\text{mcd}(a, b) = \text{mcd}(b, r_1) = \text{mcd}(r_1, r_2) = r_2$

3.2.2) Si  $r_2 \nmid r_1$ , se divide  $r_1$  por  $r_2$  obteniendo un resto  $r_3$  entonces por el algoritmo de la división se tiene

$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 \leq r_3 < r_2$$

Al igual que antes se tiene que  $\text{mcd}(r_1, r_2) = \text{mcd}(r_2, r_3)$ , y así sucesivamente.....

$$r_{n-2} = r_{n-1} \cdot q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$

Este proceso se repite hasta llegar a un resto igual a cero

$$r_{n-1} = r_n \cdot q_{n+1} + 0$$

Por lo tanto  $\text{mcd}(r_{n-2}, r_{n-1}) = \text{mcd}(r_{n-1}, r_n) = r_n$

Las igualdades que genera el algoritmo de Euclides tienen el beneficio de permitir encontrar una combinación lineal que satisfaga la identidad de Bezout:  $d = ax + by$ . Basta desandar el camino para expresar  $d = r_k$  en función de los anteriores restos y finalmente en función de  $a$  y  $b$ .

## Algoritmo de Euclides en el lenguaje de Pseint

Algoritmo CálculoMCD

Escribir ('Ingresá los números a y b con a>b')

Leer a,b

$r \leftarrow a \text{ MOD } b$

Si  $r=0$  Entonces

Escribir 'mcd(a,b)= ',b

SiNo

Si  $r>0$  Entonces

$a \leftarrow b$

$b \leftarrow r$

$r \leftarrow a \text{ MOD } b$

Si  $r=0$  Entonces

Escribir 'mcd(a,b)= ',b

FinSi

FinSi

FinSi

FinAlgoritmo

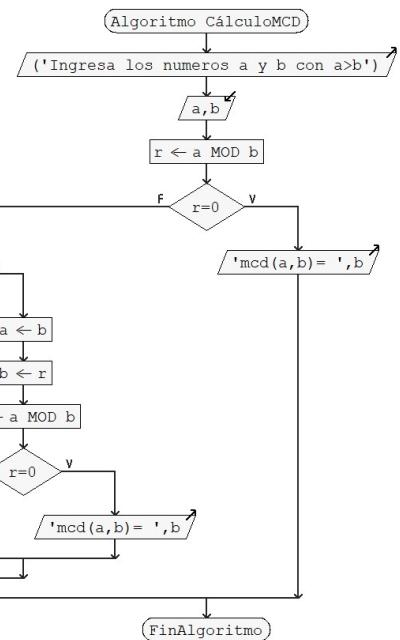


Fig. 3.4. Algoritmo Cálculo mcd

### Ejemplo 3.13

Sean  $a = 250$  y  $b = 111$ , se muestran a continuación el cálculo del  $mcd(a; b)$  y los pasos que se deben dar para expresar a  $mcd(a, b)$  como combinación lineal de  $a$  y  $b$ .

Cálculo de  $mcd(250, 111)$

- (1)  $250 = 111 \cdot 2 + 28$  con  $0 < 28 < 111$
- (2)  $111 = 28 \cdot 3 + 27$  con  $0 < 27 < 28$
- (3)  $28 = 27 \cdot 1 + 1$  con  $0 < 1 < 27$
- (4)  $27 = 1 \cdot 27$

Por tanto, el  $mcd(250; 111) = 1$  (el último resto no nulo)

Para encontrar la combinación lineal de la que habla la identidad de Bezout se deben despejar los residuos obtenidos en el algoritmo de Euclides, y se hace

una sustitución hacia atrás.

$$\begin{aligned} \text{i) } 1 &= 28 - 27 && \text{despejando de (3) el } mcd \\ &= 28 - (111 - 28 \cdot 3) && \text{despejando de (2) el resto 27} \\ &= 4 \cdot 28 - 111 \\ &= 4 \cdot (250 - 111 \cdot 2) - 111, && \text{despejando de (1) el resto 28} \\ 1 &= \underbrace{4}_{x} \cdot \underbrace{250}_{y} + \underbrace{(-9)}_{y} \cdot \underbrace{111}, && \text{luego el } mcd(250, 111) \text{ expresado} \\ &&& \text{como combinación lineal de 250 y 111.} \end{aligned}$$

### Actividad 3.6

Determinar el  $mcd(315, 113)$ . Luego expresar el resultado como combinación lineal de los enteros dados.

### ❖ Aplicación

Una aplicación interesante del algoritmo de la división permite la representación de un número entero  $a$  en una base de numeración  $b \geq 2$ .

Se recuerda que un *Sistema de Numeración* es un conjunto de reglas y convenios mediante los cuales pueden representarse todas las cantidades utilizando signos diversos. Los Sistemas conocidos son, entre otros, el romano y el decimal. Este último emplea el principio del valor relativo de cada cifra dentro de una cantidad: una cifra representa uno u otro valor según el lugar que ocupe.

Sistemas de numeración más modernos y que deben su importancia y utilización a la aparición del computador son el binario, el octal y el hexadecimal, basados, respectivamente, en los números dos, ocho y dieciséis.

En efecto, se puede poner para un número entero  $a > 0$  (a través de divisiones sucesivas y sustituciones reiteradas:

$$a = r_n b^n + r_{n-1} b^{n-1} + \dots + r_2 b^2 + r_1 b^1 + r_0, \text{ y de esta forma se indica}$$

$$a = (r_n r_{n-1} \dots r_2 r_1 r_0)_b \text{ y se dice que es la expresión de } a \text{ en base } b.$$

Por ejemplo el número entero 4165 en base 7, quedaría aplicando el algoritmo

de la división,

$$4165 = 7 \cdot 595 + 0 \rightarrow r_0$$

$$595 = 7 \cdot 85 + 0 \rightarrow r_1$$

$$85 = 7 \cdot 12 + 1 \rightarrow r_2$$

$$12 = 7 \cdot 1 + 5 \rightarrow r_3$$

$$1 = 7 \cdot 0 + 1 \rightarrow r_4$$

Se obtiene  $4165 = (15100)_7 = 0 + 0 \cdot 7 + 1 \cdot 7^2 + 5 \cdot 7^3 + 1 \cdot 7^4$

### 3.5.1 Números Coprimos o Primos relativos

#### Definición

Sean  $a, b \in \mathbb{Z}$ . Se dice que  $a$  y  $b$  son coprimos o primos relativos si y solo si  $mcd(a, b) = 1$ .

Esto es, cuando tienen un único divisor común, el 1.

#### Ejemplos 3.14

- i) 2 y 3 son coprimos ya que  $mcd(2, 3) = 1$
- ii) 16 y 15 son coprimos ya  $mcd(16, 15) = 1$
- iii) 11 y 13 son primos relativos.

#### Observación

Si dos números son coprimos no significa que sean primos.

#### Propiedades de los Números Coprimos

Sean  $a, b, c \in \mathbb{Z}$

- Si  $a$  y  $b$  son coprimos con  $c$ , entonces  $a \cdot b$  es coprimo con  $c$ .
- Si  $a$  y  $b$  son coprimos y  $c$  es un divisor común de  $a$  y  $b$ , entonces  $c = \pm 1$ .

- Si  $a, b, n \in \mathbb{Z}^+$ , si  $n|(a \cdot b)$   $\wedge$   $a$  y  $n$  son coprimos entonces  $n|b$
- Para  $a, b \in \mathbb{Z}$ ,  $a, b \neq 0$  y  $d = mcd(a, b)$  se verifica que  $a|d$  y  $b|d$  son coprimos.

### Actividad 3.7

- Encontrar números coprimos con 8
- Sean los siguientes números: 5, 10, 12, 15, 18. Determinar todas las parejas de coprimos que hay entre ellos
- Decir verdadero o Falso, justificando su respuesta:
  - Si  $3|(5 \cdot x)$  entonces  $3|x$ ,  $\forall x \in \mathbb{Z}$
  - Si  $3|(6 \cdot x)$  entonces  $3|x$ ,  $\forall x \in \mathbb{Z}$
  - Si  $5 = mcd(10 \cdot x, 25 \cdot x)$  entonces  $2x$  y  $5x$  son coprimos,  $\forall x$

### 1.7. Mínimo Común Múltiplo

#### Definición

Sean  $a, b \in \mathbb{Z}$  no ambos nulos; se dice que  $c \in \mathbb{Z}^+$  es el mínimo común múltiplo de  $a$  y  $b$  si y sólo si:

- $a|c$  y  $b|c$
- $\forall d \in \mathbb{Z}$ ,  $a|d$  y  $b|d \Rightarrow c|d$

Se indica al mínimo común múltiplo  $c$  de  $a$  y  $b$  como  $c = mcm(a, b)$

#### Observaciones

- El apartado i) nos dice que  $a$  y  $b$  son divisores de  $c$ , o que  $a$  y  $b$  dividen a  $c$ .
- El apartado ii) nos dice que  $c$  es el mínimo del conjunto de los múltiplos positivos comunes a ambos.

### □ Ejemplos 3.15

i) Si  $a = 3$  y  $b = 8$ , los múltiplos comunes a ambos son  $24, 48, 72, \dots$

El menor de ellos es  $24$ , luego  $mcm(3,8) = 24$

ii) ¿Cuál es el  $mcm(12,15)$ ?

Los conjuntos de múltiplos positivos de  $12$  y  $15$  son, respectivamente,

$$M_{12} = \{12, 24, 36, 48, 60, 72, 84, 96, 108, 120, \dots\}$$

y

$$M_{15} = \{15, 30, 45, 60, 75, 90, 105, 120, \dots\}$$

Luego el conjunto de todos los múltiplos comunes a ambos es

$$M_{12} \cap M_{15} = \{60, 120, 180, 240, \dots\}$$

Y el mínimo de este conjunto es para la relación de divisibilidad es  $60$ , luego

$$mcm(12,15) = 60.$$

### ▀ Teorema

$\forall a, b \in \mathbb{Z}^+$  se verifica que  $mcd(a,b) \cdot mcm(a,b) = a \cdot b$

### □ Ejemplos 3.16

i) El  $mcd(250,111) = 1$ , se vio en el ejemplo 3.12, luego el

$$mcm(250,111) = \frac{250 \cdot 111}{1} = 27750$$

ii) Para evaluar la suma:  $\frac{7}{12} + \frac{17}{15}$ , se necesita determinar el  $mcm(12,15)$ , que en el ejemplo anterior (3.15 ii) se calculó  $mcm(12,15) = 60$ . Entonces

$$\frac{7}{12} + \frac{17}{15} = \frac{7 \cdot 5}{60} + \frac{17 \cdot 4}{60} = \frac{35}{60} + \frac{68}{60} = \frac{103}{60}$$

## Actividad 3.8

1) Responder Verdadero o Falso, justificando su respuesta:

- i)  $\forall a, b \in \mathbb{Z}$  se verifica que  $mcd(a, b) \cdot mcm(a, b) = |a \cdot b|$
- ii)  $\forall a, b \in \mathbb{Z}$ , si  $a$  y  $b$  son coprimos entonces  $mcm(a, b) = |a \cdot b|$

2) Tres aviones de línea regular salen del aeropuerto, uno cada 3 días, otro cada 12 días y el tercero cada 18 días. Cada cuántos días saldrán los tres aviones a la vez?

### 3.6 Ecuaciones diofánticas

#### Definición

Se llama ecuación diofántica a toda ecuación, en una o más variables, con la restricción de que sus coeficientes y sus soluciones son números enteros.

La más simple es la ecuación diofántica lineal en dos variables:  $ax + by = c$  donde  $a, b$  y  $c$  son enteros con  $a$  y  $b$  no simultáneamente nulos.

#### Teorema

Sean  $a, b$  y  $c$  son enteros con  $a$  y  $b$  no simultáneamente nulos. La ecuación diofántica  $ax + by = c$  tiene soluciones enteras si y solo si  $mcd(a, b)|c$ .

Además, si la ecuación tiene soluciones, son infinitas.

#### Ejemplos 3.17

- i) La ecuación en enteros  $2x + 3y = 2$  tiene solución pues  $mcd(2,3) = 1$  y  $1|2$ .
- ii) La ecuación  $6x - 3y = 1$  no tiene soluciones enteras pues  $mcd(6,3) = 3$  y  $3 \nmid 1$
- iii) ¿Cuál sería una solución para la ecuación en enteros  $-8x + 22y = 20$ ?

Por prop. del mcd:  $mcd(-8,22) = mcd(22,8) = 2$  pues:  $22 = 2 \cdot 8 + 6$

$$8 = 6 \cdot 1 + 2$$

$$6 = 2 \cdot 3$$

y, despejando los residuos y haciendo una sustitución hacia atrás:

$$2 = 8 - 6 \cdot 1 = 8 - (22 - 2 \cdot 8) = 3 \cdot 8 - 22 = (-3) \underbrace{(-8)}_{a=-8} + (-1) \underbrace{22}_{b} \quad (1)$$

Ahora, como  $20 = 2 \cdot 10$ , multiplicando ambos miembros de (1) por 10

$$2 = (-3)(-8) + (-1)22 \rightarrow 20 = (-30)(-8) + (-10)22$$

Así, una solución de la ecuación diofántica es  $x_0 = -30$  e  $y_0 = -10$ .

### 3.6.1 Solución general

#### ☞ Teorema

Si  $a, b$  y  $c$  son enteros con  $a$  y  $b$  no nulos, la ecuación diofántica:  $ax + by = c$  tiene solución si y sólo si el  $d = mcd(a, b)|c$ . En este caso, si  $x_0$  e  $y_0$  es una solución particular, entonces la solución general está dada por:

$$x = x_0 + \frac{b}{d} \cdot k ; \quad y = y_0 - \frac{a}{d} \cdot k ; \quad \forall k \in \mathbb{Z}$$

#### Pasos para encontrar la solución general

Sea la ecuación  $ax + by = c$ , como  $d = mcd(a, b)|c$  existe una solución particular  $(x_0, y_0)$ , luego se plantean las siguientes ecuaciones:

$$\begin{cases} \frac{a}{d}x + \frac{b}{d}y = \frac{c}{d} \\ \frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d} \end{cases} \Rightarrow \text{restando m.a.m} \quad \frac{a}{d}(x - x_0) + \frac{b}{d}(y - y_0) = 0 \quad (*)$$

$$\Rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \Rightarrow \frac{b}{d} \mid \frac{a}{d}(x - x_0)$$

Pero  $\frac{a}{d}$  y  $\frac{b}{d}$  son primos entre sí, por tanto  $\frac{b}{d} \mid (x - x_0)$ , con lo cual existe  $k \in \mathbb{Z}$  tal que:  $(x - x_0) = \frac{b}{d}k$ , luego  $x = x_0 + \frac{b}{d}k$ . Sustituyendo en (\*)

$$\frac{a}{d}k \frac{b}{d} + \frac{b}{d}(y - y_0) = 0 \Rightarrow \frac{a}{d}k + (y - y_0) = 0 \Rightarrow y = y_0 - \frac{a}{d}k$$

#### ☞ Observación

En otras palabras, cuando se tiene una solución particular  $(x_0, y_0)$  y que verifica la ecuación  $ax_0 + by_0 = c$ , con  $d = mcd(a, b)|c$ ; se debe sumar y restar un múltiplo entero del  $mcm(a, b) = \frac{ab}{d}$ ; o sea  $\pm \frac{ab}{d}k, k \in \mathbb{Z}$  para encontrar la solución general, es decir:

$$ax_0 + by_0 \pm \frac{ab}{d}k = c \Rightarrow a\left(\underbrace{x_0 + \frac{b}{d}k}_x\right) + b\left(\underbrace{y_0 - \frac{a}{d}k}_y\right) = c$$

### □ Ejemplos 3.17

- 1) Existen, soluciones enteras de la ecuación diofántica  $4x - 6y = 10$  ya que  $mcd(4, -6) = mcd(6, 4) = 2$  y  $2|10$ . En este caso observe que se puede reducir la ecuación anterior dividiendo ambos miembros por  $d = 2$  y se obtiene la ecuación:  $2x - 3y = 5$ .

Una solución es  $(1, -1)$ . Las soluciones de la ecuación son de la forma:

$$x = x_0 - (b/d).k = 1 + 3k$$

$y = y_0 + (a/d).k = (-1) + 2k, \forall k \in \mathbb{Z}$ , por lo que algunas de las soluciones son:  $(1, -1), (4, 1), (7, 3), \dots, (-2, -3), (-5, -5), \dots$

- 2) Si existe, ¿cuál sería la solución general de la ecuación diofántica

$$7x - 11y = 2 \quad ?$$

Como  $7$  y  $(-11)$  son primos relativos, el  $mcd(7, -11) = 1$  y  $1|2$ .

Ahora, para encontrar una solución particular se deben seguir los pasos que permiten encontrar la combinación lineal de la que nos habla la identidad de Bezout :

$$11 = 7 \cdot 1 + 4 \quad (1)$$

$$7 = 4 \cdot 1 + 3 \quad (2)$$

$$4 = 3 \cdot 1 + 1 \rightarrow 1 = mcd(7, -11) = mcd(7, 11) \quad (3)$$

$$3 = 3 \cdot 1;$$

para expresar 1 como combinación lineal de 7 y 11, se despeja de (3):

$1 = 4 - 3 \cdot 1$  (4), se despeja de (2)  $3 = 7 - 4 \cdot 1$  y se reemplaza en (4)

$1 = 4 - (7 - 4) \cdot 1 = 2 \cdot 4 - 7$ , (5) luego de (1) se despeja:  $4 = 11 - 7 \cdot 1$  y se reemplaza en (5):

$1 = 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7$ , luego se tiene  $1 = (-3) \cdot 7 + (-2) \cdot (-11)$ . multiplicando x 2, se tiene:

$2 = (-6) \cdot 7 + (-4) \cdot (-11)$ , entonces una solución es  $(-6, -4)$ .

El resto de las soluciones son:  $x = -6 + (-11)k$  e  $y = -4 - 7k$ ; luego otra forma de expresar todas las soluciones es:

$(-6 - 11k, -4 - 7k)$ , con  $k$  entero.

### Observación

En ocasiones, además de encontrar la solución general de una ecuación diofántica, hay que buscar la solución o soluciones que satisfacen algunas condiciones adicionales, como por ejemplo que las variables sean positivas. Para ello, se encuentra en primer lugar la solución general y a continuación se determinan los valores del parámetro  $k$  para que se cumplan las condiciones adicionales.

### Ejemplo 3.18

Si en el Ejemplo 3.17 (2) hubieran pedido todas las soluciones enteras “no negativas” de la ecuación diofántica  $7x - 11y = 2$ ; se tendría que hacer cumplir la condición adicional “no negativas” a la solución general  $(-6 - 11k, -4 - 7k)$ ; es decir:

$$-6 - 11k \geq 0 \rightarrow k \leq \frac{-6}{11} \quad \text{y} \quad -4 - 7k \geq 0 \rightarrow k \leq -4/7.$$

Luego  $k = -1, -2, -3, \dots$ ;

para  $k = -1$ , la solución es  $(5, 3)$ ;

$k = -2$ , la solución es  $(16, 10)$ , ...

$k = -3$ , la solución es  $(27, 17), \dots$

### Actividad 3.9

i) Encontrar, si existen, las infinitas soluciones enteras de la ecuación:

$$243x + 198y = 9$$

ii) En un parque de diversiones cobran \$180 a los mayores y \$75 a los menores.

En un cierto día se recaudaron \$9000 y asistieron más adultos que menores.

¿Cuáles fueron los posibles números de asistentes?

### 3.7 Congruencia en $\mathbb{Z}$

Al dividir un entero  $x$  por un natural  $n > 1$  los posibles restos son:  $0, 1, 2, \dots, n - 1$ . Además observe que dos enteros tienen el mismo resto al dividirlos en  $n$  si y solo si difieren en un múltiplo de  $n$ .

Para distinguir a todos los números que al ser divididos en  $n$  tienen el mismo resto se define el concepto de congruencia.

#### Definición

Sean  $x, y \in \mathbb{Z}$  y sea  $n \in \mathbb{Z}^+$ . Se dice que “ $x$  es congruente con  $y$  módulo  $n$ ” si y solo si  $x \bmod n = y \bmod n$ .

Simbólicamente:  $x \equiv y \pmod{n} \Leftrightarrow x \bmod n = y \bmod n$

Esto significa que  $x$  e  $y$  tienen el mismo resto al dividirlos en  $n$

#### Ejemplos 3.19

- $15 \equiv 7 \pmod{2}$ ; pues  $15 \bmod 2 = 7 \bmod 2 = 1$ , pero no es cierto que  $15 \equiv 7 \pmod{3}$  dado que  $15 \bmod 3 = 0$ , y  $7 \bmod 3 = 1$ .
- $16 \equiv 24 \pmod{4}$ , y también  $-16 \equiv 24 \pmod{8}$ .

## Propiedad

Sean  $x, y \in \mathbb{Z}$  y sea  $n \in \mathbb{Z}^+$ . Se cumple que  $x$  e  $y$  son congruentes *módulo n* si y solo si la diferencia entre ellos es múltiplo de  $n$ .

Simbólicamente:  $x \equiv y \pmod{n} \Leftrightarrow n|(x-y)$

El lenguaje de congruencias fue introducido por K. Gauss a los 24 años en su libro *Disquisitiones Arithmeticae*, y hoy se sigue usando en la vida cotidiana, pues se tiene las horas de 12 en 12 (a veces de 24 en 24). Por ejemplo, si son las 10 de la mañana se dice “dentro de cuatro horas serán las 2”, y esto parece natural, que la suma de 10 y 4 sea 2. Así, sin darnos cuenta, se usa aritmética en módulo 12. Por ello se dice que la esfera de un reloj funciona con congruencias módulo 12, además otros ejemplos de la vida diaria serían los cuentakilómetros de los coches que lo hacen módulo 100000 y los meses se representan módulo 12.

### Ejemplo 3.20

- $21 \equiv 9 \pmod{4}$  porque  $21 - 9 = 12$  es un múltiplo de 4 (o bien  $4|12$ )
- $9 \equiv 0 \pmod{3}$  porque  $9 - 0 = 9$  es un múltiplo de 3.
- $2 \equiv -3 \pmod{5}$  porque  $2 - (-3) = 5$  y  $5|5$ .

### Observaciones

- De  $n|(x-y) \Leftrightarrow (x-y)$  es múltiplo de  $n$  se deduce que  $x = y + n.k$ ,  $k \in \mathbb{Z}$ , esta propiedad permite agilizar el cálculo para determinar congruencias ya que en lugar de hacer dos divisiones hay que realizar una resta y una división.

Si se fija el valor de  $y$ , para encontrar el valor de  $x$  congruente con  $y$  basta con sumar cualquier múltiplo de  $n$ .

Así fijando  $n = 4$ ; algunos números congruentes con 0 son:

$0 + 4; 0 + 2.4; 0 + 3.4; \dots$  es decir:  $4, 8, 12, 16, \dots$

Algunos números congruentes con 1 son:

$1 + 4; 1 + 2.4; 1 + 3.4; \dots$  es decir:  $5, 9, 13, 17, \dots$

Algunos números congruentes con 2 son:

$$2 + 4 ; 2 + 2 \cdot 4 ; 2 + 3 \cdot 4; \dots \text{ es decir: } 6, 10, 14, 18, \dots$$

Algunos números congruentes con 3 son:

$$3 + 4 ; 3 + 2 \cdot 4 ; 3 + 3 \cdot 4; \dots \text{ es decir: } 7, 11, 15, 19, \dots$$

- Considerando *módulo n*, observe que nunca dos números menores que *n* pueden ser congruentes *módulo n*, dado que la diferencia jamás será múltiplo de *n*. Luego el conjunto  $\{0, 1, 2, 3, \dots, n-1\}$  es de los restos posibles al dividir cualquier entero en *n*, no hay dos números congruentes entre sí *módulo n*. Entonces, si se quiere encontrar números congruentes con ellos basta con sumar *n* la cantidad de veces que se desee.

### Actividad 3.10

- a) Encontrar cinco números congruentes con 21 *módulo 3* mayores de 30
- b) Encontrar cinco números congruentes con 21 *módulo 4* menores que 30
- c) Completar las líneas punteadas.

i)  $7|(124 - 110)$  entonces .....

ii)  $5|(-21 - 29)$  entonces .....

### 3.8 Relación de Congruencia módulo n

#### Definición

Sea el conjunto  $\mathbb{Z}$ , se llama Relación de Congruencia *módulo n* a la relación *R* definida del siguiente modo:  $R = \{(x, y) / x \equiv y \pmod{n}, x, y \in \mathbb{Z}\}$

#### Propiedad

Toda Relación de congruencia *módulo n* definida en  $\mathbb{Z}$  es una relación de equivalencia, cualquiera sea *n*.

## Demostración

Debe mostrarse que  $R$  es reflexiva, simétrica y transitiva

Sea  $x \in \mathbb{Z}$ ,  $x \equiv x \pmod{n}$  ya que  $n|(x-x)$ , para todo  $x$ . Por lo tanto  $R$  es reflexiva.

Sean  $x, y \in \mathbb{Z}$ , si  $x \equiv y \pmod{n}$  entonces  $n|(x-y)$ . Por propiedad de la divisibilidad también se cumple que  $n|(y-x)$  de donde se deduce que  $y \equiv x \pmod{n}$ . Por lo tanto  $R$  es simétrica

Sean  $x, y, z \in \mathbb{Z}$ ,

si  $x \equiv y \pmod{n} \wedge y \equiv z \pmod{n}$  entonces  $n|(x-y) \wedge n|(y-z)$ .

Por propiedad de la divisibilidad también se cumple que  $n|((x-y) + (y-z))$ , esto es  $n|(x-z)$ . De aquí se deduce que  $x \equiv z \pmod{n}$ . Por lo tanto  $R$  es transitiva.

Por último se concluye que  $R$  es una relación de equivalencia.

### 3.8.1 Conjunto Cociente de una Relación de Congruencia

Como toda relación de equivalencia, las relaciones de congruencia generan una partición en el conjunto  $\mathbb{Z}$  formada por todas las clases de equivalencia distintas que dicha relación genera. Se adopta una notación especial para las clases de equivalencia para incluir al módulo del que se habla.

#### Definición

Se representa con  $[x]_n$  a la clase de equivalencia *módulo n* del elemento  $x$ , la cual se define:

$$[x]_n = \{y \in \mathbb{Z} / x \equiv y \pmod{n}\}$$

Cada clase de equivalencia queda determinada por un resto, por lo tanto hay  $n$  clases distintas, ya que en la división por  $n$  se tienen  $n$  restos posibles:

$$0, 1, 2, \dots, n-1.$$

Entonces se tiene  $n$  clases distintas:  $[0]_n, [1]_n, [2]_n, \dots, [n-1]_n$ , los valores  $0, 1, 2, \dots, n-1$  son los representantes de cada clase.

En general se puede hacer un listado de los elementos de  $[y]$ :

$$[y] = \{y, y + n, y + 2n, y + 3n, \dots, y - n, y - 2n, y - 3n, \dots\}$$

Recordar que las clases de equivalencia formaban una partición del conjunto, en este caso de  $\mathbb{Z}$ , resulta pes que las siguientes clases son la partición de  $\mathbb{Z}$  asociada a la relación  $\mathcal{R}$  de congruencia:

$$[0] = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$$

$$[1] = \{\dots, 1 - 3n, 1 - 2n, 1 - n, 1, 1 + n, 1 + 2n, 1 + 3n, \dots\}$$

$$[2] = \{\dots, 2 - 3n, 2 - 2n, 2 - n, 2, 2 + n, 2 + 2n, 2 + 3n, \dots\}$$

⋮

$$[n-1] = \{\dots, -2n-1, -n-1, -1, n-1, 2n-1, 3n-1, 4n-1, \dots, \dots\}$$

### Observaciones

$[n] = [0], [n+1] = [1]$ , etc. y que  $[-1] = [n-1], [-2] = [n-2]$ , etc.

Como consecuencia se tienen exactamente  $n$  clases distintas.

También para el Conjunto Cociente se adopta una notación especial,  $\mathbb{Z}_n$  y entonces se tiene que:

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$$

### Ejemplo 3.21

Las clases de equivalencia en  $\mathbb{Z}$  módulo 3 son  $[0], [1]$  y  $[2]$ , el conjunto cociente:

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}; \text{ donde}$$

$$[0]_3 = \{y \in \mathbb{Z} : y \equiv 0 \pmod{3}\} = \{y \in \mathbb{Z} : y = 3k, k \in \mathbb{Z}\} =$$

$$= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\};$$

$$[1]_3 = \{y \in \mathbb{Z} : y \equiv 1 \pmod{3}\} = \{y \in \mathbb{Z} : y = 1 + 3k, k \in \mathbb{Z}\} =$$

$$= \{ \dots, -8, -5, -2, 1, 4, 7, 10, \dots \}$$

$$[2]_3 = \{y \in \mathbb{Z} : y \equiv 2 \pmod{3}\} = \{y \in \mathbb{Z} : y = 2 + 3k, k \in \mathbb{Z}\} =$$

$$= \{ \dots, -4, -1, 2, 5, 8, 11, \dots \}$$

**Actividad 3.11**

a) Encontrar al conjunto  $\mathbb{Z}_5$ , describiendo a cada uno de sus elementos.

b) Realizar un diagrama de Venn para representar a  $\mathbb{Z}_5$

MATERIAL EN TRAMITE DE ISBN



# MATEMÁTICA DISCRETA

UTN – FRT

## Capítulo 4. **SUCESIONES, INDUCCIÓN Y RECURSIVIDAD**

Sucesión.

Dominio e Imagen.

Sucesiones especiales: de posiciones,  
de caracteres y numéricas.

Progresión aritmética y geométrica.

Símbolo suma. Propiedades.

Principio de Inducción Matemática.

Relaciones de recurrencia.

Clasificación de las relaciones de recurrencia.

Solución de las relaciones de recurrencia lineales.



## Introducción

El concepto abstracto de sucesión se puede asociar, en una primera aproximación, a los procesos discretos de la naturaleza o, a aquellos que se pueden describir de esta forma, por ejemplo, la evolución de una población en instantes de tiempo equiespaciados o una señal digital.

En programación, a menudo se necesita generar valores numéricos uniformemente espaciados y para ello se necesita una fórmula que proporcione los valores.

En matemáticas esos conjuntos de valores se denominan sucesiones. Aparte de su interés como mecanismo para modelar, la teoría de sucesiones aporta una importante herramienta deductiva en el Análisis Matemático. De una manera simple se puede afirmar que una sucesión es una estructura discreta que consiste en una lista ordenada de objetos, pero a continuación se formalizará el concepto simbólicamente para evitar ambigüedades.

### 4.1 Sucesión

#### Definición

Una sucesión es una función cuyo Dominio es el conjunto  $\mathbb{N}$  y cuya Imagen un conjunto  $A$  de cualquier naturaleza.

Simbólicamente, si se designa a la sucesión con la letra  $S$  se tendrá

$$S: \mathbb{N} \rightarrow A$$

y se indica los valores del Conjunto Imagen (o términos de la sucesión) del siguiente modo:

$$S(1) = a_1; \quad S(2) = a_2; \quad S(3) = a_3; \dots$$

donde  $a_1, a_2, a_3, \dots \in A$

En general, si  $n \in \mathbb{N}$  se dice que  $a_n$  es el  $n$ -ésimo término de la sucesión o término general de la sucesión.

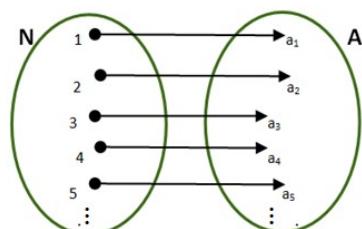


Fig.4.1 Función sucesión.

## Notación

Por simplicidad una sucesión suele indicarse dando sólo los valores imágenes de la función según sus subíndices, de menor a mayor

$$S : a_1, a_2, a_3, \dots$$

### Observaciones

- La notación  $(a_n) : a_1, a_2, a_3, \dots$  no es más que una forma abreviada de escribir una función como un conjunto de pares ordenados:  $\{(1, a_1), (2, a_2), (3, a_3), \dots\}$ .
- El dominio de la sucesión también puede ser  $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ , el conjunto de enteros no negativos. En este caso, el primer término de la sucesión será  $a_0$ , el segundo  $a_1$ , etc. Esto es:

$$(a_n) : a_0, a_1, a_2, \dots \quad n \in \mathbb{N}_0$$

- Los términos de la sucesión pueden o no repetirse

### Definiciones

- El conjunto correspondiente a una sucesión o conjunto Imagen de la función es el conjunto de todos los elementos distintos de la sucesión.
- La sucesión es finita cuando finaliza después de una cantidad determinada de términos. En caso contrario se dice infinita.

### Ejemplos 4.1

- a)  $S_1 : 0, 1, 0, 1, 0, 1, \dots$  es la sucesión infinita que alterna ceros y unos. Su conjunto correspondiente es  $\{0, 1\}$ .
- b)  $S_2 : a, b, c, d, e$  es la sucesión finita de las 5 primeras letras en orden alfabético. Su conjunto correspondiente es  $\{a, b, c, d, e\}$
- c)  $S_3 : 1, 3, 5, 7$  es la sucesión finita de los 4 primeros números impares.

Su conjunto correspondiente es { 1 , 3 , 5 , 7 }

- d)  $S_4 : 1, 0, 0, 1, 0, 0, 0, 1, 1$  es una sucesión finita con elementos repetidos.

Su conjunto correspondiente es { 0 , 1 }. Observe que no existe un patrón para los elementos de esta sucesión

- e)  $S_5 : 1, 2, 4, 8, 16, 32, \dots$  es una sucesión infinita donde se observa que cada término se obtiene duplicando el término anterior. Su conjunto imagen se puede expresar del siguiente modo  $\{a_n / a_n = 2^{n-1}, n \in \mathbb{N}\}$ . También se puede expresar  $S_5 : a_n = 2^{n-1}$  con  $n \in \mathbb{N}$

## 4.2 Igualdad de sucesiones

### Definición

Dos sucesiones son iguales si y sólo si coinciden sus valores término a término. Simbólicamente:

$$(a_n) = (b_n) \Leftrightarrow a_n = b_n, \forall n$$

### Ejemplo 4.2

Las sucesiones generadas por las fórmulas  $a_n = (-1)^n$  y  $b_n = (-1)^{2+n}$  con  $n \in \mathbb{N}$  son iguales. En ambos casos los términos son  $-1, 1, -1, 1, -1, \dots$

### Actividad 4.1

Dar el valor de verdad de las siguientes afirmaciones, justificando su respuesta:

- El conjunto correspondiente a la sucesión 1 , 1 , 1 , 1 , 1 es {1}
- Si  $a_n = (-2)^{2n}$  con  $n \in \mathbb{N}$  es una sucesión infinita y su conjunto correspondiente es {2}
- La sucesión 2 , 4 , 6 , ... , 12 es finita y está formada por 6 términos
- Las sucesiones  $a_n = (-2)^{2n}$  y  $b_n = 2^{2n}$  con  $n \in \mathbb{N}$  son iguales

## 4.3 Sucesiones particulares

### 4.3.1 Arreglos

#### Definición

Un arreglo es una sucesión de posiciones de memoria o celdas vacías que pueden ser llenadas por cualquier elemento de un conjunto

Sea  $S$  el arreglo, el elemento asignado a la posición  $n$  será denotado por  $S(n)$ , y a la sucesión  $S(1), S(2), S(3), \dots$  se la llamará sucesión de valores del arreglo  $S$ . La sucesión se considera como un objeto bien definido, aun cuando algunas de las posiciones no se les haya asignado valores o si se cambian algunos valores durante la discusión.

### 4.3.2 Palabras

Para generar palabras se necesita disponer de un alfabeto que es un conjunto no vacío de símbolos cualesquiera, que se designa con la letra  $\Sigma$ .

#### Definiciones

- Palabra, cadena o strings es cualquier sucesión de símbolos del alfabeto  $\Sigma$ .

La cantidad de símbolos que integran la palabra es conocida como la longitud de la misma. La palabra vacía o cadena vacía, la que no contiene símbolos, se designa por la letra griega  $\lambda$ , cuya longitud  $|\lambda| = 0$

El conjunto de palabras generadas por símbolos del alfabeto  $\Sigma$ , se denomina Lenguaje, y se denota  $L$ .

El lenguaje vacío es aquel que no contiene palabras:  $L = \{\}$ , y no es lo mismo que el lenguaje formado por la palabra vacía,  $L_\lambda = \{\lambda\}$ .

El Conjunto de todas las palabras generadas por  $\Sigma$ , se denomina Lenguaje Universal y se denota con  $\Sigma^*$

En el contexto de  $\Sigma^*$ ,  $\Sigma$  representa el alfabeto como lenguaje unisimbólico, eso

significa que las palabras son de un solo símbolo que se corresponden con los símbolos del alfabeto.

Donde  $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \dots \cup \Sigma^\infty$  (Estrella de Kleene)

### □ Ejemplo 4.3

Sea el alfabeto  $\Sigma = \{a, b, c\}$  entonces el lenguaje universal generado por  $\Sigma$  es  $\Sigma^* = \{\lambda, a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, aab, \dots\}$  y por lo tanto se tiene que  $w_1 = aabccc; w_2 = abcc$  y  $w_3 = ccbacba$  pertenecen a  $\Sigma^*$

### Actividad 4.2

Sea el alfabeto  $\Sigma = \{a,b,c\}$ , responder verdadero o falso, y justificar la respuesta

a)  $aaaa \in \Sigma^* \wedge aaa+aabaca \in \Sigma^*$

b) Sea  $L_1 = \{x / x$  es la palabra vacía o es una palabra de longitud 2 generada por el alfabeto  $\Sigma\}$  entonces  $|L_1| = 10$

c) Si  $L_2 = \{x / x$  es una palabra de long. 3 y de símbolos distintos} entonces  $|L_2| = 27$ .

## 4.4 Sucesiones Numéricas

### ➲ Definición

Una sucesión numérica es aquella función cuyo dominio son los naturales y el conjunto de llegada es cualquier subconjunto de los números reales. Simbólicamente

$$S: \mathbb{N} \rightarrow \mathbb{R}$$

### □ Ejemplos 4.4

a)  $(a_n): 1, 4, 9, 16, 25, \dots$  sucesión de los cuadrados de los números naturales.

b)  $(b_n): 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \dots$  sucesión de los inversos de los números naturales.

## Definición

Se dice que una sucesión ( $a_n$ ) está dada por su forma explícita, cuando el término general se expresa mediante una fórmula que depende del índice  $n$  (la posición).

## Ejemplo 4.5

Para encontrar la fórmula explícita de la sucesión dada por:  $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots$  una buena sugerencia es asociar a cada valor de la sucesión con el subíndice correspondiente. Entonces si se denota a la sucesión  $a_1, a_2, a_3, \dots$  se tendrá:

$$a_1 = 1 ; a_2 = \frac{1}{2} ; a_3 = \frac{1}{4} ; a_4 = \frac{1}{8} ; \dots$$

Se observa que el numerador es siempre 1 y en el denominador aparecen las potencias de 2 comenzando con la potencia de exponente cero.

$$a_1 = \frac{1}{2^0} ; a_2 = \frac{1}{2^1} ; a_3 = \frac{1}{2^2} ; a_4 = \frac{1}{2^3} ; \dots$$

Entonces se puede expresar a cada término en función del subíndice del mismo ya que el valor del exponente es el natural anterior al subíndice:

$$a_1 = \frac{1}{2^{1-1}} ; a_2 = \frac{1}{2^{2-1}} ; a_3 = \frac{1}{2^{3-1}} ; a_4 = \frac{1}{2^{4-1}} ; \dots$$

Por lo tanto se puede escribir el término general del siguiente modo:

$$a_n = \frac{1}{2^{n-1}}, n \in \mathbb{N}$$

## Observaciones

En el Ejemplo 4.5 también hubiera sido válido representar a la sucesión comenzando en  $a_0$  de tal modo que:

$$a_0 = 1 ; a_1 = \frac{1}{2} ; a_2 = \frac{1}{4} ; a_3 = \frac{1}{8} ; \dots$$

con lo cual la fórmula del término general sería

$$a_n = \frac{1}{2^n} , \quad n \in \mathbb{N}_0$$

Se puede observar que las fórmulas explícitas no son únicas y que iniciar a  $n$  en cero puede llevarnos a una forma más simple.

#### 4.4.1 Progresión Aritmética

##### Definición

Una progresión aritmética es una sucesión numérica donde cada término, salvo el primero, se obtiene sumando una constante al anterior. A dicha constante se le dice diferencia de la progresión y se denota  $d$ .

El término general de una progresión aritmética es:

$$a_n = a_1 + d(n - 1) , \quad n \in \mathbb{N}$$

donde  $a_1$  es el primer término y  $d$  es la diferencia.

##### Ejemplos 4.6

- a) El término general de la progresión aritmética ( $a_n$ ): 3, 7, 11, 15, .... donde el primer término es 3 y la diferencia 4 es

$$a_n = 3 + 4(n - 1) , \quad n \in \mathbb{N}$$

- b) El término general de la progresión aritmética ( $a_n$ ): -3, -5, -7, -9, .... donde el primer término es -3 y la diferencia -2 es

$$a_n = -3 - 2(n - 1) , \quad n \in \mathbb{N}$$

- c) Hay sucesiones que no son aritméticas porque son de signos alternados pero, configurando el signo con una potencia de -1, el valor absoluto de los valores responde a una sucesión aritmética. Es el caso de la progresión aritmética ( $a_n$ ): -3, 7, -11, 15, -19, .... cuyo término general se puede expresar

$$a_n = (-1)^n[3 + 4(n - 1)] , \quad n \in \mathbb{N}$$

- d) En Matemática Financiera es muy frecuente utilizar sucesiones numéricas.

Por ejemplo, para determinar el alquiler  $A$ , de una casa donde se acuerda pagar \$ 9000 al mes durante el primer año, y en donde cada año aumentará el alquiler en \$ 500 mensuales más. ¿Cuánto se pagará mensualmente al cabo de 4 años? ¿Cuánto se pagará al cabo de  $n$  años?

En el 1º año:  $A_1 = 9000$

2º año:  $A_2 = 9000 + 500$

3º año:  $A_3 = 9000 + 500 + 500 = 9000 + 2 \cdot 500$

4º año:  $A_4 = 9000 + 500 + 500 + 500 = 9000 + 3 \cdot 500 = 10500$

Al cabo de  $n$  años:  $A_n = 9000 + (n - 1)500$ ,  $n \in \mathbb{N}$

#### 4.4.2 Progresión Geométrica

##### Definición

Una progresión geométrica es una sucesión numérica donde cada término, salvo el primero, se obtiene multiplicando el término anterior por una constante. A dicha constante se le llama razón y se denota como  $r$ .

El término general de una progresión geométrica es:

$$a_n = a_1 \cdot r^{n-1}, \quad n \in \mathbb{N}$$

donde  $a_1$  es el primer término y  $r$  la razón.

##### Ejemplos 4.7

- a) El término general de la progresión geométrica  $(a_n)$ : 2, 6, 18, 54, ... donde el primer término es 2 y la razón es 3 es

$$a_n = 2 \cdot 3^{n-1}, \quad n \in \mathbb{N}$$

- b) El término general de la progresión geométrica  $(b_n)$ : 1,  $\frac{1}{2}$ ,  $\frac{1}{4}$ ,  $\frac{1}{8}$ , ...

donde el primer término es 1 y la razón es  $\frac{1}{2}$  es

$$b_n = \left(\frac{1}{2}\right)^{n-1}, \quad n \in \mathbb{N}$$

- c) Volviendo al contexto de la Matemática Financiera, si se supone que el propietario y el inquilino pactan un alquiler inicial de \$9000 y que cada año se aumentará un 5% ¿Cuánto se pagará mensualmente al cabo de 4 años? Y ¿Cuánto se pagará al cabo de  $n$  años?

El cálculo sería el siguiente:

$$\text{En el } 1^{\circ} \text{ año: } A_1 = 9000$$

$$2^{\circ} \text{ año: } A_2 = 9000 + 0,05 \cdot 9000 = 9000 \cdot (1 + 0,05) = 9000 \cdot 1,05$$

$$3^{\circ} \text{ año: } A_3 = 9000 \cdot 1,05 + 0,05 \cdot 9000 \cdot 1,05 = 9000 \cdot 1,05(1 + 0,05) = 9000 \cdot 1,05^2$$

$$4^{\circ} \text{ año: } A_4 = 9000 \cdot 1,05^2 + 0,05 \cdot 9000 \cdot 1,05^2 = 9000 \cdot 1,05^3$$

$$\text{Al cabo de } n \text{ años: } A_n = 9000 \cdot 1,05^{n-1}, \quad n \in \mathbb{N}$$

### Actividad 4.3

- a) Escribir los 6 primeros términos de las sucesiones y luego el término general:
- i) A cada número natural  $n$  le corresponde el cuadrado de su siguiente
  - ii) A cada número natural  $n$  le corresponde el siguiente de su cuadrado
  - iii) A cada número natural  $n$  le corresponde su triple disminuido 1
- b) Para cada sucesión, encontrar su término general:
- |  |                                  |
|--|----------------------------------|
| i) 2, 7, 12, 17, 22, ...                                       | ii) -5, -13, -21, -29, ...       |
| iii) 1, -1, 1, -1, 1, -1, ...                                  | iv) -2, 2, -2, 2, -2, 2, -2, ... |
| v) $10, 1, \frac{1}{10}, \frac{1}{100}, \frac{1}{1000}, \dots$ | vi) 3, -9, 27, -81, ...          |

### 4.5 Símbolo Suma

De ahora en adelante, solo por una cuestión de conveniencia de notación se representará a las sucesiones usando al subíndice  $k$ .

En algunas situaciones puede ser interesante sumar los términos de una sucesión. Por ejemplo si se quiere sumar los seis primeros términos de la

sucesión  $a_k = 3k - 2$ , con  $k \in \mathbb{N}$  se tendrá:

$$(3.1 - 2) + (3.2 - 2) + (3.3 - 2) + (3.4 - 2) + (3.5 - 2) = 1 + 4 + 7 + 10 + 13$$

Ahora si se quiere sumar los  $n$  primeros términos la suma sería

$$(3.1 - 2) + (3.2 - 2) + (3.3 - 2) + \dots + (3.k - 2) = 1 + 4 + 7 + 10 + \dots + (3.n - 2)$$

Esta expresión se lee, diciendo: “Es la suma de los términos de la sucesión  $a_k = 3k - 2$ , con  $k = 1, 2, \dots, n$ ”

Si se tiene una suma tal que la cantidad de términos es grande al punto de que genera incomodidad expresarla entera, ¿se la podría simplificar aprovechando que los términos corresponden a una sucesión? La respuesta es sí, y es por medio de la notación Sigma.

### ☞ Definición

El símbolo Suma, representado por la letra griega Sigma ( $\Sigma$ ), se usa para representar la suma de los  $n$  primeros términos de una sucesión de término general  $a_k$ . Se escribe:

$$a_1 + a_2 + a_3 + \dots + a_n = \sum_{k=1}^n a_k$$

Se lee: “Suma de los  $a_k$  desde  $k = 1$  hasta  $k = n$ ”

A los números 1 y  $n$ , se les llama respectivamente “límite inferior” y “límite superior” de la suma, a  $a_k$  se llama “término general” de la suma,  $k$  recibe el nombre de “índice de la suma” y toma todos los valores enteros consecutivos desde el límite inferior hasta el límite superior.

### ☞ Observaciones

- El límite inferior del subíndice puede ser cualquier otro valor  $m$  siempre que  $m < n$ . Y en este caso, la cantidad de términos de  $\sum_{k=m}^n a_k$  es  $n - m + 1$ .

- El valor de una suma no depende de la letra que se use como índice. Es decir, será lo mismo:

$$\sum_{k=m}^n a_k = \sum_{i=m}^n a_i = \sum_{j=m}^n a_j$$

- El índice puede ocupar cualquier posición en el término general de una suma.
- Se pueden sacar términos de una sumatoria lo cual sería consecuencia de la propiedad asociativa de la suma. Esto es

$$\sum_{k=1}^n a_k = a_1 + \sum_{k=2}^n a_k = \sum_{k=1}^{n-1} a_k + a_n$$

### □ Ejemplos 4.8

- a) La suma de los términos de la sucesión  $a_k = 3k$  con  $k = 1, 2, \dots, 7$  se puede expresar de dos maneras:

$$3 + 6 + 9 + 12 + 15 + 18 + 21 \quad o \quad \sum_{k=1}^7 3k$$

- b) La suma de los términos de la sucesión  $a_k = \frac{k}{k+1}$  con  $k = 1, 2, \dots, 6$  se puede expresar de dos maneras:

$$\frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \frac{4}{5} + \frac{5}{6} + \frac{6}{7} \quad o \quad \sum_{k=1}^6 \frac{k}{k+1}$$

- c) La suma de los términos de la sucesión  $a_k = 5(-1)^k \cdot 2^k$  con  $k = 0, 1, \dots, 5$  se puede expresar de dos maneras:

$$5 - 10 + 20 - 40 + 80 - 160 \quad o \quad \sum_{j=0}^5 5(-1)^j \cdot 2^j$$

#### Actividad 4.4

a) Decir cuántos términos tienen las siguientes sumas y luego desarrollar a las mismas:

i)  $\sum_{j=1}^{n-1} \left(\frac{1}{2}\right)$

ii)  $\sum_{k=2}^{20} (3k-2)$

iii)  $\sum_{i=3}^n (-2)^i$

b) Usar el símbolo  $\Sigma$  para representar a las siguientes sumas considerando que ambas tienen n términos

i)  $\frac{5}{4} + \frac{7}{9} + \frac{9}{16} + \frac{11}{25} + \dots$

ii)  $(a + \sqrt{b}) + (a + 2\sqrt{b}) + (a + 3\sqrt{b}) + (a + 4\sqrt{b}) + (a + 5\sqrt{b}) + \dots$

iii)  $(1 + \sqrt{b}) + (2 + 3\sqrt{b}) + (3 + 5\sqrt{b}) + (4 + 7\sqrt{b}) + (5 + 9\sqrt{b}) + \dots$

#### 4.6 Inducción Matemática

Peano G.(1858–1932) propuso cinco propiedades fundamentales que caracterizan a los números naturales, conocidos como Axiomas de Peano. Una de ellas es el Principio de Inducción Matemática que es actualmente una herramienta de uso práctico y teórico principalmente para matemáticos y personas que trabajan en Ciencias Computacionales.

La inducción matemática es un método de demostración que se utiliza cuando se trata de establecer la veracidad de una lista infinita de proposiciones. El método es bastante natural para usarse en una variedad de situaciones en la ciencia de la computación. Algunas aplicaciones tienen un sabor muy matemático, tal como verificar que todo entero positivo satisface cierta fórmula. Otra utilización frecuente es la de demostrar que un programa de computación o que un algoritmo con ciclos funciona como se espera.

## Principio de Inducción Matemática

Supóngase que  $n, n_0 \in \mathbb{Z}$  y sea  $P(n)$  una propiedad de sobre  $n$

Si se cumplen las siguientes condiciones:

- a)  $P(n_0)$  es verdadera (Paso básico)
- b)  $P(k) \Rightarrow P(k + 1), \forall k \geq n_0$  (Paso inductivo)

Entonces  $P(n)$  es verdadera  $\forall n \geq n_0$  con  $n, n_0 \in \mathbb{Z}$

¿Cuál es la idea detrás del Principio de Inducción?

La misma que la del famoso juego que se construye con las fichas de dominó, las cuales están ubicadas una detrás de otra, todas a la misma distancia. Si se hace caer la primera, caen todas.



Fig. 4.2. Efecto dominó.

### Ejemplo 4.9

Para demostrar que  $\sum_{i=1}^n i = \frac{n(n+1)}{2}, \forall n \in \mathbb{N}$  (la suma de “ $n$ ” números naturales consecutivos está dada por el semiproducto de “ $n$ ” por su sucesor) se procede del siguiente modo:

1° Paso (o paso base): Se demuestra que la igualdad vale para  $n = 1$

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

$$1 = \frac{1 \cdot 2}{2}$$

$$1 = 1$$

2° Paso (paso inductivo): Se demuestra que la igualdad se cumple para el

siguiente de cualquier entero. Esto significa probar la implicación lógica:

$$P(k) \Rightarrow P(k+1), \forall k \in \mathbb{N}$$

Por lo tanto se debe partir de suponer que se cumple  $P(k), \forall k$

$$\sum_{i=1}^k i = \frac{k(k+1)}{2}$$

Y se debe demostrar que se cumple  $P(k+1), \forall k$ . Esto es hay que probar la siguiente igualdad

$$\underbrace{\sum_{i=1}^{k+1} i}_{I} = \underbrace{\frac{(k+1)(k+2)}{2}}_{II}$$

Si se designa al primer miembro  $I$  y al segundo miembro  $II$ , hay que demostrar que  $I = II$ . Para ello, se podría trabajar con los dos miembros por separado.

$$\begin{aligned} I &= \sum_{i=1}^{k+1} i = \sum_{i=1}^k i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k^2 + k + 2k + 2}{2} = \frac{k^2 + 3k + 2}{2} \\ II &= \frac{(k+1)(k+2)}{2} = \frac{k^2 + k + 2k + 2}{2} = \frac{k^2 + 3k + 2}{2} \end{aligned}$$

Se observa que  $I = II$

Por lo tanto queda demostrado que

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}, \quad \forall n \in \mathbb{N}$$

#### Actividad 4.5

Interpretar la siguiente igualdad y demostrarla

$$\sum_{i=1}^n (3i - 1) = \frac{n(3n + 1)}{2}, \quad \forall n \in \mathbb{N}$$

## 4.7 Recursión o Recursividad

### Definición

Una función se dice recursiva si hace referencia a ella misma. Esto es, para calcular un nuevo valor, necesita de valores anteriores de la misma función.

### Ejemplo 4.10

El factorial de un número natural está dado por

$$n! = n \cdot (n - 1)! \quad \forall n \in \mathbb{N} \quad \text{con} \quad 0! = 1.$$

Observar que, por ejemplo, en el caso de  $6!$  se necesita el valor de  $5!$  ya que  $6! = 6 \cdot 5!$  lo que nos lleva a necesitar el valor de  $4!$ , ya que  $5! = 5 \cdot 4!$  y así sucesivamente se tendrá que

$$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$

Por lo expuesto se deduce que la función factorial es recursiva.

En general existen sucesiones que pueden definirse en forma recursiva, de tal modo que cada término haga referencia a los términos anteriores

### Definición

Se dice que una sucesión  $(a_n)$  está dada por una fórmula recursiva (o es recurrente de orden  $k$ ) cuando se especifican los primeros  $k$  términos de la sucesión,  $a_1, a_2, \dots, a_k$  y luego a partir del término  $a_{k+1}$ , todos los términos de la sucesión se pueden obtener a partir de los  $k$  anteriores mediante alguna relación aritmética.

A los primeros  $k$  términos de la sucesión, se les llama condiciones iniciales o condiciones de frontera de la sucesión.

Simbólicamente, dada una función  $f: \mathbb{R}^k \rightarrow \mathbb{R}$  y  $k$  valores a priori,  $a_1, a_2, \dots, a_k$ , se define una sucesión recurrente de orden  $k \in \mathbb{N}$  de la siguiente manera:

$$\begin{cases} a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-k}), & n \geq 1 \\ a_1, a_2, \dots, a_k \text{ son conocidos} & \end{cases} \quad \begin{array}{l} \text{(ley de recurrencia)} \\ \text{(condiciones iniciales)} \end{array}$$

## Observaciones

- La fórmula que define a las sucesiones en forma recursiva recibe el nombre de relación de recurrencia, ecuación de recurrencia o ecuación en diferencias.
- El número de condiciones iniciales:  $k$ , puede ser cualquiera, pero siempre como mínimo 1

## Ejemplos 4.11

- a) La fórmula recursiva de la sucesión aritmética 2, 4, 6, 8, 10,... es:

$$\begin{cases} a_1 = 2 \\ a_n = a_{n-1} + 2, \quad n \geq 2 \end{cases}$$

- b) La fórmula recursiva de la sucesión aritmética 3, 8, 13, 18, 23,... es

$$\begin{cases} b_1 = 3 \\ b_n = b_{n-1} + 5, \quad n \geq 2 \end{cases}$$

- c) La fórmula recursiva de la progresión geométrica 3, 9, 27, 81,... es

$$\begin{cases} b_1 = 3 \\ b_n = b_{n-1} \cdot 3, \quad n \geq 2 \end{cases}$$

- d) Los primeros cinco términos de la sucesión:

$$\begin{cases} c_1 = 1 \\ c_2 = 1 \\ c_n = c_{n-1} + c_{n-2}, \quad n \geq 3 \end{cases}$$

son 1, 1, 2, 3, 5, 8, 13, 21, ... (sucesión de Fibonacci)

Posteriormente, se estudiará las relaciones de recurrencia por su utilidad en matemáticas y sobre todo en informática. El objetivo será, no sólo de obtener o plantear esas relaciones, sino además resolverlas, encontrar la fórmula explícita correspondiente.

### Actividad 4.6

- a) Encontrar los seis primeros términos de la sucesión definida por

$$\begin{cases} c_n = -2c_{n-1} & , \quad \forall n \in \mathbb{N}, \quad n \geq 2 \\ c_1 = 5 & \end{cases}$$

- b) Encontrar la forma recursiva de la sucesión dada por

i)  $a_n = -2n + 5$  ,  $\forall n \in \mathbb{N}$

ii)  $a_n = (-2)^n$  ,  $\forall n \in \mathbb{N}_0$

- c) Encontrar la fórmula recursiva de las siguientes sucesiones:

i) -1 , 1 , -1 , 1 , -1 , 1 ...

ii) 3 , 6 , 12 , 24 , ...

#### 4.7.1 Solución de una relación de recurrencia

##### Definición

Una sucesión recibe el nombre de solución de la relación de recurrencia si su término general, expresado mediante la fórmula explícita, verifica dicha relación y a sus condiciones iniciales.

##### Ejemplos 4.12

- 1) Sean las sucesiones

$$S_1: 2, 8, 32, 128, \dots \quad \text{y} \quad S_2: 3, 12, 48, 192, \dots$$

Observar que en las dos sucesiones, cada término se obtiene del término anterior multiplicándolo por 4. En ambos casos la relación de recurrencia que las identifica es:  $a_n = 4 a_{n-1}$

Sin embargo las sucesiones no son las mismas dado que difieren en el valor inicial. Para  $S_1$ ,  $a_1 = 2$  y para  $S_2$ ,  $a_1 = 3$ .

Las fórmulas recursivas son:

$$S_1: \begin{cases} a_1 = 2 \\ a_n = 4 a_{n-1} \end{cases} \quad \text{y} \quad S_2: \begin{cases} a_1 = 3 \\ a_n = 4 a_{n-1} \end{cases}$$

Si se expresan los cuatro primeros términos de cada una de las sucesiones se tiene:

Para  $S_1$

$$a_1 = 2$$

$$a_2 = 2 \cdot 4$$

$$a_3 = 2 \cdot 4 \cdot 4 = 2 \cdot 4^2$$

$$a_4 = 2 \cdot 4 \cdot 4 \cdot 4 = 2 \cdot 4^3$$

Para  $S_2$

$$a_1 = 3$$

$$a_2 = 3 \cdot 4$$

$$a_3 = 3 \cdot 4 \cdot 4 = 3 \cdot 4^2$$

$$a_4 = 3 \cdot 4 \cdot 4 \cdot 4 = 3 \cdot 4^3$$

De aquí se induce que las soluciones generales de las sucesiones  $S_1$  y  $S_2$  son, respectivamente:

$$a_n = 2 \cdot 4^{n-1} \quad \forall n \in \mathbb{N}$$

y

$$a_n = 3 \cdot 4^{n-1} \quad \forall n \in \mathbb{N}$$

2) Se quiere verificar que  $a_n = 3n + 6$ ,  $\forall n \in \mathbb{N}_0$  es solución de la relación de recurrencia  $a_n = 2a_{n-1} - a_{n-2}$  con las condiciones iniciales  $a_0 = 6$  y  $a_1 = 9$

Considerando que  $a_n = 3n + 6$  se tendrá que

$$a_0 = 3 \cdot 0 + 6 = 6$$

$$a_1 = 3 \cdot 1 + 6 = 9$$

$$a_{n-1} = 3(n-1) + 6 = 3n + 3$$

$$a_{n-2} = 3(n-2) + 6 = 3n$$

Para verificar que  $a_n = 3n + 6$  satisface  $a_n = 2a_{n-1} - a_{n-2}$  se calcula previamente

$$a_{n-1} = 3(n-1) + 6 = 3n + 3$$

$$a_{n-2} = 3(n-2) + 6 = 3n$$

Y reemplazando

$$3n + 6 = 2 \cdot (3n + 3) - 3n$$

$$3n + 6 = 6n + 6 - 3n$$

$$3n + 6 = 3n + 6$$

Con lo cual se observa que la formula explícita de la función satisface la fórmula recursiva y por lo tanto es su solución.

### Actividad 4.7

1) Obtener la solución de la siguiente sucesión dada por su fórmula recursiva

$$a_n = -\frac{1}{2}a_{n-1}, \forall n \in \mathbb{N} \text{ con valor inicial } a_0 = 1$$

2) Determinar cuál de las siguientes fórmulas es la solución de la fórmula de recurrencia  $a_n = -7a_{n-1} - 10a_{n-2}, \forall n \in \mathbb{N}, n \geq 2$  con valores iniciales  $a_1 = 3$  y  $a_2 = -21$

- i)  $a_n = (-2)^n - (-5)^n, \forall n \in \mathbb{N}$
- ii)  $a_n = (-2)^n + (-5)^n, \forall n \in \mathbb{N}$

## 4.8 Clasificación de las Relaciones de Recurrencia

### Definición

- El orden de una relación de recurrencia es la mayor diferencia entre los subíndices de los elementos de la sucesión que figuran en la fórmula de recurrencia. Es decir, el orden indica cuantos términos anteriores hay que conocer para obtener uno nuevo.
- El grado de una relación de recurrencia es el mayor exponente al que están elevados los términos de la sucesión que figuran en la relación de recurrencia.
- Se dice que una relación de recurrencia es Homogénea si es satisfecha por la sucesión idénticamente nula,  $a_n = 0, \forall n$ . En caso contrario, se llama relación de recurrencia no homogénea.
- Se dice que una relación de recurrencia es de coeficientes constantes si ninguno de los coeficientes de los términos de la sucesión dependen de  $n$ . Por el contrario, si alguno depende de  $n$ , se dice que es una ecuación de coeficientes variables.

### □ Ejemplos 4.13

- a) La relación de recurrencia  $b_n = 2b_{n-1} + 3$  es de orden 1 porque diferencia entre  $n$  y  $n - 1$  es 1, grado 1 o lineal (exponentes 1), no homogénea pues  $b_n = 0$  no satisface la ecuación, y de coeficientes (los de los términos de la sucesión) constantes.
- b) La relación de recurrencia  $a_n = 2a_{n-1} + a_{n-2}$  es de orden 2, lineal, homogénea y de coeficientes constantes.
- c) La relación de recurrencia  $a_n^2 = a_{n-1} - 3$  es de orden 1, grado 2, no homogénea y coeficientes constantes.
- d) La relación de recurrencia  $2a_n = n^2 \cdot a_{n-2}$  es de orden 2, lineal, homogénea y de coeficientes variables.

### Actividad 4.8

Clasificar las siguientes relaciones de recurrencia:

- a)  $a_{n+1} = 4 \cdot a_n$
- b)  $c_n = \frac{1}{2}c_{n-1} - c_{n-2}$
- c)  $a_n = 4 \cdot a_{n-1} + 5$
- d)  $a_{n+1} + a_n^2 - 2na_{n-1} + 5a_{n-2} = 0$

A continuación se presentan dos teoremas por medio de los cuales se pueden encontrar las soluciones de dos tipos de relaciones de recurrencia muy frecuentes.

#### 4.8.1 Solución de las relaciones de recurrencia lineales, de primer orden, homogéneas y de coeficientes constantes.

##### ■ Teorema

Sea la sucesión  $(a_n)$  dada por su relación de recurrencia lineal, homogénea, de primer orden:  $a_n = k \cdot a_{n-1}$ , con  $k$  constante no nula y con condición inicial  $a_1$ .

En estos casos la solución general está dada por:

$$a_n = a_1 \cdot k^{n-1}, \quad \forall n \in \mathbb{N}$$

### Observación

Si la relación de recurrencia estuviera dada por  $a_n = k \cdot a_{n-1}$  con condición inicial  $a_0$  entonces la solución general estaría dada por:

$$a_n = a_0 k^n , \quad \forall n \in \mathbb{N}_0$$

### Ejemplos 4.14

- 1) La solución general de  $a_{n+1} = 3 \cdot a_n$  con el valor inicial  $a_0 = 2$  es

$$a_n = 2 \cdot 3^n , \quad \forall n \in \mathbb{N}_0$$

- 2) La relación de recurrencia  $3a_{n+1} - 5a_n = 0$  con  $a_1 = 4$  es equivalente a

$$a_{n+1} = \frac{5}{3}a_n \text{ tiene por solución general a } a_n = 4 \cdot \left(\frac{5}{3}\right)^{n-1} , \quad \forall n \in \mathbb{N}$$

### Actividad 4.9

Resolver las siguientes relaciones de recurrencia:

- a)  $a_{n+1} = -4 \cdot a_n$  con condición inicial  $a_0 = -1$   
b)  $c_n = \frac{1}{2}c_{n-1}$  con condición inicial  $c_1 = -2$

### 4.8.2 Solución de las relaciones de recurrencia lineal, de segundo orden, homogéneas y con coeficientes constantes

#### Teorema

Sea la sucesión  $(a_n)$  dada por su relación de recurrencia lineal, homogénea, de segundo orden, y de coeficientes constantes,

$$a_{n+2} + k_1 a_{n+1} + k_2 a_n = 0 , \quad \forall n \in \mathbb{N}$$

Si se consideran las raíces de la ecuación:  $x^2 + k_1x + k_2 = 0$ , llamada ecuación característica de la relación de recurrencia, se puede demostrar que la solución general será de alguno de los siguientes tipos:

- i)  $a_n = u \cdot r_1^n + v \cdot r_2^n , \quad \forall n$  en el caso de que la ecuación característica tenga

dos raíces reales y distintas,  $r_1$  y  $r_2$

ii)  $a_n = u \cdot r^n + n \cdot v \cdot r^n$ ,  $\forall n$  en el caso de que la ecuación característica tenga dos raíces reales e iguales,  $r_1 = r_2 = r$ .

En ambos casos son constantes a determinar dadas por las condiciones iniciales.

### □ Ejemplos 4.15

Resolver las siguientes relaciones de recurrencia:

1)  $a_n - 5a_{n-1} + 6a_{n-2} = 0$  con  $a_0 = 3$  y  $a_1 = 5$

Su ecuación característica es  $x^2 - 5x + 6 = 0$ , cuyas raíces son reales y distintas,  $r_1 = 2$  y  $r_2 = 3$

Entonces, por el teorema 4.10, la solución general es del tipo :  $a_n = u \cdot 2^n + v \cdot 3^n$  y ahora resta calcular  $u$  y  $v$  teniendo en cuenta las condiciones iniciales

$$\begin{aligned} a_0 = 3 &\Rightarrow u \cdot 2^0 + v \cdot 3^0 = 3 \Rightarrow \begin{cases} u + v = 3 \\ 2u + 3v = 5 \end{cases} \\ a_1 = 5 &\Rightarrow u \cdot 2^1 + v \cdot 3^1 = 5 \end{aligned}$$

Queda por resolver un sistema de dos ecuaciones lineales con dos incógnitas, del modo que el estudiante prefiera, cuya solución es:  $u = 4$  y  $v = -1$

Por lo tanto, la solución general de la relación de recurrencia:

$$a_n - 5a_{n-1} + 6a_{n-2} = 0 \text{ con } a_0 = 3 \text{ y } a_1 = 5 \text{ es: } a_n = 4 \cdot 2^n - 3^n, \quad \forall n \in \mathbb{N}_0$$

2)  $a_{n+2} = 4a_{n+1} - 4a_n = 0$  con  $a_1 = -3$  y  $a_2 = 2$

Su ecuación característica es  $x^2 - 4x + 4 = 0$  cuyas sus raíces son reales e iguales,  $r = 2$ . Entonces, por el teorema 4.10, la solución general es del tipo:

$a_n = u \cdot 2^n + n \cdot v \cdot 2^n$ , a continuación se calcula  $u$  y  $v$  teniendo en cuenta las condiciones iniciales:

$$\begin{aligned} a_1 = -3 &\Rightarrow u \cdot 2^1 + 1 \cdot v \cdot 2^1 = -3 \Rightarrow \begin{cases} 2u + 2v = -3 \\ 4u + 8v = 2 \end{cases} \\ a_2 = 2 &\Rightarrow u \cdot 2^2 + 2 \cdot v \cdot 2^2 = 2 \end{aligned}$$

Resolviendo el sistema se determina que:  $u = -\frac{7}{2}$  y  $v = 2$

Por lo tanto, la solución general de la relación de recurrencia:

$$a_{n+2} = 4a_{n+1} - 4a_n = 0 \text{ con } a_1 = -3 \text{ y } a_2 = 2 \text{ es}$$

$$a_n = -\frac{7}{2} \cdot 2^n + 2n \cdot 2^n , \quad \forall n \in \mathbb{N}$$

### Observación

Note que, por medio de las propiedades de la potenciación y del producto la solución anterior, también se la puede escribir como:

$$a_n = -\frac{7}{2} \cdot 2^n + n \cdot 2^{n+1} , \quad \forall n \in \mathbb{N}$$

O bien:

$$a_n = 2^n \left( -\frac{7}{2} + 2n \right) , \quad \forall n \in \mathbb{N}$$

### Actividad 4.10

Encontrar la solución general para las siguientes relaciones de recurrencia:

- 1)  $a_n - a_{n-1} + 6a_{n-2} = 0$  con  $a_1 = 1$  y  $a_2 = 3$
- 2)  $c_n - 6c_{n-1} + 9c_{n-2} = 0$  con  $c_0 = 1$  y  $c_1 = 2$
- 3)  $a_{n+2} - \frac{5}{2}a_{n+1} - \frac{3}{2}a_n = 0$  con  $a_0 = -1$  y  $a_1 = 1$



# MATEMÁTICA DISCRETA

UTN – FRT

## Capítulo 5. GRAFOS Y DIGRAFOS. ÁRBOLES

Grafo. Subgrafo.

Caminos, Circuitos y Ciclos.

Representaciones matriciales

Grafos Especiales.

Grafos conexos.

Caminos y Circuitos de Euler.

Caminos y Ciclos de Hamilton.

Árbol no dirigido.

Digrafo o Grafo dirigido.

Caminos y Circuitos en Digrafos.

Representaciones matriciales.

Árbol Dirigido y Árbol con raíz.

Árboles binarios. Recorridos.

Notaciones Prefija, Infija y Posfija.



## Introducción

El ser humano, ante el planteo de un problema, tiende a hacer un diagrama en el que representa por medio de puntos (o círculos) las actividades a realizar, o las etapas de un proyecto, localidades o individuos, etc. uniéndolos por medio de líneas o arcos indicando alguna relación entre ellos. Por ejemplo:

- Un ingeniero dibuja un diagrama de una malla eléctrica,
- Un químico realiza un esquema para mostrar cómo se unen mediante enlaces químicos los átomos de una compleja molécula,
- Un comandante del ejército traza en un mapa una red de líneas de suministros,
- Un sociólogo desarrolla en un elaborado diagrama la estructura de poder de una gran empresa,

Así, diferentes problemáticas asociadas a distintas disciplinas dieron lugar a esta teoría.

En sus comienzos, desde un punto de vista matemático, la Teoría de Grafos parecía bastante insignificante, puesto que se ocupaba principalmente de pasatiempos y rompecabezas. El primer artículo científico, fue escrito en 1736 por el matemático suizo L. Euler (1707-1783) en el conocido acertijo de los puentes de Königsberg. En 1936 el matemático alemán D. König bautizó a estos diagramas con el nombre de “grafos” e hizo un estudio sistemático de sus propiedades.

### 5.1 Grafo no dirigido

#### Definición

Dados dos conjuntos finitos  $V$  y  $A$  se llama grafo a toda terna  $G = (V, A, \phi)$  tal que:

- i)  $V \neq \emptyset$ ,    ii)  $\phi : A \rightarrow V^{(2)}$ , donde  $V^{(2)} = \{H \subseteq V, |H| = 1 \text{ o } |H| = 2\}$

A los elementos del conjunto  $V$  se les llama vértices o nodos y a los elementos del conjunto  $A$  se les llama aristas o lados.

A  $\phi$  se le llama función de incidencia y establece la correspondencia entre

cada arista y un subconjunto de uno o dos vértices.

### Casos particulares

- Si  $|V| = 1$  y  $A = \emptyset$ , a  $G$  se le llama grafo trivial
- +Si  $|V| = n$  y  $A = \emptyset$ , a  $G$  se le llama grafo vacío

### Representación gráfica

La representación gráfica de un grafo consiste en representar: a los elementos del conjunto  $V$ , por medio de puntos o círculos; al conjunto  $A$  y a la función de incidencia  $\varphi$  de tal manera que si a una arista le corresponden dos vértices, éstos estarán unidos por una línea que representa a la arista; y en el caso en que le corresponda a la arista solo un vértice se lo indicara por medio de una línea que entre y salga del vértice.

En la Figura 5.0 se representa la existencia de dos aristas  $a_1$  y  $a_2$  tal que  $\varphi(a_1) = \{u, v\}$  y  $\varphi(a_2) = \{v\}$

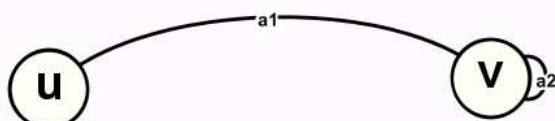


Fig. 5.0. Representación de vértices y aristas

### Ejemplo 5.1

Sea  $G = (V, A, \varphi)$  donde  $V = \{v_1, v_2, v_3, v_4\}$ ,  $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$  y  $\varphi$  dada por la tabla 5.1

| $a_i$          | $a_1$          | $a_2$          | $a_3$          | $a_4$          | $a_5$          | $a_6$     |
|----------------|----------------|----------------|----------------|----------------|----------------|-----------|
| $\varphi(a_i)$ | $\{v_1, v_2\}$ | $\{v_3, v_4\}$ | $\{v_1, v_3\}$ | $\{v_2, v_4\}$ | $\{v_2, v_1\}$ | $\{v_2\}$ |

Tabla 5.1. Función  $\varphi$  de Ejemplo 5.1.

Para el diseño del grafo se eligen, en el plano, ubicaciones arbitrarias para los vértices y formas cualesquiera para las aristas.

La Figura 5.1 es la representación de G

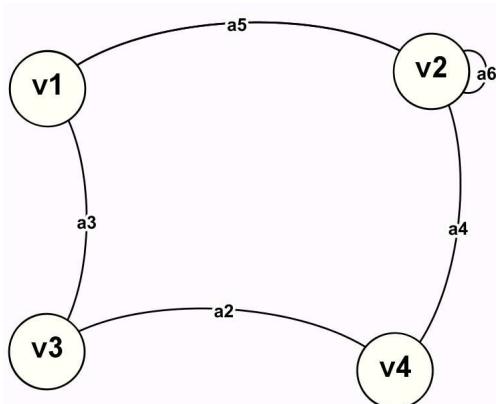


Fig. 5.1. Representación del Grafo de Ejemplo 5.1.

### Observación

Los conceptos geométricos como posición, longitud y formas no tienen importancia en el tema de grafos.

A partir de aquí se presentan una serie de definiciones relativas a vértices y aristas.

### Definiciones

Sea  $G = (V, A, \varphi)$  un grafo y sean  $v_1, v_2 \in V, a_1, a_2 \in A$ .

- Si  $\varphi(a_1) = \{v_1, v_2\}$  se dice que  $v_1$  y  $v_2$  son los extremos de  $a_1$  y que  $a_1$  incide en  $v_1$  y  $v_2$ . También se dice de  $v_1$  y  $v_2$  que son adyacentes
- Si  $\varphi(a_1) = \{v_1\}$  se dice que  $a_1$  es un lazo o bucle.
- Si  $\varphi(a_1) = \varphi(a_2)$  entonces  $a_1$  y  $a_2$  se dicen aristas paralelas
- Si  $\varphi(a_1) \neq \varphi(a_2)$  y  $\varphi(a_1) \cap \varphi(a_2) \neq \emptyset$  entonces  $a_1$  y  $a_2$  se dicen aristas adyacentes
- Si un vértice no es adyacente a ningún otro se dice vértice aislado
- Si un grafo no posee lazos ni aristas paralelas se dice grafo simple

### Ejemplo 5.2

Observando el grafo dado por la Figura 5.1, se tiene que:

- $v_1$  es adyacente a  $v_2$  y  $v_3$ , mientras que  $v_2$  es adyacente a  $v_1$ ,  $v_4$  y a sí mismo.
- $a_1$  y  $a_5$  son aristas paralelas.
- El grafo no posee vértices aislados y como posee lazo y aristas paralelas no es un grafo simple.

### 5.1.1 Grado de un vértice

#### Definición

Sea un grafo  $G = (V, A, \varphi)$ . Se denomina grado o valencia de un vértice, y se denota  $g(v)$ , a la función  $g: V \rightarrow \mathbb{N}_0$  definida como la cantidad de aristas que inciden en  $v$ , contando los lazos por dos”

#### Observaciones

- Si  $g(v) = 0$  entonces  $v$  es un vértice aislado
- Si  $g(v) = 1$  de  $v$  se dice que es un vértice pendiente.

#### Propiedad de los grados de los vértices

Sea el grafo  $G = (V, A, \varphi)$ , entonces

$$\sum_{v \in V} g(v) = 2|A|$$

#### Observaciones

- La suma de los grados de los vértices es siempre par.
- El número de vértices de grado impar es un número par.

### Actividad 5.1

Sea  $G = (V, A, \varphi)$  donde  $V = \{a, b, c, d, e, f\}$ ,  $A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}\}$  y la función  $\varphi$  dada por la tabla 5.2

| $a_i$          | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ | $a_8$ | $a_9$ | $a_{10}$ | $a_{11}$ | $a_{12}$ |
|----------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|
| $\varphi(a_i)$ | {a,b} | {a,c} | {a,e} | {a,f} | {b,f} | {b,d} | {b,c} | {c,e} | {c,d} | {d,e}    | {d,f}    | {e,f}    |

Tabla 5.2. Función  $\varphi$  de Actividad 5.1.

Responder a cada una de las siguientes preguntas, y justificar la respuesta:

- a) ¿Es un grafo simple?
- b) ¿Cuáles son los vértices adyacentes a f?
- c) ¿Cuáles son las aristas adyacentes a  $a_7$ ?
- d) ¿Se verifica la propiedad de los grados?

## 5.2 Subgrafos

### Definición

Sea  $G = (V, A, \varphi)$  un grafo, se dice que  $G_1 = (V_1, A_1, \varphi_1)$  es un subgrafo del grafo  $G$  si: i)  $V_1 \subseteq V$ ; ii)  $A_1 \subseteq A$ , y iii)  $\varphi_1 = \varphi / A_1$  siendo  $\varphi_1$  es la restricción de la función  $\varphi$  al conjunto  $A_1$

### Observación

Si  $V_1 = V$ ,  $G_1$  recibe el nombre de subgrafo maximal.

### Ejemplo 5.3

Dada la Figura 5.2, observar que  $G_1$  es un subgrafo de  $G$ , dado que:

- i)  $V_1 = \{a, b, e\} \subseteq V = \{a, b, c, d, e, f\}$ ;
- ii)  $A_1 = \{a_1, a_4, a_6\} \subseteq A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}\}$  y
- iii)  $\varphi_1 = \varphi / A_1$

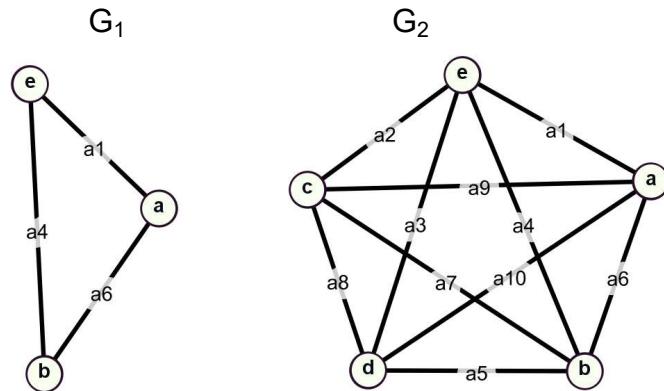


Fig. 5.2. G1 subgrafo de G

### 5.2.1 Subgrafos particulares

#### Definición

Sean  $G = (V, A, \varphi)$  un grafo,  $v \in V$  y  $a \in A$ :

- Si se suprime  $v$  y todas las aristas que inciden en él, el subgrafo restante se denota  $\tilde{G}_v$
- Si se suprime  $a$ , el subgrafo restante se denota  $\tilde{G}_a$
- Si  $B \subseteq V$ ,  $\tilde{G}_B$  es el subgrafo de  $G$  que resulta de eliminar todos los vértices de  $B$  y todas las aristas que inciden en ellos
- Si  $E \subseteq A$ ,  $\tilde{G}_E$  es el subgrafo de  $G$  que resulta de eliminar todas las aristas que pertenecen a  $E$ .

#### Ejemplo 5.4

Dado el grafo de la Figura 5.3

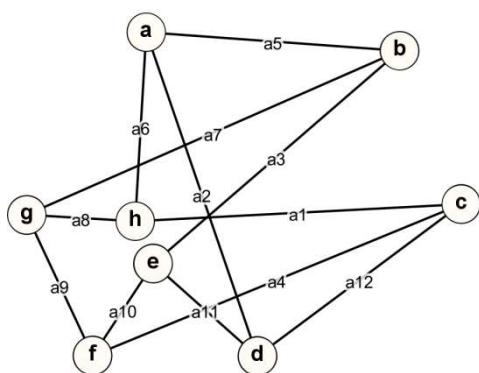


Fig. 5.3. Grafo del Ejemplo 5.4.

Los siguientes son subgrafos de él:

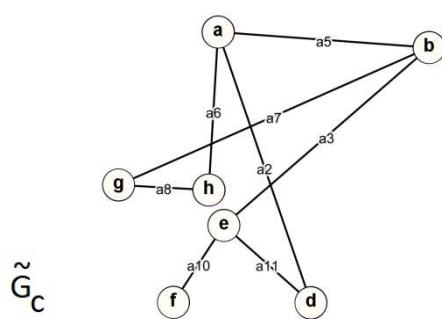


Fig. 5.4. Subgrafo  $\tilde{G}_c$ .

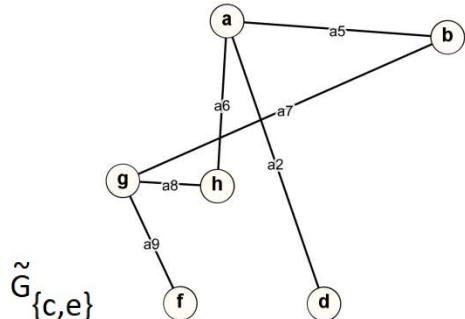


Fig. 5.5. Subgrafo  $\tilde{G}_{\{c,e\}}$ .

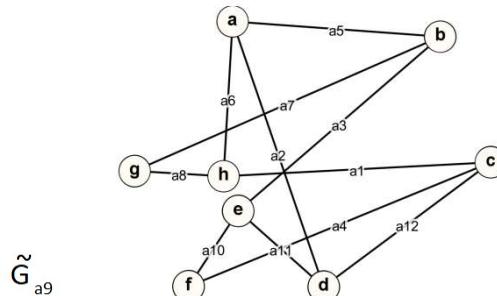


Fig. 5.6. Subgrafo  $\tilde{G}_{a_9}$ .

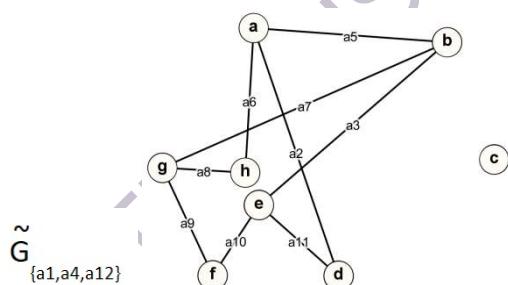


Fig. 5.7. Subgrafo  $\tilde{G}_{\{a_1,a_4,a_{12}\}}$ .

### Actividad 5.2

a) Dado el grafo  $G = (V, A, \varphi)$

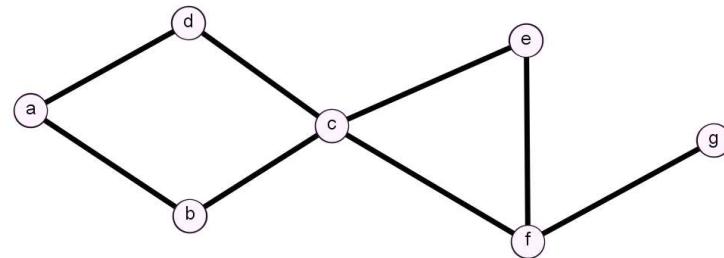


Fig. 5.8. Representación de  $G$ .

Obtener los siguientes subgrafos de  $G$ :

- i)  $\tilde{G}_c$
- ii)  $\tilde{G}_8$
- iii)  $\tilde{G}_{\{a,e,g\}}$
- iv)  $\tilde{G}_{\{4,5,6\}}$

a) Indicar si los siguientes grafos son subgrafos de  $G$

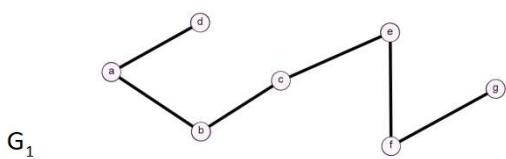


Fig. 5.9. Grafo  $G_1$ .

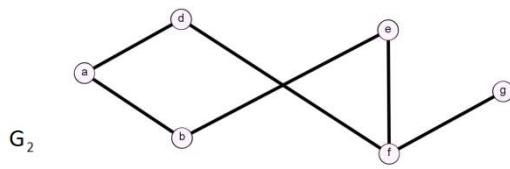


Fig. 5.10. Grafo  $G_2$ .

### 5.3 Caminos en un Grafo no Dirigido

#### Definiciones

- Dado un grafo  $G = (V, A, \varphi)$ , se denomina camino (o trayectoria) en  $G$  a una secuencia de  $n$  aristas para las cuales existe una secuencia de  $(n + 1)$  vértices tales que cada vértice es adyacente al siguiente.
- Longitud de un camino es la cantidad total de aristas intervenientes.
- Un camino es cerrado si el último vértice de la secuencia es igual al primero, en caso contrario el camino es abierto.

Simbólicamente al camino se lo expresa por medio de la secuencia de aristas involucradas,  $a_1, a_2, \dots, a_n$ ; o por la secuencia de vértices extremos de dichas aristas  $v_1, v_2, v_3, \dots, v_n, v_{n+1}$ . Es frecuente usar una notación simplificadora indicando al primer y último vértice:  $v_1 - v_{n+1}$

En el caso de que el camino involucre a aristas paralelas se lo debe indicar por medio de una secuencia alternada de vértices y aristas:

$$v_1, a_1, v_2, a_2, v_3, \dots, v_n, a_n, v_{n+1}$$

#### Ejemplo 5.5

Dado el siguiente grafo simple (Figura 5.11), se observa que hay dos caminos de longitud 2 desde el vértice 4 hasta el vértice 2, que se pueden representar como sucesiones de vértices: 4, 3, 2 y 4, 1, 2 o bien, como sucesiones de aristas:  $a_7, a_3$  y  $a_4, a_1$ , ambos de longitud 2.

Una pregunta interesante sería determinar ¿Cuántos caminos de longitud 5 que comienzan en el vértice 4 existen en el grafo?

Más adelante se verá un teorema que dará la respuesta.

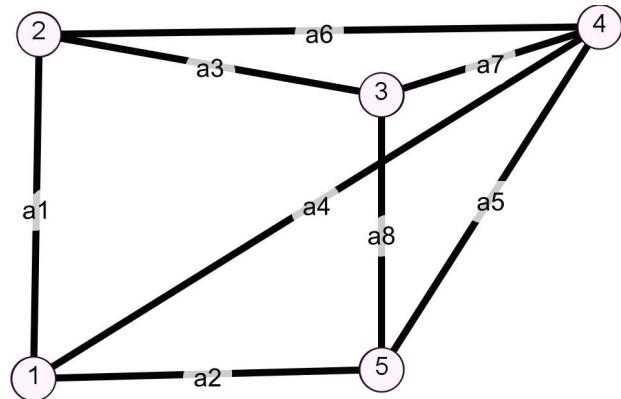


Fig. 5.11. Grafo Ejemplo 5.5.

### ☞ Definición

Se dice que un camino es simple si y sólo si no repite aristas.

### □ Ejemplos 5.6

Considerando el grafo de la Figura 5.11

- i) El camino 4 - 2 definido por los vértices: 4 , 3 , 5 , 1 , 4 , 2 es un camino simple de longitud 5.
- ii) El camino 4 - 2 definido por los vértices: 4 , 3 , 5 , 1 , 4 , 3 , 2 tiene longitud 6 pero no es un camino simple.

### ☞ Definición

Un camino se dice elemental si y sólo si es un camino simple sin vértices repetidos.

### ☞ Observación

- Una secuencia formada por un único vértice puede considerarse como un camino, camino simple o camino elemental de longitud cero.

- No existe una nomenclatura uniforme a la hora de definir los distintos tipos de caminos. Así, un camino simple recibe el nombre de path o trail, en inglés, un camino elemental puede designarse por simple path o path. Debido a esta variedad de conceptos se debe insistir en que al consultar distintas bibliografías, deberán considerarse las propias definiciones introducidas por cada autor.

### □ Ejemplo 5.7

Dado el siguiente grafo G:

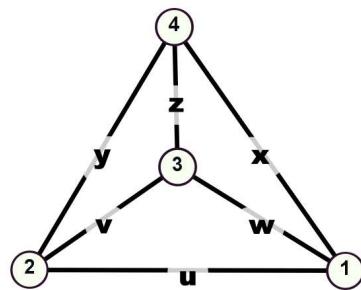


Fig. 5.12. Grafo G.

Se observa que:

- La sucesión de aristas: x, z, v, u, x, y es un camino, pero no es un camino simple por repetir la arista x, ni elemental por no ser camino simple. Tiene longitud 6 y es abierto.
- La sucesión de vértices: 1, 2, 3, 1, 4 constituye un camino simple por no tener aristas repetidas, pero no es un camino elemental al repetirse el vértice 1.
- La sucesión de vértices: 2, 4 , 3 , 1, es un camino elemental de longitud 3.
- La longitud del mayor camino elemental cerrado que se puede encontrar en él es 4.

### ☞ Definiciones

Dado un grafo G:

- un circuito es un camino simple cerrado, es decir, un camino sin aristas

repetidas y en el que coinciden los vértices inicial y final.

- un ciclo es un camino elemental cerrado, es decir, un camino que no posee aristas ni vértices repetidos y en el que coinciden los vértices inicial y final.

#### □ Ejemplo 5.8

En el grafo de la Figura 5.12, la sucesión de vértices: 1, 2, 3, 4, 1 constituye un **ciclo** de longitud 4, por ser un camino que no repite vértices ni aristas, y en el que coinciden los vértices inicial y final.

#### Actividad 5.3

Dado el grafo de la Figura 5.13, marcar con una tilde la clasificación que corresponda para cada sucesión de vértices que se dan en la Tabla 5.3 e indicar la longitud, como en el ejemplo dado.

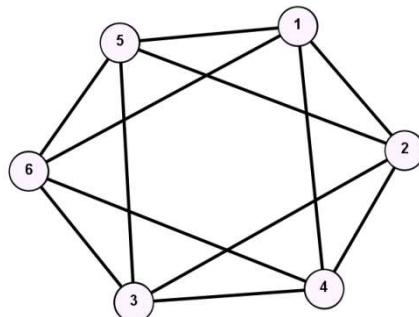


Fig. 5.13. Grafo de la Actividad 5.3.

|                           | Trayectoria<br>(o Camino) | Camino<br>simple | Camino<br>elemental | Círcito | Ciclo | Long. |
|---------------------------|---------------------------|------------------|---------------------|---------|-------|-------|
| 1,5,2,3,4                 | ✓                         | ✓                | ✓                   |         |       | 4     |
| 6,3,4,5,3,6               |                           |                  |                     |         |       |       |
| 1,4,5,3,2,6,1             |                           |                  |                     |         |       |       |
| 5,1,2,5,3,2,6,4           |                           |                  |                     |         |       |       |
| 1,4,6,3,5,2               |                           |                  |                     |         |       |       |
| 6,4,3,6,1,2               |                           |                  |                     |         |       |       |
| 2,5,4,3,6,4,1,5,3,2,1,6,2 |                           |                  |                     |         |       |       |

Tabla 5.3. Actividad 5.3.

## 5.4 Representaciones matriciales de un grafo

### 5.4.1 Matriz de Adyacencia

#### Definición

Dado un grafo  $G = (V, A, \varphi)$  sin aristas paralelas y con  $n$  vértices. Se llama matriz de adyacencia de  $G$  a la matriz  $M_a = (m_{ij})$  tal que:

$$m_{ij} = \begin{cases} 1 & \text{si } v_i \text{ y } v_j \text{ son adyacentes} \\ 0 & \text{en otro caso} \end{cases}$$

#### Observación

- La matriz de adyacencia es una matriz booleana, cuadrada y simétrica
- Los lazos están representados por unos en la diagonal principal mientras que no permite representar aristas paralelas. Si un vértice es aislado, tendrá la fila y columna correspondientes llenas de ceros.
- Si el grafo es simple, el grado de cada vértice estaría dado por la suma de la fila o la columna correspondiente.

Pasos para construir la matriz de adyacencia de un grafo no dirigido:

- 1) Se selecciona un orden arbitrario para los vértices y se etiquetan a las filas y columnas de la matriz usando dicho orden
- 2) Se asigna a cada elemento de la matriz el valor booleano uno (1) si los vértices correspondientes a la fila y a la columna de dicho elemento son adyacentes, y cero (0) en caso contrario.

#### Propiedad de la Matriz de Adyacencia

Si  $M_a$  es la matriz de adyacencia de un grafo simple, el elemento  $ij$  de  $M_a^k = M_a \times M_a \times \dots \times M_a$  ( $k$  veces); representa la cantidad de caminos diferentes de longitud “ $k$ ” del vértice  $i$  al vértice  $j$ . Donde  $\times$  es el producto usual de matrices

### □ Ejemplo 5.9

Dado el grafo de la Figura 5.14

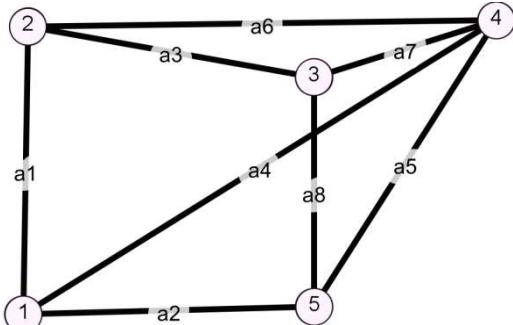


Fig. 5.14. Grafo G.

Su matriz de adyacencia es:

$$M_a(G) = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

$$(M_a)^2 = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 1 & 3 & 1 & 2 & 3 \\ 3 & 1 & 3 & 2 & 1 \\ 2 & 2 & 2 & 4 & 2 \\ 1 & 3 & 1 & 2 & 3 \end{pmatrix}$$

Hay tres caminos, de longitud dos, del vértice 2 al 5.

$C_1: 2, 1, 5; C_2: 2, 3, 5;$   
 $C_3: 2, 4, 5.$

Hay cuatro caminos, de longitud dos, del vértice 4 al 4. Ellos son:

$C_1: 4, 1, 4; C_2: 4, 2, 4;$   
 $C_3: 4, 3, 4; C_4: 4, 5, 4$

## 5.5 Matriz de Incidencia

### Definición

Dado  $G = (V, A, \varphi)$  donde  $|V| = n$  y  $|A| = k$ . Se llama matriz de incidencia de  $G$  a aquella matriz  $M_i = (m_{ij})$  tal que:

$$m_{ij} = \begin{cases} 1 & \text{si } v_i \text{ es extremo de } a_j \\ 0 & \text{en otro caso} \end{cases}$$

Pasos para construir la matriz de incidencia de un grafo no dirigido:

1. Seleccionar un orden arbitrario para los vértices y aristas.
2. Etiquetar las filas de la matriz con los vértices y a las columnas con las aristas, de acuerdo al orden seleccionado.
3. Cada elemento de la matriz es 1 o 0, según si la arista dispuesta en la columna incide en el vértice correspondiente a la fila o no.

### Observaciones

- La matriz de incidencia es una matriz booleana, rectangular de orden  $n \times k$ .
- Columnas iguales significan que hay aristas paralelas y columnas con un solo 1 indican la presencia de lazos, lo cual significa que esta matriz es ideal para los casos de grafos no simples.

### Ejemplo 5.10

Observando el grafo de la Figura 5.14, la matriz de incidencia es:

$$M_i(G) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

### Actividad 5.4

Sea  $G = (V, A, \varphi)$  donde  $V = \{a, b, c, d, e, f\}$ ;  $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$  y  $\varphi$  dada por

|                |            |            |            |            |            |            |
|----------------|------------|------------|------------|------------|------------|------------|
| $a_i$          | $a_1$      | $a_2$      | $a_3$      | $a_4$      | $a_5$      | $a_6$      |
| $\varphi(a_i)$ | $\{c, d\}$ | $\{a, b\}$ | $\{d, b\}$ | $\{c, e\}$ | $\{b, e\}$ | $\{a, e\}$ |

Tabla 5.4. Función  $\varphi$  de la Actividad 5.4.

- i) Representar gráficamente y determinar las correspondientes matrices.
- ii) Calcular la cantidad de caminos de longitud 3 del vértice b al e y encontrarlos

## 5.6 Grafos especiales

### 5.6.1 Grafos conexos

#### Definición

Un grafo  $G = (V, A, \varphi)$  es conexo si y solo si existe un camino de cualquier longitud entre cualquier par de vértices. En caso contrario, recibe el nombre de grafo no conexo (o desconexo).

#### Ejemplo 5.11

El grafo de la Figura 5.15 es conexo mientras que el de la Figura 5.16 es no conexo

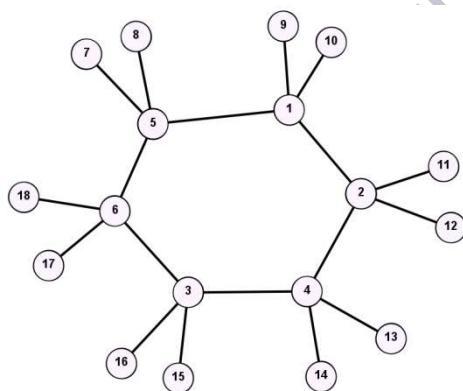


Fig. 5.15. Grafo Conexo.

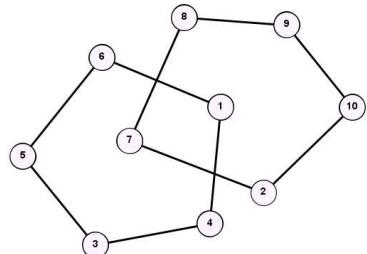


Fig. 5.16. Grafo no conexo.

#### Definiciones

Sea  $G = (V, A, \varphi)$  un grafo conexo, sean  $v \in V$  y  $a \in A$ . Entonces:

- Se dice que  $v$  es un vértice istmo si y solo si el subgrafo  $\tilde{G}_v$  no es conexo
- Se dice que  $a$  es una arista puente si y sólo si el subgrafo  $\tilde{G}_a$  no es conexo.

### □ Ejemplo 5.12

En el grafo de la Figura 5.15 hay seis vértices istmos: 1, 2, 3, 4, 5, 6, y 12 aristas puentes: {1, 9}, {1, 10}, {2, 11}, {2, 12}, {3, 15}, {3, 16}, {4, 13}, {4, 14}, {5, 7}, {5, 8}, {6, 17}, {6, 18}.

### Actividad 5.5

Dado el grafo de la Figura 5.17, responder verdadero o falso a las siguientes afirmaciones y justificar la respuesta:

- i) No posee vértices istmos
- ii) Todas las aristas son puentes
- iii)  $\tilde{G}_3$  es conexo
- iv)  $\tilde{G}_c$  no es conexo

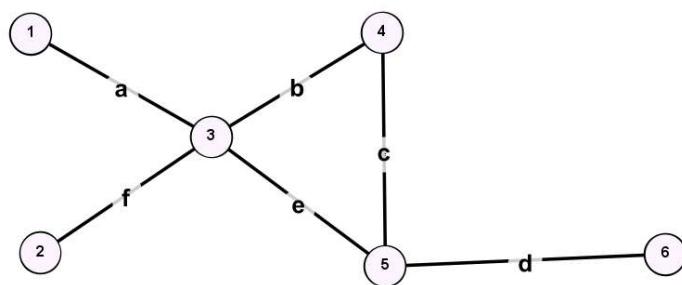


Fig. 5.17. Grafo Actividad 5.5.

### 5.6.2 Grafo completo

#### □ Definición

Sea  $G = (V, A, \varphi)$  un grafo simple tal que  $|V| = n$ . Se dice que  $G$  es un grafo Completo de  $n$  vértices si y solo sí posee una arista entre todo par de vértices distintos. Se denotan  $K_n$

$$\text{Cantidad de aristas de } K_n = |A| = \frac{n(n-1)}{2}$$

### □ Ejemplo 5.13

Las Figuras 5.18 y 5.19 corresponden a grafos completos

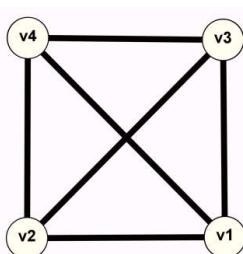


Fig. 5.18. Grafo  $K_4$ .

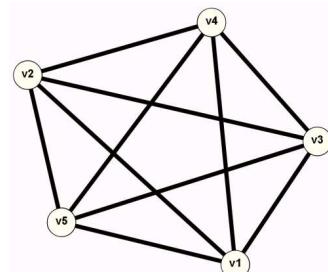


Fig. 5.19. Grafo  $K_5$ .

### 5.6.3 Grafo bipartito

#### Definición

Sea  $G = (V, A, \varphi)$  un grafo simple,  $G$  es bipartito (o bipartido) si y sólo si existe una partición de  $V$  compuesta de dos subconjuntos,  $\{V_1, V_2\}$  de manera que cada arista de  $G$  es de la forma  $\varphi(a) = \{v_1, v_2\}$  donde  $v_1 \in V_1$  y  $v_2 \in V_2$ .

Si además, cada vértice de  $V_1$  está unido con cada vértice de  $V_2$ , entonces  $G$  se dice bipartito completo. En este caso, si es con  $|V_1| = n$  y  $|V_2| = m$ , el grafo se denota por  $K_{n,m}$

Cantidad de aristas de  $K_{n,m} = |A| = n \cdot m$

### □ Ejemplo 5.14

El grafo de la Figura 5.20 es bipartito no completo mientras que el de la Figura 5.21 es bipartito completo, es  $K_{3,4}$

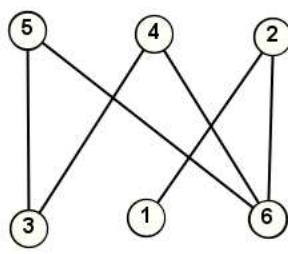


Fig. 5.20. Grafo  $G_1$ .

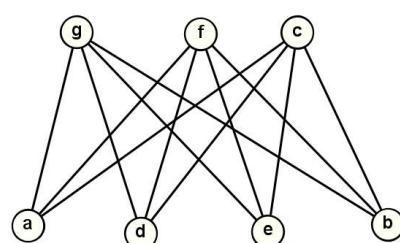


Fig. 5.21. Grafo  $K_{3,4}$ .

#### 5.6.4 Grafo regular

##### Definición

Un grafo  $G = (V, A, \varphi)$  se dice  $k$  – regular si y solo si todos los vértices tienen grado  $k$ .

Si  $|V| = n$  entonces  $|A| = \frac{n.k}{2}$

##### Ejemplo 5.15

El grafo de la Figura 5.22 es 2-regular con siete vértices mientras que el de la Figura 5.23 es 3-regular con seis vértices.

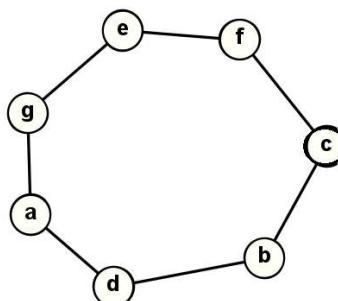


Fig.5.22. Grafo 2-regular.

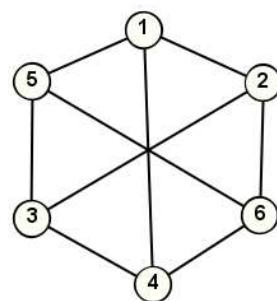


Fig. 5.23. Grafo 3-regular

#### Actividad 5.6

- a) Responder Verdadero o Falso, y justificar la respuesta:
- i) Todo grafo completo es regular
  - ii) Todo grafo regular es completo
  - iii) No existe un grafo  $k$ -regular de  $n$  vértices donde tanto  $k$  como  $n$  son números impares
  - iv) Existe un grafo 5-regular con 25 aristas
- b) Dados los siguientes grafos conexos, clasificar según sean completos, bipartitos y/o regulares. Además indicar si poseen vértices istmos y/o aristas puentes.

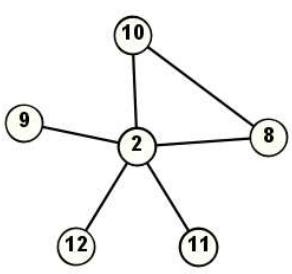


Fig. 5.24. Grafo  $G_1$ .

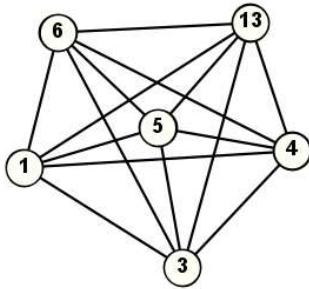


Fig. 5.25. Grafo  $G_2$ .

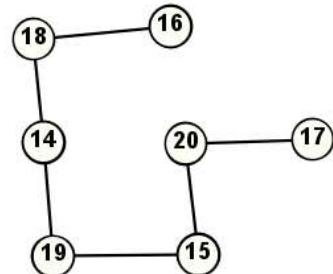


Fig. 5.26. Grafo  $G_3$ .

## 5.7 Caminos y circuitos de Euler

Durante el primer tercio del siglo XVIII, en la ciudad de Königsberg (hoy Kaliningrado) se planteó un famoso problema conocido como el problema de los puentes de Königsberg (en algunos textos se escribe Koenigsberg).

En esa época existían siete puentes que cruzaban el río Pregel (actualmente solo hay cinco), conectando las cuatro regiones que creaba éste, y los ciudadanos se planteaban si existía alguna ruta que permitiese cruzar todos los puentes una y solo una vez, volviendo o no al punto de partida.

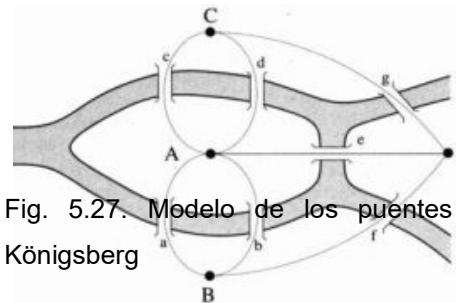


Fig. 5.27. Modelo de los puentes de Königsberg

La respuesta a esta situación llegó en 1736

de la mano del matemático, físico y filósofo Leonard Euler (1707-1783), quien demostró que no era posible salir de una región, atravesar todos los puentes una sola vez y regresar al punto de partida.

Para su demostración lo que hizo fue modelar la situación para quedarse solo con aquello que era trascendente para el problema, en este caso las cuatro regiones y los siete puentes que las conectaban.

La estrategia de resolución del problema se considera el inicio de la Teoría de Grafos, así como de la Topología.

### Definición

- Sea  $G = (V, A, \varphi)$ . Un camino (o trayectoria) en  $G$  se dice de Euler si y solo si existe un camino simple de  $G$  que pasa por todas las aristas de  $G$  sólo una vez.
- Un circuito en  $G$  se dice de Euler si y solo si es un camino de Euler cerrado.

### Ejemplo 5.16

El grafo de la Figura 5.28 posee camino de Euler.

Uno de ellos es la sucesión:

1 , 5 , 2 , 1 , 6 , 2 , 3 , 6 , 4 , 3 , 5 , 4

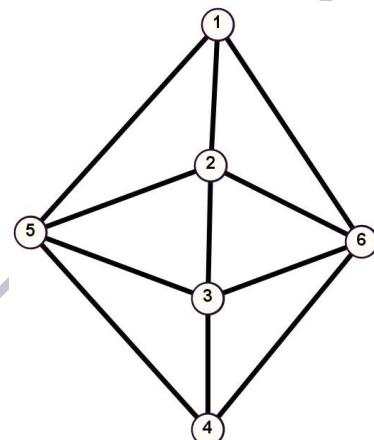


Fig. 5.28. Grafo con camino Euleriano

Pero no es el único, también es un camino de Euler para el mismo grafo la secuencia:

4 , 6 , 2 , 5 , 1 , 2 , 3 , 5 , 4 , 3 , 6 , 1

Se puede comprobar que este grafo no posee circuito de Euler, esto es, no hay modo de recorrerlo entero, pasando una vez por cada arista y volver al punto de partida.

### 5.7.1 Condiciones necesarias y suficientes para la existencia de caminos y ciclos de Euler

### Teorema

Sea  $G = (V, A, \varphi)$ ,

- $G$  posee al menos un camino de Euler si y solo si es conexo y posee exactamente dos vértices de grado impar, los cuales serán el inicio y fin de cualquier trayectoria.
- $G$  posee al menos un circuito de Euler si y solo si es conexo y todos los vértices poseen grado par.

### □ Ejemplo 5.17

El grafo de la Figura 5.29 posee Circuito de Euler (por ejemplo: 1, 6, 5, 2, 6, 4, 1, 3, 5, 1) ; el de la Figura 5.30 solo posee Camino de Euler (por ejemplo: 5, 1, 4, 7, 3, 5, 2, 8, 6, 4, 3, 2, 6, 1)

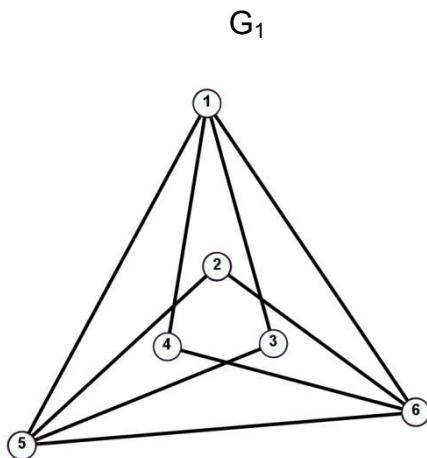


Fig. 5.29. Grafo  $G_1$ .

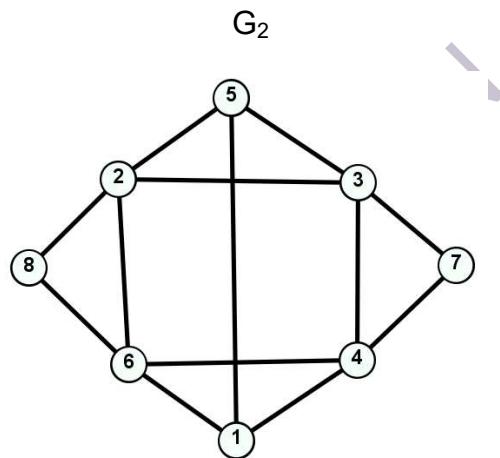


Fig. 5.30. Grafo  $G_2$ .

## 5.8 Caminos y Ciclo de Hamilton

En 1859 el matemático, físico y astrónomo irlandés William Hamilton (1805-1865) inventó un juego que consistía en un dodecaedro regular de madera con 20 vértices que representaban a importantes ciudades del mundo : Bruselas, Cantón, Delhi, Frankfurt, etc.

El dodecaedro, figura tridimensional , se encuentra plasmado en la Figura 5.31

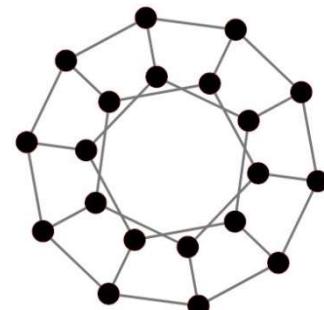


Fig.5.31. Dodecaedro.

El jugador debía encontrar un recorrido a lo largo de las aristas del dodecaedro, que pase exactamente una vez por cada ciudad, y volver a la ciudad de la cual se partió.

Por ser el dodecaedro incomodo de manejar, Hamilton desarrolló una versión del juego en dos dimensiones representado por la Figura 5.32 y a la trayectoria que

cumpla con la consigna se le llama Ciclo de Hamilton en honor al famoso matemático.

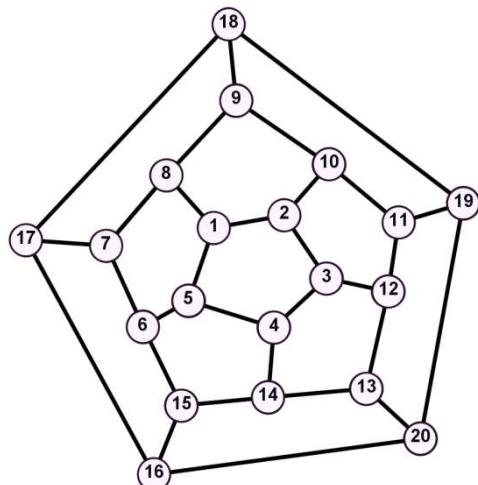


Fig.5.32. Grafo plano del dodecaedro.

### Definición

Sea  $G = (V, A, \varphi)$  un grafo.

- Se dice que un camino es de Hamilton en  $G$  si es un camino elemental que contiene todos los vértices de  $G$ .
- Un camino de Hamilton cerrado es un ciclo de Hamilton.

### Ejemplos 5.18

- a) Todos los grafos completos poseen ciclo de Hamilton. En las Figuras 5.33 se puede observar a  $K_6$  y uno de sus ciclos : 1 , 3 , 4 , 2 , 5 , 6 , 1

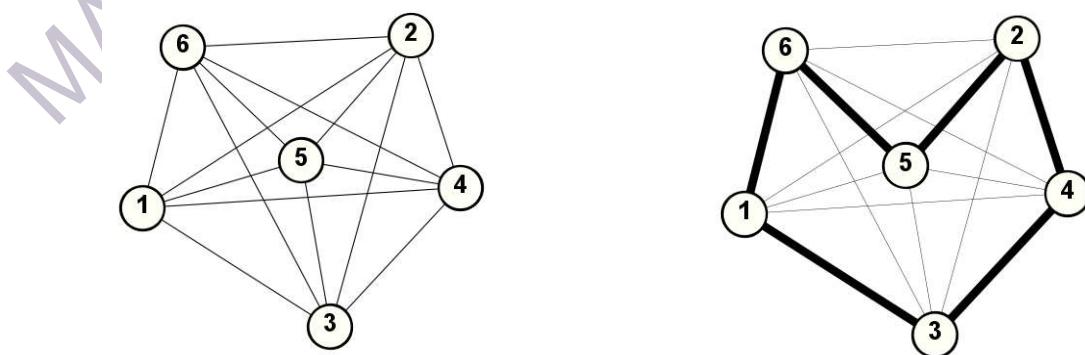


Fig.5.33. Grafo  $K_6$  y un Ciclo de Hamilton

- b) Observe el grafo de la Figura 5.34, que tienen un vértice istmo , luego no posee Ciclo de Hamilton sino solo un Camino: 6, 1, 5, 2, 3,4

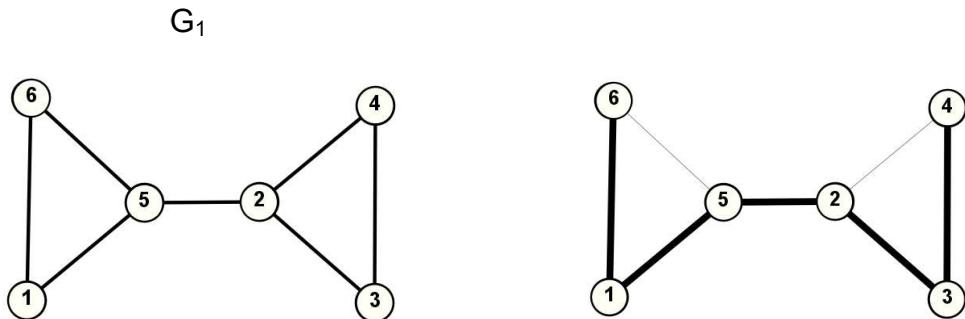


Fig. 5.34. Grafo  $G_1$  y un Camino hamiltoniano en para él

- c) El juego del dodecaedro tiene solución. En la Figura 5.35 se observa al ciclo  
1 , 8 , 9 , 10, 2, 3, 12, 11, 19, 18, 17, 7 , 6 , 15, 16, 20, 13, 14 , 4 , 5, 1

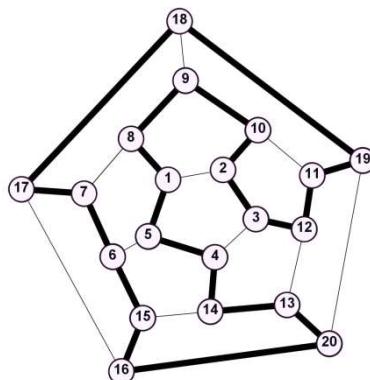


Fig. 5.35. Una solución para el Grafo de Hamilton

### 5.8.1 Condiciones Suficientes para la existencia de caminos y ciclos de Hamilton

#### Teorema

Sea  $G = (V, A, \varphi)$  un grafo simple con tres o mas vértices. Se cumple que

- Si  $g(u) + g(v) \geq n$  ,  $\forall u, v \in V$  no adyacentes, entonces  $G$  posee un ciclo hamiltoniano.
- Si  $g(v) \geq \frac{n}{2}$  ,  $\forall v \in V$  entonces  $G$  posee ciclo de Hamilton.
- Si  $|A| \geq \frac{n^2 - 3n + 6}{2}$  , entonces  $G$  tiene un ciclo hamiltoniano.

## Actividad 5.7

Dados los grafos de las Figuras 5.36 a 5.38:

- Analizar si se puede aplicar los Teoremas que hablan sobre la existencia de Ciclos de Euler y de Hamilton.
- En cada grafo obtener ambos, siempre que existan.

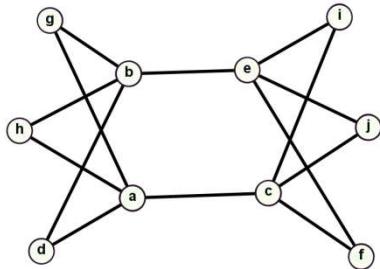


Fig. 5.36. Grafo  $G_1$ .

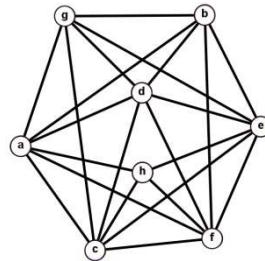


Fig. 5.37. Grafo  $G_2$ .

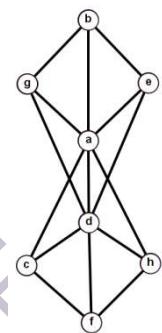


Fig. 5.38. Grafo  $G_3$ .

## 5.9 Isomorfismos de Grafos

### Definición

Sean  $G_1 = (V_1, A_1, \varphi_1)$  y  $G_2 = (V_2, A_2, \varphi_2)$  dos grafos no dirigidos.

Se dice que  $G_1$  y  $G_2$  son isomorfos si y solo sí existen dos funciones biyectivas  $f: V_1 \rightarrow V_2$  y  $g: A_1 \rightarrow A_2$  tales que  $\forall a \in A_1, \varphi_2(g(a)) = f(\varphi_1(a))$ .

Si no hay aristas paralelas, entonces es suficiente:

$$\forall v_1, v_2 \in V_1: \{v_1, v_2\} \in A_1 \Rightarrow \{f(v_1), f(v_2)\} \in A_2.$$

### Notación

Si  $G_1$  y  $G_2$  son isomorfos, se expresa  $G_1 \approx G_2$  y se dice que la función  $f$  es un isomorfismo entre ellos.

Nótese que  $\forall \{v_1, v_2\} \in A_1$  significa que  $v_1, v_2 \in V_1$  son adyacentes en  $G_1$  y que  $\{f(v_1), f(v_2)\} \in A_2$  significa que  $f(v_1)$  y  $f(v_2)$  son adyacentes en  $G_2$ , lo que

se deduce que si en el primer grafo hay una arista entre dos vértices, los correspondientes a estos vértices en el segundo grafo también deben estar unidos por una arista.

La correspondencia de vértices de un isomorfismo de grafos mantiene las adyacencias. Puesto que el hecho de que los pares de vértices sean adyacentes o no es la única propiedad esencial de un grafo no dirigido, de esta forma se preserva la estructura de los grafos, es decir sus vértices están relacionados de igual forma aunque estén dibujados de manera distinta.

### Observación

- Si los grafos no tienen lados paralelos, entonces la aplicación  $f$  determina de forma única a la aplicación que se da entre los conjuntos de las aristas. De ahí, que normalmente, para dar un isomorfismo de grafos se da únicamente como actúa la función sobre los vértices.

#### 5.9.1 Condiciones invariantes bajo isomorfismo

Hay cantidades que mantienen su valor entre grafos isomorfos. Ellas se dicen cantidades invariantes bajo isomorfismo, por ejemplo, “número de vértices o aristas”, “el grado de un vértice”, “caminos de determinada longitud”; “cantidad de ciclos de determinada longitud”, etc. Es decir que son condiciones necesarias para que los grafos sean isomorfos, pero no son suficientes, o sea que aunque se cumplan puede ser que los grafos no sean isomorfos.

### Definición

Una propiedad se dice invariante por isomorfismo si dados dos grafos isomorfos  $G_1$  y  $G_2$ , uno satisface la propiedad si, y sólo si, la satisface el otro.

Dado que las incidencias y adyacencias se deben conservar, se puede usar las matrices de ambos grafos para mostrar que hay un isomorfismo. Se tiene entonces el siguiente resultado.

### Teorema sobre Isomorfismos

- Dos grafos son isomorfos si y solo si las matrices de incidencia, para alguna disposición de sus vértices y aristas, son iguales.
- En el caso de grafos simples basta con mostrar que las matrices de adyacencia son iguales, para un determinado orden de los vértices y ésta también es una condición necesaria y suficiente.

#### Ejemplo 5.19

Para averiguar si los grafos de las Figuras 5.39 y 5.40 son isomorfos:

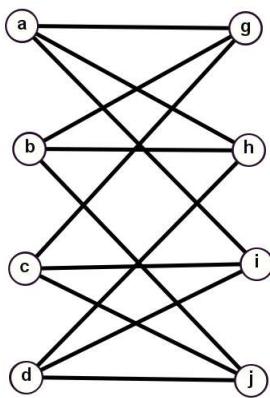


Fig. 5.39. Grafo  $G_1$ .

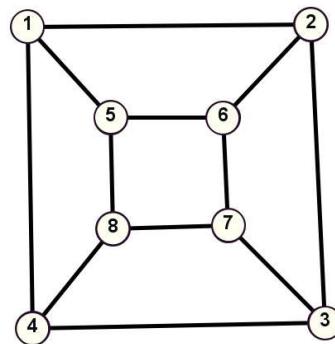


Fig. 5.40. Grafo  $G_2$ .

Se analiza primero, si se cumplen las condiciones necesarias: igual cantidad de vértices, igual cantidad de aristas, igual cantidad de ciclos de la misma longitud, etc. Si algún invariante no se cumple se deduce que los grafos no son isomorfos. Pero si se cumplen, no son condiciones suficientes para decir que los dos grafos son isomorfos. Como no hay aristas paralelas, se busca la función  $f$  o bien se construye la matriz de adyacencia de ambos de acuerdo a dicha correspondencia.

Dado que todos los vértices tienen grado 3 la primera asignación sería indistinta por lo que se comienza eligiendo que  $f(a) = 1$ . De allí en más se asigna a los vértices adyacentes al vértice  $a$ , vértices adyacentes a 1, por lo tanto se elige  $f(g) = 5$ ,  $f(h) = 2$ ,  $f(i) = 4$ . (Observe que no es la única elección posible). Y así se sigue asignando de acuerdo a la adyacencia en cada grafo. Luego una posible función  $f$  sería:

$$f: V_1 \rightarrow V_2$$

$$\begin{aligned}
a \rightarrow 1 &\Leftrightarrow f(a) = 1 \\
g \rightarrow 5 &\Leftrightarrow f(g) = 5 \\
b \rightarrow 6 &\Leftrightarrow f(b) = 6 \\
h \rightarrow 2 &\Leftrightarrow f(h) = 2 \\
d \rightarrow 3 &\Leftrightarrow f(d) = 3 \\
j \rightarrow 7 &\Leftrightarrow f(j) = 7 \\
c \rightarrow 8 &\Leftrightarrow f(c) = 8 \\
i \rightarrow 4 &\Leftrightarrow f(i) = 4
\end{aligned}$$

La definición dice que si entre dos vértices cualesquiera del primer grafo hay una arista, también debe haber una arista entre los vértices correspondientes en el segundo grafo.

Por ejemplo entre  $a$  y  $g$  hay una arista en  $G_1$ , y también hay una arista entre  $f(a)$  y  $f(g)$  en  $G_2$ . Lo mismo habría que comprobar para cada arista.

Se puede comprobar, lo anterior, para todas las aristas juntas con la matriz de adyacencia de ambas, ordenando convenientemente los vértices de acuerdo a la función biyectiva definida entre los vértices.

$$M_{G_1} = \begin{pmatrix} a & g & b & h & d & j & c & i \\ \begin{matrix} a \\ g \\ b \\ h \\ d \\ j \\ c \\ i \end{matrix} & \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \end{pmatrix}$$

$$M_{G_2} = \begin{pmatrix} 1 & 5 & 6 & 2 & 3 & 7 & 8 & 4 \\ \begin{matrix} 1 \\ 5 \\ 6 \\ 2 \\ 3 \\ 7 \\ 8 \\ 4 \end{matrix} & \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{pmatrix}$$

Como las matrices de adyacencia son iguales, se infiere que los grafos  $G_1$  y  $G_2$  son isomorfos.

### Observación

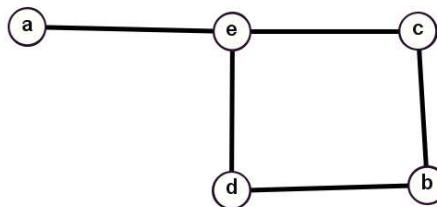
- Si dadas dos matrices de adyacencia correspondientes a dos grafos, ellas no son iguales, no significa que los grafos no sean isomorfos, pues tal vez reordenando una de ellas se pueda lograr que sean iguales. Para poder

afirmar que dos grafos no son isomorfos hay que mostrar alguna propiedad estructural no compartida (invariante) o bien probar que todos los ordenamientos posibles de las matrices no coinciden. Esto último no es práctico pues la cantidad de ordenamientos posibles de  $n$  elementos es igual a  $n!$  (factorial de  $n$ ), lo cual es una cantidad muy grande.

### Actividad 5.8

Dados los siguientes pares de grafos, determinar si son isomorfos. Justificando en cada caso su respuesta:

a)  $G_1$



$G_2$

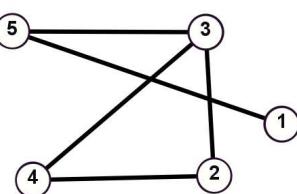
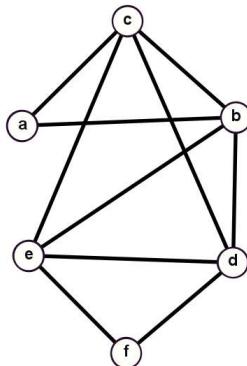


Fig. 5.41. Grafos  $G_1$  y  $G_2$ .

b)  $G_3$



$G_4$

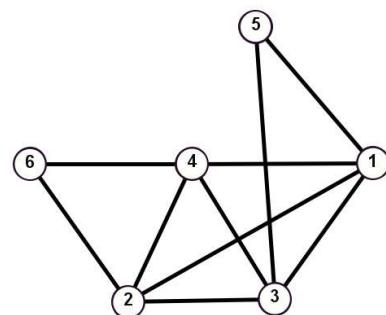
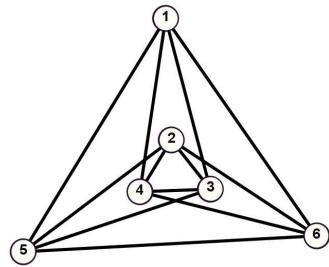
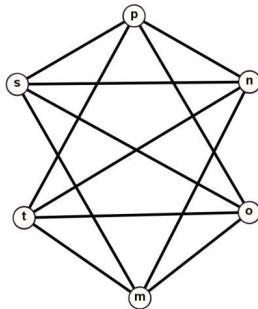


Fig. 5.42. Grafos  $G_3$  y  $G_4$ .

c)  $G_5$  $G_6$ Fig. 5.43. Grafos  $G_5$  y  $G_6$ .

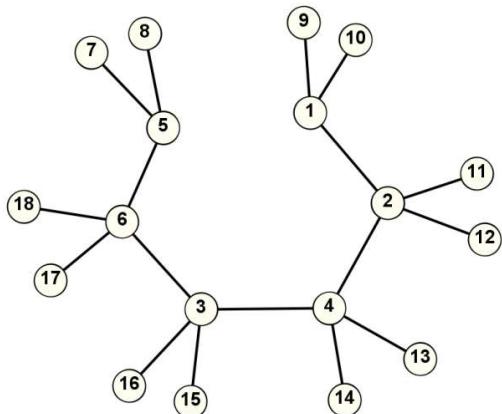
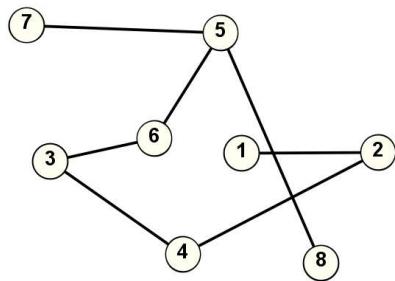
## 5.10 Árbol no dirigido

### Definición

Un grafo no dirigido  $G = (V, A, \varphi)$  es un árbol no dirigido si y solo si es conexo y acíclico (sin ciclos).

### Ejemplo 5.20

Los grafos de las Figuras 5.44 y 5.45 son árboles no dirigidos. Se puede comprobar que hay conexidad y no posee ciclos.

Fig. 5.44. Grafo  $G_1$ .Fig. 5.45. Grafo  $G_2$ .

### Definiciones

- $G = (V, A, \varphi)$  se dice árbol trivial si y solo si  $|V|=1$ .
- Un vértice se denomina hoja o vértice pendiente si y solo si  $g(v) = 1$ .

## Observaciones

Sea  $G = (V, A, \varphi)$  un árbol.

- Un árbol no tiene lazos ni aristas paralelas, es decir es un grafo simple; pero no todo grafo simple es un árbol.
- Si se agrega una arista a  $G$ , se genera un ciclo.
- Todas las aristas son puentes.
- Todo vértice no pendiente es un istmo y recíprocamente.
- Si  $G$  no es el trivial existen por lo menos 2 vértices pendientes.

## Teorema

Si  $G = (V, A, \varphi)$  es árbol no dirigido, entonces  $|V| = |A| + 1$

## Ejemplos 5.21

- a) El árbol de la Figura 5.44 tiene 18 vértices y 17 aristas
- b) El árbol de la Figura 5.45 tiene 8 vértices y 7 aristas

## Actividad 5.9

- i) Determinar si los grafos de las Figuras 5.46 y 5.47 son árboles. En los casos afirmativos verificar la propiedad que se refiere a la cantidad de vértices y aristas.

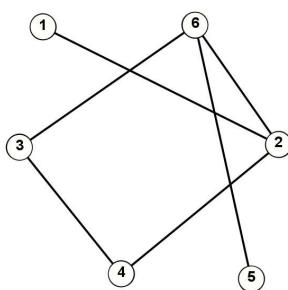


Fig. 5.46. Grafo  $G_1$ .

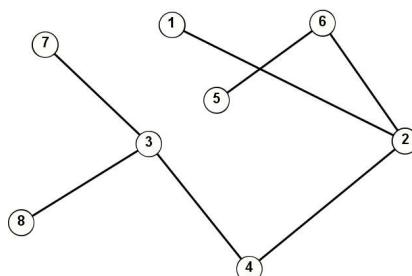


Fig. 5.47. Grafo  $G_2$ .

- ii)** Decir si son Verdaderas o Falsas las siguientes afirmaciones y justificar la respuesta:
- Existe un árbol (no dirigido) de 10 vértices y 10 aristas
  - Si un grafo posee 10 vértices y 9 aristas entonces es un árbol
  - En un árbol todos los vértices son istmos y todas las aristas son puentes.
  - Existe un árbol con 5 vértices de los cuales solo uno es istmo.

### 5.10.1 Digrafo o Grafo Dirigido

#### Definición

Se llama digrafo  $D$  a toda terna  $D = (V, A, \varphi)$  donde  $V$  y  $A$  son dos conjuntos finitos de objetos cualesquieras tal que:

- i)  $V \neq \emptyset$  y ii)  $\varphi: A \rightarrow V \times V$

donde a los elementos de  $V$  se les llama vértices o nodos, a los elementos de  $A$  aristas (lados o arcos) y la función  $\varphi$  se llama función de incidencia dirigida ya que ella asigna a cada arista un par ordenado de vértices

#### Casos particulares

- Si  $|V| = 1$  y  $A = \emptyset$ , a  $D$  se le llama digrafo trivial
- Si  $|V| = n$  y  $A = \emptyset$ , a  $D$  se le llama digrafo vacío

### 5.10.2 Representación gráfica

El dibujo de un digrafo es un diagrama que consiste en representar por puntos (o círculos) a los elementos de  $V$  y por flechas a los elementos de  $A$  de tal manera que si  $\varphi(a) = (u, v)$  significa que la arista  $a$  va desde  $u$  hacia  $v$ .

#### Ejemplo 5.22

Sea  $D = (V, A, \varphi)$  donde  $V = \{v_1, v_2, v_3\}$ ,  $A = \{a_1, a_2, a_3, a_4\}$  y  $\varphi$  dada por

| $a_i$          | $a_1$        | $a_2$        | $a_3$        | $a_4$        |
|----------------|--------------|--------------|--------------|--------------|
| $\varphi(a_i)$ | $(v_1, v_2)$ | $(v_2, v_1)$ | $(v_2, v_3)$ | $(v_2, v_2)$ |

Tabla 5.5

La representación gráfica está dada por la Figura 5.48, corresponde recordar que conceptos geométricos como posición, forma, longitud, distancia, etc no tienen importancia en estos temas. En el caso de presencia de aristas antiparalelas suele graficarse con flechas bidireccionales.

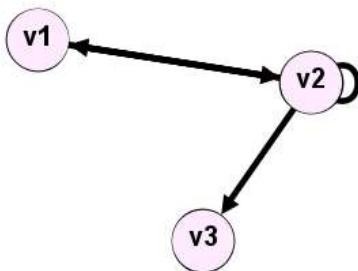


Fig. 5.48. Dagrafo D.

### Observación

Todo digrafo representa una relación binaria finita y recíprocamente toda relación binaria finita se representa por medio de un digrafo.

A partir de aquí se presentan definiciones relativas a vértices y aristas.

### Definiciones

Sea  $D = (V, A, \varphi)$  un digrafo, y sean  $a_1, a_2 \in A$ ,  $v_1, v_2 \in V$ .

Si  $\varphi(a_1) = (v_1, v_2)$  entonces:

- Se dice que  $v_1$  adyacente a  $v_2$ , siendo  $v_1$  el vértice inicial y  $v_2$  el vértice final o terminal de la arista  $a_1$ . También se dice que la arista  $a_1$  llega al vértice  $v_2$  y sale del vértice  $v_1$  o que  $a_1$  incide en  $v_1$  y  $v_2$ .
- Si  $v_1 = v_2$ , se dice que  $a_1$  es un lazo.
- $v_1$  se dice vértice aislado si y solo si no existe una arista (que no sea lazo) que incida en él.
- Se dice que  $v_1$  es un vértice pozo si y solo si no es aislado y  $v_1$  no es vértice inicial de ninguna arista.
- Se dice que  $v_1$  es un vértice fuente si y solo si no es aislado y  $v_1$  no es vértice terminal de ninguna arista.
- Se dice que  $a_1$  y  $a_2$  son aristas paralelas si y solo si  $\varphi(a_1) = \varphi(a_2) = (v_1, v_2)$

- Se dice que  $a_1$  y  $a_2$  son aristas antiparalelas si y solo si  $\varphi(a_1) = (v_1, v_2)$  y  $\varphi(a_2) = (v_2, v_1)$  con  $v_1 \neq v_2$ .
- Se dice que  $a_1$  y  $a_2$  son aristas adyacentes si y solo si  $\exists v_1, v_2, v_3 \in V$  tales que  $a_1$  y  $a_2$  no son paralelas y se cumple que:
  - $\varphi(a_1) = (v_1, v_2)$  y  $\varphi(a_2) = (v_2, v_3)$  o
  - $\varphi(a_1) = (v_1, v_2)$  y  $\varphi(a_2) = (v_3, v_2)$  o
  - $\varphi(a_1) = (v_2, v_1)$  y  $\varphi(a_2) = (v_2, v_3)$ .
- Se dice que  $D$  es un dígrafo simple si y solo si no tiene lazos, aristas paralelas ni antiparalelas.

### 5.10.3 Grados de un vértice

#### Definición

Dado  $D = (V, A, \varphi)$  y sea  $v \in V$ , se definen las funciones grado positivo y grado negativo de  $v$  como sigue:

$g^+ : V \rightarrow \mathbb{N}_0$  /  $g^+(v)$  es la cantidad de aristas que llegan a  $v$ .

$g^- : V \rightarrow \mathbb{N}_0$  /  $g^-(v)$  es la cantidad de aristas que salen de  $v$ .

Además se denomina grado total (o valencia total) de  $v$ , y se denota  $g(v)$ , a

$$g(v) = g^+(v) + g^-(v)$$

Se denomina grado neto (o valencia neta) de  $v$ , y se denota  $g_n(v)$ , a

$$g_n(v) = g^+(v) - g^-(v)$$

#### Observaciones

- A la función  $g^+$  también se le llama grado interno o de entrada.
- A la función  $g^-$  también se le llama grado externo o de salida.
- Si  $v$  es un vértice aislado y sin lazo entonces  $g^+(v) = g^-(v) = 0$

### Propiedades de los grados

Dado un dígrafo  $D = (V, A, \varphi)$  entonces:

a)  $\sum_{v \in V} g^+(v) = \sum_{v \in V} g^-(v) = |A|$ ;    b)  $\sum_{v \in V} g(v) = 2|A|$ ;    c)  $\sum_{v \in V} g_n(v) = 0$

### Actividad 5.10

Dado el dígrafo  $D = (V, A, \varphi)$  de la Figura 5.49

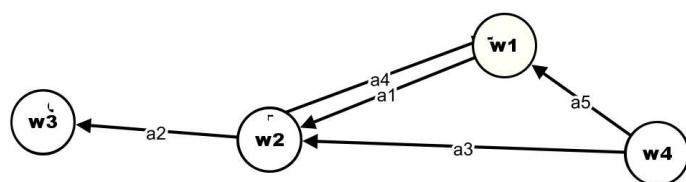


Fig. 5.49. Dígrafo D

Se pide:

- Indicar cuáles son los vértices adyacentes a cada uno
- Indicar cuáles son las aristas adyacentes a  $a_5$
- Buscar vértices pozos y fuentes, si existen.
- Encontrar las funciones grado positivo, negativo, total y neto. Presentar a las cuatro funciones en una misma tabla
- Verificar las propiedades de los grados

### 5.11 Caminos, Caminos Simples, Caminos Elementales, Circuitos y Ciclos

#### Definición

Dados  $D = (V, A, \varphi)$  un dígrafo,  $n \in \mathbb{N}$  y  $v_1, v_{n+1} \in V$ , se denomina camino  $v_1 - v_{n+1}$  de longitud  $n$  a una sucesión de  $n$  aristas que comienza en  $v_1$  y termina en  $v_{n+1}$  tales que el vértice final de una arista es el vértice inicial de la siguiente.

#### Notación

En el caso de caminos que involucran aristas paralelas se debe indicar como

una sucesión alternada de vértices y aristas

$$v_1, a_1, v_2, a_2, \dots, a_{n-1}, v_n, a_n, v_{n+1}$$

Caso contrario basta con indicar la sucesión de vértices involucrados o la sucesión de aristas correspondientes

$$v_1, v_2, \dots, v_n, v_{n+1} \quad \text{O} \quad a_1, a_2, \dots, a_{n-1}, a_n$$

### Definiciones

- Un camino se dice simple si todas las aristas involucradas son distintas.
- Un camino se dice elemental si todos los vértices involucrados son distintos.
- Un camino de longitud  $n$  de  $v_1$  a  $v_{n+1}$  es cerrado si y solo si  $v_1 = v_{n+1}$
- Un circuito es un camino simple cerrado.
- Un ciclo es un camino elemental cerrado.

### Ejemplo 5.23

Se puede encontrar todos los caminos que parten de determinado vértice ayudados por un diagrama de árbol. Es el caso del procedimiento que se aplicará en el digrafo de la Figura 5.50 para encontrar todos los caminos elementales que comiencen en 3 y no sean ciclos.

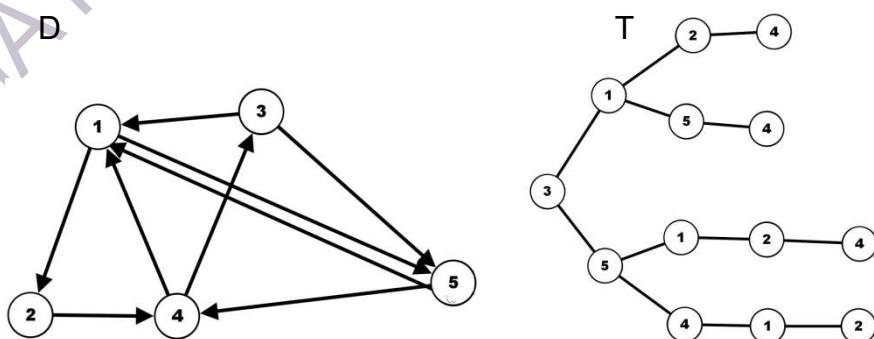


Fig. 5.50. Digrafo D y Árbol T que representan a todos los caminos elementales en D que comienzan en 3.

Se comienza con el vértice 3 y desde allí se construye el árbol de acuerdo a los vértices adyacentes que se encuentren. Luego de finalizada la construcción se extrae la información. En este ejemplo se encuentran los siguientes caminos elementales que no son ciclos:

$$C_1: 3, 1;$$

$$C_2: 3, 1, 2;$$

$$C_3: 3, 1, 2, 4;$$

$$C_4: 3, 1, 5;$$

$$C_5: 3, 1, 5, 4;$$

$$C_6: 3, 5;$$

$$C_7: 3, 5, 1;$$

$$C_8: 3, 5, 1, 2;$$

$$C_9: 3, 5, 1, 2, 4;$$

$$C_{10}: 3, 5, 4;$$

$$C_{11}: 3, 5, 4, 1;$$

$$C_{12}: 3, 5, 4, 1, 2.$$

### Actividad 5.11

Con referencia al digrafo  $D = (V, A, \varphi)$  de la Figura 5.51

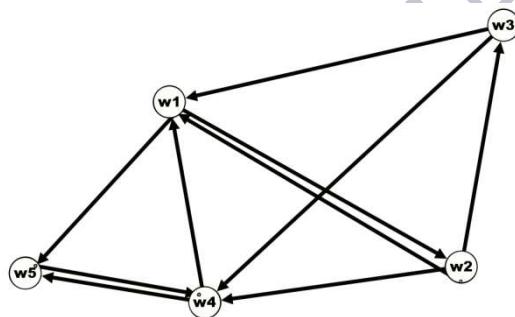


Fig. 5.51. Digrafo D

Responder:

- ¿Cuáles son todos los caminos simples y circuitos cuyo vértice inicial es  $w_4$ ? Dar la longitud de cada uno.
- ¿Cuáles son todos los caminos elementales y ciclos cuyo vértice inicial es  $w_3$ ? Dar la longitud de cada uno.
- ¿Existen vértices pozos o vértices fuentes?

## 5.12 Representaciones matriciales de un digrafo

### 5.12.1 Matriz de Adyacencia

#### Definición

Sea  $D = (V, A, \varphi)$  un digrafo sin aristas paralelas y con  $n$  vértices, se llama matriz de adyacencia a la matriz  $M_a = (m_{ij})$  booleana de orden  $n$  cuyo elemento genérico es:

$$m_{ij} = \begin{cases} 1 & \text{si } \exists a \in A, \varphi(a) = (v_i, v_j) \\ 0 & \text{caso contrario} \end{cases}$$

#### Observaciones

- $M_a$  fue presentada en el capítulo II como matriz de una relación binaria, no necesariamente simétrica.
- La presencia de lazos se manifiesta por unos en la diagonal principal de la matriz.

#### Ejemplo 5.24

Dado el digrafo D de la Figura 5.52:

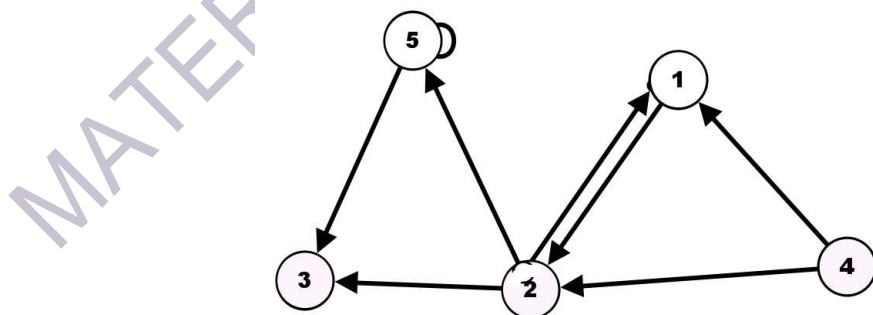


Fig. 5.52. Digrafo D.

Su matriz de adyacencia está dada por:

$$Ma = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 0 \\ 4 & 1 & 1 & 0 & 0 \\ 5 & 0 & 0 & 1 & 0 \end{pmatrix}$$

### Propiedad de la Matriz de Adyacencia de un digrafo

Si  $M_a$  es la matriz de adyacencia de un digrafo sin aristas paralelas, el elemento genérico  $m_{ij}$  de  $M_a^k = Ma \times Ma \times \dots \times Ma$  ( $k$  veces); es igual al número de caminos diferentes de longitud “ $k$ ” del vértice  $i$  al vértice  $j$  y donde la operación  $\times$  es el producto usual de matrices.

### Ejemplo 5.25

Para contar la cantidad de caminos de longitud 2, 3 y 4 que hay entre todos los vértices del dígrafo de la Figura 5.52, se parte de la matriz de adyacencia, que representa todos los caminos de longitud 1 que hay entre los vértices del dígrafo, luego se calculan las potencias de ella. Para los caminos de longitud 2 (*dos*), se determina  $M_a^2$ :

$$M_a^2 = M_a \times M_a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 0 \\ 4 & 1 & 1 & 0 & 0 & 0 \\ 5 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Hay 1 camino de longitud dos, del vértice 2 al 3.  
Desde el vértice 3 a cualquier otro vértice No hay caminos de longitud dos.  
Hay 1 camino de longitud dos, del vértice 5 al 5.

La siguiente matriz  $M_a^3$  representa todos los caminos de longitud 3 que hay entre los vértices del digrafo

$$M_a^3 = M_a^2 \times M_a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 0 \\ 4 & 1 & 1 & 1 & 0 & 1 \\ 5 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Hay 2 caminos de longitud tres, del vértice 2 al 3.  
Hay 1 camino de longitud tres, del vértice 5 al 3.

La matriz  $M_a^4$  representa todos los caminos de longitud 4 que hay entre los vértices del dígrafo

$$M_a^4 = M_a^3 \times M_a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 1 & 0 & 2 & 0 & 2 \\ 3 & 0 & 0 & 0 & 0 & 0 \\ 4 & 1 & 1 & 2 & 0 & 2 \\ 5 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 2 & 0 & 2 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 3 & 0 & 3 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Hay 2 caminos de longitud cuatro, del vértice 2 al 3.  
Hay 3 caminos de longitud cuatro, del vértice 4 al 5.  
Hay 1 camino de longitud cuatro, del vértice 5 al 3.

### Actividad 5.12

Sea  $D = (V, A, \varphi)$  donde  $V = \{a, b, c, d, e, f\}$ ;  $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$  y  $\varphi$  dada por la Tabla 5.6

| $a_i$          | $a_1$  | $a_2$  | $a_3$  | $a_4$  | $a_5$  | $a_6$  |
|----------------|--------|--------|--------|--------|--------|--------|
| $\varphi(a_i)$ | (c, d) | (a, b) | (d, b) | (c, b) | (b, e) | (a, e) |

Tabla 5.6

Usando matrices demostrar que:

- a) No existen circuitos de ninguna longitud
- b) Existe un único camino de longitud 3
- c) No existen caminos de longitud 4 en adelante

#### 5.12.2 Matriz de Incidencia

##### Definición

Sea  $D = (V, A, \varphi)$  un dígrafo sin lazos con  $n$  vértices y  $k$  aristas, se llama matriz de incidencia a la matriz  $M_i$ , de orden  $nxk$ , a la matriz cuyo elemento genérico  $m_{ij}$  está dado por:

$$m_{ij} = \begin{cases} 1 & \text{si } v_i \text{ es el vértice inicial de } a_j \\ -1 & \text{si } v_i \text{ es el vértice terminal de } a_j \\ 0 & \text{si } v_i \text{ no es vértice de } a_j \end{cases}$$

### Actividad 5.13

Para el dígrafo de la Figura 5.53 obtener la matriz de incidencia y responder las preguntas que se hacen a continuación:

- a) ¿Qué representa la suma de los elementos de cada fila?
- b) ¿Qué representa la suma de los valores absolutos de los elementos de cada fila?

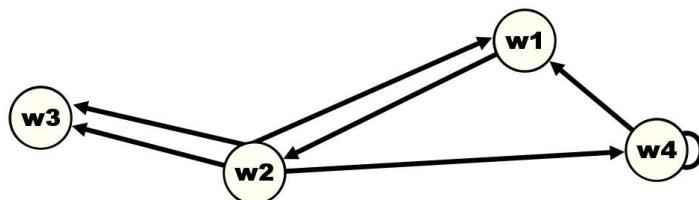


Fig. 5.53. Dígrafo D

### 5.13 Grafo Asociado o subyacente a un dígrafo

#### Definición

Sea  $D = (V, A, \varphi)$  un dígrafo, se dice que  $G = (V, A, \gamma)$  es su grafo asociado si se obtiene del dígrafo ignorando el sentido de las aristas. Si en el dígrafo hay aristas paralelas o antiparalelas, en el grafo asociado sólo se representa una de ellas.

#### Ejemplo 5.26

El grafo asociado al dígrafo D de la Figura 5.54 es el grafo G, que se muestra en la Figura 5.55

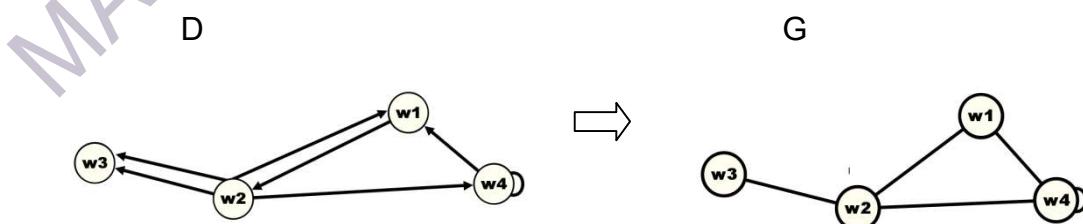


Fig. 5.54. Dígrafo D.

Fig. 5.55. G, grafo asociado de D.

## 5.14 Dígrafo conexo

### Definición

Un dígrafo  $D = (V, A, \varphi)$  se dice conexo si y solo si su grafo asociado es conexo.

### Ejemplo 5.27

El grafo G de la Figura 5.54 es conexo.

## 5.15 Caminos y Circuitos de Euler.

### Definiciones

Sea  $D = (V, A, \varphi)$  un dígrafo.

- Se dice que  $D$  posee camino de Euler o Euleriano si y solo si posee un camino simple que contiene todas las aristas de  $D$ .
- Se dice que  $D$  posee circuito de Euler si y solo si posee un circuito que contiene todas las aristas de  $D$ .

### Condiciones necesarias y suficientes para la existencia de caminos y circuitos de Euler en un dígrafo

Sea  $D = (V, A, \varphi)$  un dígrafo.

- $D$  posee al menos un camino de Euler si y solo si es conexo y  $\forall v \in V$  se cumple que  $g^+(v) = g^-(v)$  a excepción de 2 vértices  $u$  y  $w$ , para los cuales:

$$g^+(u) = g^-(u) - 1 \quad \text{y} \quad g^+(w) = g^-(w) + 1$$

Donde  $u$  sería el vértice de partida y  $w$  el vértice final de todo camino de Euler

- $D$  posee circuito de Euler si y solo si es conexo y  $\forall v \in V$  se cumple que

$$g^+(v) = g^-(v)$$

### □ Ejemplo 5.28

El digrafo de la Figura 5.56 posee circuito de Euler ya que cumple la condición necesaria y suficiente enunciada en el teorema 5.10.1.

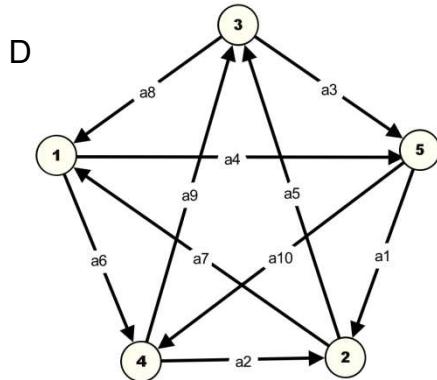


Fig. 5.56. Digrafo con circuito de Euler

Por ejemplo, todos los circuitos cuya secuencia comienza en 4315 estarían representados en el árbol de la Figura 5.57

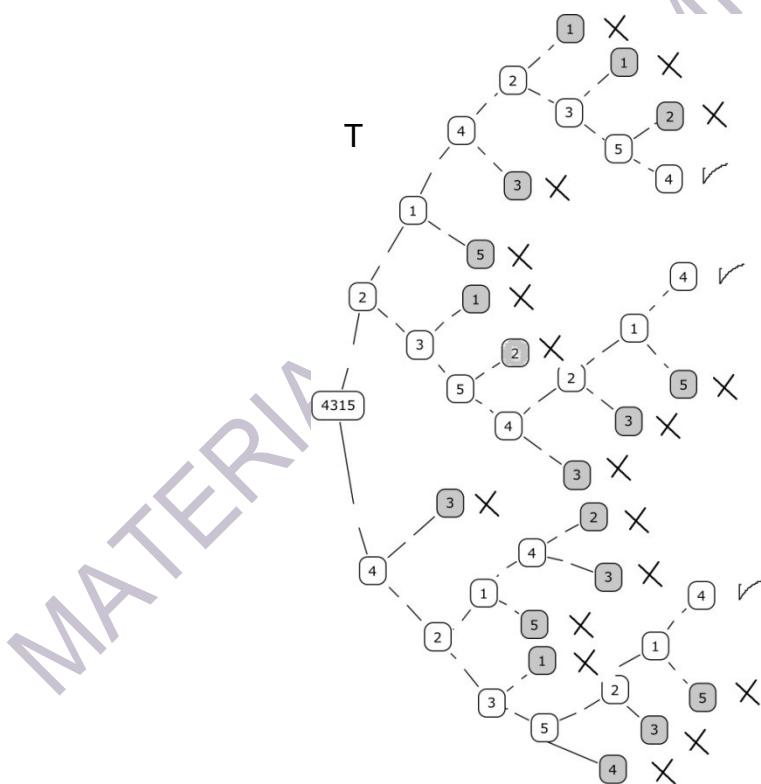


Fig. 5.57. Árbol T.

Del árbol T se desprende que hay tres circuitos de Euler que comienzan con la secuencia 4315, ellos son

$C_1: 43152142354$  ;  $C_2: 43152354214$  y  $C_3: 43154235214$

Observe que se abandonaron los caminos que repetían aristas, por ejemplo la secuencia 431521421; dejándose indicado esto con una cruz al final del camino.

## 5.16 Caminos y Ciclos de Hamilton

### Definiciones

Sea  $D = (V, A, \varphi)$  un digrafo conexo

- Se dice que  $D$  posee caminos de Hamilton si y sólo si posee al menos un camino elemental que pasa por todos los vértice de  $D$  sólo un vez.
- Se dice que  $D$  posee un Ciclo de Hamilton si y solo si posee un camino de Hamilton que es a su vez un ciclo.

### Ejemplos 5.29

El digrafo  $D_1$  (Figura 5.58) posee camino y también ciclo de Hamilton, mientras que  $D_2$  (Figura 5.59) posee camino pero no ciclo de Hamilton.

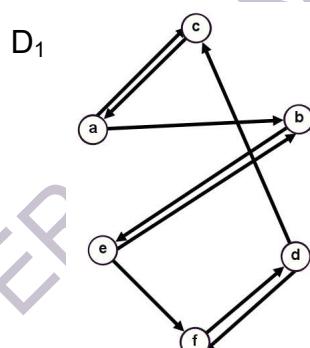


Fig. 5.58. Digrafo  $D_1$ .

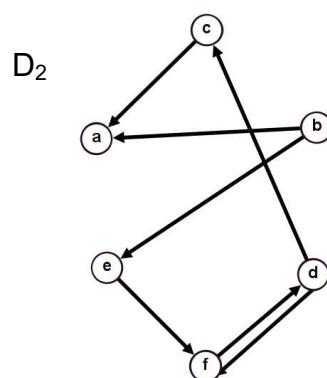


Fig. 5.59. Digrafo  $D_2$ .

En  $D_1$  se puede encontrar al menos el ciclo:  $b \rightarrow f \rightarrow d \rightarrow c \rightarrow b$  y el camino:  $e \rightarrow f \rightarrow d \rightarrow c \rightarrow a$  mientras que en  $D_2$ , observando los grados de los vértices  $a$  y  $b$ , es imposible circular por todos los vértices y volver al punto de partida, pues al visitar el vértice  $a$  no se puede salir de él y nunca se puede visitar  $b$  a menos que se parta de él. Sí posee camino de Hamilton, y uno de ellos es:  $b \rightarrow e \rightarrow f \rightarrow d \rightarrow c \rightarrow a$ .

## Observaciones

- La eliminación de cualquier arista de un ciclo de Hamilton da como resultado un camino de Hamilton.
- Se puede omitir la coma en las secuencias de los caminos, circuitos o ciclos a menos que sea absolutamente necesario usarla.
- Se deja para el estudiante investigar si existen condiciones necesarias y suficientes para la existencia de caminos o ciclos de Hamilton.

### Actividad 5.14

- a) Dado el digrafo  $D_1$  encontrar, si existe, al menos un circuito de Euler y un Ciclo de Hamilton.

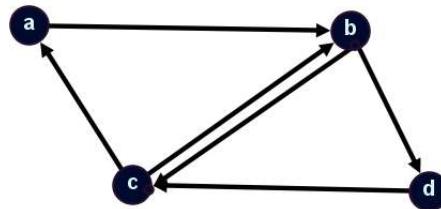


Fig. 5.60. Digrafo  $D_1$ .

- b) Si es que existen, hallar todos los caminos de Euler del digrafo  $D_2$

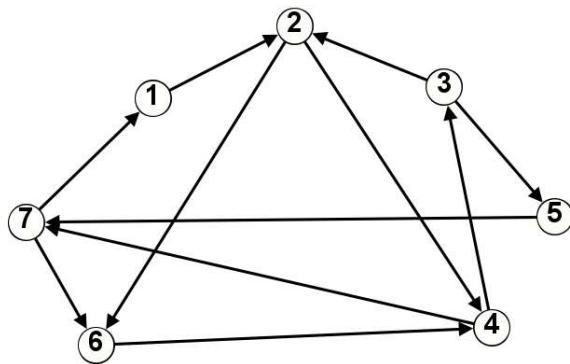


Fig. 5.61. Digrafo  $D_2$ .

- c) Hallar todos los ciclos de Hamilton que comienzan en 7 del digrafo  $D_2$ .

## 5.17 Árbol Dirigido

### Definición

Sea  $D = (V, A, \varphi)$  un dígrafo. Se dice que  $D$  es un árbol dirigido si y solo si su grafo asociado es un árbol no dirigido.

### Notación

En lugar de  $D = (V, A, \varphi)$  se usará frecuentemente  $T = (V, A, \varphi)$

### Caso particular

Si  $|V| = 1$  y  $A = \emptyset$ , a  $T$  se le dice árbol trivial

### Observaciones

- Todo árbol dirigido representa una relación binaria pero no toda relación binaria es un árbol.
- Al no poseer ciclos siempre habrá caminos únicos.

### Cantidad de vértices y aristas de un árbol dirigido

Si  $T = (V, A, \varphi)$  es árbol dirigido, entonces  $|V| = |A| + 1$

### Ejemplo 5.30

El dígrafo de la Figura 5.62 es un árbol dirigido mientras que el de la Figura 5.63 no lo es dado que su grafo asociado es conexo pero con ciclos.

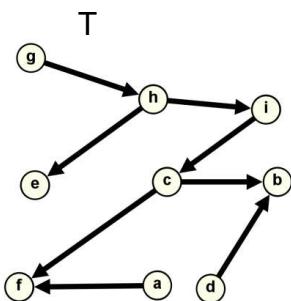


Fig. 5.62. Árbol T.

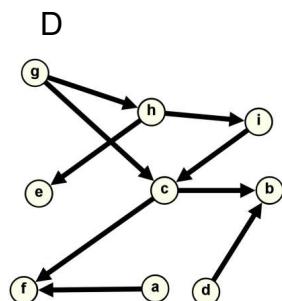


Fig. 5.63. Dígrafo D.

Observar que se verifica el teorema en el árbol que corresponde al dígrafo de la Figura 5.62, posee nueve vértices y ocho aristas.

## 5.18 Árbol Dirigido con Raíz

### Definición

Sea  $D = (V, A, \phi)$  un digrafo, se dice que  $D$  es árbol dirigido con raíz o enraizado si y solo sí existe un vértice  $r$ , tal que:

- i)  $g^+(r) = 0$
- ii)  $\forall v \in V, v \neq r \Rightarrow g^+(v) = 1$

### Notación

Si  $D = (V, A, \phi)$  es un árbol con raíz  $r$  se denota  $T = (V, r)$

### Observación

- Si  $V = \{r\}$  entonces el árbol se dice trivial.

### Ejemplo 5.31

El árbol dirigido  $T$  de la Figura 5.62 no es un árbol con raíz porque no se cumple la definición, mientras que el árbol dirigido de la Figura 5.64 es enraizado con raíz en  $i$ .

Los grados de todos los vértices son:

$$\begin{aligned}g^+(i) &= 0; \\g^+(a) &= g^+(f) = g^+(g) = g^+(c) = g^+(b) = g^+(h) \\&= g^+(e) = g^+(d) = 1\end{aligned}$$

Los cuales cumplen con la definición, de ser un árbol enraizado.

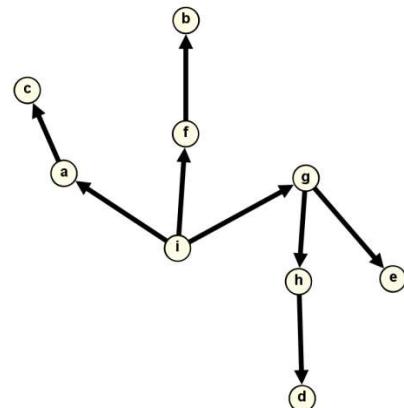


Fig. 5.64. Árbol  $T$ .

### Definiciones

Sea  $T = (V, r)$  un árbol con raíz. Sea  $v \in V$

- Si  $g^-(v) = 0$  entonces se dice que  $v$  es un vértice hoja o terminal.
- Si  $v \neq r$  y  $v$  no es hoja, entonces se dice que  $v$  es un vértice interno.

- Se dice que  $v$  está ubicado en el “nivel  $t$ ”, donde  $t \in \mathbb{N}$ , si y solo si  $v \neq r$  y hay un único camino simple de longitud  $t$  desde  $r$  y hasta  $v$ .
- Se dice que la raíz  $r$  está en el “nivel 0”.
- Se denominas altura del árbol  $T$  al mayor número de nivel alcanzado por las hojas de  $T$ .
- Sean  $v, w \in V$  con  $v \neq w$ . Se dice que  $w$  es antecesor de  $v$  (o que  $v$  es sucesor de  $w$ ) si y sólo si hay un único camino simple de  $w$  a  $v$ .
- Sean  $v, w \in V$  con  $v \neq w$ . Si  $w$  es antecesor de  $v$  y el camino simple que existe de  $w$  a  $v$  es de longitud 1, entonces se dice que  $w$  es padre de  $v$  y  $v$  es hijo de  $w$ .
- Sean  $v, w \in V$  con  $v \neq w$ , ambos en el mismo nivel. Entonces se dice que  $v$  y  $w$  son hermanos si y sólo si tienen el mismo parente.

### Diseño de un árbol con raíz

Se aconseja representar un árbol con raíz del siguiente modo:

- 1) Se ubica a la raíz  $r$ , de la cual se dirá que está en el nivel 0.
- 2) Las aristas que salen de  $r$  se trazan hacia abajo, quedando los hijos de la raíz en el nivel 1
- 3) Se trazan las aristas que salen del nivel 1 hacia abajo, quedando los hijos de los vértices del nivel 1 ubicados en el nivel 2
- 4) Y así sucesivamente con cada nivel....

#### Ejemplo 5.32

La representación aconsejada para el árbol  $T$  de la Figura 5.64 es la que se muestra en la Figura 5.65:

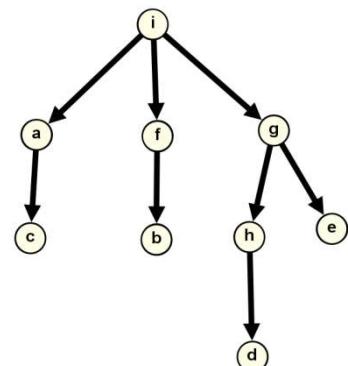


Fig. 5.65. Árbol  $T(i)$ .

### 5.18.1 Propiedades de los árboles con raíz

Sea  $T = (V, r)$  un árbol con raíz. Se cumplen las siguientes propiedades:

- $T$  no tiene circuitos.
- La raíz  $r$  es única.
- Existe un único camino desde la raíz hacia cualquier otro vértice.
- $T$  es una relación arreflexiva, asimétrica y atransitiva.

#### Actividad 5.15

Distinguir cuál de los siguientes dígrafos son árboles con raíz y en caso afirmativo reconocer: raíz, vértices hojas, vértices internos, altura del árbol y nivel de cada vértices.

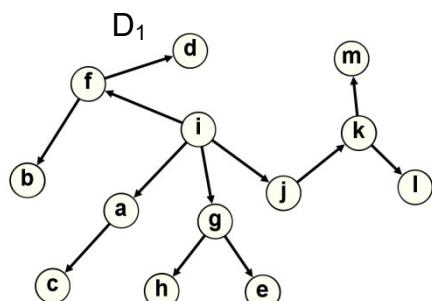


Fig. 5.66. Digrafo  $D_1$ .

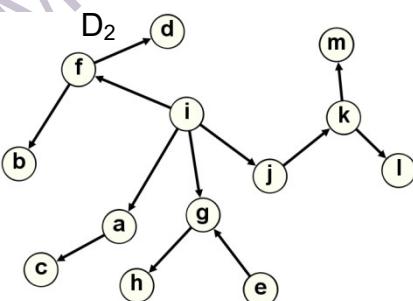


Fig. 5.67. Digrafo  $D_2$ .

#### Definiciones

Sea  $T = (V, r)$  un árbol con raíz  $r$  y sea  $n \in \mathbb{N}$ .

- Se dice que  $T$  es un árbol  $n$ -ario ( $n$ -árbol)  $\Leftrightarrow \forall v \in V : g^-(v) \leq n$ . Esto significa que en este tipo de árboles cada vértice tiene a lo sumo  $n$  hijos.
- Se dice que  $T$  es un árbol  $n$ -ario completo si y sólo si todos los vértices de  $T$ , salvo las hojas, son tales que  $g^-(v) = n$ . Esto significa que en este tipo de árboles cada vértice tiene exáctamente  $n$  hijos.
- $T$  es un árbol 2-ario (o binario) si y solo si cada vértice, salvo las hojas, tiene

a lo sumo 2 hijos.

- T es un árbol binario completo (o regular) si y solo si cada vértice, salvo las hojas, tiene exactamente 2 hijos.
- T es un árbol binario completo y total (o pleno) cuando todas las hojas se encuentran en el mismo nivel

### Propiedades de los árboles binarios

- Sea  $T = (V, r)$  un árbol binario completo, tal que  $|V| = n$ . Sean además  $i$  y  $h$  la cantidad de vértices internos y la cantidad de hojas de  $T$  respectivamente. Entonces se cumple que:

$$h = i + 1 \quad \text{y} \quad n = 2i + 1$$

- Si además  $T$  es un árbol completo y total de altura  $a$ , se cumple que:

$$h = 2^a \quad \text{y} \quad n = 2^{a+1} - 1$$

### Actividad 5.16

Clasificar a los siguientes árboles según la cantidad de hijos. En el caso de ser binarios decir si son completos y totales.

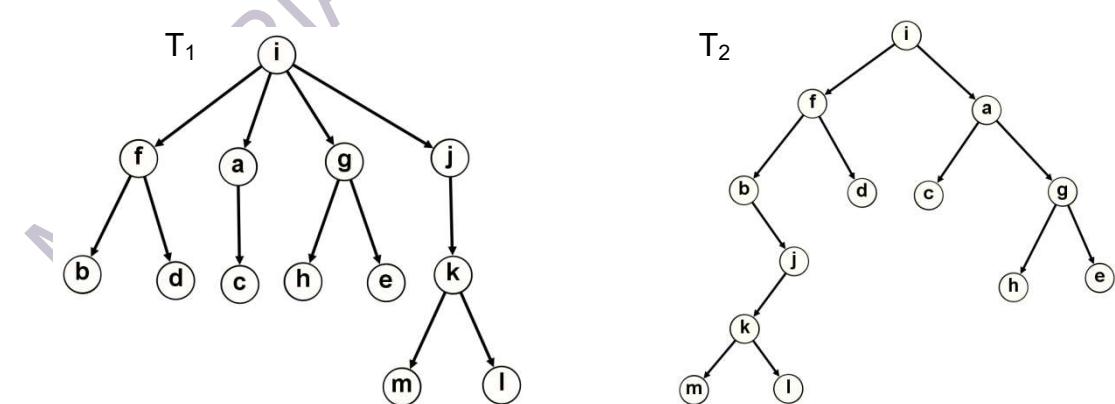


Fig. 5.68. Árbol  $T_1$ .

Fig. 5.69. Árbol  $T_2$ .

$T_3$

$T_4$

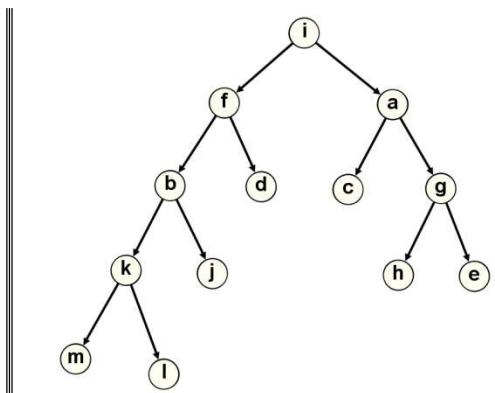


Fig. 5.70. Árbol  $T_3$ .

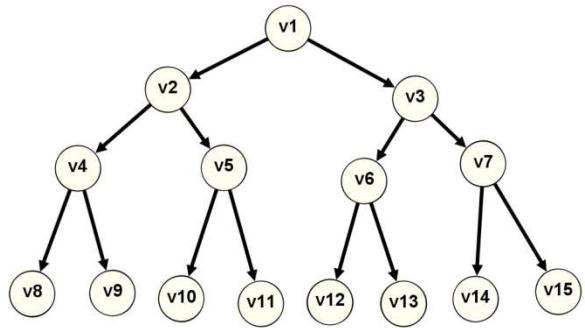


Fig. 5.71. Árbol  $T_4$ .

## 5.19 Subárbol

### Definición

Sea  $T = (V, r)$  un árbol con raíz  $r$  y sea  $v \in V$  tal que  $v \neq r$ . Se llama subárbol de  $T$  de raíz  $v$  y se denota  $T(v)$ , al árbol cuya raíz será  $v$  y sus vértices internos y hojas serán todos los descendientes de  $v$ .

### Ejemplos 5.33

Sea el árbol  $T = (V, v_1)$  de la Figura 5.71. Los subárboles  $T(v_2)$ ,  $T(v_6)$  y  $T(v_{14})$  de  $T$  se muestran en las Figuras 5.72 a 5.74:

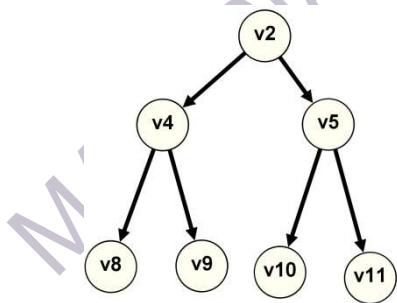


Fig. 5.72. Árbol  $T(v_2)$ .

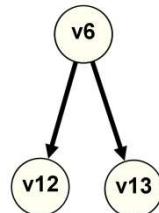


Fig. 5.73. Árbol  $T(v_6)$ .



Fig. 5.74. Árbol  $T(v_{14})$ .

### Observación

Si el vértice considerado es una hoja, el subárbol es un árbol trivial.

## 5.20 Árboles binarios posicionales

### Definición

Sea  $T = (V, r)$  un árbol binario. Se dice que  $T$  es un árbol binario posicional si cada vértice tiene una posición definida: izquierda o derecha.

### Notación

Sea  $T = (V, r)$  un árbol binario posicional, y sea  $r_l$  el hijo izquierdo de  $r$  y  $r_d$  el hijo derecho de  $r$ , donde uno o ambos pueden estar ausentes. Entonces, si existe  $r_l$ , a  $T(r_l)$  se le llama subárbol izquierdo de  $r$  y si existe  $r_d$ , a  $T(r_d)$  se le llama subárbol derecho de  $r$ .

### Observaciones

- Hay árboles binarios posicionales completos y no completos.
- En el caso de los árboles binarios posicionales completos cada vértice interno de un árbol es raíz de un subárbol y por lo tanto poseerá los respectivos subárboles izquierdo y derecho.

### Ejemplos 5.34

Sea el árbol  $T = (V, v_1)$  binario posicional de la Figura 5.75:

Para  $v_1$ ,  $T(v_2)$  es su subárbol izquierdo y  $T(v_3)$  su subárbol derecho.

Para  $v_2$ ,  $T(v_4)$  es su subárbol izquierdo y  $T(v_5)$  su subárbol derecho.

Para  $v_4$ ,  $T(v_8)$  es su subárbol izquierdo y  $T(v_9)$  su subárbol derecho.

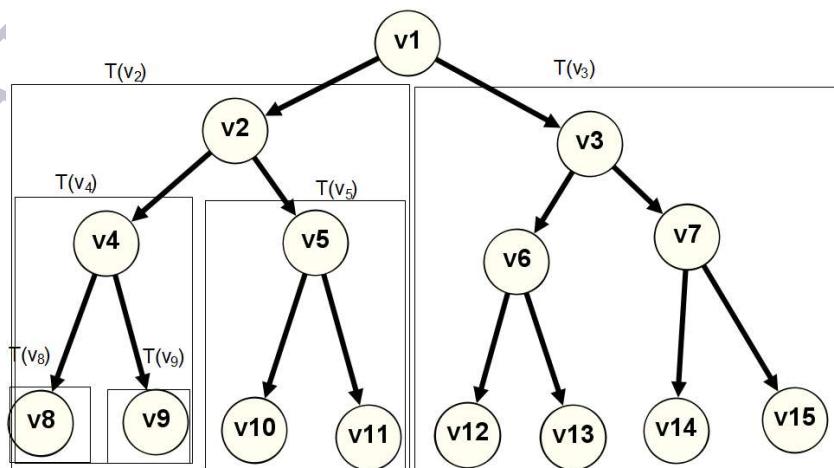


Fig. 5.75. Árbol  $T(v_1)$ .

## 5.21 Recorrido de árboles binarios posicionales

Los árboles binarios posicionales son la base de ciertas aplicaciones como: acceso a datos almacenados en la memoria de un ordenador, representación de expresiones algebraicas en las que se incluyen cantidades numéricas, variables y signos de operación, evaluación de expresiones algebraicas, etc.

Para realizar tales aplicaciones es básico recorrer el árbol posicional, es decir, visitar, de acuerdo a ciertas reglas, todos y cada uno de los vértices que forman ese árbol y anotar la sucesión generada.

Los algoritmos encaminados a visitar los vértices de un árbol ordenado con raíz reciben el nombre de algoritmos de recorrido y los más comunes son: recorrido preorden (orden previo); recorrido entreorden (orden simétrico) y recorrido postorden (orden posterior).

### 5.21.1 Recorrido o Búsqueda en preorden

Sea  $T = (V, r)$  un árbol binario posicional

Paso 1: Visitar  $r$  (anotar)

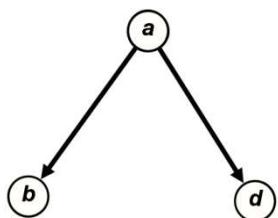
Paso 2: Si existe  $r_i$ , entonces aplicar este algoritmo a  $T(r_i)$

Paso 3: Si existe  $r_d$ , entonces aplicar este algoritmo a  $T(r_d)$

Paso 4: Fin del algoritmo

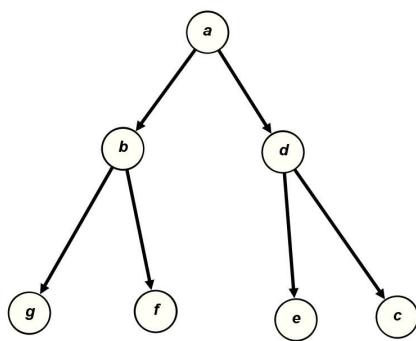
### Ejemplos 5.35

Dados los siguientes árboles, los recorridos en preorden se dan a la derecha de cada figura



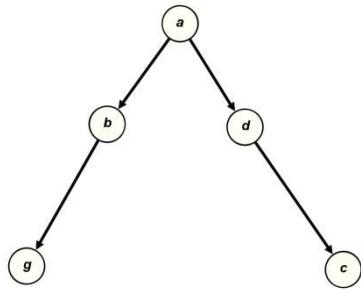
Recorrido en preorden de  $T_1$ : a b d

Fig. 5.76. Árbol  $T_1(a)$ .



Recorrido en preorden de  $T_2$ : a b g f d e c

Fig. 5.77. Árbol  $T_2(a)$ .



Recorrido en preorden de  $T_3$ : a b g d c

Fig. 5.78. Árbol  $T_3(a)$ .

### 5.21.2 Recorrido o Búsqueda en entreorden

Sea  $T = (V, r)$  un árbol binario posicional

Paso 1: Si existe  $r_i$ , entonces aplicar este algoritmo a  $T(r_i)$

Paso 2: Visitar  $r$

Paso 3: Si existe  $r_d$ , entonces aplicar este algoritmo a  $T(r_d)$

Paso 4: Fin del algoritmo

### □ Ejemplos 5.36

El recorrido en entreorden de  $T_1$  (Figura 5.76): b a d

El recorrido en entreorden de  $T_2$  (Figura 5.77): g b f a e d c

El recorrido en entreorden de  $T_3$  (Figura 5.78): g b a d c

### 5.21.3 Recorrido o Búsqueda en posorden

Sea  $T = (V, r)$  un árbol binario posicional

Paso 1: Si existe  $r_i$ , entonces aplicar este algoritmo a  $T(r_i)$

Paso 2: Si existe  $r_d$ , entonces aplicar este algoritmo a  $T(r_d)$

Paso 3: Visitar  $r$

Paso 4: Fin del algoritmo

### □ Ejemplos 5.37

El recorrido en posorden de  $T_1$  (Figura 5.76): b d a

El recorrido en posorden de  $T_2$  (Figura 5.77): g f b e c d a

El recorrido en posorden de  $T_3$  (Figura 5.78): g b c d a

### Actividad 5.17

Obtener los recorridos de los siguientes árboles enraizados:

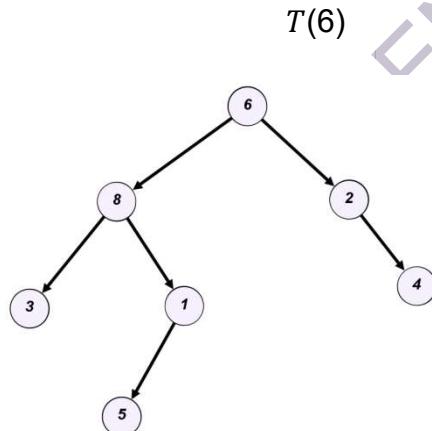


Fig. 5.79. Árbol  $T(6)$ .

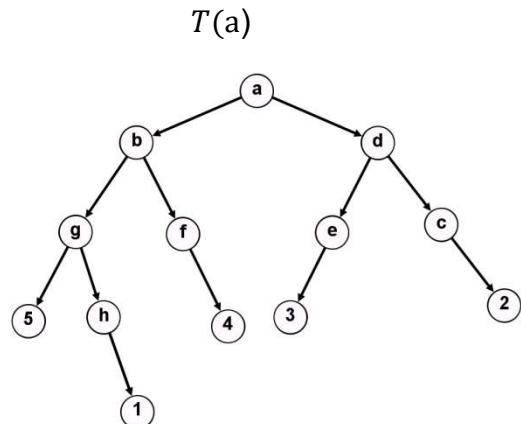


Fig. 5.80.  $T(a)$ .

## 5.22 Aplicación de expresiones algebraicas representadas por medio de árboles dirigidos etiquetados

Para muchos usos de los árboles en las ciencias de la computación, es útil etiquetar los vértices o aristas de un digrafo con información que representa al contexto de la aplicación. Por ejemplo, los árboles binarios etiquetados sirven, para representar operaciones binarias, donde las etiquetas de los vértices son las operaciones y términos involucrados.

### □ Ejemplos 5.38

Las expresiones  $a + b$ ,  $x^y$  y  $p \rightarrow q$  se representan por medio de los siguientes árboles binarios completos:

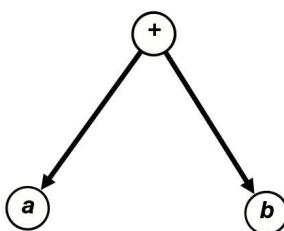


Fig. 5.81. Árbol binario para  $a+b$ .

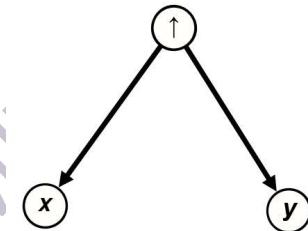


Fig. 5.82. Árbol binario para  $x^y$

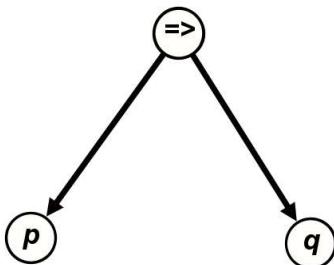


Fig. 5.83. Árbol binario para  $p \rightarrow q$

### Procedimiento para encontrar el árbol etiquetado de una expresión algebraica

- 1) Se etiqueta la raíz con el operador principal de la expresión.
- 2) Se etiqueta a los hijos izquierdo y derecho de la raíz mediante el operador principal de las expresiones para los argumentos de la izquierda y derecha, respectivamente.
- 3) Si un argumento es constante o variable, se lo utiliza para etiquetar el

vértice hoja que corresponde.

- 4) Se continúa con este proceso hasta concluir con la expresión.

□ **Ejemplo 5.39**

La expresión  $(4 + 5(1 + x)) - \frac{z-2}{3}$  se representa por el árbol de la Figura 5.84

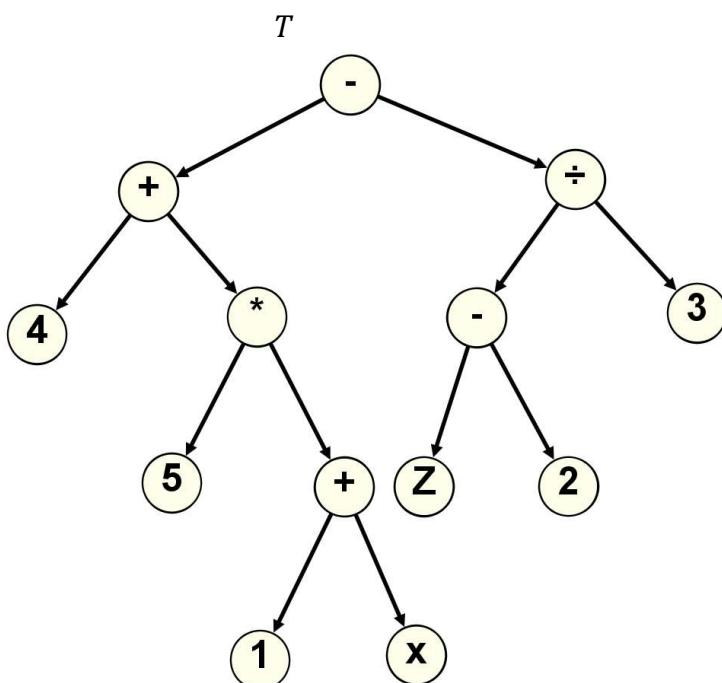


Fig. 5.84. Árbol  $T$ .

**Actividad 5.18**

Confeccionar el árbol correspondiente a las siguientes expresiones algebraicas y responder

a)  $\sqrt{\frac{2}{\frac{1}{x} - (x^2 - y^2)}}$

b)  $\frac{(2-3x)^2}{\sqrt{\frac{x}{5}+1}}$

- a) ¿Cuál es la altura de cada uno de ellos?
- b) ¿Los vértices hojas pueden estar etiquetados con operadores?
- c) Dar el nivel de cada operación en ambos casos.

## 5.23 Notaciones correspondientes a expresiones algebraicas

En el caso de árboles binarios que representen a expresiones algebraicas, los recorridos vistos anteriormente generan notaciones computacionales de las cuales las generadas por el recorrido en preorden y posorden son las más usadas por el ahorro en paréntesis que ellas implican.

La notación generada por el recorrido en preorden se denomina notación infija (o notación polaca), la generada por el recorrido en posorden se denomina notación posfija y la notación generada por el recorrido en entreorden se denomina notación infija, esta última necesita paréntesis en la mayoría de los casos.

### Observaciones

Cabe aclarar que la notación infija, si bien es a la que se está acostumbrado, no coincide totalmente con la notación usual matemática. Esto se ve claramente en los casos de las operaciones división, potenciación y radicación. Por ejemplo:

| Notación infija         | Notación usual                    |
|-------------------------|-----------------------------------|
| $a \div b$              | $\frac{a}{b}$                     |
| $a \uparrow n$          | $a^n$                             |
| $a \uparrow (1 \div n)$ | $a^{\frac{1}{n}}$ o $\sqrt[n]{a}$ |

Tabla 5.7. Diferencias entre las notaciones infija y usual

### Ejemplos 5.40

- a) En la Figura 5.85 se presenta el árbol que representa a la expresión  $\frac{a}{2}$  y a sus correspondientes notaciones

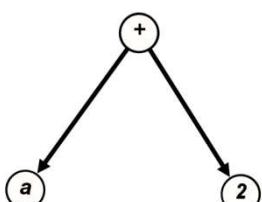


Fig. 5.85.

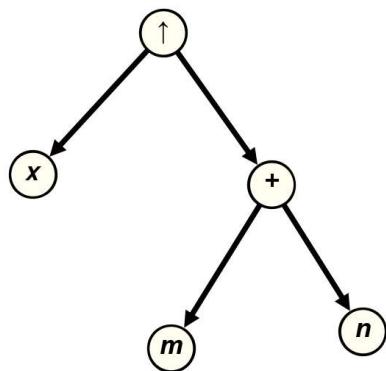
Notación prefija:  $\div a 2$

Notación posfija:  $a 2 \div$

Notación infija:  $a \div 2$

Notación usual:  $\frac{a}{2}$

b) En la Figura 5.86 se presenta el árbol que representa a la expresión  $x^{m+n}$  y a sus correspondientes notaciones



Notación prefija:  $\uparrow x + m n$

Notación posfija:  $x m n + \uparrow$

Notación infija:  $x \uparrow (m + n)$

Notación usual:  $x^{m+n}$

Fig. 5.86.

### Actividad 5.19

- 1) Encontrar los recorridos del árbol  $T$  representado por la Figura 5.84
- 2) Encontrar las notaciones prefija, infija y posfija de las expresiones algebraicas que se dan en cada apartado.

a)  $\sqrt{\frac{2}{\frac{1}{x} - (x^2 - y^2)}}$

b)  $\frac{(2-3x)^2}{\sqrt{\frac{x}{5}+1}}$

- 3) Dada la expresión algebraica:

$$2 \ 3 \ 2 \ a \uparrow * - \ b \ c + 2 \uparrow -$$

Responder

- a) ¿En qué notación está?
- b) ¿Cuáles son las otras notaciones correspondientes a la misma expresión?
- c) ¿Cuál es el valor de la expresión para  $a = 1, b = 2, c = -1$

- 4) Si  $a b + = 7$  y  $b 2 \div = 4$ , calcular el valor de las expresiones que se dan en cada apartado:

- a)  $a 2 b 4 \div \uparrow +$
- b)  $+ \uparrow a 2 \uparrow \div b 2 a$

MATEMÁTICA DISCRETA

UTN – FRT

**Capítulo 6. ESTRUCTURAS ALGEBRAICAS FINITAS**

**Operaciones binarias y unarias cerradas.**

**Propiedades.**

**Principales estructuras algebraicas:**

**Monoides.**

**Semigrupos.**

**Grupos.**

**Anillos.**

**Cuerpos.**

**Álgebras Booleanas.**



## Introducción

En matemáticas aparecen distintos conjuntos cuyos elementos se operan de varias maneras. Los conjuntos numéricos más usuales:  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$  y  $\mathbb{R}$  son ejemplos claros. Otros ejemplos ya conocidos por el estudiante de nivel superior son el conjunto de matrices, el conjunto de vectores y conjunto de funciones con sus operaciones definida de acuerdo a la naturaleza del conjunto.

Por otro lado es fácil observar que operaciones distintas sobre conjuntos distintos tienen propiedades análogas. Estas analogías permiten englobar en una misma "categoría" a distintos conjuntos con operaciones diversas. A dichas categorías se las llama Estructuras Algebraicas.

### 6.1 Estructuras Algebraicas

#### Definición

Una Estructura Algebraica es un objeto matemático consistente en uno o más conjuntos no vacíos, una o más operaciones definidas en ellos. Simbólicamente se lo indica entre paréntesis para indicar que es un objeto único.

(Conjuntos, operación 1 , operación 2 , ...)

#### Ejemplos 6.1

Las siguientes son estructuras ya conocidas por el estudiante. Ellas son:

- $(\mathbb{N}, -)$ , conjunto de los Números Naturales respecto de la operación diferencia usual
- $(\mathbb{Z}, +)$ , conjunto de los Números Enteros respecto de la operación suma usual
- $(\mathbb{R}, +, \cdot)$ , conjunto de los Números Reales respecto de las operaciones suma y producto usuales.
- $(\wp(X), \cup, \cap)$ , donde  $\wp(X)$  es el conjunto Potencia de un conjunto cualquiera  $X$  respecto de las operaciones unión, intersección.
- $(M_{n \times n}(\mathbb{R}), +, \cdot)$ , donde  $M_{n \times n}(\mathbb{R})$  es el conjunto de todas las matrices cuadradas de orden  $n$  de números reales con las operaciones suma y

producto usual.

- f) ( $S$ ,  $\vee$ ,  $\wedge$ ) donde  $S$  es el conjunto de todas las proposiciones respecto de las operaciones disyunción y conjunción.

Según las propiedades de las que gozan las operaciones las estructuras algebraicas se designan con nombres distintos: Monoides, Semigrupos, Grupos, Anillos, Cuerpos, Espacios Vectoriales, Algebras booleanas, etc.

En particular, si el conjunto es finito se tiene una estructura algebraica finita.

## 6.2 Operaciones

Las operaciones son funciones que se aplican sobre el conjunto no vacío y pueden ser del tipo *binarias* o *unarias*.

### 6.2.1 Operación binaria

#### Definición

Sea  $A \neq \emptyset$ , se llama operación binaria sobre  $A$  a toda función cuyo dominio es  $A \times A$ .

Además, la operación binaria es cerrada sobre  $A$  si su imagen es  $A$ . Simbólicamente, si  $*$  es una operación binaria cerrada sobre  $A$ , se lo indica:

$$*: A \times A \rightarrow A$$

$$(a, b) \rightarrow a * b$$

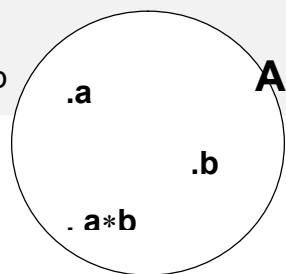


Fig.6.1. Conjunto A.

#### Observación

Las operaciones binarias cerradas (ley de cierre o ley de composición interna) se pueden denotar con el símbolo  $*$  o cualquier otro, como por ejemplo  $+$ ,  $\cdot$ ,  $\otimes$ ,  $\oplus$ ,  $\cup$ ,  $\cap$ ,  $\vee$ ,  $\wedge$ ,  $\blacklozenge$ ,  $\Delta$ ,  $\square$ , etc.

## Notación

Para indicar que en el conjunto A está definida la operación \* se escribe  $(A, *)$ .

La expresión  $a * b$  indica que  $a$  y  $b$  son los operandos izquierdo y derecho respectivamente de  $*$ .

Si el conjunto  $A = \{x_1, x_2, \dots, x_n\}$  es finito, la operación binaria  $* : A \times A \rightarrow A$  puede definirse por medio de una tabla de doble entrada donde se indicará a los elementos de  $A$  en el mismo orden.

| *     | $x_1$ | ... | $x_j$       | ... | $x_n$ | → elementos de A  |
|-------|-------|-----|-------------|-----|-------|---|
| $x_1$ |       |     |             |     |       |   |
| ⋮     |       |     |             |     |       |   |
| $x_i$ |       |     | $x_i * x_j$ |     |       | → La posición $(i, j)$ corresponde al resultado de operar $x_i$ con $x_j$ . |
| ⋮     |       |     |             |     |       |   |
| $x_n$ |       |     |             |     |       |   |

↑  
Tabla 6.1  
↓  
elementos de A

## □ Ejemplos 6.2

- La adición y la multiplicación, denotados respectivamente por “+” y “•”, son cerradas en cada uno de los conjuntos numéricos:  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  y  $\mathbb{C}$
- La adición usual en  $A = \{1, 2, 3, 4, 5\}$  no es cerrada ya que  $3 + 4 \notin A$ .
- En  $A = \{a, b, c\}$  y la operación \* definida por Tabla 6.2 es cerrada en  $A$

| * | a | b | c |
|---|---|---|---|
| a | a | c | b |
| b | b | a | c |
| c | c | b | a |

## Actividad 6.1

Tabla 6.2

Determinar si las siguientes son leyes de composición interna (u operaciones

cerradas) en el conjunto indicado:

- Las operaciones resta y división en los conjuntos numéricos  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  y  $\mathbb{R}$
- Las operaciones suma y multiplicación usual en el conjunto

$$A = \{ x \in \mathbb{Z} / x \text{ es un entero impar}\}$$

- La operación  $*$  :  $A \times A \rightarrow A$  donde  $A = \{-1, 0, 1\}$  y  $*$  está dada por:

|    |    |   |    |
|----|----|---|----|
| *  | -1 | 0 | 1  |
| -1 | 1  | 0 | -1 |
| 0  | 0  | 1 | 0  |
| 1  | -1 | 0 | 1  |

Tabla 6.3

### 6.2.2 Operación Unaria

#### Definición

Sea  $A \neq \emptyset$ , se llama operación unaria sobre  $A$  a toda función con dominio en  $A$ .

Además una operación unaria es cerrada si su dominio e imagen es  $A$ . Simbólicamente, considerando al símbolo ‘’ como identificador de una operación unaria cerrada sobre  $A$ , se tiene:

$$\begin{aligned} ' &: A \rightarrow A \\ a &\rightarrow a' \end{aligned}$$

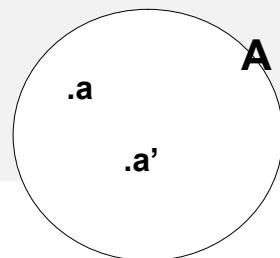


Fig. 6.2. Conjunto A.

#### Observación

Una operación unaria es aquella operación que sólo necesita un operando para encontrar el resultado.

#### Ejemplos 6.3

Son operadores unarios:

- a) La función valor absoluto de un número real,  $| \cdot |$
- b) La operación complemento de un conjunto.
- c) La operación transposición de matrices

### Actividad 6.2

Determinar si los siguientes son operadores unarios cerrados

- a) En  $S = \{ p / p \text{ es una proposición} \}$ , la operación negación
- b) En  $M_{2x3}(\mathbb{R})$ , la operación transposición
- c) En  $M_{3x3}(\mathbb{R})$ , la operación transposición

Hasta ahora se vio lo que significa que una operación sea cerrada en un conjunto. A continuación se verán las propiedades que pueden tener las operaciones cerradas y que son las que marcan la diferencia entre una estructura y otra.

## 6.3 Propiedades de una Operación Cerrada

### 6.3.1 Propiedad conmutativa

#### Definición

Sea  $A$  un conjunto no vacío y sea la operación  $* : A \times A \rightarrow A$ .

Se dice que  $*$  es conmutativa en  $A \Leftrightarrow \forall a, b \in A : a * b = b * a$

#### Ejemplos 6.4

- a) La adición y la multiplicación son conmutativas en  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$  y  $\mathbb{R}$ .
- b) La potenciación en  $\mathbb{Z}$  no es conmutativa, ya que por ejemplo:  $2^3 \neq 3^2$ .
- c) Sea  $A = \{a, 0, b\}$  y la operación binaria  $\otimes$  dada por la siguiente tabla es conmutativa, ya que  $a \otimes 0 = 0 \otimes a ; a \otimes b = b \otimes a ; 0 \otimes b = b \otimes 0$

|           |   |   |   |
|-----------|---|---|---|
| $\otimes$ | a | 0 | b |
|-----------|---|---|---|

|   |   |   |   |
|---|---|---|---|
| a | b | 0 | a |
| 0 | 0 | 0 | 0 |
| b | a | 0 | b |

Tabla 6.4

### Observación

- Los elementos que están “por encima” de la diagonal deben ser los mismos que los que están “por debajo” de la misma. Se observa simetría en la matriz que representa a los resultados, luego  $\otimes$  es conmutativa.

### 6.3.2 Propiedad asociativa

#### Definición

Sea  $A$  un conjunto no vacío y sea la operación  $* : A \times A \rightarrow A$ .

Se dice que  $*$  es asociativa  $\Leftrightarrow \forall a, b, c \in A : a*(b*c) = (a*b)*c$

### Observación

- Los elementos  $a$ ,  $b$  y  $c$  no necesariamente deben ser distintos, por lo que se debe verificar la propiedad en un conjunto finito con menos de 3 elementos.
- Para la demostración de la propiedad asociativa se debe considerar todos los casos posibles. Si  $|A| = n$ , el número total de ternas a considerar es  $n^3$ .

#### Ejemplos 6.5

- La adición y la multiplicación son asociativas en  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$  y  $\mathbb{R}$
- La intersección y unión de conjuntos son asociativas, propiedad ya probada en el capítulo 2.
- La disyunción y la conjunción de proposiciones son operaciones asociativas, propiedad ya probada en el capítulo 1.

### Actividad 6.3

Investigar si las siguientes operaciones son conmutativas y asociativas en los conjuntos dados

- a) En  $S = \{ p / p \text{ es una proposición simple}\}$ , las operaciones  $\rightarrow$  y  $\leftrightarrow$
- c) En  $A = \{a, b\}$ , la operación  $* : A \times A \rightarrow A$  dada por la Tabla 6.5

|   |   |   |
|---|---|---|
| * | a | b |
| a | b | a |
| b | a | b |

Tabla 6.5

### 6.3.3 Existencia del elemento neutro

#### Definición

Sea  $A$  un conjunto no vacío y sea la operación  $* : A \times A \rightarrow A$ .

Se dice que  $A$  posee elemento neutro (o identidad) respecto de  $*$   $\Leftrightarrow$

$$\exists e \in A, \forall a \in A, e * a = a * e = a$$

Es decir, al operar cualquier elemento del conjunto con el neutro el resultado que devuelve es el elemento original.

### 6.3.4 Teorema: Unicidad del elemento neutro

Sea  $A$  un conjunto y sea  $*$  definida en él. Si  $A$  tiene elemento neutro respecto de  $*$  éste es único.

#### Observación

Cuando se trata de un conjunto finito y la operación se presenta por medio de una tabla, para hallar el elemento neutro “ $e$ ” se procede de la siguiente forma: observar si existe un elemento tal que operando por izquierda (ver fila) y por derecha (ver columna) reproduce los encabezados de la tabla.

#### Ejemplos 6.6

- a) En  $\mathbb{Z}$  el número cero es el neutro respecto de la operación suma pues

$$x + 0 = 0 + x = x , \quad \forall x.$$

b) En  $\mathbb{Z}$  el número uno es el neutro respecto de la operación multiplicación pues

$$x \cdot 1 = 1 \cdot x = x , \quad \forall x.$$

c) En el conjunto  $\wp(X)$ , potencia de  $X$  ( $X$ , un conjunto cualquiera), el neutro respecto de la operación unión es  $\emptyset$  y el neutro respecto de la operación intersección es  $X$ , que sería en este caso el universo, ya que para cualquier conjunto  $A \in \wp(X)$  se tendrá que

$$\emptyset \cup A = A \cup \emptyset = A \quad y \quad A \cap X = X \cap A = A$$

d) La operación potenciación no posee neutro en ningún conjunto numérico dado que no existe un elemento  $e$  tal que  $a^e = e^a = a$ .

e) En  $A = \{a, 0, b\}$  existe el elemento neutro respecto de  $\otimes$  dada por la Tabla 6.6

|           |   |   |   |
|-----------|---|---|---|
| $\otimes$ | a | 0 | b |
| a         | b | 0 | a |
| 0         | 0 | b | 0 |
| b         | a | 0 | b |

Tabla 6.6

El elemento neutro es  $b$  ya que  $b \otimes a = a \otimes b = a$ ,  $b \otimes 0 = 0 \otimes b = 0$  y  $b \otimes b = b$

f) La Tabla 6.7 define a la operación  $\oplus$  la cual no posee elemento neutro en el conjunto  $A = \{a, 0, b\}$

|          |   |   |   |
|----------|---|---|---|
| $\oplus$ | a | 0 | b |
| a        | a | 0 | b |
| 0        | 0 | 0 | a |
| b        | a | 0 | b |

Tabla 6.7

### 6.3.5 Existencia de elementos inversos

#### Definición

Sea  $A \neq \emptyset$  y sea la operación binaria cerrada  $*$  respecto de la cual existe

elemento neutro “e”.

Se dice que b es el inverso de a respecto de \* si y solo si  $a * b = b * a = e$

Para indicar que b es el inverso de a generalmente se acostumbra escribir  $a'$  en lugar de b.

Y si se cumple que  $\forall a \in A, \exists a' \in A / a * a' = a' * a = e$  se dice que el conjunto A posee inverso respecto de \*.

### Observaciones

- Si A respecto de la operación \* no posee neutro, entonces tampoco posee elementos inversos.
- Si b es el inverso de a, también se cumple que a es el inverso de b. Esto se desprende de la definición de inverso, observando que en la igualdad planteada ambos elementos juegan el mismo rol
- Cuando se trata de un conjunto finito y la operación está tabulada, para tener el inverso de cada elemento, se detecta en cada fila al elemento neutro (si es que existe). La fila y la columna donde aparece el neutro están señalando a los elementos que son inversos mutuamente.

### Ejemplos 6.7

a) En  $\mathbb{Z}$  existe el inverso respecto de la operación adición, se le llama inverso aditivo (u opuesto). Esto es:

$$\forall a \in \mathbb{Z}, \exists a' = -a \in \mathbb{Z} / a + (-a) = (-a) + a = 0$$

b) En  $\mathbb{R} - \{0\}$  existe el inverso respecto de la multiplicación, se le llama inverso multiplicativo (o recíproco). Esto es:

$$\forall a \in \mathbb{R} - \{0\}, \exists a' = 1/a \in \mathbb{R} - \{0\} / a \cdot (1/a) = (1/a) \cdot a = 1$$

c) En  $A = \{a, 0, b\}$  y la operación  $\otimes$  definida por la tabla 5 donde el elemento neutro es b se tiene que  $a' = a$ ,  $0' = 0$  y  $b' = b$ , luego se puede decir que en el conjunto A todos los elementos poseen inverso respecto de  $\otimes$ .

|           |   |   |   |
|-----------|---|---|---|
| $\otimes$ | a | 0 | b |
| a         | b | 0 | a |
| 0         | 0 | b | 0 |
| b         | a | 0 | b |

Tabla 6.8

**Actividad 6.4**

Determinar si en los siguientes conjuntos existe elemento neutro respecto de las operaciones dadas. Además, en los casos afirmativos investigar si existe el inverso de cada elemento.

- a) En  $M_{n \times n}(\mathbb{R})$ , respecto de la suma y multiplicación usual de matrices
- b) En  $A = \{a, 0, b\}$  y la operación binaria  $\otimes : A \times A \rightarrow A$ , dada por la Tabla 6.9

|           |   |   |   |
|-----------|---|---|---|
| $\otimes$ | a | 0 | b |
| a         | a | 0 | b |
| 0         | 0 | 0 | a |
| b         | b | a | b |

Tabla 6.9

- c) Determinar las propiedades de la operación \* en  $A = \{a, b, c\}$  con la operación \* dada por la Tabla 6.10

|   |   |   |   |
|---|---|---|---|
| * | a | b | c |
| a | c | a | b |
| b | a | b | c |
| c | b | c | a |

Tabla 6.10.

Hasta aquí se presentaron diferentes propiedades que pueden cumplir las operaciones cerradas. Además con las operaciones conocidas, se puede definir nuevas operaciones basándonos en ellas.

**Ejemplo 6.8**

En  $\mathbb{Z}$  se define la operación \* por medio de

$a * b = a + b + 2$ , donde  $+$  es la suma usual

¿Cuáles son las propiedades de  $*$ ?

a) ¿Es  $*$  una operación cerrada en  $\mathbb{Z}$ ? ¿Se cumple que  $\forall a, b \in \mathbb{Z}, a * b \in \mathbb{Z}$ ?

Para la demostración, se toman dos elementos:

Sean  $a \in \mathbb{Z} \wedge b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}$  por ser la suma cerrada en  $\mathbb{Z}$ . Luego como  $2 \in \mathbb{Z} \Rightarrow a + b + 2 \in \mathbb{Z} \Rightarrow a * b \in \mathbb{Z}$ . Por lo tanto la respuesta es sí, la operación  $*$  es cerrada en  $\mathbb{Z}$ .

b) ¿Es  $*$  asociativa en  $\mathbb{Z}$ ?

¿Se cumple que  $\forall a, b, c \in \mathbb{Z}, a * (b * c) = (a * b) * c$ ?

Para la demostración, se desarrolla cada miembro de la igualdad a probar por separado:

$$(I) \quad a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4$$

$$(II) \quad (a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4$$

Las expresiones finales (I) y (II) son iguales. Por lo tanto,  $*$  es asociativa en  $\mathbb{Z}$ .

c) ¿Es  $*$  conmutativa? Para ello se debe analizar si  $\forall a, b \in \mathbb{Z}, a * b = b * a$

Para la demostración, se desarrolla cada miembro de la igualdad a probar por separado:

$$(I) \quad a * b = a + b + 2$$

$$(II) \quad b * a = b + a + 2 = a + b + 2 \text{ por la propiedad conmutativa de la } + \text{ en } \mathbb{Z}.$$

Las expresiones finales (I) y (II) son iguales. Por lo tanto,  $*$  es conmutativa en  $\mathbb{Z}$ .

d) ¿Posee  $*$  elemento neutro en  $\mathbb{Z}$ ?  $\exists e \in \mathbb{Z}, \forall a \in \mathbb{Z}, e * a = a * e = a$ ?

Como se sabe que  $*$  es conmutativa, se busca el neutro sólo a derecha y el mismo será neutro a izquierda.

$$a * e = a \Rightarrow a + e + 2 = a \Rightarrow e + 2 = 0 \Rightarrow e = -2 \in \mathbb{Z}$$

Por lo tanto – 2 es el elemento neutro respecto \* en  $\mathbb{Z}$

e) ¿Existe el elemento inverso respecto de \* para cada elemento de  $\mathbb{Z}$ ?

Se debe analizar si  $\forall a \in \mathbb{Z}, \exists a' \in \mathbb{Z}, a * a' = a' * a = -2$

Como \* es conmutativa, se puede buscar el inverso sólo a derecha y el mismo será inverso a izquierda.

$$a * a' = -2 \Rightarrow a + a' + 2 = -2 \Rightarrow a' = -4 - a \in \mathbb{Z}$$

Esto es, el inverso de cualquier elemento a es  $-4 - a$  el cual existe para todo a.

Por ejemplo,  $5' = -9$ .

La conclusión es que la operación \* posee inverso para todos los elementos del conjunto  $\mathbb{Z}$ .

### Actividad 6.5

En el conjunto  $\mathbb{Z}$  se definen las operaciones  $\circ$  y  $*$  por medio de

$a \circ b = a + b + a.b$  y  $a * b = a + b + 1$  donde '+' y '.' son las operaciones suma y producto usuales.

Determinar si  $\circ$  y  $*$  son operaciones conmutativas y asociativas

Cuando en un conjunto están definidas dos operaciones binarias y cerradas pueden estar vinculadas por alguna propiedad. Por ejemplo, es conocido por todos los estudiantes que en el conjunto de los números reales  $\mathbb{R}$ , la multiplicación es distributiva respecto de la adición. En el conjunto potencia  $\wp(X)$  la unión y la intersección se relacionan por la absorción y la propiedad distributiva. A continuación se definirá formalmente la distributividad.

#### 6.3.6 Distributividad

##### Definición

Sean \* y  $\circ$  dos operaciones cerradas en A. Se dice que  $\circ$  es distributiva

respecto de  $*$   $\Leftrightarrow$

$$\forall a, b, c \in A, a \circ (b * c) = (a \circ b) * (a \circ c) \text{ (distributividad a izquierda)}$$

$$\forall a, b, c \in A, (b * c) \circ a = (b \circ a) * (c \circ a) \text{ (distributividad a derecha)}$$

y, recíprocamente, se dice que  $*$  es distributiva respecto de  $\circ$   $\Leftrightarrow$

$$\forall a, b, c \in A, a * (b \circ c) = (a * b) \circ (a * c) \text{ (distributividad a izquierda)}$$

$$\forall a, b, c \in A, (b \circ c) * a = (b * a) \circ (c * a) \text{ (distributividad a derecha)}$$

Si se cumple que  $\circ$  es distributiva respecto de  $*$  y que  $*$  es distributiva respecto de  $\circ$  se dice que  $*$  y  $\circ$  son mutuamente distributivas

### Ejemplos 6.9

a) En  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$  y  $\mathbb{R}$  la multiplicación es distributiva respecto de la adición:

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad \forall x, y, z$$

$$(y + z) \cdot x = y \cdot x + z \cdot x, \quad \forall x, y, z$$

b) En el conjunto  $\wp(X)$  la unión y la intersección son distributivas mutuamente ya que

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \quad \forall A, B, C$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad \forall A, B, C$$

### Actividad 6.6

a) En  $\mathbb{Z}$  se definen las operaciones  $\circ$  y  $*$  por medio de

$a \circ b = a + b + a \cdot b$  y  $a * b = a + b + 1$  donde '+' y '.' son las operaciones suma y producto usuales.

Determinar si  $\circ$  y  $*$  son distributivas mutuamente.

b) En  $A = \{0, 1\}$  y las operaciones  $+$  y  $\cdot$  definidas por las tablas 6.11 y 6.12.

Determinar si  $\circ$  y  $*$  son distributivas mutuamente

|         |   |   |
|---------|---|---|
| $\circ$ | 0 | 1 |
| 0       | 0 | 1 |

|   |   |   |
|---|---|---|
| * | 0 | 1 |
| 0 | 0 | 0 |

|   |   |   |
|---|---|---|
| 1 | 1 | 1 |
|---|---|---|

Tabla 6.11

|   |   |   |
|---|---|---|
| 1 | 0 | 1 |
|---|---|---|

Tabla 6.12

## 6.4 Principales Estructuras Algebraicas

Las estructuras algebraicas (o sistemas axiomáticos) se clasifican según las propiedades que cumplen las operaciones sobre el conjunto dado. Las principales son:

### 6.4.1 Monoide

#### Definición

Sea  $A \neq \emptyset$ . Se dice que  $M = (A, *)$  es Monoide si y sólo si  $*$  es una operación cerrada ó ley de composición interna.

#### Ejemplos 6.10

- 1)  $(\mathbb{N}, +)$  es un monoide mientras que  $(\mathbb{N}, -)$  no lo es.
- 2)  $(\mathbb{N}, *)$  donde  $*$  está definido como  $a * b = \max \{a, b\}$  es un monoide.

### 6.4.2 Semigrupo

#### Definición

Sea  $A \neq \emptyset$ . Se dice que  $S = (A, *)$  es Semigrupo si y sólo si  $*$  cumple las siguientes condiciones:

- i)  $*: A \times A \rightarrow A$  (\* es ley de composición interna)
- ii)  $\forall a, b, c \in A : a * (b * c) = (a * b) * c$  (\* es asociativa en A)

#### Observaciones

- Si la ley de composición interna también es conmutativa se llama semigrupo conmutativo.
- Si existe el elemento neutro se dice que es un semigrupo con unidad

## □ Ejemplos 6.11

- 1)  $(\mathbb{N}, +)$  es un semigrupo conmutativo sin unidad (sin elemento neutro)
- 2)  $(\mathbb{N}_0, +)$  es un semigrupo conmutativo con unidad (el elemento neutro es 0).
- 3)  $(\mathbb{N}, \cdot)$  es un semigrupo conmutativo con 1 como elemento neutro ó identidad
- 4)  $(M_{m \times n}(\mathbb{R}), +)$ ,  $(\wp(X), \cap)$  y  $(\wp(X), \cup)$  son semigrupos conmutativos con unidad

## Actividad 6.7

Entre las siguientes duplas hay Monoides y Semigrupos. Determinar en cada caso a que estructura corresponde cada apartado

- a)  $(P_n, +)$  donde  $P_n$  es el conjunto de polinomios de grado menor o igual que  $n$ , con coeficientes reales y  $+$  es la operación suma usual de polinomios
- b)  $(A, *)$  siendo  $A = \{1, 2, 3\}$  y  $*$  definida por medio de la Tabla 6.13

|   |   |   |   |
|---|---|---|---|
| * | 1 | 2 | 3 |
| 1 | 3 | 2 | 1 |
| 2 | 2 | 3 | 1 |
| 3 | 1 | 1 | 1 |

Tabla 6.13

### 6.4.3 Grupo

#### Definición

Sea  $A \neq \emptyset$ . Se dice que  $G = (A, *)$  es Grupo si y sólo si  $*$  cumple las siguientes condiciones:

- i)  $*: A \times A \rightarrow A$  (\* es ley de composición interna)
- ii)  $\forall a, b, c \in A, a*(b*c) = (a*b)*c$  (\* es asociativa en A)
- iii)  $\exists e \in A, \forall a \in A / e * a = a * e = a$  (A posee elemento neutro respecto de \*)
- iv)  $\forall a \in A, \exists a' \in A / a * a' = a' * a = e$  (Todos los elementos de A poseen elemento inverso respecto de \*)

#### Observaciones

- Si además  $*$  es conmutativa entonces  $(A; *)$  se dice Grupo ABELIANO, en honor al matemático N. Henrik Abel (1802-1829).
- Si  $G = (A, *)$  es un grupo, se dice que es un grupo finito si el conjunto A es finito y su cardinal se llama orden del grupo.

#### Ejemplos 6.12

- a)  $(\mathbb{Q} - \{0\}, \cdot)$  y  $(\mathbb{R} - \{0\}, \cdot)$  son grupos respecto del producto usual.
- b)  $(\mathbb{N}, +)$  No es grupo, no tiene elemento neutro y por lo tanto tampoco inverso.
- c)  $(\mathbb{N}_0, +)$  No es grupo, aunque tiene neutro, el 0, pero no tiene inverso aditivo.

#### Actividad 6.8

- a) ¿Es  $(M_{2 \times 3}(\mathbb{R}), +)$  grupo abeliano, donde  $M_{2 \times 3}(\mathbb{R})$  es el conjunto de todas las matrices de números reales de orden  $2 \times 3$  y  $+$  es la suma usual? Justificar la respuesta dada.
- b) Sea  $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$  el conjunto de las clases de congruencia módulo 5 en  $\mathbb{Z}$ . Se define la operación suma de clases de

congruencia de la siguiente manera  $[a]_5 + [b]_5 = [a + b]_5$

Determinar que estructura posee  $(\mathbb{Z}_5, +)$

#### 6.4.4 Propiedades de los grupos

Sea  $(A, *)$  un grupo. Entonces se cumple que:

- El inverso de cada elemento es único.
- Si  $a, b \in A$ , entonces las ecuaciones del tipo  $x * a = b$  y  $a * x = b$  admiten solución única en  $A$ .
- $(x')' = x$
- $(x * y)' = y' * x'$

#### Actividad 6.9

- Demostrar que  $(\mathbb{Z}, *)$  es grupo abeliano, donde  $*$  es la operación definida como  $a * b = a + b + 3$
- Completar las tablas 6.14 y 6.15 de tal modo que  $A = \{e, a, b\}$  tenga estructura de Grupo con la operación dada en cada una.
  - $e$  es el elemento neutro
  - $a$  es el elemento neutro y además  $e * b = a$

|   |   |   |   |
|---|---|---|---|
| * | e | a | b |
| e |   |   |   |
| a |   |   |   |
| b |   | e | a |

Tabla 6.14

|   |   |   |   |
|---|---|---|---|
| * | e | a | b |
| e |   |   |   |
| a |   |   |   |
| b |   |   |   |

Tabla 6.15

#### 6.4.5 Subgrupo

##### Definición

Sea  $(A, *)$  un grupo y sea  $B \neq \emptyset$  y  $B \subseteq A$ .

Se dice que  $(B, *)$  es subgrupo de  $(A, *)$  si y solo si  $(B, *)$  es un grupo por sí mismo respecto de la misma operación  $*$

### □ Ejemplo 6.13

$(\mathbb{Z}, +)$  es un subgrupo de  $(\mathbb{Q}, +)$  mientras que  $(\mathbb{N}, +)$  no es subgrupo de  $(\mathbb{Z}, +)$

### 6.4.6 Propiedad de los subgrupos

Sea  $(A, *)$  un grupo y sea  $B \neq \emptyset$  tal que  $B \subseteq A$ , entonces  $B$  es subgrupo de  $A$  si y solo si  $a * b \in B, \forall a, b \in B$

### Actividad 6.10

Dado el grupo  $(A, *)$ , donde  $A = \{a, b, c, d\}$  y  $*$  definida por la tabla 6.16

|   |   |   |   |   |
|---|---|---|---|---|
| * | a | b | c | d |
| a | a | b | c | d |
| b | b | a | d | c |
| c | c | d | a | b |
| d | d | c | b | a |

Tabla 6.16

Demostrar que:

- $B = \{a, b, c\}$  no es subgrupo de  $A$
- $B = \{a, b\}$  es subgrupo de  $A$

### 6.4.7 Anillo

#### Definición

Dado  $A \neq \emptyset$  y dos leyes de composición interna  $*$  y  $\bullet$ , se dice que  $(A, *, \bullet)$  tiene estructura de Anillo si y solo si

- $*$  es asociativa:  $(a * b) * c = a * (b * c)$ ,  $\forall a, b, c \in A$
- $*$  posee elemento neutro en  $A$ :  $\exists e \in A / a * e = e * a = a$ ,  $\forall a$
- Todo elemento de  $A$  posee inverso respecto de  $*$ :  $\forall a, \exists a' \in A / a * a' = a' * a = e$
- $*$  es conmutativa:  $a * b = b * a$ ,  $\forall a, b \in A$
- $\bullet$  es asociativa:  $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ ,  $\forall a, b, c \in A$
- $\bullet$  es distributiva respecto de  $*$ :

$$a \bullet (b * c) = (a \bullet b) * (a \bullet c) \quad y \quad (b * c) \bullet a = (b \bullet a) * (c \bullet a), \quad \forall a, b, c \in A$$

Resumiendo se tiene que:

$(A, *, \bullet)$  es un Anillo si y solo si

- $(A, *)$  es un grupo abeliano ;
- $(A, \bullet)$  es un semigrupo y
- la segunda operación,  $\bullet$ , se distribuye sobre la primera,  $*$ .

#### Observaciones

- Es común escribir  $(A, +, \bullet)$  para representar a una estructura algebraica, tal vez un anillo, pero  $+$  y  $\bullet$  no son forzosamente las operaciones suma y producto usual, salvo que ello esté expresamente indicado.
- El elemento neutro de la operación  $+$  se representa con el símbolo 0 (cero) y el neutro de la operación  $\bullet$  con el símbolo 1 (uno) sin que ellos sean necesariamente los números reales 0 y 1.

Si en el anillo  $(A, *, \bullet)$  se cumple además que:

La operación  $\bullet$  es conmutativa entonces  $(A, *, \bullet)$  es un Anillo conmutativo.

La operación  $\bullet$  posee elemento neutro en A, entonces  $(A, *, \bullet)$  es un Anillo con identidad o Anillo con unidad.

Todo elemento de A distinto de cero es invertible en A respecto de  $\bullet$  entonces  $(A, *, \bullet)$  se llama Anillo de división.

Si además se cumple que elementos no nulos de A dan producto no nulo se dice que  $(A, *, \bullet)$  es un anillo sin divisores de cero.

#### □ Ejemplos 6.14

- \$(\mathbb{Z}, +, \bullet)\$ con las operaciones usuales, es un anillo conmutativo con unidad y sin divisores de cero.
- \$(\mathbb{N}, +, \bullet)\$ con las operaciones conocidas no es un anillo, pues en \$\mathbb{N}\$ no existe neutro para la adición.
- Tampoco lo es \$(\mathbb{N}\_0, +, \bullet)\$ con las operaciones conocidas, pues \$\mathbb{N}\_0\$ carece de inversos aditivos.

#### Actividad 6.11

Sea \$X = \{a, b\}\$ y sea \$A = \wp(X) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}\$.

Demostrar que \$(\wp(X), \oplus, \cap)\$ es un anillo, donde \$\oplus\$, la operación diferencia simétrica y \$\cap\$, la operación intersección están dadas por las tablas 6.16 y 6.17

| $\oplus$    | $\emptyset$ | $\{a\}$     | $\{b\}$     | $\{a,b\}$   |
|-------------|-------------|-------------|-------------|-------------|
| $\emptyset$ | $\emptyset$ | $\{a\}$     | $\{b\}$     | $\{a,b\}$   |
| $\{a\}$     | $\{a\}$     | $\emptyset$ | $\{a,b\}$   | $\{b\}$     |
| $\{b\}$     | $\{b\}$     | $\{a,b\}$   | $\emptyset$ | $\{a\}$     |
| $\{a,b\}$   | $\{a,b\}$   | $\{b\}$     | $\{a\}$     | $\emptyset$ |

Tabla 6.16

| $\cap$      | $\emptyset$ | $\{a\}$     | $\{b\}$     | $\{a,b\}$   |
|-------------|-------------|-------------|-------------|-------------|
| $\emptyset$ | $\emptyset$ | $\emptyset$ | $\emptyset$ | $\emptyset$ |
| $\{a\}$     | $\emptyset$ | $\{a\}$     | $\emptyset$ | $\{a\}$     |
| $\{b\}$     | $\emptyset$ | $\emptyset$ | $\{b\}$     | $\{b\}$     |
| $\{a,b\}$   | $\emptyset$ | $\{a\}$     | $\{b\}$     | $\{a,b\}$   |

Tabla 6.17

Sugerencia: Usar los conceptos vistos de Teoría de Conjuntos para justificar sus afirmaciones

### 6.4.8 Cuerpo

#### Definición

Sea  $A \neq \emptyset$  y sean dos operaciones binarias  $*$  y  $\bullet$  definidas en  $A$ . Se dice que  $(A, *, \bullet)$  es un cuerpo si y solo si

- i)  $(A, *)$  es un grupo abeliano.
- ii)  $(A - \{0\}, \bullet)$  es un grupo abeliano, donde 0 es el neutro respecto de  $*$ .
- iii)  $\bullet$  se distribuye respecto de  $*$ .

En resumen,  $(A, *, \bullet)$  es un cuerpo si y solo si  $(A, *, \bullet)$  es un anillo conmutativo, con unidad y cuyos elementos no nulos admiten inverso multiplicativo.

#### Ejemplos 6.15

- 1)  $(\mathbb{Z}, +, \bullet)$  con las operaciones suma y producto usual no es cuerpo, pues  $\mathbb{Z}$  carece de inversos multiplicativos.
- 2)  $(\mathbb{Q}, +, \bullet)$ ,  $(\mathbb{R}, +, \bullet)$  y  $(\mathbb{C}, +, \bullet)$  con las operaciones suma y producto usual son cuerpos.

#### Actividad 6.12

Determinar si cada uno de los siguientes conjuntos tiene estructura de Cuerpo

- a)  $A$  es el conjunto de los enteros pares respecto de la suma y producto usuales.
- b)  $A = \{0, 1\}$  y las operaciones '+' y '.' definidas por las siguientes tablas:

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Tabla 6.18

| . | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Tabla 6.19

## 6.5 Álgebra de Boole

### Definición

Sea  $B$  un conjunto con al menos dos elementos que se indican con  $0$  y  $1$ ; y sean dos operaciones binarias cerradas denotadas con  $+$  y  $\cdot$ .

Se dice que la terna  $(B, +, \cdot)$  es un Álgebra de Boole si y solo si se satisfacen las siguientes propiedades:

1) leyes asociativas:  $\forall x, y, z \in B$ ,

$$x + (y + z) = (x + y) + z$$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

2) leyes conmutativas:  $\forall x, y \in B$ ,

$$x + y = y + x$$

$$x \cdot y = y \cdot x$$

3) Leyes distributivas:  $\forall x, y, z \in B$

$$x + y \cdot z = (x + y) \cdot (x + z)$$

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

4) Existencia de elementos neutros (Ley de Identidad):

$$\exists 0 \in B / \forall x \in B, x + 0 = 0 + x = x$$

$$\exists 1 \in B / \forall x \in B, x \cdot 1 = 1 \cdot x = x$$

5) Existencia de complemento:

$$\forall x \in B, \exists x' \in B / x + x' = 1 \quad y \quad x \cdot x' = 0$$

M

### Actividad 6.13

Sea  $B = \{0, 1\}$  y las operaciones  $+$  y  $\cdot$  definidas por las tablas 6.20 y 6.21

|   |   |   |
|---|---|---|
| + | 0 | 1 |
| 0 | 0 | 1 |

|   |   |   |
|---|---|---|
| . | 0 | 1 |
| 0 | 0 | 0 |

|   |   |   |
|---|---|---|
| 1 | 1 | 1 |
|---|---|---|

Tabla 6.20

|   |   |   |
|---|---|---|
| 1 | 0 | 1 |
|---|---|---|

Tabla 6.21

Demostrar que  $(B, +, \cdot)$  tiene estructura de Álgebra de Boole.

### 6.5.1 Álgebra de Boole de los Conjuntos Potencias

#### Teorema

Sea  $X$  conjunto finito y sea  $\wp(X)$  el conjunto potencia de  $X$ .

$(\wp(X), \cup, \cap)$  es un Álgebra de Boole para todo conjunto  $X$ .

#### Demostración

Se demostraron en el capítulo 2 las propiedades de las operaciones unión e intersección. En particular, se vio que:

i) la asociatividad se cumple para ambas operaciones

$$A \cup (B \cup C) = (A \cup B) \cup C \quad A \cap (B \cap C) = (A \cap B) \cap C$$

ii) Se cumple la comutatividad para ambas operaciones

$$A \cup B = B \cup A \quad A \cap B = B \cap A$$

iii) Se cumple la distributividad mutua de ambas operaciones

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

iv) Se observa la existencia de los elementos neutros

$$A \cup \emptyset = A, \quad A \cap U = A \text{ (en este caso el universo es } X\text{)}$$

Siempre existe el conjunto complemento de cada conjunto

$$\forall A \in \wp(X), \exists A' \in \wp(X) / A' = X - A$$

Por lo tanto  $(\wp(X), \cup, \cap)$  es un Álgebra de Boole, para todo  $X$

### □ Ejemplo 6.16

Si  $X = \{a, b, c\}$  entonces  $\wp(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}$  entonces  $(\wp(X), \cup, \cap)$  es un Álgebra de Boole cuyos neutros son  $\emptyset$  y  $X$  son los neutros respecto de  $\cup$  e  $\cap$  respectivamente y los complementos son:

$$\emptyset' = X \quad y \quad X' = \emptyset \quad \text{ya que } \emptyset \cup X = X \quad y \quad \emptyset \cap X = \emptyset$$

$$\{a\}' = \{b, c\} \quad y \quad \{b, c\}' = \{a\} \quad \text{ya que } \{a\} \cup \{b, c\} = X \quad y \quad \{a\} \cap \{b, c\} = \emptyset$$

$$\{b\}' = \{a, c\} \quad y \quad \{a, c\}' = \{b\} \quad \text{ya que } \{b\} \cup \{a, c\} = X \quad y \quad \{b\} \cap \{a, c\} = \emptyset$$

$$\{c\}' = \{a, b\} \quad y \quad \{a, b\}' = \{c\} \quad \text{ya que } \{c\} \cup \{a, b\} = X \quad y \quad \{c\} \cap \{a, b\} = \emptyset$$

### 6.5.2 Álgebra de Boole de los divisores de un número entero positivo

Sea  $n \in \mathbb{N}$  y sea  $D_n = \{x \in \mathbb{N}, x | n\}$  el conjunto de los divisores positivos de  $n$

Definiendo las siguientes operaciones

$$x + y = mcm\{x, y\}$$

$$x * y = mcd\{x, y\}$$

Se genera la estructura  $(D_n, +, *)$  y de allí surge la pregunta ¿Cuáles son las propiedades de las operaciones '+' y '\*'?

### Teorema sobre las Álgebras Booleanas $D_n$

$D_n$  es un Álgebra Booleana si y solo si  $n = p_1 \cdot p_2 \dots \cdot p_k$  donde  $p_1, p_2, \dots, p_k$  son números primos distintos.

### □ Ejemplos 6.17

$D_2$  es un álgebra booleana pues  $2=2$

$D_6$  es un álgebra booleana pues  $6 = 2 \cdot 3$

$D_8$  no es un álgebra booleana pues  $8 = 2 \cdot 2 \cdot 2$

$D_{20}$  no es un álgebra booleana pues  $20 = 2 \cdot 2 \cdot 5$

$D_{30}$  es un álgebra booleana pues  $30 = 2 \cdot 3 \cdot 5$

En el caso del Álgebra Booleana  $D_{30}$  las tablas de las operaciones '+' y '\*' serían las siguientes:

| +  | 1  | 2  | 3  | 5  | 6  | 10 | 15 | 30 |
|----|----|----|----|----|----|----|----|----|
| 1  | 1  | 2  | 3  | 5  | 6  | 10 | 15 | 30 |
| 2  | 2  | 2  | 6  | 10 | 6  | 10 | 30 | 30 |
| 3  | 3  | 6  | 3  | 15 | 6  | 30 | 15 | 30 |
| 5  | 5  | 10 | 15 | 5  | 30 | 10 | 15 | 30 |
| 6  | 6  | 6  | 6  | 30 | 6  | 30 | 30 | 30 |
| 10 | 10 | 10 | 30 | 10 | 30 | 10 | 30 | 30 |
| 15 | 15 | 30 | 15 | 15 | 30 | 30 | 15 | 30 |
| 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 |

Tabla 6.22

| *  | 1 | 2 | 3 | 5  | 6 | 10 | 15 | 30 |
|----|---|---|---|----|---|----|----|----|
| 1  | 1 | 1 | 1 | 1  | 1 | 1  | 1  | 1  |
| 2  | 1 | 2 | 1 | 1  | 2 | 2  | 1  | 2  |
| 3  | 1 | 1 | 3 | 1  | 3 | 1  | 3  | 3  |
| 5  | 1 | 1 | 1 | 5  | 1 | 10 | 5  | 5  |
| 6  | 1 | 2 | 3 | 1  | 6 | 2  | 3  | 6  |
| 10 | 1 | 2 | 1 | 10 | 2 | 10 | 5  | 10 |
| 15 | 1 | 1 | 3 | 5  | 3 | 5  | 15 | 15 |
| 30 | 1 | 2 | 3 | 5  | 6 | 10 | 15 | 30 |

Tabla 6.23

Observe que los neutros son : 1 para la operación '+' y 30 para la operación '\*'.

Los complementos son:

$$1' = 30 \text{ y } 30' = 1 \text{ ya que } 1 + 30 = 30 \text{ y } 1 \cdot 30 = 1$$

$$2' = 15 \text{ y } 15' = 2 \text{ ya que } 2 + 15 = 30 \text{ y } 2 \cdot 15 = 1$$

$$3' = 10 \text{ y } 10' = 3 \text{ ya que } 3 + 10 = 30 \text{ y } 3 \cdot 10 = 1$$

$$5' = 6 \text{ y } 6' = 5 \text{ ya que } 5 + 6 = 30 \text{ y } 5 \cdot 6 = 1$$

#### Actividad 6.14

- a) Determinar si los siguientes conjuntos son Algebras de Boole usando el teorema 6.6.3.

$$D_{21}, D_{25}, D_{40}, D_{60}, D_{105}, D_{165}$$

- b) En los casos afirmativos confeccione las tablas de las operaciones '+' y '\*', y determine los neutros y complementos en cada caso.



# Contenido

|   |    |
|---|----|
| Capítulo 1. LÓGICA PROPOSICIONAL Y DE PRIMER ORDEN..... | 0  |
| 1.1 Proposición .....                                   | 2  |
| 1.1.1 Valor de verdad .....                             | 4  |
| 1.1.2 Proposiciones Simples y Compuestas .....          | 5  |
| 1.2 Conectivos lógicos .....                            | 7  |
| 1.2.1 Negación .....                                    | 8  |
| 1.2.2 Conjunción o Producto Lógico.....                 | 9  |
| 1.2.3 Disyunción Inclusiva o Suma Lógica .....          | 10 |
| 1.2.4 Disyunción Excluyente o Diferencia Simétrica..... | 10 |
| 1.2.5 Implicación o condicional .....                   | 11 |
| 1.2.6 Bicondicional o doble implicación .....           | 12 |
| 1.2.7 Tablas de verdad.....                             | 13 |
| 1.3 Tautologías, Contradicciones y Contingencias .....  | 16 |
| 1.4 Conectivo Principal .....                           | 16 |
| 1.5 Equivalencias Lógicas .....                         | 17 |
| 1.5.1 Principales leyes lógicas .....                   | 18 |
| 1.5.2 Expresiones lógicas duales .....                  | 24 |
| 1.6 Implicación Lógica .....                            | 25 |
| 1.6.1 Razonamientos o Argumentos.....                   | 26 |
| 1.6.2 Validez de un argumento .....                     | 27 |
| 1.7 Reglas de Inferencia .....                          | 28 |
| 1.7.1 Modus Ponens (MP) .....                           | 28 |
| 1.7.2 Modus Tollens (MT) .....                          | 29 |
| 1.7.3 Adición disyuntiva.....                           | 31 |
| 1.7.4 Combinación conjuntiva.....                       | 32 |

|  |           |
|--|-----------|
| 1.7.5 Simplificación de la conjunción .....                          | 33        |
| 1.7.6 Silogismo hipotético (SH) .....                                | 34        |
| 1.7.7 Silogismo disyuntivo (SD) .....                                | 36        |
| <b>1.8 Tipos de demostraciones para validar un razonamiento.....</b> | <b>37</b> |
| 1.8.1 Método directo.....  | 38        |
| 1.8.2 Métodos Indirectos .....                                       | 40        |
| <b>1.9 Lógica de Predicados de Primer Orden .....</b>                | <b>45</b> |
| 1.9.1 Predicados.....  | 45        |
| 1.9.2 Cuantificadores .....  | 46        |
| 1.9.3 Predicados equivalentes.....                                   | 49        |
| 1.9.4 Implicación entre predicados.....                              | 49        |
| 1.9.5 Negación de Cuantificadores.....                               | 50        |
| 1.9.6 Reglas de Inferencias.....                                     | 52        |
| <b>Capítulo 2. CONJUNTOS Y RELACIONES.....</b>                       | <b>59</b> |
| 2.1 Conjuntos y Elementos .....                                      | 61        |
| 2.1.1 Determinación por Extensión .....                              | 62        |
| 2.1.2 Determinación por Comprensión.....                             | 62        |
| 2.2 Conjuntos finitos e infinitos.....                               | 63        |
| 2.3 Conjuntos especiales: Vacío, Unitario, Universal.....            | 65        |
| 2.4 Igualdad de Conjuntos .....                                      | 66        |
| 2.5 Conjuntos Disjuntos .....  | 67        |
| 2.6 Diagramas de Venn .....  | 67        |
| 2.7 Inclusión de conjuntos. Subconjuntos .....                       | 69        |
| 2.8 Conjunto Potencia de un conjunto finito.....                     | 73        |
| 2.9 Álgebra de Conjuntos: Operaciones .....                          | 75        |
| 2.9.1 Unión .....  | 75        |

|   |            |
|---|------------|
| 2.9.2 Intersección.....                           | 76         |
| 2.9.3 Diferencia .....                            | 76         |
| 2.9.4 Complemento.....                            | 77         |
| 2.9.5 Diferencia simétrica.....                   | 78         |
| <b>2.10 Leyes del Álgebra de Conjuntos .....</b>  | <b>82</b>  |
| 2.10.1 Leyes de Idempotencia .....                | 82         |
| 2.10.2 Leyes Conmutativas .....                   | 82         |
| 2.10.3 Leyes Asociativas .....                    | 83         |
| 2.10.4 Leyes Distributivas .....                  | 83         |
| 2.10.5 Leyes de Absorción .....                   | 84         |
| 2.10.6 Leyes de los Complementos .....            | 85         |
| 2.10.7 Ley de Involución o Involutiva .....       | 85         |
| 2.10.8 Leyes de De Morgan.....                    | 86         |
| 2.10.9 Leyes de los elementos neutros .....       | 86         |
| 2.10.10 Leyes de Dominación .....                 | 87         |
| <b>2.11 Partición de un conjunto .....</b>        | <b>88</b>  |
| <b>2.12 Producto Cartesiano.....</b>              | <b>89</b>  |
| <b>2.13 Relaciones entre conjuntos .....</b>      | <b>91</b>  |
| 2.13.1 Relaciones binarias .....                  | 92         |
| 2.13.2 Dominio e Imagen .....                     | 93         |
| 2.13.3 Conjunto Relativo de un elemento .....     | 93         |
| 2.13.4 Función .....                              | 94         |
| <b>2.14 Matriz de una Relación Binaria.....</b>   | <b>96</b>  |
| 2.14.1 Operaciones con matrices booleanas .....   | 97         |
| 2.14.2 Matriz de adyacencia de una Relación ..... | 100        |
| <b>2.15 Digrafo .....</b>                         | <b>101</b> |

|   |     |
|---|-----|
| 2.15.1 Representación gráfica de un Dígrafo .....                                   | 102 |
| 2.16 Composición de Relaciones .....  | 103 |
| 2.17 Relaciones Compuestas .....  | 104 |
| 2.17.1 Trayectorias en Dígrafos .....   | 106 |
| 2.18 Propiedades de las Relaciones Binarias.....                                    | 106 |
| 2.18.1 Reflexividad.....  | 106 |
| 2.18.2 Simetría.....  | 107 |
| 2.18.3 Asimetría .....  | 108 |
| 2.18.4 Antisimetría .....   | 108 |
| 2.18.5 Transitividad.....   | 109 |
| 2.19 Relaciones de Equivalencia.....  | 111 |
| 2.19.1 Dígrafo asociado a una Relación de Equivalencia .....                        | 114 |
| 2.19.2 Clase de equivalencia de un elemento .....                                   | 114 |
| 2.19.3 Conjunto Cociente de una Relación de Equivalencia.....                       | 115 |
| 2.20 Relaciones de Orden .....  | 119 |
| 2.20.1 Conjuntos parcialmente ordenados.....  | 121 |
| 2.20.2 Elementos comparables en un conjunto ordenado .....                          | 122 |
| 2.20.3 Diagrama de Hasse .....  | 122 |
| 2.20.4 Elementos extremos de una Relación de Orden .....                            | 124 |
| Capítulo 3. TEORÍA DE NÚMEROS ENTEROS .....   | 127 |
| 3.1 El conjunto de los Números Enteros .....  | 129 |
| 3.1.1 Propiedades de las operaciones adición y multiplicación en $\mathbb{Z}$ ..... | 130 |
| 3.2 División en $\mathbb{Z}$ .....  | 133 |
| 3.2.1 Operadores binarios <b><i>div</i></b> y <b><i>mod</i></b> .....               | 135 |
| 3.3 Divisibilidad: Divisores y múltiplos.....                                       | 137 |
| 3.3.1 Propiedades de la divisibilidad .....   | 139 |

|  |   |     |
|--|---|-----|
| 3.4  | Números Primos y Compuestos .....   | 142 |
| 3.5  | Máximo Común Divisor.....   | 148 |
| 3.5.1  | Números Coprimos o Primos relativos.....  | 155 |
| 3.6  | Ecuaciones diofánticas .....  | 158 |
| 3.6.1  | Solución general .....  | 159 |
| 3.7  | Congruencia en $\mathbb{Z}$ .....   | 162 |
| 3.8  | Relación de Congruencia módulo n.....   | 164 |
| 3.8.1  | Conjunto Cociente de una Relación de Congruencia .....  | 165 |
| Capítulo 4. SUCESIONES, INDUCCIÓN Y RECURSIVIDAD ..... |   | 169 |
| 4.1  | Sucesión .....  | 171 |
| 4.2  | Igualdad de sucesiones .....  | 173 |
| 4.3  | Sucesiones particulares.....  | 174 |
| 4.3.1  | Arreglos .....  | 174 |
| 4.3.2  | Palabras.....   | 174 |
| 4.4  | Sucesiones Numéricas.....   | 175 |
| 4.4.1  | Progresión Aritmética.....  | 177 |
| 4.4.2  | Progresión Geométrica .....   | 178 |
| 4.5  | Símbolo Suma .....  | 179 |
| 4.6  | Inducción Matemática .....  | 182 |
| 4.7  | Recursión o Recursividad .....  | 185 |
| 4.7.1  | Solución de una relación de recurrencia.....  | 187 |
| 4.8  | Clasificación de las Relaciones de Recurrencia .....  | 189 |
| 4.8.1  | Solución de las relaciones de recurrencia lineales, de primer orden, homogéneas y de coeficientes constantes..... | 190 |
| 4.8.2  | Solución de las relaciones de recurrencia lineal, de segundo orden, homogéneas y con coeficientes constantes..... | 191 |

|   |     |
|---|-----|
| Capítulo 5. GRAFOS Y DIGRAFOS. ÁRBOLES .....  | 195 |
| 5.1    Grafo no dirigido.....   | 197 |
| Representación gráfica .....  | 198 |
| 5.1.1 Grado de un vértice.....  | 200 |
| 5.2    Subgrafos.....   | 201 |
| 5.2.1 Subgrafos particulares .....  | 202 |
| 5.3    Caminos en un Grafo no Dirigido .....  | 204 |
| 5.4    Representaciones matriciales de un grafo .....   | 208 |
| 5.4.1 Matriz de Adyacencia.....   | 208 |
| 5.5    Matriz de Incidencia .....   | 209 |
| 5.6    Grafos especiales .....  | 211 |
| 5.6.1 Grafos conexos .....  | 211 |
| 5.6.2 Grafo completo .....  | 212 |
| 5.6.3 Grafo bipartito .....   | 213 |
| 5.6.4 Grafo regular.....  | 214 |
| 5.7    Caminos y circuitos de Euler.....  | 215 |
| 5.7.1 Condiciones necesarias y suficientes para la existencia de caminos y ciclos de Euler..... | 216 |
| 5.8    Caminos y Ciclo de Hamilton .....  | 217 |
| 5.8.1 Condiciones Suficientes para la existencia de caminos y ciclos de Hamilton                | 219 |
| 5.9    Isomorfismos de Grafos .....   | 220 |
| 5.9.1 Condiciones invariantes bajo isomorfismo.....   | 221 |
| 5.10    Árbol no dirigido .....   | 225 |
| 5.10.1 Digrafo o Grafo Dirigido.....  | 227 |
| 5.10.2 Representación gráfica .....   | 227 |
| 5.10.3 Grados de un vértice .....   | 229 |

|             |   |     |
|-------------|---|-----|
| 5.11        | Caminos, Caminos Simples, Caminos Elementales, Circuitos y Ciclos<br>230                                |     |
| 5.12        | Representaciones matriciales de un digrafo.....   | 233 |
| 5.12.1      | Matriz de Adyacencia .....  | 233 |
| 5.12.2      | Matriz de Incidencia .....  | 235 |
| 5.13        | Grafo Asociado o subyacente a un digrafo.....   | 236 |
| 5.14        | Digrafo conexo .....  | 237 |
| 5.15        | Caminos y Circuitos de Euler. ....  | 237 |
| 5.16        | Caminos y Ciclos de Hamilton.....   | 239 |
| 5.17        | Árbol Dirigido .....  | 241 |
| 5.18        | Árbol Dirigido con Raíz.....  | 242 |
| 5.18.1      | Propiedades de los árboles con raíz .....   | 244 |
| 5.19        | Subárbol .....  | 246 |
| 5.20        | Árboles binarios posicionales .....   | 247 |
| 5.21        | Recorrido de árboles binarios posicionales .....  | 248 |
| 5.21.1      | Recorrido o Búsqueda en preorden .....  | 248 |
| 5.21.2      | Recorrido o Búsqueda en entreorden.....   | 249 |
| 5.21.3      | Recorrido o Búsqueda en posorden .....  | 250 |
| 5.22        | Aplicación de expresiones algebraicas representadas por medio de<br>árboles dirigidos etiquetados ..... | 251 |
| 5.23        | Notaciones correspondientes a expresiones algebraicas.....  | 253 |
| Capítulo 6. | ESTRUCTURAS ALGEBRAICAS FINITAS .....   | 255 |
| 6.1         | Estructuras Algebraicas .....   | 257 |
| 6.2         | Operaciones .....   | 258 |
| 6.2.1       | Operación binaria .....   | 258 |
| 6.2.2       | Operación Unaria.....   | 260 |

|  |     |
|--|-----|
| 6.3 Propiedades de una Operación Cerrada.....                              | 261 |
| 6.3.1 Propiedad conmutativa .....  | 261 |
| 6.3.2 Propiedad asociativa .....   | 262 |
| 6.3.3 Existencia del elemento neutro.....                                  | 263 |
| 6.3.4 Teorema: Unicidad del elemento neutro .....                          | 263 |
| 6.3.5 Existencia de elementos inversos .....                               | 264 |
| 6.3.6 Distributividad.....   | 268 |
| 6.4 Principales Estructuras Algebraicas.....                               | 270 |
| 6.4.1 Monoide.....   | 270 |
| 6.4.2 Semigrupo.....   | 270 |
| 6.4.3 Grupo .....  | 272 |
| 6.4.4 Propiedades de los grupos .....                                      | 273 |
| 6.4.5 Subgrupo.....  | 273 |
| 6.4.6 Propiedad de los subgrupos .....                                     | 274 |
| 6.4.7 Anillo .....   | 275 |
| 6.4.8 Cuerpo .....   | 277 |
| 6.5 Algebra de Boole.....  | 278 |
| 6.5.1 Álgebra de Boole de los Conjuntos Potencias.....                     | 279 |
| 6.5.2 Álgebra de Boole de los divisores de un número entero positivo ..... | 280 |