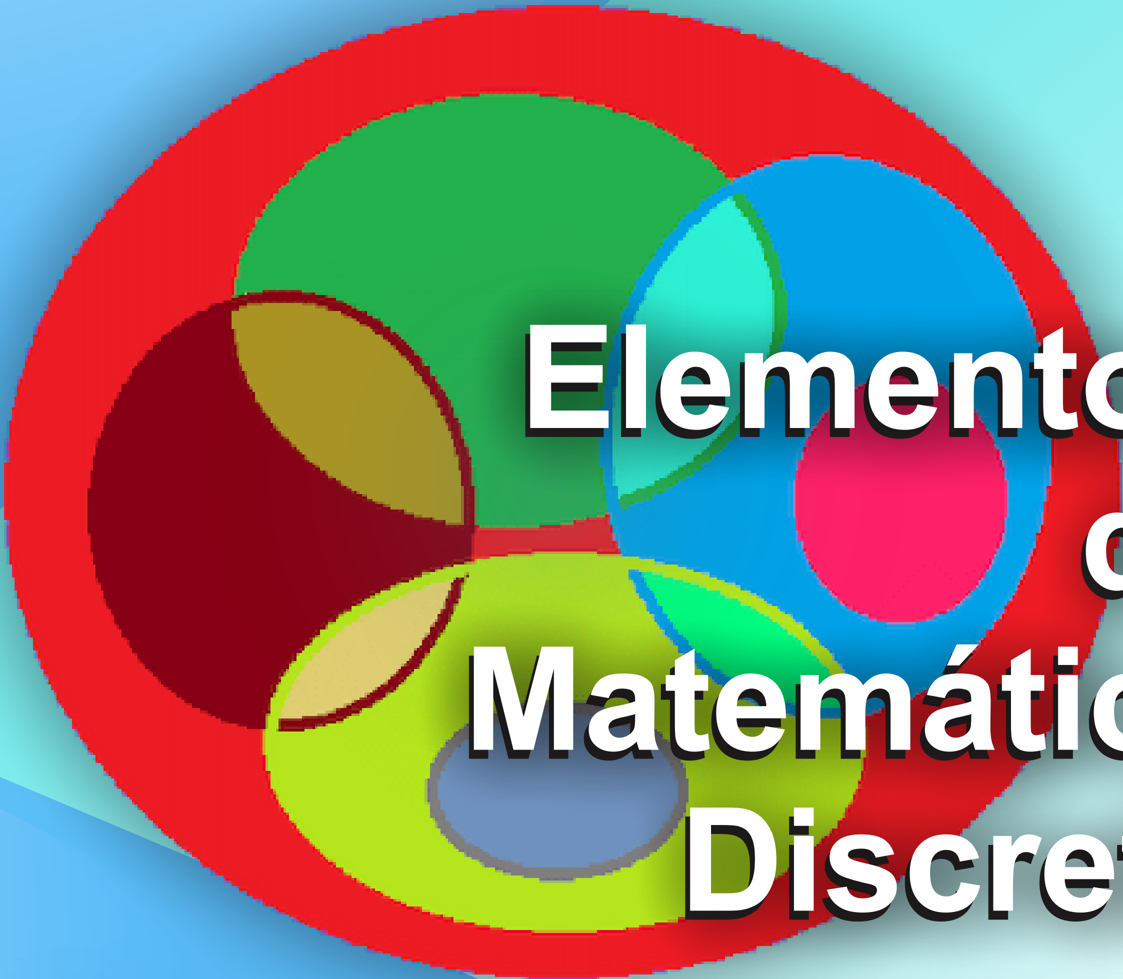
Gladys Mónica Romano

Lidia Beatriz Esper



Elementos de Matemática Discreta

70 años
UON·UTN
1948 2018

UTN
FACULTAD REGIONAL TUCUMÁN

CIN REUN
Red de Editoriales de Universidades Nacionales de la Argentina

LUA
Libro Universitario Argentino

edUTecNe

UTN UNIVERSIDAD TECNOLÓGICA NACIONAL

Elementos de Matemática Discreta

Primera Edición

Gladys Mónica Romano

Lidia Beatriz Esper

edUTecNe

Buenos Aires, 2019

Romano, Gladys Mónica; Lidia Beatriz Esper
Elementos de matemática discreta / Gladys Mónica Romano ; Lidia Beatriz Esper ; editado por Fernando Cejas. - 1a ed . - Ciudad Autónoma de Buenos Aires : edUTecNe, 2019.
Libro digital, PDF
Archivo Digital: descarga y online

ISBN 978-987-4998-18-7

1. Matemática. 2. Enseñanza. 3. Tucumán. I. Esper, Lidia Beatriz. II. Título.
CDD 512

Diseño de tapa: Lidia Esper, Gladys Romano, Fernando Cejas, Carlos Busqued

Universidad Tecnológica Nacional – República Argentina
Rector: Ing. Hector Eduardo **Aiassa**
Vicerrector: Ing. Haroldo **Avetta**
Secretaria Académica: Ing. Liliana Raquel **Cuenca Pletsch**

Universidad Tecnológica Nacional – Facultad Regional Túcuman
Decano: Mg. Ing. Walter Fabián **Soria**
Vicedecano: Ing. Juan Esteban **Campos**

edUTecNe – Editorial de la Universidad Tecnológica Nacional
Coordinador General a cargo: Fernando H. **Cejas**
Área de edición y publicación: Carlos Busqued
Director Colección Energías Renovables, Uso Racional de Energía, Ambiente: Dr. Jaime **Moragues.**

http://www.edutecne.utn.edu.ar
edutecne@utn.edu.ar

Queda hecho el depósito que marca la Ley Nº 11.723

Sarmiento 440, Piso 6 (C1041AAJ)
Buenos Aires, República Argentina
Publicado Argentina – Published in Argentina

ISBN 978-987-4998-18-7

A nuestras familias y

A nuestros estudiantes.

Contenido

PRÓLOGO

Matemática Discreta es la rama de la Matemática que se encarga del estudio de conjuntos discretos y proporciona los fundamentos apropiados para las Ciencias en Computación.

Son muchos los tópicos que pueden considerarse dentro de *Matemática Discreta* pero en este libro, el cual consta de seis capítulos, se decidió desarrollar los conceptos relacionados con Cálculo Proposicional y de Predicados; Conjuntos y Relaciones; Teoría de Números Enteros; Sucesiones, Inducción y Recursividad; Grafos, Dígrafos y Árboles, y Estructuras Algebraicas Finitas, tópicos que responden a los contenidos mínimos que figuran en el plan de estudio de la carrera de Ingeniería en Sistema de Información de la Facultad Regional Tucumán, Universidad Tecnológica Nacional (UTN). Por ello este material está dirigido a nuestros estudiantes de primer año y a cualquier estudiante de Ciencias de la Computación.

Como resultado de varios años de docencia en la cátedra, de una lectura amplia de la bibliografía disponible, de aunar criterios con distintas cátedras de la misma área y con otras regionales de la UTN, las autoras proponen este material curricular con el propósito de que resulte útil, ameno y didáctico para el estudiante. En este texto se encontrará la teoría necesaria para abordar los tópicos antes mencionados y algunas demostraciones de teoremas o propiedades que son consideradas apropiadas a la carga horaria asignada. Además incluye actividades a desarrollar y también algunas rutinas con PSeint para fortalecer en el estudiante su formación en Programación.

Si bien es conveniente e imprescindible que los ingresantes se acostumbren a consultar más de una fuente, también es cierto que el contar con un libro de texto que se ajuste a los contenidos de la materia, donde emplee un lenguaje matemático preciso y un nivel de explicación adecuado, contribuya al ahorro de tiempo y esfuerzo, y les sirva como columna vertebral de lo que va a estudiar. Se espera que el estudiante complemente su aprendizaje realizando la práctica de manera autónoma y que el texto sea una herramienta de apoyo.

Agradecimientos

A la valiosa colaboración de Malva Alberto por las observaciones y sugerencias realizadas en la presente obra.

A edUTecNe, la editorial de la Universidad Tecnológica Nacional por la posibilidad de la difusión de este material curricular.

Las autoras

Capítulo 1. CÁLCULO PROPOSICIONAL Y DE PREDICADOS

Proposiciones.

Conectivos lógicos. Operaciones lógicas.

Tautología, Contradicciones y Contingencias.

Equivalencia Lógica y Principales Leyes lógicas.

Implicaciones lógicas. Razonamientos.

Validez de un razonamiento. Principales Reglas de Inferencia.

Tipos de demostraciones para validar un razonamiento.

Lógica de Primer Orden. Cuantificadores.

Reglas de Generalización y Especificación Universal.

Introducción

La lógica surge desde el momento en que el hombre comienza a observar, experimentar, deducir y razonar lo que observa en la naturaleza que lo rodea. En general se aplica en los quehaceres diarios, ya que cualquier trabajo que se realiza tiene un procedimiento lógico.

La lógica es la rama de la Matemática que analiza la forma en la que razonamos. Es la disciplina que por medio de reglas y estrategias determina la validez de un argumento.

La lógica es la base de todo razonamiento automatizado que es primordial en informática. Su importancia en los diseños curriculares de las carreras que tienen que ver con las ciencias de la computación va tomando cuerpo propio debido a sus aplicaciones prácticas en contextos específicos tales como lenguajes de programación, ingeniería de software, bases de datos, inteligencia artificial, entre otros.

También desempeña un papel central en muchas otras ciencias, y es ampliamente aplicada por ejemplo en la Filosofía, pues una frase puede tener diferentes interpretaciones y la lógica permite saber el significado correcto; en las Ciencias Física y Naturales, para sacar conclusiones de experimentos; en Estadística y Matemática, para demostrar teoremas e inferir resultados que luego podrán ser aplicados en investigaciones. Por ello, es necesario un correcto uso del lenguaje a los efectos de evitar toda ambigüedad que muchas veces se presenta en el lenguaje corriente, motivo por el cual 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, la formalización del “lenguaje lógico” nos permite examinar más fácilmente las estructuras del pensamiento y aplicando sus leyes determinar si nuestro pensamiento sea correcto. Es por ello que la lógica proposicional es la parte de la Lógica que estudia las formas en que se relacionan unas proposiciones con otras, sin atender a su contenido, y sobre todo, las relaciones que se da entre las proposiciones que integran un razonamiento.

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 las olimpíadas matemáticas"

"10 es número primo"

"Hayelem no estudia informática pero si abogacía"

"Los elementos del lenguaje L son las palabras de L"

"La lógica se centra en las relaciones entre los enunciados"

También son proposiciones todas las leyes científicas, las fórmulas matemáticas y esquemas lógicos, donde se usan literales que tienen sentido en un universo dado.

Son proposiciones $E = mc^2$ y $a^2 - b^2 = (a + b)(a - b)$ donde los símbolos intervinientes toman valores de un dominio determinado

No son proposiciones las opiniones, proverbios, refranes, modismos, suposiciones o juicios de valor, las oraciones interrogativas, las exhortativas o imperativas, las desiderativas; las exclamativas o admirativas y los enunciados abiertos. En efecto, no son proposiciones porque de ninguna de ellas se puede afirmar verdadero o falso sin incurrir en ambigüedades.

❒ 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 una fantasía’

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) ‘El triángulo es inteligente’

i) ‘Eduardo es un número racional’

👁 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 usarán $p, q, r, \ldots$ Estas letras son variables de enunciado, por lo que mientras no se les asigne una proposición en particular, pueden representar a cualquiera. Es por ello que a $p, q, r, \ldots$ se les denomina variables proposicionales.

1.1.1 Valor de verdad

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.

"V" y "F" representan los valores de verdad verdadero y falso, respectivamente y 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, y ésta es la notación que usaremos más frecuentemente.

Ejemplos 1.3

Sean las proposiciones

p: "Ayer dejó de funcionar la PC de Gabriel"

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.

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:

$$q = 1 \;,\quad r = 0 \quad \text{y} \quad s = 0$$

1.1.2 Proposiciones Simples

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.

Ejemplos 1.4

Las siguientes oraciones son proposiciones simples:

i) “Evangelina programa en C++”

ii) “Los ordenadores de 64 bits tienen capacidad de hacer más en menos tiempo”

iii) “Lógica es una rama de las Matemáticas”

iv) “La PC de Zoe tiene poca memoria”

v) “Euclides y Boole son condiscípulos”

vi) “Marcelo e Imanol son hermanos”

Son proposiciones simples ya que carecen del adverbio de la negación “no” o sus equivalentes y no se las puede separar en dos proposiciones simples porque carecerían de significado en caso de hacerlo.

En el ejemplo v) y vi) la palabra “y” tiene carácter relacional. No se puede descomponer en más de una proposición.

1.2 Conectivos lógicos

Los siguientes enunciados, vinculan a una o más proposiciones simples:

i) “3 no es par”

ii) “Python o Prolog o C++ son lenguajes de programación”

iii) “La adición y la multiplicación de números naturales son operaciones asociativas y conmutativas”

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”

vi) “8 es divisible por dos si y solo si es par”

Cuando se vinculan o combinan proposiciones simples a través de palabras que funcionan como nexos: no, o, y, pero, si...entonces, …si y solo si …., se obtienen otras proposiciones, llamadas proposiciones compuestas.

El vínculo se establece a través de los llamados conectivos lógicos.

Definición

Los conectivos lógicos son símbolos o partículas lógicas mediante los cuales se conectan dos o más proposiciones simples, o se modifica una proposición dada.

Se trabajará con los siguientes conectivos lógicos, cuyo nombre, símbolo y lectura se detallan en la siguiente tabla.

Nombre	Símbolo	Se leen
negación	$\neg$, $\sim$	no, no es cierto, no ocurre
conjunción	$\wedge$	y, pero, también, sin embargo, aunque,
Disyunción inclusiva	$\vee$	"o" con sentido incluyente
Disyunción exclusiva	$\underline{\vee}$	"o" con sentido excluyente
Condicional	$\rightarrow$	si...entonces,
Bicondicional	$\leftrightarrow$	… si y sólo sí…

Tabla 1.1. Conectivos, significado y operación asociada.

1.2.1 Proposición Compuesta

Definición

Una proposición es compuesta cuando se obtiene a partir de proposiciones simples ligadas por los conectivos lógicos.

Ejemplos 1.5

i) "Los números naturales, los enteros y los fraccionarios son racionales"

En este caso está formado por tres proposiciones simples, ligadas todas a través del conectivo lógico "y".

ii) "Los números naturales son pares o impares"

Esta proposición compuesta está formada por dos proposiciones simples, ligadas a través del conectivo lógico "o"

iii) "Si los números racionales considerados son fracciones de denominar uno, entonces dichos números son enteros"

La vinculación de dos proposiciones se establece a través de "Si…entonces…"

1.2.2 Tablas de Verdad

Definición

Una tabla de verdad es un arreglo (o cuadro) que refleja los posibles valores de verdad de una proposición compuesta a partir de todas las combinaciones posibles de los valores de verdad de las proposiciones simples que la componen.

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 dos y tres variables proposicionales. Se representa al valor verdadero con V o con el símbolo 1, y al valor falso con F o con el símbolo 0.

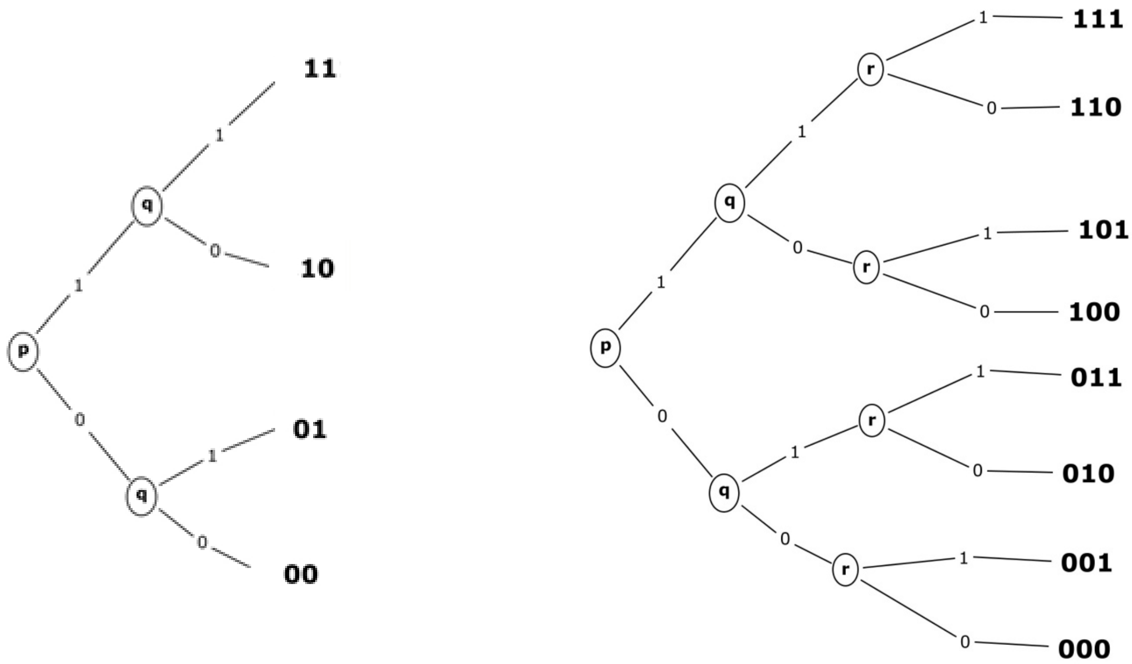


Fig.1.1. Valores de verdad para 2 y 3 proposiciones.

1.3 Operaciones lógicas

Al proceso que permite construir proposiciones a partir de otras usando los conectivos se llama operación lógica.

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

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

El operador unario y tiene un solo alcance: hacia la derecha, es decir afecta a una sola variable.

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.

1.3.1 Negación

Definición

Si p es una proposición cualquiera su negación se simboliza con $\neg p$, la cual se lee "No p".

La proposición compuesta $\neg p$ toma el valor de verdad contrario al valor de verdad de la proposición p.

Esto se refleja en la siguiente tabla de valores, donde se representa al valor de verdad verdadero con el símbolo 1, y al valor de verdad falso con 0.

p	$\neg p$
0	1
1	0

Tabla 1.2. Valores de verdad de la Negación.

Observaciones

- Se trata de una operación unaria pues tiene un único alcance.
- Otras maneras de leer $\neg p$: "No es cierto que p" , "Es falso 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", dado que lo contrario de blanco no es negro. Lo correcto sería: "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", pues negar "es mayor que" correspondería a "es menor o igual que".

Ejemplo 1.6

Sea la proposición p: "100 es par", su negación $\neg p$ puede expresarse como:

- ✓ "100 no es par"
- ✓ "No es cierto que 100 sea par"
- ✓ "Es falso que 100 es par"
- ✓ "100 es impar"

1.3.2 Conjunción o Producto Lógico

Definición

Dadas dos proposiciones cualesquiera p y q, la conjunción de p y q es la proposición compuesta que se denota simbólicamente " $p \wedge q$" y se lee "p y q", que sólo es verdadera si las dos proposiciones p y q son verdaderas. En todo otro caso es falsa. La tabla de verdad correspondiente es la tabla 1.3:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Tabla 1.3. Tabla de verdad para la conjunción

Observaciones

- Las proposiciones conjuntivas llevan "y", o sus formas equivalentes como "pero", "aunque", "e", "aun", "tanto…como…", "sin embargo", "además", etc.
- Se trata de una operación binaria con dos alcances (derecho e izquierdo)
- Se puede tener la conjunción de dos o más proposiciones: $p \wedge q \wedge r \wedge s$… El pasaje de operar con dos proposiciones y luego pasar a un número finito se resuelve introduciendo el uso de "paréntesis" que son los símbolos de puntuación de la lógica. Por ejemplo: $(((p \wedge q) \wedge r) \wedge s)$, o bien sin considerar los paréntesis y cuando los conectivos son todos iguales, operar de izquierda a derecha para determinar el valor de verdad de esta proposición compuesta.
- La expresión "ni" significa "y no".

Ejemplos 1.7

i) "3 es un número impar y 7 es un número primo"

Se trata de la conjunción de las proposiciones: p: "3 es un número impar" y q: "7 es un número primo" . Por ser p = 1 y q = 1, se tiene que ($p \wedge q$) = 1

ii) "Ignacio juega futbol, rugby y vóley"

Se trata de la conjunción de las proposiciones p: "Ignacio juega futbol"; q: "Ignacio juega rugby" y r: "Ignacio juega vóley"

La proposición dada, en forma simbólica es: $p \wedge q \wedge r$. Será falsa si alguna proposición o todas son falsas.

1.3.3 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" que sólo es falsa si las dos proposiciones componentes son falsas. En todo otro caso es verdadera.

El sentido de la disyunción "o" es incluyente, lo cual significa que para ser verdadera se necesita que al menos una de ellas sea verdadera, pudiendo ocurrir que ambas lo sean. Será falsa solo en el caso en que ambas sean falsas

La tabla de verdad correspondiente es la tabla 1.4:

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Tabla 1.4. Tabla de verdad para la disyunción incluyente.

Observaciones

- Otra forma de leer $p \vee q$: "p y/o q", "p o q o ambas"
- Es un operador binario.
- Se puede tener disyunción entre dos o más proposiciones: $p \vee q \vee r \vee s$ que como la conjunción, para evaluar esta proposición compuesta sin paréntesis se opera de izquierda a derecha.

Ejemplos 1.8

i) "Hoy llueve o es un día de sol"

Representa una disyunción incluyente de proposiciones, por lo tanto su forma simbólica es: $p \vee q$, donde p: "Hoy llueve" y q: "Hoy es un día de sol".

ii) "5 es mayor o igual a 2"

Si q: "5 es mayor a 2" y r: "5 es igual a 2", la expresión dada se simboliza: $q \vee r$, y resulta una proposición verdadera porque q = 1 y r=0.

1.3.4 Disyunción Excluyente

Definición

Dadas dos proposiciones cualesquiera p, q la expresión simbólica $p \veebar q$ denota la disyunción excluyente entre p y q, y se lee "p o q, pero no ambas", que es verdadera si una y sólo una de las proposiciones componentes es verdadera.

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

La tabla de verdad correspondiente es la tabla 1.5:

p	q	$p \veebar q$
0	0	0
0	1	1
1	0	1
1	1	0

Tabla 1.5. Tabla de verdad para la disyunción excluyente.

Observación

- $p \veebar q$: se lee también como " o bien p o bien q" , "o p o q" o " p o q pero no ambas"

Ejemplos 1.9

i) "El rector se elige por consulta popular o por una comisión del consejo"

Es una disyunción de las proposiciones:

p: “El rector se elige por consulta popular”;

r: “El rector se elige por una comisión del consejo”

Se observa que 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: $p \veebar r$.

ii) “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 se la expresa como: $r \veebar t$ que es verdadera, ya que r es verdadera y t es falsa.

1.3.5 Implicación o Condicional

Definición

Dadas dos proposiciones cualesquiera p, q la implicación o condicional de p y q es la proposición $p \to q$, que se lee “Si p entonces q”.

Se dice que p es el antecedente y q el consecuente del condicional. Esta proposición compuesta sólo es falsa cuando el antecedente es verdadero y el consecuente es falso. En cualquier otro caso es verdadera.

La tabla de verdad correspondiente es la tabla 1.6:

p	q	$p \longrightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Tabla 1.6. Tabla de verdad del Condicional.

Observación

El condicional $p \rightarrow q$ puede ser leído también de las siguientes maneras:

- Si p, q
- p sólo si q
- p es suficiente para q
- p implica q
- Cuando p, q
- q si p
- Sólo si q , p
- q es necesario para p
- p entonces q
- Para que p, q

Ejemplo 1.10

"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:

- "Si 28 es par, es divisible por 2"
- "28 es par, implica que 28 es divisible por 2"
- "28 es par solo si es divisible por 2"
- "Solo si 28 es divisible por 2, es par"
- "Es suficiente que 28 sea par para que sea divisible por 2"
- "Es necesario que 28 sea divisible por 2 para que sea par"

1.3.6 Bicondicional o Doble Implicación

Definición

Dadas dos proposiciones cualesquiera p, q la doble implicación o bicondicional de p y q es la proposición $p \leftrightarrow q$, que se lee " p si y solo si q", y sólo es verdadera sólo si ambas proposiciones tienen el mismo valor de verdad. En todo otro caso es falsa.

La tabla de verdad correspondiente es la tabla 1.7:

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Tabla 1.7. Tabla de verdad del Bicondicional.

Observaciones

- $p \leftrightarrow q$ puede leerse también como: "p es necesario y suficiente para q"; "p siempre y cuando q".
- "p si y solo si q" se abrevia del siguiente modo: "p sii q".

Ejemplos 1.11

i) "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: $p \leftrightarrow q$.

ii) "El cuadrado de un número natural es par siempre y cuando la base sea par". Expresión que se escribe simbólicamente como: $q \leftrightarrow r$, donde q: "El cuadrado de un número natural es par y r: "la base de un número natural es par".

Actividad 1.1

a) 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"

b) Sean las proposiciones p: “Luis circula en moto” y q: “Luis usa casco”; dar la interpretación coloquial y el valor de verdad, de las fórmulas lógicas:

“$\neg p$” , “$p \wedge q$”, “ $p \vee q$” , “$p \veebar q$” , “$p \rightarrow q$” y “$p \leftrightarrow q$”

Definición

Una Expresión Lógica es toda proposición lógica ya sea simple o compuesta, y se las denotará con letras mayúsculas: A, B, C,…, etc.

A la hora de confeccionar la tabla de verdad de una expresión lógica con dos o más conectivos lógicos se debe tener en cuenta la presencia de paréntesis para determinar el orden de los cálculos; y en el caso de una expresión sin ellos hay que respetar las prioridades de los conectivos y determinar cuál es el principal.

¿Pero cuál es la prioridad o jerarquía de los conectivos?

Es el orden en el que se resuelve una expresión lógica, y está dado por la siguiente regla de prioridad:

1°. Si los conectivos son los mismos, se resuelve de izquierda a derecha,

2°. La prioridad de mayor a menor está dada por el siguiente orden, (de izquierda a derecha): $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

1.4 Conectivo Principal

Definición

Se define conectivo principal de una expresión lógica al conectivo que nos da el valor de verdad resultante.

Ejemplos 1.12

i) En una expresión lógica completamente entre paréntesis como

$((\neg(p \vee q) \rightarrow r) \wedge q)$, es claro quién es el conectivo principal ($\wedge$).

ii) En las siguientes expresiones lógicas, se señala el conectivo principal (cp):

$\underset{\substack{\downarrow \\ \text{cp}}}{\neg}(p \wedge q)$; $(p \vee q) \wedge s \underset{\substack{\downarrow \\ \text{cp}}}{\rightarrow} p$; $p \rightarrow q \underset{\substack{\downarrow \\ \text{cp}}}{\rightarrow} ((r \vee p) \wedge \neg q)$

iii) El conectivo principal de la expresión lógica: $p \leftrightarrow (q \rightarrow \neg q) \wedge p$ es el bicondicional ($\leftrightarrow$); y su correspondiente tabla de verdad es la tabla 1.8:

p	$\leftrightarrow$	$(q$	$\rightarrow$	$\neg p)$	$\wedge$	p
1	0	1	0	0	0	1
1	1	0	1	0	1	1
0	1	1	1	1	0	0
0	1	0	1	1	0	0

Tabla 1.8. Tabla de verdad para $p \leftrightarrow (q \rightarrow \neg q) \wedge p$.

Actividad 1.2

i) Determinar el conectivo principal en las siguientes afirmaciones

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

ii) 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.

iii) Sin realizar la tabla de verdad determinar los valores de verdad de las proposiciones intervinientes sabiendo que:

a) $[p \wedge q \wedge r]$ = 1 b) $[(\neg p \vee F) \wedge q]$ = 1 c) $[(p \wedge q \wedge r) \rightarrow (s \vee t)]$ = 0

1.5 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 1.13

i) Las expresiones: $p \vee T$ y $p \vee \neg p$ son tautologías.

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

iii) Son contingencias las expresiones: $p \wedge T$, $p \vee F$, $p \wedge p$, $p \vee q$.

Actividad 1.3

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

1.6 Equivalencias Lógicas

Definición

Se dice que dos expresiones lógicas cualesquiera A y B, son lógicamente equivalentes y se denota A ⇔ B (o A ≡ 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 intervinientes.

Como *consecuencia* de esta definición se tiene que:

A ⇔ B si y solo si A ↔ B es tautología

Ejemplo 1.14

$p \wedge q \Leftrightarrow q \wedge p$ pues $p \wedge q \leftrightarrow q \wedge p$ es una tautología.

1.6.1 Principales Leyes Lógicas

Las Equivalencias Lógicas más simples son la base del Algebra Proposicional y se denominan Leyes Lógicas. 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.

A continuación se da el listado de las principales leyes lógicas las cuales se demuestran confeccionando sus tablas de verdad.

Considerando que p, q y r son proposiciones simples cualesquiera, V es una proposición siempre verdadera y F una proposición siempre falsa se cumple que:

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

Tabla 1.9. Principales Leyes Lógicas.

Las siguientes equivalencias, igualmente importantes, tienen que ver con el comportamiento de los conectivos condicional y bicondicional ; ellas son:

11.	$p \veebar q \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p)$	Ley de la disyunción excluyente
12.	$(p \veebar q) \veebar r \Leftrightarrow p \veebar (q \veebar r)$	Ley asociativa de la disyunción excluyente
13.	$p \rightarrow q \Leftrightarrow \neg p \vee q$	Ley del condicional

14.	$p \rightarrow q \;\Leftrightarrow\; \neg q \rightarrow \neg p$	Ley del contrarecírpoco del condicional
15.	$\neg (p \rightarrow q) \;\Leftrightarrow\; p \wedge \neg q$	Ley de la negación de la condicional
16.	$p \leftrightarrow q \;\Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$	Ley de la bicondicional
17.	$\neg(p \leftrightarrow q) \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p)$	Ley de la Negación de la bicondicional

Tabla 1.10. Leyes lógicas vinculadas a los conectivos: $\veebar$, $\rightarrow$ y $\leftrightarrow$.

Actividad 1.4

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.

1.7 🛠 Aplicaciones: Circuitos digitales

La lógica proposicional también se utiliza para diseñar circuitos digitales, los que transforman secuencias de señales de 1's y 0's en otras secuencias de señales de 1's y 0's a través de compuertas (dispositivos electrónicos) que realizan operaciones lógicas

Compuertas

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

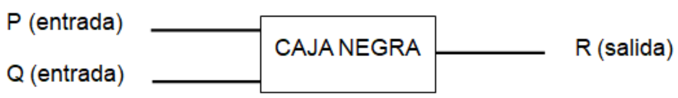


Fig.1.2. Representación circuito digital

Las operaciones que realiza la caja negra se hallan completamente especificada al construir una tabla entrada/salida que liste todos los posibles valores de entrada con su respectivo valor de salida.

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:

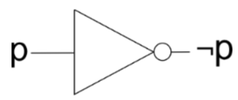
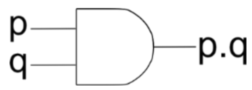
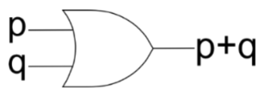
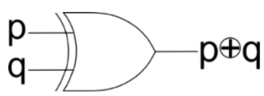
<table>
<tr><th>Tipo de compuerta</th><th>Representación simbólica</th><th>Acción</th></tr>
<tr><td>Inversora
NOT</td><td>
</td><td>
<table>
<tr><th>Entrada
p</th><th>Salida
¬p</th></tr>
<tr><td>0</td><td>1</td></tr>
<tr><td>1</td><td>0</td></tr>
</table>
</td></tr>
<tr><td>Multiplicadora
AND</td><td>
</td><td>
<table>
<tr><th colspan="2">Entradas</th><th>Salida</th></tr>
<tr><th>p</th><th>q</th><th>p.q</th></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>0</td></tr>
<tr><td>1</td><td>0</td><td>0</td></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Suma inclusiva
OR</td><td>
</td><td>
<table>
<tr><th colspan="2">Entradas</th><th>Salida</th></tr>
<tr><th>p</th><th>q</th><th>p+q</th></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>1</td></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Suma exclusiva
XOR</td><td>
</td><td>
<table>
<tr><th colspan="2">Entradas</th><th>Salida</th></tr>
<tr><th>p</th><th>q</th><th>p⊕q</th></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>1</td></tr>
<tr><td>1</td><td>1</td><td>0</td></tr>
</table>
</td></tr>
</table>

Tabla 1.11. 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 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, se interpretará a las operaciones lógicas mediante circuitos eléctricos. Cada proposición está representada por una llave o interruptor, tal que si es verdadera deja pasar corriente y si es falsa la corta. El resultado de la proposición compuesta se interpreta como el pasaje de corriente de un terminal T_1 a T_2.

Negación

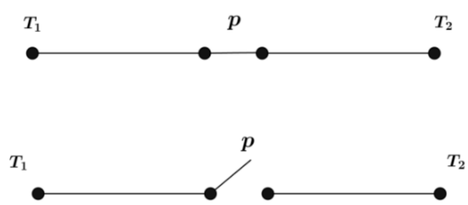


Fig. 1.3. Circuito de la Negación.

En la Figura 1.3 se ilustran los dos posibles casos, llave cerrada y llave abierta. En el primer caso si ingresa corriente por T_1 sale corriente por T_2 y en el segundo caso si ingresa corriente por T_1 no sale corriente por T_2.

Conjunción

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

Fig. 1.4. Circuito de la conjunción.

En la Figura 1.4 se ilustra solo el caso en que ambas llaves dejan pasar corriente, esto es, el caso donde p = 1 ; q = 1 y por lo tanto si ingresa corriente por T_1 saldrá corriente por T_2

Disyunción Inclusiva

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

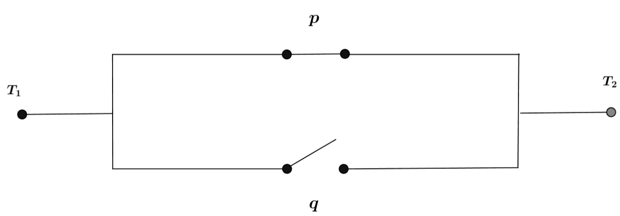


Fig.1.5. Circuito de la disyunción inclusiva.

En la Figura 1.5 se ilustra solo el caso en que exactamente una llave deja pasar corriente, esto es, el caso donde p = 1 ; q = 0 y por lo tanto si ingresa corriente por T_1 saldrá corriente por T_2.

1.7.1 Expresiones lógicas duales

Se observa en la Tabla 1.9, que salvo 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) $(p \vee q) \wedge F$ y $(p \wedge q) \vee T$

¿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 será necesario probar la equivalencia entre sus expresiones duales.

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

Las leyes lógicas se usan para:

i) para demostrar otras equivalencias, especialmente donde intervienen muchas variables proposicionales,

ii) para encontrar frases equivalentes, que transmitan el mismo mensaje y, por supuesto, conserven el valor de verdad, y

iii) para demostrar la validez de un razonamiento, concepto que se verá más adelante.

Actividad 1.5

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 ⇔ ....

ii) No estudie inglés ni francés ⇔ ....

iii) No es cierto que, comeré chocolates o caramelos ⇔ ....

iv) No es cierto que, si cobro el dinero viajare al sur ⇔ ....

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.

1.8 Implicaciones Lógicas

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 ⇒ B.

Como consecuencia de esta definición se tiene que:

A ⇒ B si y solo si A → B es tautología.

Ejemplo 1.16

Observar los renglones 3° y 4° de la Tabla 1.12, 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 1.12. Valores de verdad de $p \rightarrow p \vee q$.

Además observar que "p es condición suficiente para pvq", es decir en los renglones de la tabla donde p es verdadera resulta pvq verdadera.

Actividad 1.6

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

a) $[(p \longrightarrow q) \wedge \neg q] \Rightarrow \neg p$ b) $[(p \longrightarrow q) \wedge (q \longrightarrow r)] \Rightarrow (p \longrightarrow r)$

1.9 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 que la conclusión no se deduce de las premisas.

Este ejemplo nos muestra que existen argumentos no válidos.

1.9.1 Validez de un Razonamiento

Definición

Se dice que un razonamiento o argumento es válido cuando la conclusión se infiere o se deduce de las premisas.

Por lo tanto una manera de 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.

Simbólicamente

$p_1, p_2, \dots, p_n \rightarrow q$ es un razonamiento válido si y solo si $p_1 \wedge p_2 \wedge \dots \wedge p_n \Rightarrow q$.

De aquí se desprende que todas las implicaciones lógicas brindan razonamientos válidos.

Observación

Como de la definición, se desprende que la conclusión es verdadera cada vez que las premisas lo sean, no hace falta hacer toda la tabla de verdad de

$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$, sólo se necesita analizar el/los renglones donde las premisas $p_1, p_2, \ldots, p_n$ son verdaderas y se debe constatar que la conclusión q es verdadera también.

1.10 Principales Reglas de Inferencia

Definición

Al conjunto de razonamientos válidos más elementales se les llama Reglas de Inferencia.

La Tabla 1.13 describe a las principales reglas de inferencias:

	Regla de Inferencia	**Implicación Lógica asociada**	**Nombre**
1.	p $\underline{p \rightarrow q}$ $\therefore q$	$[\,p \wedge (\,p \rightarrow q)\,] \Rightarrow q$	Modus Ponens (MP)
2.	$p \rightarrow q$ $\underline{\neg q}$ $\therefore \neg p$	$[\,(\,p \rightarrow q) \wedge \neg q] \Rightarrow \neg p$	Modus Tollens (MT)
3.	$\underline{p}$ $\therefore p \vee q$	$p \Rightarrow (p \vee q)$	Adición disyuntiva
4.	p $\underline{q}$ $\therefore p \wedge q$	$p \wedge q \Rightarrow p \wedge q$	Combinación Conjuntiva
5.	$\underline{p \wedge q}$ $\therefore p$	$(\,p \wedge q\,) \Rightarrow p$	Simplificación Conjuntiva

6.	$p \rightarrow q$ $\underline{q \rightarrow r}$ $\therefore\ p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \Rightarrow (p \rightarrow r)$	Silogismo Hipotético(SH)
7.	$p \vee q$ $\underline{\neg p}$ $\therefore\ q$	$[(p \vee q) \wedge \neg q] \Rightarrow p$	Silogismo Disyuntivo (SD)

Tabla 1.13. Principales Reglas de Inferencia

1.10.1 Regla de Modus Ponens (MP)

La regla de inferencia llamada modus ponens permite demostrar q a partir de $p \longrightarrow q$ y p. La misma regla se aplica si el antecedente o el consecuente es una proposición simple o compuesta.

❒ Ejemplos 1.18

Los siguientes argumentos válidos, responden al MP:

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

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

Su forma simbólica es:

$$\begin{array}{l} p \longrightarrow q \\ \underline{p \qquad} \\ \therefore\ q \end{array}$$

ii) “Si Juan José no aprueba Matemática I, no cursará Matemática II. Juan José no aprueba Matemática I. Luego, Juan José no cursará Matemática II.”

Su forma simbólica es:

$$\begin{array}{l} \neg p \longrightarrow \neg q \\ \underline{\neg p \qquad} \\ \therefore\ \neg q \end{array}$$

Con p:" Juan José aprueba Matemática I" y q:" Juan José cursará Matemática II".

iii) En cada uno de los siguientes argumentos, la regla *modus ponens* permite pasar de dos premisas (una es un condicional y la otra es el antecedente del condicional) a la conclusión.

a) $\begin{array}{l} p \\ \underline{p \to \neg q} \\ \therefore \neg q \end{array}$ b) $\begin{array}{l} \neg p \to q \\ \underline{\neg p \quad\quad} \\ \therefore q \end{array}$ c) $\begin{array}{l} p \wedge q \to r \\ \underline{p \wedge q \quad\quad} \\ \therefore r \end{array}$ d) $\begin{array}{l} p \\ \underline{p \to q \wedge r} \\ \therefore q \wedge r \end{array}$

1.10.2 Regla de Modus Tollens (MT)

Esta regla de inferencia se aplica también cuando una premisa es un condicional y la otra es la negación del consecuente, para inferir a la negación del antecedente.

$$\begin{array}{l} p \longrightarrow q \\ \underline{\neg q \quad\quad} \\ \therefore \neg p \end{array}$$

🗒 Ejemplos 1.19

Las deducciones siguientes ejemplifican el uso del modus tollens.

i) "Si tiene luz propia, entonces el astro es una estrella. El astro no es una estrella. Por tanto no tiene luz propia."

Si p: "Tiene luz propia" y q: "El astro es una estrella", el argumento se simboliza de la siguiente manera:

$$\begin{array}{l} p \longrightarrow q \\ \underline{\neg q \quad\quad} \\ \therefore \neg p \end{array}$$

ii) "Si la memoria de la pc no es la correcta, el análisis de la base de dato no se podrá realizar. Pero se pudo realizar el análisis de la base de dato. Luego, la memoria de la pc es la correcta."

Sean p: "La memoria de la pc es correcta"; r: "El análisis de la base de dato se puede realizar", la forma del razonamiento es:

$$\begin{array}{l} \neg p \rightarrow \neg r \\ \underline{r \qquad\qquad} \\ \therefore\ p \end{array}$$

, que coincide con la estructura válida del Modus Tollens.

iii) En los argumentos siguientes, también se usa la regla MT:

a) $\begin{array}{l} q \\ \underline{p \rightarrow \neg q} \\ \therefore \neg p \end{array}$ b) $\begin{array}{l} \neg p \rightarrow q \\ \underline{\neg q \qquad} \\ \therefore p \end{array}$ c) $\begin{array}{l} p \wedge q \rightarrow r \\ \underline{\neg r \qquad\quad} \\ \therefore \neg(p \wedge q) \end{array}$ d) $\begin{array}{l} \neg(q \vee r) \\ \underline{p \rightarrow\ q \vee r} \\ \therefore \neg p \end{array}$

1.10.3 Regla de Adición disyuntiva

La regla de adición disyuntiva 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".

En forma simbólica la *regla de adición* quedaría:

Así: $\begin{array}{l} \underline{\quad p \quad} \\ \therefore p \vee q \end{array}$ o así: $\begin{array}{l} \underline{\quad p \quad} \\ \therefore q \vee p \end{array}$, gracias a la conmutatividad de $\vee$.

Una justificación es recordar el significado de la disyunción "$p \vee q$", que indica que por lo menos una de las dos proposiciones ligadas por el término de enlace "o" ha de ser cierta para que la disyunción sea verdadera. 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.

❒ Ejemplos 1.20

i) Con ejemplos en lenguaje natural u 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 a las siguientes proposiciones que son 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 infinitas conclusiones.

En todos estos ejemplos una parte (un alcance) es cierta y esto es todo lo que se necesita saber para que una disyunción sea cierta.

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

$$p \vee q \text{ o } p \vee r \text{ o } s \vee p \text{ o } t \vee p \ldots.$$

ii) Otros ejemplos de la ley de adición son:

a) $\begin{array}{l} \underline{\quad q \quad\quad} \\ \therefore q \vee \neg r \end{array}$ b) $\begin{array}{l} \underline{\neg r \quad\quad} \\ \therefore p \vee \neg r \end{array}$ c) $\begin{array}{l} \underline{\; p \wedge \neg q \;\;} \\ \therefore (p \wedge \neg q) \vee r \end{array}$ d) $\begin{array}{l} \underline{\;\; \neg p \quad\quad\quad} \\ \therefore \neg p \vee \neg q \end{array}$

1.10.4 Regla de Combinación conjuntiva

La regla que permite pasar de dos premisas verdaderas a la conjunción de ellas como conclusión, se denomina regla de combinación conjuntiva o de adjunción. De manera simbólica se puede representar a la regla así:

$$\begin{array}{l} p \\ \underline{q \quad\quad} \\ \therefore p \wedge q \end{array} \qquad\qquad\qquad \begin{array}{l} p \\ \underline{q \quad\quad} \\ \therefore q \wedge p \end{array}$$

El orden de las premisas es indiferente, y también en la conclusión se puede alterar el orden de la conjunción por la ley conmutativa.

Ejemplos 1.21

i) Dadas dos proposiciones como premisas, p: "El número atómico del hidrógeno es 1"; q: "El número atómico del helio es 2."

Una conclusión podría ser: "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".

ii) En los siguientes argumentos, se utiliza la regla de combinación o adjunción:

a) $q \wedge r$
$\underline{\quad p \wedge q \quad}$
$\therefore p \wedge q \wedge r$

b) $\neg p$
$\underline{\neg q \quad\quad}$
$\therefore \neg p \wedge \neg q$

c) $p \wedge q$
$\underline{\neg\, r \quad\quad}$
$\therefore\ (p \wedge q \wedge \neg r)$

d) $\neg(q \vee r)$
$\underline{\quad p \quad}$
$\therefore \neg(q \vee r) \wedge p$

1.10.5 Regla de Simplificación de la conjunción

La regla que permite pasar de una conjunción a cualquiera de los dos alcances se denomina regla de simplificación.

En forma simbólica la regla de simplificación es:

$$\frac{p \wedge q}{\therefore p} \qquad \text{o} \qquad \frac{p \wedge q}{\therefore q}$$

🗒 Ejemplos 1.22

i) 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.

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

a) $\underline{p \wedge (\, q \rightarrow r)}$
$\therefore q \rightarrow r$

b) $\underline{(p \vee q) \wedge r}$
$\therefore (p \vee q)$

c) $\underline{\neg p \wedge \neg q}$
$\therefore \neg p$

d) $\underline{p \wedge \neg q}$
$\therefore \neg q$

1.10.6 Regla de Silogismo hipotético (SH)

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

En forma simbólica:

$$\begin{array}{l} p \to q \\ \underline{q \to r} \\ \therefore p \to r \end{array}$$

☐ **Ejemplos 1.23**

i) Sea el siguiente razonamiento:

“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.”

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.

Sean las premisas,

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”,

y la conclusión: q: “Si 4 es mayor que 3 entonces 4 es mayor que 2”.

Para expresar simbólicamente el argumento, sean las proposiciones simples:

p: “4 es mayor que 3”;

q: “3 es mayor que 2”,

y r: “4 es mayor que 2”,

tales que: $(p_1) \quad p \to q$

$\underline{(p_2) \quad q \to r}$

$\therefore p \to r$, Fórmula que coincide con la estructura válida del SH.

ii) 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.

a) $\neg p \to \neg q$ b) $\neg p \to q \vee r$ c) $s \to t$ d) $(q \vee r) \to s$

$\underline{\neg q \to \neg r}$ $\underline{q \vee r \to \neg t}$ $\underline{t \to r \vee q}$ $\underline{s \to p}$

$\therefore \neg p \to \neg r$ $\therefore \neg p \to \neg t$ $\therefore s \to r \vee q$ $\therefore (q \vee r) \to p$

1.10.7 Regla de Silogismo disyuntivo (SD)

Esta regla dice que si una premisa es una disyunción y la otra es contraria a un alcance de la disyunción (no importa cuál sea el alcance negado, el derecho o el izquierdo), la conclusión afirma el otro alcance. Simbólicamente, el silogismo disyuntivo se puede expresar:

$$\begin{array}{l} p \vee q \\ \underline{\neg p \quad} \\ \therefore q \end{array} \qquad \text{o} \qquad \begin{array}{l} p \vee q \\ \underline{\neg q \quad} \\ \therefore p \end{array}$$

🗒 Ejemplos 1.24

Los siguientes razonamientos reflejan el SD:

i) “Esta sustancia contiene hidrógeno o contiene oxígeno. Esta sustancia no contiene oxígeno. Luego, 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”

Por lo tanto la forma simbólica de este razonamiento es:

$$\begin{array}{l} p \vee q \\ \underline{\neg q \quad} \\ \therefore p \end{array}$$

ii) Se tiene también esta regla en el caso de que los alcances de la disyunción sean proposiciones compuestas, como ser:

a) $(p \to q) \vee \neg r$

$\underline{\quad r \quad\quad\quad}$

$\therefore p \to q$

b) $\neg p \vee t$

$\underline{\neg t \quad}$

$\therefore \neg p$

c) $(p \wedge q) \vee s$

$\underline{\neg s \quad\quad}$

$\therefore (p \wedge q)$

d) $\neg q \vee \neg r$

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

$\therefore \neg r$

Actividad 1.7

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, ……………………….

1.11 Tipos de demostraciones para validar un razonamiento

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

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

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

1.11.1 Método directo

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

En la tabla de verdad de la implicación (Tabla 1.14),en los 3° y 4° renglones se puede observar que bajo el supuesto de que p sea verdadera la única condición para que la implicación sea verdadera es que q sea verdadera.

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Tabla 1.14. Condicional donde p = 1.

En el caso de la demostración de la validez de un razonamiento $p_1, p_2, \dots, p_n \to q$, 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 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 (la tesis).

🗒 Ejemplos 1.25

i) Para demostrar la validez del siguiente argumento:

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

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

Pasos	Razones
1) p	premisa 1
2) $p \to q$	premisa 2
3) $\neg r \to \neg q$	premisa 3
4) $s \vee \neg r$	premisa 4
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.

ii) Para demostrar que el siguiente razonamiento es válido se utiliza el proceso de derivación formal

$$\begin{array}{l} \neg p \to q \\ \underline{\neg p \vee\ r} \\ \neg q \to r \end{array}$$

Pasos	Razones
1) $\neg p \to q$	premisa 1
2) $\neg p \vee\ r$	premisa 2
3) $p \to r$	(2) Ley del condicional
4) $\neg q \to p$	(1) Contrarecíproca y Doble negación
5) $\neg q \to r$	(4 y 3) S. H. (conclusión)

👁 Observaciones

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. Debe trabajarse con todas las premisas.

Actividad 1.8

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

a) $p \rightarrow q$

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

$\therefore \neg p$

b) $p \rightarrow q \vee r$

$p \rightarrow \neg q$

$\underline{p}$

$\therefore \neg r$

Puede ocurrir que sea dificultoso o imposible realizar la demostración directa de un razonamiento. En tales casos se puede intentar otras estrategias utilizando la equivalencia lógica del contrarecíproco o incorporando la negación de la conclusión, lo cual resultaría en métodos de demostración indirectos.

1.11.2 Métodos Indirectos

a) Método por contraposición o contrarecíproco

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

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 $\neg q \longrightarrow \neg p$.

Entonces demostrar que $p_1 \wedge p_2 \wedge \ldots \wedge p_n \Rightarrow q$ será equivalente a demostrar que $\neg q \Rightarrow \neg(p_1 \wedge p_2 \wedge \ldots \wedge p_n)$

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 1.26

i) 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:

$$\begin{array}{l} p_1: \ p \longrightarrow r \\ p_2: \ \underline{\neg r \quad} \\ \quad\therefore \neg p \end{array}$$

Suponiendo que la conclusión $(\neg p)$ es falsa, entonces 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 tiene una premisa falsa.

ii) Si el razonamiento fuera el siguiente:

$$\begin{array}{l} p_1: \ p \longrightarrow r \\ p_2: \ \underline{\neg p \quad} \\ \quad\therefore r \end{array}$$

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.

b) Método por Reducción al Absurdo (o Contradicción)

Existe otra regla de inferencia interesante que dice así:

$$\underline{\neg p \to F}$$

$$\therefore p$$

Es decir, si suponer $\neg p$ te lleva a una contradicción, entonces quien se cumple es p.

Aplicando este concepto para la demostración de razonamientos con más de una premisa del tipo $p_1, p_2,...,p_n \Rightarrow q$, para demostrar que es válido se debe probar que suponer la coexistencia de las premisas y de la negación de la conclusión nos llevaría a una contradicción. Esto es, se debe mostrar que

$$(p_1, p_2,...,p_n) \wedge \neg q \quad \Rightarrow \quad F$$

Procedimiento de deducción

1. Suponer que las premisas son verdaderas y que la conclusión es falsa.
2. Buscar que se produzca una contradicción.
3. Una vez ocurrida la contradicción se concluye que el razonamiento es válido, pues estaría probado que suponer que las premisas son verdaderas y simultáneamente la conclusión es falsa es una contradicción.

Ejemplo 1.27

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

$$\neg p \to q$$

$$\underline{\neg p \vee r}$$

$$\neg q \to r$$

Se utiliza derivación formal:

<u>Pasos</u>	<u>Razones</u>
1. $\neg p \to q$	premisa 1
2. $\neg p \vee r$	premisa 2

3. $\neg(\neg q \rightarrow r)$ premisa 3 (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, y DN

8. $\neg p$ SD con 2 y 6

9. F Combinación 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 1.15 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 1.15. Comparación deducción vs computación.

Ejemplo 1.28

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
```

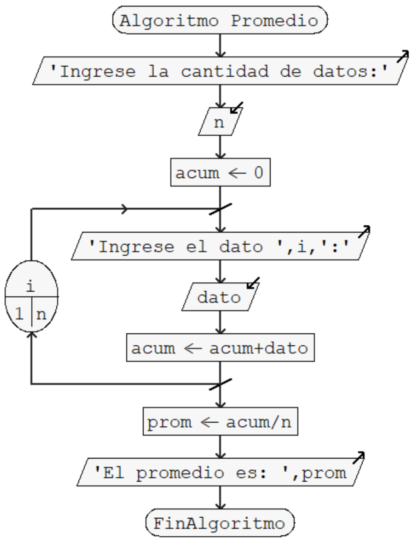


Fig.1.6. Diagrama de Flujo realizado con el software PSeint.

1.12 Lógica de Predicado (o de Primer Orden)

1.12.1 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, a través de los conectivos de la lógica proposicional, por ejemplo: p(x) $\longrightarrow$ q(x) ; p(x) $\vee$ q(x), etc.

Las opciones permisibles de reemplazo, 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.

Ejemplos 1.29

Sean los predicados p(x) y q(x) definidos en el universo U=$\mathbb{Z}$.

p(x): "El numero x es par" ; q(x): "El numero x es divisible por 4".

Dando valores a x se tiene que:

p(3): "El número 3 es par" y p(3)=0

p(2): "El número 2 es par" y p(2) =1,

q(1) : "El número 1 es divisible por 4" y q(1) = 0.

p(8) $\longrightarrow$ q(8): " Si 8 es par entonces es divisible por 4" y [p(8) $\longrightarrow$ q(8)] = 1

p(2) $\longrightarrow$ q(2): " Si 2 es par entonces es divisible por 4" y [p(2) $\longrightarrow$ q(2)] = 0

p(6) $\vee \neg$ q(6): "El numero 6 es par o no es divisible por 4"y [p(6) $\vee \neg$ q(6)] = 1.

Actividad 1.9

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

b) Suponer que es verdadero que Juan curse Algebra pero que no regularizó

Análisis Matemático I, siendo alumno de la UTN; y encontrar el valor de verdad de las dos expresiones lógicas de a).

1.12.2 Cuantificadores

Definición

Un cuantificador es una palabra (o símbolo) que indica la frecuencia con la que un predicado se cumple en un determinado conjunto.

Algunas de las palabras que cuantifican al predicado son: algunos (alguien, existe o hay), todo (o siempre o cada), nadie (ninguno), etc.

Para denotar un enunciado cuantificado se escribe el cuantificador correspondiente seguido del predicado del enunciado cuantificado. Las nuevas frases formadas automáticamente se convierten en proposición pues poseen valor de verdad.

Ejemplos 1.30

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

"Todos los estudiantes asisten a las clases de M. Discreta",

"Algún estudiante asiste a las clases de M. Discreta",

"Alguien asiste a las clases de M. Discreta".

Existen diversos tipos de cuantificadores, entre ellos, los más utilizados son el cuantificador existencial y el cuantificador universal.

Definición

El cuantificador existencial de un predicado p(x) expresa que p(x) se cumple para algún valor de x.

Genera la siguiente proposición: "Para algún x (del dominio), se cumple o se verifica la propiedad p(x)".

Simbólicamente se representa: "$\exists$x p(x)"

🗒 Ejemplos 1.31

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

“Hay números primos que son pares”

“Algún matemático es filósofo”

“Existe un software que se convierte en obsoleto”

“Existe al menos un entero tal que sumado a dos da distinto de cero”

¿Qué valor de verdad tiene la proposición: $\exists x\ p(x)$?

- Es Verdadera si para al menos un a del universo, se cumple que $p(a)$ es verdadera.
- Es Falsa si para cada a del universo, se cumple que $p(a)$ es falsa.

🗒 Ejemplos 1.32

i) Sea $p(x)$: $(x+2)^2 = x^2 + 4$; con U = $\mathbb{R}$, luego la expresión “Hay un número real tal que $(x+2)^2 = x^2 + 4$” se representa simbólicamente: $\exists x,\ p(x)$, y resulta ser verdadera. Pues existe un valor que hace cierta esta expresión y es x = 0.

ii) La proposición: $\exists\ x \in \mathbb{R}$, tal que $\frac{-3}{x-4} = 0$, es falsa, pues no existe un valor de x que haga cero el numerador de la fracción.

👁Observaciones

- Si un enunciado cuantificado existencialmente es verdadero es suficiente buscar un ejemplo para probar la existencia.
- Si un enunciado cuantificado existencialmente es falso, hay que probarlo usando definiciones o propiedades y mostrar que es falso para todos los valores del dominio de discurso.

Definición

El cuantificador universal de un predicado p(x) expresa que p(x) se cumple para todos los valores de x.

Genera la siguiente proposición: "Para todos los x (del dominio), se cumple la propiedad p(x)".

Simbólicamente se representa "$\forall$x p(x)".

Ejemplos 1.33

Las palabras que cuantifican universalmente, son: "Todo/s", "Para todo/s", "Cualquier", "Para cualquier", "Un", "cada", "cada uno", etc.

"Todos los alumnos aprobaron el evaluativo"

"Cualquier persona razona"

"Todo número real elevado al cuadrado es no negativo"

"Cada uno de los estudiantes debe traer su documento para rendir"

¿Qué valor de verdad tiene la proposición: $\forall$x p(x)?

- Es verdadera cuando para cada a del universo, $p(a)$ es verdadera.
- Es falsa cuando para al menos un a del universo, $p(a)$ es falsa

Ejemplos 1.34

i) "Todo número entero es racional" es una proposición verdadera, pues cualquiera sea $x \in \mathbb{Z}$, x se puede escribir como $\frac{x}{1} \in \mathbb{Q}$.

ii) "Cualquier entero es impar" es falsa, pues existe $x = 4$, $x \in \mathbb{Z}$ tal que 4 no es impar.

Observaciones

- Cuando un enunciado cuantificado universalmente es verdadero, entonces no es posible probar su veracidad con un ejemplo. Se debe usar propiedades, definiciones, etc. y probar que vale para cada uno de los elementos del universo de discurso sin particularizar.

- Cuando un enunciado cuantificado universalmente es falso, es suficiente probar con un ejemplo su falsedad. (Es lo que se llama un “contraejemplo”)

Actividad 1.10

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

i) $\forall x , \ x > 0$ 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.

1.12.3 Negación de Cuantificadores

Propiedad

En Lógica de Predicados se dan las siguientes equivalencias:

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

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

Ejemplos 1.35

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

i) La proposición “Hay números pares” es verdadera ya que existe el número 2 que es par y 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”, que resulta ser una proposición falsa.

ii) La proposición “Todos los números son primos” es falsa ya que existe el 6 que no es primo y 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: “Existen números que no son primos”, la cual es verdadera.

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”.

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”.

Actividad 1.11

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”

Ejemplos 1.36

Sean p(x): “x es par”; q(x): “x es divisible en 2”; r(x): “x es primo”, definidas en el universo de los números enteros. Entonces:

“Todos los pares son divisible en 2”, se representa $\forall$x p(x) $\rightarrow q$(x)

donde p(x) : “x es par” y q(x) : “x es divisible en 2”

“Algunos pares no son primos”, se representa $\exists$x p(x) $\wedge \neg r$ (x)

donde p(x) : “x es par” y r(x) : “x es primo”

“Hay números divisibles en 2 que son primos”, se representa $\exists$x q(x) $\wedge\, r$(x)

donde q(x) : “x es divisible en 2” y r(x) : “x es primo”

1.12.4 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 "∀x [p(x) ⇔ q(x)] cuando la bicondicional $p(a) \leftrightarrow q(a)$ es verdadera para cada reemplazo a del universo dado.

Ejemplo 1.37

En el universo U = 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 "∀x [|x| < 3 ⇔ -3< x < 3]" y se dirá que los predicados "|x| < 3" **y** " -3 < x < 3" son equivalentes.

1.12.5 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 ∀x [p(x) ⇒ q(x)].

Ejemplo 1.38

En el universo de los números reales sean p(x): "|x| > 3" ∧ 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 ejemplo para $a = -5$.

Por lo tanto p(x) y q(x) no son equivalentes, solo se cumple que ∀x [q (x) ⇒ p(x)] y diremos que q (x) implica lógicamente a 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 predicados equivalentes o cuáles son implicaciones de otros.

1.12.6 Asociatividad y Distributividad

1. El cuantificador universal es asociativo respecto del conectivo lógico conjunción. Este resultado se expresa por la siguiente equivalencia

$$\forall x\,[\,p(x) \wedge q(x)\,] \Leftrightarrow [\,\forall x\, p(x)\,] \wedge [\,\forall x\, q(x)\,]$$

2. El cuantificador existencial es asociativo respecto del conectivo lógico disyunción. Este resultado se expresa por la siguiente equivalencia

$$\exists x\,[\,p(x) \vee q(x)\,] \Leftrightarrow [\,\exists x\, p(x)\,] \vee [\,\exists x\, q(x)\,] :$$

En los siguientes casos, sólo se da la implicancia lógica:

3. $[\,\forall x\, p(x)\,] \vee [\,\forall x\, q(x)\,] \Rightarrow \forall x\,[\,p(x) \vee q(x)\,]$

4. $\exists x\,[\,p(x) \wedge q(x)\,] \Rightarrow [\,\exists x\, p(x)\,] \wedge [\,\exists x\, q(x)\,]$

El siguiente contraejemplo pone de manifiesto lo que dice el ítem 3.

Supongamos que U = $\mathbb{Z}$, y sean los predicados:

p(x) : " x es un número par"

q (x) : "x es un número impar"

Entonces, la proposición,

$[\,\exists\, x\ \ p\,(x)\,] \wedge [\,\exists\, x\ \ q\,(x)\,]$ significa que existe, al menos, un número entero que es par y también existe, al menos, un entero que es impar, lo cual, evidentemente, es verdad.

Por otra parte, la proposición, $\exists\, x\ \ [\,p\,(x) \wedge q\,(x)\,]$ significa que hay, al menos, un número entero que es, al mismo tiempo, par e impar, lo cual es falso.

Por lo tanto, la veracidad de la conclusión no se sigue de la veracidad de la hipótesis y no habría, consecuentemente, implicación lógica, es decir,

$$[\,\exists\, x\ \ p\,(x)\,] \wedge [\,\exists\, x\ \ q\,(x)\,] \;\not\Rightarrow\; \exists\, x\ \ [\,p\,(x) \wedge q\,(x)\,]$$

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 es posible de aplicar, es el llamado método exhaustivo, el cual propone que si se necesita demostrar 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 1.39

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."

Dado que el Universo U = {2, 4, 6, 8, 10} es 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 infinitos que no se prestan al método exhaustivo, para ello se presentan las siguientes reglas que ayudan a la demostración de tales teoremas.

1.12.7 Reglas de Inferencias

a) 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"

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

❒Ejemplo 1.40

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 $a^2 = a.a \geq 0$ por definicion 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 $\forall x \in R$.

b) 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"

$$\frac{\forall x \ p(x)}{p\,(c)}$$

Ejemplo 1.41

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.

Ejemplos 1.42

Para establecer si el siguiente argumento es válido

i)
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:

$$\forall x\, [p(x) \longrightarrow q(x)]$$
$$\underline{p(\text{Beltran})\qquad .}$$
$$\therefore q(\text{Beltran})$$

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

Pasos	Razones
1. $\forall x\, [p(x) \longrightarrow q(x)]$	Premisa
2. p(Beltran)	Premisa
3. p(Beltran)→ q(Beltran)	1. P.U.
4. q(Beltran)	2 y 3 M.P (Modus Ponens)

Por lo tanto el razonamiento es válido.

ii) En el siguiente razonamiento:

Todos los enteros son racionales

<u>El número π no es racional .</u>

∴ El número π no es entero

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

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

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

$\therefore \neg p(\pi)$, para demostrar su validez, se usa la derivación formal.

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

Por lo tanto el razonamiento es válido.

Actividad 1.13

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

a) Si n es múltiplo de 4 entonces n es par
<u>10 es par</u>
$\therefore 10$ es múltiplo de 4

b) Todo polígono cerrado de cuatro lados es un cuadrilátero
<u>Un cuadrilátero es tal que la suma de sus ángulos interiores es 360°</u>
∴ Cada polígono cerrado de cuatro lados es tal que la suma de sus ángulos interiores es 360°.

🛠 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

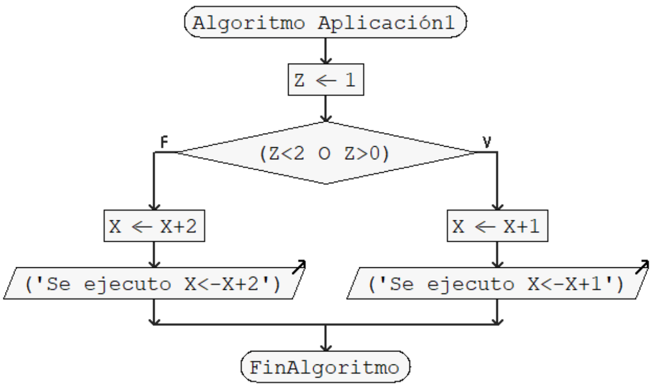


Fig. 1.7. Diagrama de Flujo Aplicación 1.

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 <- 2
        Si ((Z<0 Y Z>1) O Z>3) Entonces
                X <- X+1
                Escribir ('Se ejecuto X<-X+1')
        SiNo
                X <- X+2
                Escribir ('Se ejecuto X<-X+2')
        FinSi
FinAlgoritmo
```

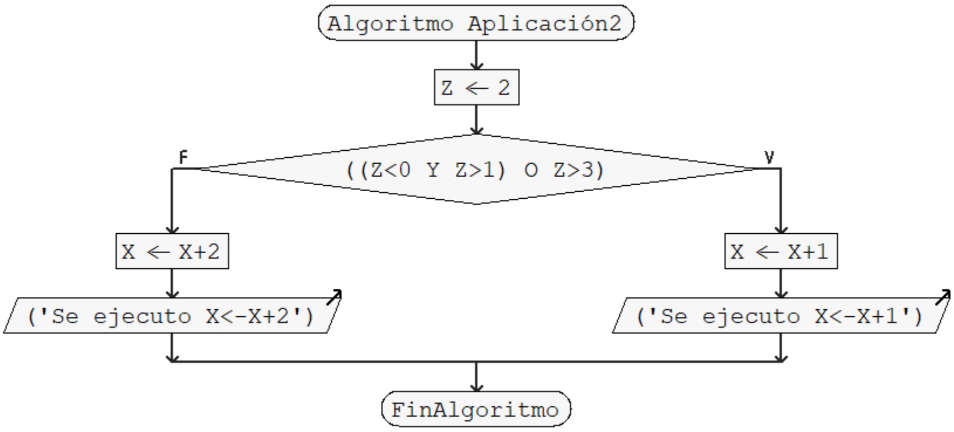


Fig. 1.8. Diagrama de Flujo Aplicación 2.

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

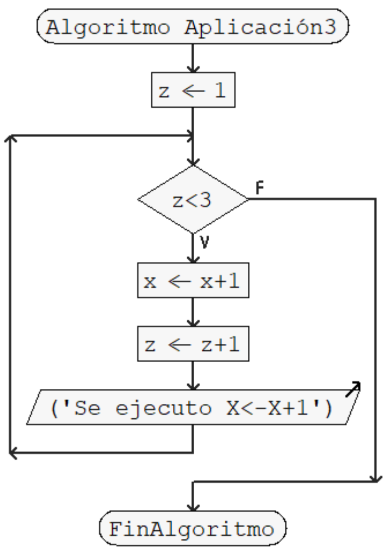


Fig. 1.9. Diagrama de Flujo Aplicación 3.

Capítulo 2. CONJUNTOS Y RELACIONES

Conjuntos y Elementos.

Inclusión de conjuntos. Subconjuntos.

Algebra de conjuntos. Operaciones con conjuntos.

Partición de un conjunto.

Relación. Función.

Matrices y Digrafos.

Composición de Relaciones. Propiedades.

Relación de Equivalencia y Conjunto Cociente.

Relación de Orden y Diagrama de Hasse.

Introducción

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, minería 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. A los elementos del conjunto se los encierra entre llaves y la afirmación "el elemento a pertenece al conjunto A" se denota $a \in$ A y si "a no pertenece al conjunto A" se escribe $a \notin$ A (negación del hecho de que $a \in$ 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.

2.1.1 Conjuntos finitos e infinitos

Definición

Un conjunto A se dice finito si y sólo si tiene n elementos distintos, con $n \in \mathbb{N}_0$. Caso contrario se dice infinito

Si A es finito, y tiene n elementos, se dice que el cardinal de A es n y se indica $|A| = n$.

Ejemplos 2.1

a) Si A es el conjunto de las letras del abecedario, A es finito, y su $|A| = 27$, o sea A tiene 27 elementos, incluida la letra ñ de nuestro idioma castellano.
b) El conjunto de los estudiantes de la UTN es finito.
c) El conjunto de las materias del diseño curricular de Ingeniería en Sistemas es finito.
d) El conjunto de los números naturales es infinito mientras que el conjunto de los dígitos usados en el sistema de numeración decimal es finito.

Por otro lado los conjuntos infinitos se clasifican en numerables y no numerables.

Son numerables cuando se pueden poner en correspondiencia biunívoca con los Numeros Naturales. Caso contrario se dicen no numerables

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

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

$\mathbb{Z}$: Conjunto de los Números Enteros

$\mathbb{N}$ o $\mathbb{Z}^+$: Conjunto de los Números Naturales o Enteros Positivos.

$\mathbb{N}_0$: Conjunto de los Enteros No Negativos.

$\mathbb{Q}$: Conjunto de los Racionales.

$\mathbb{R}$: Conjunto de los Números Reales

$\mathbb{R}^+$: Conjunto de los Reales positivos

Todos son conjuntos infinitos, pero $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ se caracterizan por ser numerables mientras que $\mathbb{R}$ es no numerable.

2.1.2 Determinación de Conjuntos

Un conjunto se puede definir por extensión o por comprensión. Existen conjuntos que pueden definirse de ambas maneras, pero otros solo de una de las formas.

Determinación por Extensión

Definición

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

Ejemplos 2.2

Los siguientes conjuntos están definidos por extensión.

i) El conjunto de las vocales del alfabeto.

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

ii) El conjunto de los números enteros pares no negativos y menores que mil.

$$B = \{0, 2, 4, 6, 8, ..., 1000\}$$

Observación

- Los conjuntos finitos definidos por extensión se indican como una lista de elementos encerrada entre llaves, separados por comas, sin importar el orden y sin repetir.
- Los elementos de un conjunto infinito, salvo aquellos que se puedan enumerar, no pueden especificarse por extensión; consecuentemente, se necesita una forma alternativa de describir tales conjuntos implícitamente.

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 se hace a menudo mediante un predicado con una variable. El conjunto estará determinado por aquellos elementos del universo que hacen del predicado una proposición verdadera.

De aquí que, si p(x) es un predicado en x, la notación A = {x $\in$ U / p (x)} denota al conjunto A formado por los elementos x $\in$ U para los cuales p (x) es verdadero.

Ejemplos 2.3

i) El conjunto de los enteros mayores que diez, definido por comprensión:

$A = \{ x \in \mathbb{Z} \ / \ x > 10 \};$

por ser un conjunto infinito numerable también podría escribirse por extensión:

A = { 11, 12, 13, …}

ii) El conjunto de los enteros pares, definido por comprensión:

$B = \{ x \in \mathbb{Z} \ / \ x = 2k \ , k \in \mathbb{Z} \}$

definido por extensión: B = { …, -4, -2, 0, 2, 4, …}.

iii) El conjunto {1, 2, 3, 4, 5}, ya está expresado por extensión, luego expresado por comprensión se tiene: $C = \{ x \in \mathbb{Z} \ / 1 \leq x \leq 5 \}$

Observación

Cuando el universo se da por sobreentendido se puede indicar simplemente

A = {x / p (x)}.

2.1.3 Conjuntos especiales: Vacío, Unitario, Universal

Definiciones

a) Un conjunto se dice Vacío si y solo si no tiene elementos. Su cardinal es 0 y se representa ∅ o por { }.

b) Un conjunto se dice Unitario si y solo 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 2.4

i) El conjunto de personas que tiene el cargo de Decano de la FRT es unitario.

ii) El conjunto de personas que trabajan en la FRT y que viajaron a la luna es vacío.

iii) El universo correspondiente al conjunto de las vocales puede ser el conjunto de las letras del abecedario de nuestro idioma o un conjunto más amplio que incluya símbolos usados en otro idioma.

iv) El universo correspondiente al conjunto de los estudiantes de ISI puede ser el conjunto de los estudiantes de la UTN o un conjunto más amplio que incluya a todos los estudiantes universitarios.

Actividad 2.1

¿Cuál de los siguientes conjuntos es vacío? ¿Cuál es unitario? Indique cuál es el universo correspondiente a cada conjunto.

$A = \{x \in \mathbb{N} \ / \ x - 3 = 5\}$; $B = \{x \in \mathbb{R} \ / \ x^2 = 5\}$

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

2.2 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. Simbólicamente, éto se expresa:

$$A = B \iff \forall x\, [(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)]$$

O bien,

$$A = B \iff \forall x\, (x \in A \iff x \in B)$$

Observación

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

Ejemplos 2.5

i) Considerando $U = \mathbb{Z}$ se analizará cuáles de los siguientes conjuntos son iguales.

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

$B = \{ x \,/\, x = 2y \text{ para algún } y \}$

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

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

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

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

$G = \{ x \,/\, x^2 + 1 = 0 \}$

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 , por lo tanto $A = \emptyset$.
- Para el conjunto B, se tiene que $x \in B \Leftrightarrow x = 2y$ para algun $y \Leftrightarrow$ x es par, luego $B = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$
- El conjunto C ya está definido por extensión, $C = \{ 1, 2, 3 \}$
- El conjunto D ya está definido por extensión, $D = \{ 0, 2, -2, 3, -3, 4, -4, \ldots\}$
- Dando valores enteros a x se tiene que $E = \{ 0, 2, -2, 4, -4, 6, -6, \ldots\}$
- El conjunto F ya está definido por extensión, $F = \{ 3 , 2 , 1 \}$
- Como no existen enteros que satisfagan la ecuación $x^2 + 1 = 0$, se tiene que $G = \emptyset$.

De todo lo anterior, se sigue que $A = G$; $B = E$ y $C = F$. Además se tiene que que el conjunto D no es igual a ninguno de los otros.

ii) Para encontrar una condición necesaria y suficiente para que dos conjuntos sean distintos, se considerará: $\neg(A = B)$.

Para ello, sean A y B dos conjuntos cualesquiera de un universal arbitrario U. Por igualdad de conjuntos, se tiene $A = B \;\Leftrightarrow\; \forall x\, (x \in A \Leftrightarrow x \in B)$

Negando miembro a miembro :

$A \neq B \Leftrightarrow \neg \forall x \, (x \in A \Leftrightarrow x \in B) \Leftrightarrow \exists x \, [\, (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B) \,]$

Así pues, una condición necesaria y suficiente para que dos conjuntos, A y B, sean distintos es que exista, al menos, un elemento en A que no esté en B o que exista un elemento en B que no esté en A.

2.3 Conjuntos Disjuntos

Definición

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

Simbólicamente:

$$A \text{ y } B \text{ son disjuntos} \Leftrightarrow \neg \exists x \; (x \in A \wedge x \in B)$$

Ejemplo 2.6

¿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 disyuntos porque tienen a 1 como elemento en común.

Actividad 2.2

Sea $U = \mathbb{N}$ 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 $B = \{x \in \mathbb{N} \,/\, x \text{ es impar}\}$

c) $A = \{x \in \mathbb{N} \,/\, 2x \text{ es par}\}$ y $B = \{x \in \mathbb{N} \,/\, 3x \text{ es par}\}$

2.4 Diagramas de Venn

Son diagramas propuestos por John Venn (1834-1923) para cálculos lógicos, en la actualidad se emplean para representar gráficamente los conjuntos y sus relaciones. 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.

2.4.1 Diagramas de Venn para dos Conjuntos

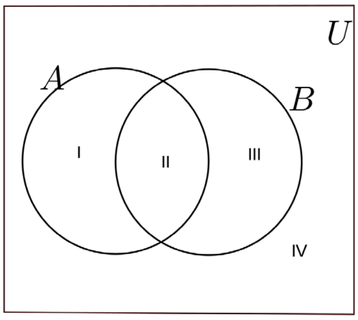


Fig. 2.1. Diagrama de Venn para dos subconjuntos de U

En la Figura 2.1, se observan cuatro regiones: I, II, III, IV.

Si A y B son dos conjuntos arbitrarios, entonces es posible que algunos elementos estén en A pero no en B (región I), algunos en B pero no en A (región II), algunos en los dos: A y B (región IIII), y algunos ni en A, ni en B (región IV).

👁 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.

2.4.2 Diagramas de Venn para Tres Conjuntos

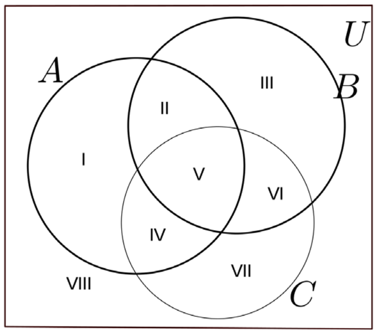


Fig. 2.2. Diagrama de Venn para tres subconjuntos de U.

En la Figura 2.2, se observan ocho regiones: I, II, III, IV, V, VI, VII, VIII.

Si A, B y C son tres conjuntos arbitrarios, entonces es posible que algunos elementos pertenezcan a solo uno de ellos (sólo a A, región I; sólo a B, región III; sólo a C, región VIII), a dos (pertenecen sólo a A y B, región II; pertenecen sólo a B y C, región VI; pertenecen sólo a A y C, región IV), a los tres conjuntos (región V) o a ninguno (región VIII).

Ejemplo 2.7

El elemento a pertenece sólo al conjunto A, c pertenece sólo a B y f pertenece sólo a C.

El elemento b pertenece sólo a A y B; g pertenece sólo a B y C; y e pertenece sólo a A y C.

El elemento d pertenece a los tres conjuntos, y los elementos i y h, sólo son elementos de U, no pertenecen a ninguno de los tres conjuntos.

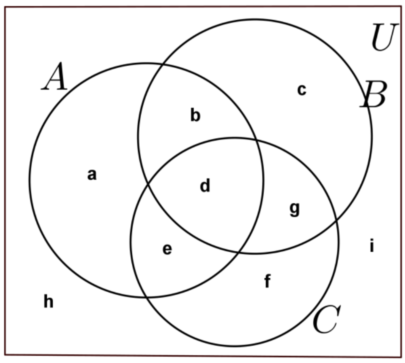


Fig. 2.3. Diagrama de Venn, del Ejemplo 2.7.

Actividad 2.3

i) Suponga que U = { x / x es alumno de la FRT} , A = { x $\in$ U / x cursa Matemática Discreta } y B = {x $\in$ U / x cursa Algebra}

Diga cuales son las características de cada una de las regiones delimitadas en un diagrama de Venn

ii) Si U = { x / x es alumno de la UTN-FRT} y los conjuntos A, B y C definidos como sigue:

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

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

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

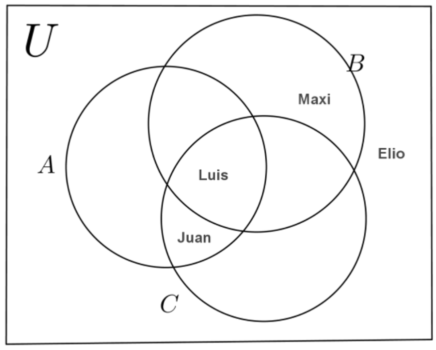


Fig. 2.4. Diagrama de Venn de la Actividad 2.3.

Responder y justificar:

i) ¿Luis trabaja? ¿Cuántos trabajan? ¿Juan tiene hijos y trabaja?

ii) ¿Elio es alumno de la FRT? ¿Cuántos alumnos tiene la FRT?

iii) ¿Maxi es un alumno de la FRT menor de 20 años?

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

v) ¿Quienes trabajan y no tienen hijos?

2.5 Inclusión de conjuntos. Subconjuntos

Definición

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

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

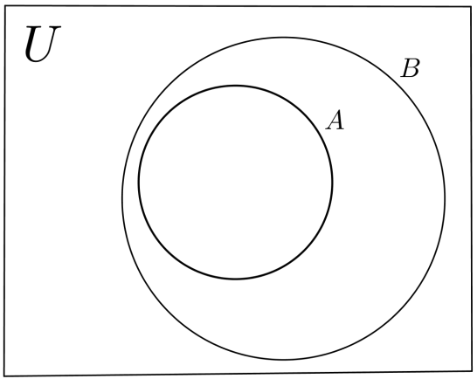


Fig.2.5.Inclusión.

Observaciones

- 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.

  $$A \not\subseteq B \Leftrightarrow \neg (A \subseteq B) \Leftrightarrow \neg[\forall\, x, (x \in A \Rightarrow x \in B)] \Leftrightarrow \exists\, x, (x \in A \wedge x \notin B)$$

- Si $A \subseteq B$, también se dice que B contiene a A.

- El símbolo $\subseteq$ se llama "Símbolo de inclusión amplia". Si en particular A es subconjunto de B y en 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".
- Si se usa el símbolo de inclusión amplia ($\subseteq$) cuando se cumple la inclusión estricta ($\subset$) no se considera error, ya que el primero es un símbolo que acepta ambas posibilidades: la inclusión estricta y la igualdad.

Ejemplos 2.8

i) Para probar que $A = \{ x \in \mathbb{R} \,/\, x^2 - 3x + 2 = 0 \}$ es subconjunto de $B = \{1, 2, 4\}$ se toma un elemento cualquiera de A y se demuestra que pertenece a B.

Sea $a \in A$, luego este elemento debe verificar la ecuación:

$$a^2 - 3a + 2 = 0 \Leftrightarrow a = 2 \vee a = 1 \Rightarrow a \in B$$

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

ii) ¿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, $4^2 - 3.\ 4 + 2 \neq 0$, luego $4 \notin A$, es decir, hay un elemento en B que no está en A, por lo tanto, $B \not\subset A$.

Actividad 2.4

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

i) $\mathbb{N}$ ... $\mathbb{Z}$ y $\mathbb{R}$ .... $\mathbb{Z}$

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

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

b) Sean $A = \{ x \in \mathbb{Z} \ / \ x = 3k \ , \ k \in \mathbb{Z} \}$, $B = \{ x \in \mathbb{Z}^+ \ / \ x = 3k \ , \ k \in \mathbb{Z} \}$ y $C = \{ x \in \mathbb{Z} \ / \ x = 6k \ , \ k \in \mathbb{Z} \}$. Indicar Verdadero o Falso, justificando su respuesta:

i) $B \subset A$ ii) $C \subseteq A$

iii) $C \subseteq B$ iv) $B \not\subseteq C$

Propiedades de la Inclusión

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

a) $\varnothing \subseteq A$ El vacío es subconjunto de cualquier conjunto

b) $A \subseteq A$ Todo conjunto es subconjunto de sí mismo

c) $A \subseteq U$ Todo conjunto es subconjunto del conjunto Universal

Demostraciones

1a) Por definición: $A \subseteq B \Leftrightarrow \forall x, (x \in A \Rightarrow x \in B)$

Si se considera la siguiente proposición: $\forall x, (x \in \varnothing \Rightarrow x \in A)$ ésta es Verdadera, por ser el antecedente Falso. En consecuencia de acuerdo a la definición de inclusión: $\varnothing \not\subseteq A$.

1b) (directa)

Es evidente que se cumple que $\forall x \in A, (x \in A \Rightarrow x \in A)$, luego por definición de inclusión: $A \subseteq A$, que se lee “Todo elemento de A, pertenece a A”.

1c) (trivial)

Para demostrar que $A \subseteq U$, se tiene que demostrar que $\forall x \in A, (x \in A \Rightarrow x \in U)$.

Pero $x \in U$ es verdadero para todos los x, (por definición de conjunto universal) luego la implicación también es verdadera ya que su consecuente es verdadero siempre (por ser una tautología), por lo tanto $A \subseteq U$.

2) Caracterización de la Igualdad

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

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

Demostración

En efecto, sea

$A = B \Leftrightarrow \forall x\, [(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)]$, por definición de igualdad de conjuntos,

$\Leftrightarrow [\forall x\, (x \in A \Rightarrow x \in B)] \wedge [\forall x\, (x \in B \Rightarrow x \in A)]$, por asociativdad de $\forall$

$\Leftrightarrow A \subseteq B \wedge B \subseteq A$, por definición de inclusión de conjuntos.

3) Transitividad de la Inclusión

Sean A, B y $C \subseteq U$. 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 $\forall x, (x \in A \Rightarrow x \in C)$, por la regla de Generalización Universal (GU). Luego, $A \subseteq C$.

👁 **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}.
- Sea A es un conjunto cualquiera, luego {A} es un conjunto con un único elemento A, sin importar cuantos elementos tenga A, luego ambos conjuntos: A y {A} son conjuntos distintos.

Ejemplos 2.9

¿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: el $\emptyset$. Luego, se tiene que $\emptyset \in \{\emptyset\}$ e incluso $\emptyset \subseteq \{\emptyset\}$, pero $\emptyset \neq \{\emptyset\}$.
- $\{ \emptyset, \{\emptyset\} \}$ es el conjunto con dos elementos: $\emptyset$ y $\{\emptyset\}$.

2.6 Conjunto Potencia de un conjunto finito

Definición

Dado un conjunto A, llamamos Conjunto Potencia de A a la colección de todos los subconjuntos de A. Se denota por P(A).

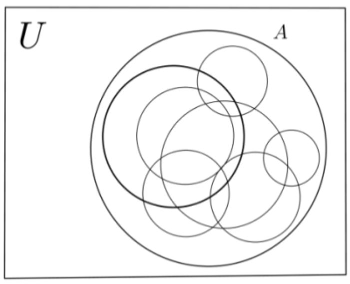


Fig. 2.6. Potencia de A.

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.

Ejemplos 2.10

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

De la propiedad de la inclusión, se sigue que $\emptyset$ es uno de sus elementos ya que Ø $\subseteq$ A. 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 de aquí que P (A) = {Ø, $\{a\}$, $\{b\}$, A}

ii) Si A = {1, 2, 3}, entonces, P(A) = { Ø, {1}, {2}, {3}, {1,2}, {1,3}, {2,3}, A}

2.6.1 Cardinal del Conjunto Potencia

Definición

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

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 cardinal 4. ¿Hay elementos de P(A) con cardinal 5?

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

2.7 Álgebra de Conjuntos: Operaciones

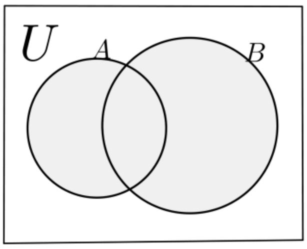
2.7.1 Unión

Definición

La unión de dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a A, a B, o a ambos. Se denota A $\cup$ B. Simbólicamente se escribe: $A \cup B = \{ x \in U \ / \ x \in A \vee x \in B \}$

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:



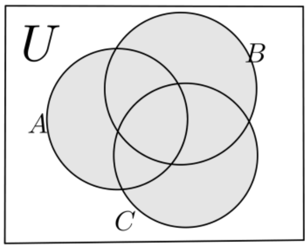


Fig.2.7. $A \cup B$.

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

2.7.2 Intersección

Definición

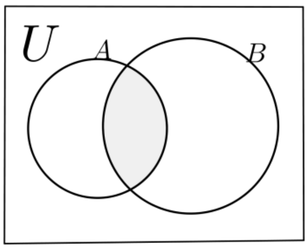
La Intersección de dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a ambos conjuntos a la vez. Se denota $A \cap B$. Simbólicamente se escribe: $A \cap B = \{ x \ / \ x \in A \ \wedge \ x \in B \}$.

Observaciones

- Si A y B son disjuntos, entonces $A \cap B = \varnothing$

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:



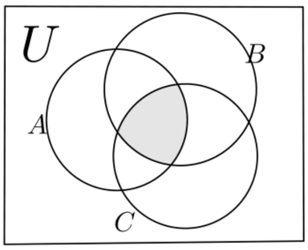


Fig. 2.9. $A \cap B$.

Fig. 2.10. $A \cap B \cap C$.

2.7.3 Diferencia

Definición

La diferencia entre dos conjuntos A y B es el conjunto formado por todos los elementos de A que no pertenecen a B. Se denota por A – B, y se lee “A menos B”. Simbólicamente se escribe: $A - B = \{x \in U / x \in A \;\wedge\; x \notin B\}$

Generalizando para tres conjuntos:

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

$= \{ x \in U / x \in (A - B) \wedge x \notin C\} = \{ x \in U / x \in A \;\wedge\; x \notin B \wedge x \notin C \}$

Las regiones sombreadas representan a las operaciones indicadas:

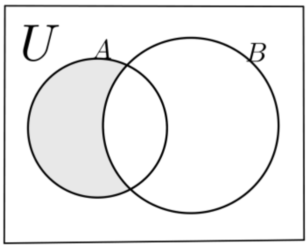


Fig. 2.11. A - B.

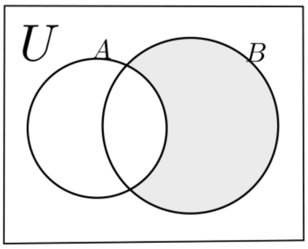


Fig.2.12. B - A.

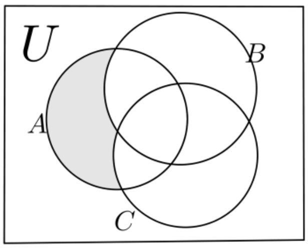


Fig. 2.13. A – B – C.

Observaciones

- Siguiendo la definición, se tiene que: $B - A = \{x \in U / x \in B \;\wedge\; x \notin A\}$
- Existe una estrecha vinculación entre el concepto de diferencia y las operaciones lógicas de conjunción y negación
- $A - B = A$ y $B - A = B$ si y solo si $A \cap B = \varnothing$.

2.7.4 Complemento

Definición

El complemento de A es el conjunto formado por todos los elementos de universo que no pertenecen a A. Se denota A’ o A^c. Simbólicamente se escribe

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

👁 **Observaciones**

- Existe una estrecha vinculación entre el concepto de complemento y la operación lógica de negación.
- De la definición se desprende que A’ = U – A.

Las regiones sombreadas representan a las operaciones indicadas:

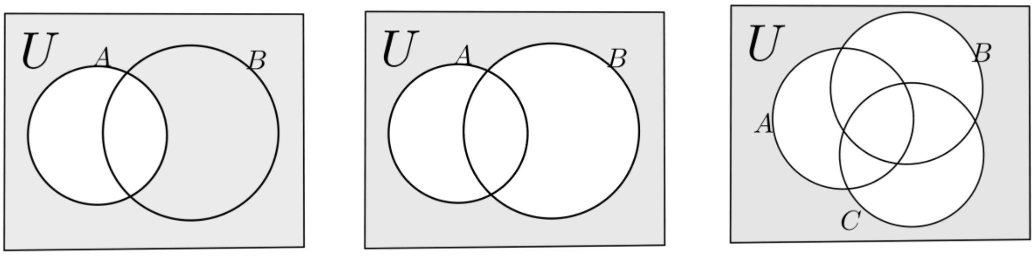


Fig. 2.14. A’. Fig. 2.15. $(A \cup B)$. Fig.2.16. $(A \cup B \cup C)'$.

2.7.5 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 $A \oplus B$. Simbólicamente se escribe: $A \oplus B = \{ x \ / \ x \in A \ \underline{\vee} \ x \in B \}$

Otra forma equivalente de expresar:

$A \oplus B = \{ x \ / \ x \in A \ \underline{\vee} \ x \in B \} = \{ x \ / \ (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \}$, por ley de la disyunción excluyente,

$= \{ x \ / \ (x \in A \wedge x \in B') \vee (x \in B \wedge x \in A') \}$, por definición de complemento de un conjunto,

$= \{ x \ / \ (x \in A - B) \vee (x \in B - A) \}$,por definición de diferencia de conjunto,

Luego: $A \oplus B = (A – B) \cup (B – A)$, por definición de unión de conjunto.

En el caso de tener tres conjuntos:

$$A \oplus B \oplus C = (A – B – C) \cup (B – A – C) \cup (C – A – B) \cup (A \cap B \cap C)$$

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

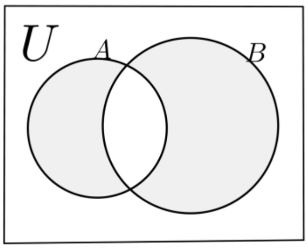


Fig.2.17. A ⊕ B.

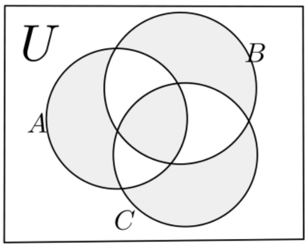


Fig.2.18. A ⊕ B ⊕ C.

Observación

- Existe una estrecha vinculación entre el concepto de diferencia simétrica y la operación lógica de disyunción excluyente.
- De la definición se desprende $A \oplus B = (A \cap B') \cup (B \cap A')$.

Ejemplos 2.11

Sean los conjuntos $A = \{ n \in \mathbb{Z}^+ / n < 9 \}$; $B = \{ n \in \mathbb{Z}^+ / n \text{ es par} \wedge n \leq 16 \}$ y $C = \{n \in \mathbb{Z}^+ : n \text{ es impar} \wedge n < 15\}$, entonces:

i) $A \cup B = \{ n \in \mathbb{Z}^+ / n < 9 \vee (n \text{ es par} \wedge n \leq 16)\}$

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

ii) $A \cup B \cup C = \{ n \in \mathbb{Z}^+ / n < 9 \vee (n \text{ es par} \wedge n \leq 16) \vee (n \text{ es impar} \wedge n < 15) \}$

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

iii) $A \cap B = \{ n \in \mathbb{Z}^+ / n < 9 \wedge (n \text{ es par} \wedge n \leq 16)\} = \{ 2, 4, 6, 8\}$

iv) $A \cap B \cap C = \{ n \in \mathbb{Z}^+ / n < 9 \wedge (n \text{ es par} \wedge n \leq 16) \wedge (n \text{ es impar} \wedge n < 15) \} = \varnothing$

v) $A - B = \{ n \in \mathbb{Z}^+ / n < 9 \wedge \neg(n \text{ es par} \wedge n \leq 16) \} =$

$= \{ n \in \mathbb{Z}^+ / n < 9 \wedge (n \text{ es impar} \vee n > 16) \} = \{1 , 3 , 5 , 7\}$

vi) $B - A = \{ n \in \mathbb{Z}^+ / n \text{ es par} \wedge n \leq 16 \wedge n \geq 9 \} = \{ 10 , 12 , 14 , 16 \}$

vii) $A - B - C = (A - B) - C = \{1 , 3 , 5 , 7\} - \{1 , 3 , 5 , 7 , 9 , 11, 13\} = \varnothing$

viii) $A' = \{ n \in \mathbb{Z}^+ / n \geq 9 \} = \{9, 10, 11, 12, 13 , 14 , 15 , 16 , 17 , 18, 19, ... \}$

ix) $B' = \{ n \in \mathbb{Z}^+ / \neg (n \text{ es par} \wedge n \leq 16)\} = \{ n \in \mathbb{Z}^+ / n \text{ es impar} \vee n > 16 \}$

$= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 18, 19, 20, 21, 22, 23, 24, \ldots\}$

x) $A' \cap B' = \{9, 11, 13, 15, 17, 18, 19, 20, 21, 22, 23, \ldots\}$

xi) $A \oplus B = (A - B) \cup (B - A) = \{1, 3, 5, 7\} \cup \{10, 12, 14, 16\}$

$= \{1, 3, 5, 7, 10, 12, 14, 16\}$

xii) $A \oplus B \oplus C = (A \oplus B) \oplus C = \{1, 3, 5, 7, 10, 12, 14, 16\} \oplus$

$\{1, 3, 5, 7, 9, 11, 13\} = \{9, 10, 11, 12, 13, 14, 16\}$

Ejemplos 2.12

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.

i) $B - A \subseteq B$

Se toma un elemento arbitrario x de U: $x \in B - A \Leftrightarrow x \in B \wedge x \notin A$ (por definición de diferencia) $\Rightarrow x \in B$ (ley de simplificación de la conjunción)

Luego, por la regla de G.U. se tendrá $\forall x\, [x \in (B - A) \Rightarrow x \in B]$ y por definición de subconjuntos: $B - A \subseteq B$.

ii) $A \subseteq A \cup B$

Sea x un elemento arbitrario de U, entonces

$x \in A \Rightarrow x \in A \vee x \in B$ (por ley de adición disyuntiva) $\Leftrightarrow x \in (A \cup B)$ (por definición de unión).

Luego, por la regla de GU: $\forall x\, [x \in A \Rightarrow x \in (A \cup B)]$, por definición de subconjuntos: $A \subseteq A \cup B$

iii) $A \cap B \subseteq B$

Sea x un elemento arbitrario de U, entonces

$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$ (definición de intersección) $\Rightarrow x \in B$ (simplificación)

Luego, por la regla de GU: $\forall x\, [x \in (A \cap B) \Rightarrow x \in B]$, por def. de contención:

$$A \cap B \subseteq B$$

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) $c \in A'$

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

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

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

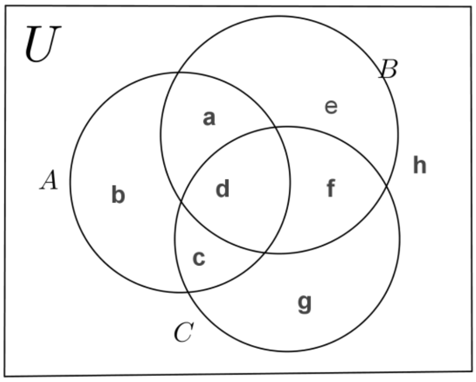


Fig.2.19. Actividad 2.6.

b) Sin expresar por extensión, 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) $(C \cup B) - A$

2.8 Leyes del Álgebra de Conjuntos

En el álgebra de conjuntos, también 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 $\varnothing$ por el U, y viceversa, se obtiene otra expresión (o ley), que se llama su expresión dual.

Las operaciones entre conjuntos cumplen las siguientes propiedades o leyes, que se resumen en la Tabla 2.1:

1.	$(A')' = A$		Ley de involución
2.	$A \cup A = A$	$A \cap A = A$	Leyes de Idempotencia
3.	$A \cup B = B \cup A$	$A \cap B = B \cap A$	Leyes conmutativas
4.	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$	Leyes asociativas
5.	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Leyes distributivas
6.	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$	Leyes de Absorción
7.	$A \cup A' = U$	$A \cap A' = \emptyset$	Leyes de los complementos
8.	$(A \cup B)' = A' \cap B'$	$(A \cap B)' = A' \cup B'$	Leyes de De Morgan
9.	$A \cup \emptyset = A$	$A \cap U = A$	Leyes de los Neutros
10	$A \cap \emptyset = \emptyset$	$A \cup U = U$	Leyes de Dominación

Tabla 2.1. Principales Leyes del Algebra

2.8.1 Ley de Involución

Sea $A \subseteq U$, se verifica que:

$$(A')' = A$$

Demostración

Por definición de complemento se tiene que: $A' = \{x \in U \,/\, \neg (x \in A)\}$

Luego $(A')' = \{x \in U \,/\, \neg [\neg (x \in A)]\}$ (Doble Negacion)

Por lo tanto $(A')' = \{x \in U \,/\, x \in A\} = A$. En consecuencia $(A')' = A$

2.8.2 Leyes de Idempotencia

Sea $A \subseteq U$, entonces:

i) $A \cup A = A$ ii) $A \cap A = A$

Demostración

i) Sea x un elemento arbitrario de U.

Entonces, $x \in (A \cup A) \Leftrightarrow x \in A \vee x \in A$ (Definición de unión)

$\Leftrightarrow x \in A$ (Idempotencia de $\vee$)

De la arbitrariedad de x se sigue que: $\forall x\ [x \in (A \cup A) \Leftrightarrow x \in A]$ (Regla de la G.U.). De aquí que $A \cup A = A$

ii) $A \cap A = A$, se cumple por ser dual de $A \cup A = A$.

2.8.3 Leyes Conmutativas

Sean $A, B \subseteq U$, se verifica que:

i) $A \cup B = B \cup A$ ii) $A \cap B = B \cap A$

Demostración

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

$x \in (A \cup B) \Leftrightarrow x \in A \vee x \in B$ (Definición de unión)

$\Leftrightarrow x \in B \vee x \in A$ (Conmutatividad de $\vee$)

$\Leftrightarrow x \in (B \cup A)$ (Definición de unión)

Como x es cualquiera de U, se sigue que (Generalización universal)

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

ii) $A \cap B = B \cap A$ se cumple por ser dual de $A \cup B = B \cup A$.

2.8.4 Leyes Asociativas

Sean A, B , C $\subseteq$ U , se verifica que:

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

Demostración

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

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

$\Leftrightarrow x \in A \vee (x \in B \vee x \in C)$ (Definición de unión)

$\Leftrightarrow (x \in A \vee x \in B) \vee x \in C$ (Asociatividad de $\vee$)

$\Leftrightarrow x \in (A \cup B) \vee x \in C$ (Definición de unión)

$\Leftrightarrow x \in (A \cup B) \cup C$ (Definición de unión)

De la arbitrariedad de x se sigue que (Generalización universal)

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

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

ii) $A \cap (B \cap C)=(A \cap B) \cap C$ se cumple por ser dual de $A \cup (B \cup C)=(A \cup B) \cup C$

2.8.5 Leyes Distributivas

Sean A, B , C $\subseteq$ U , se verifica que:

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

Demostración

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

$x \in A \cup (B \cap C) \Leftrightarrow x \in A \vee [x \in (B \cap C)]$ (Definición de unión)

$\Leftrightarrow x \in A \vee (x \in B \wedge x \in C)$ (Definición de intersección)

$\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ (Distributividad)

$\Leftrightarrow x \in (A \cup B) \wedge x \in (A \cup C)$ (Definición de unión)

$\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$ (Definición de intersección)

Al ser x cualquier elemento de U, se sigue que (Generalización universal)

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

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

ii) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ se cumple por ser dual de $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$

2.8.6 Leyes de Absorción

Sean A, B $\subseteq$ U , se verifica que:

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

Demostración

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

$x \in A \cup (A \cap B) \Leftrightarrow x \in A \vee [x \in (A \cap B)]$ (Definición de unión)

$\Leftrightarrow x \in A \vee (x \in A \wedge x \in B)$ (Definición de intersección)

$\Leftrightarrow x \in A$ (Absorción)

Al ser x cualquier elemento de U, se sigue que (Generalización universal)

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

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

ii) $A \cap (A \cup B) = A$ se cumple por ser dual de $A \cup (A \cap B) = A$

2.8.7 Leyes de los Complementos

Sea $A \subseteq U$, se verifica que:

i) $A \cup A' = U$ ii) $A \cap A' = Ø$

Demostración

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

$x \in (A \cup A') \Leftrightarrow x \in A \vee x \in A'$ (Definición de unión)

$\Leftrightarrow x \in A \vee x \notin A$ (Complementario)

$\Leftrightarrow x \in U$ (Tautología)

Luego, $\forall x, [x \in (A \cup A') \Leftrightarrow x \in U]$. (Generalización universal)

Por lo tanto, $A \cup A' = U$

ii) $A \cap A' = Ø$ se cumple por ser dual de $A \cup A' = U$.

2.8.8 Leyes de De Morgan

Sean A, B $\subseteq$ U , se verifica que:

i) $(A \cup B)' = A' \cap B'$ ii) $(A \cap B)' = A' \cup B'$

Demostración

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

$$
\begin{aligned}
x \in (A \cup B)' &\Leftrightarrow x \notin (A \cup B) && \text{(complemento)}\\
&\Leftrightarrow \neg[\, x \in (A \cup B)] && \text{(negación)}\\
&\Leftrightarrow \neg[\,(x \in A) \vee (x \in B)] && \text{(unión)}\\
&\Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) && \text{(De Morgan para } \vee)\\
&\Leftrightarrow x \notin A \wedge x \notin B && \text{(negación)}\\
&\Leftrightarrow x \in A' \wedge x \in B' && \text{(complemento)}\\
&\Leftrightarrow x \in A' \cap B' && \text{(intersección)}
\end{aligned}
$$

Al ser x cualquier elemento de U, se sigue que

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

Luego $(A \cup B)' = A' \cap B'$.

ii) $(A \cap B)' = A' \cup B'$ se cumple por ser dual de $(A \cup B)' = A' \cap B'$.

2.8.9 Leyes de los elementos neutros

Sea A $\subseteq$ U , se verifica que:

i) $A \cup Ø = A$ ii) $A \cap U = A$

Demostración

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

$x \in A \cup Ø \Leftrightarrow (x \in A) \vee (x \in Ø)$ (unión) $\Leftrightarrow x \in A$ (dado que $x \in Ø$ es falso)

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

ii) $A \cap U = A$ se cumple por ser dual de $A \cup Ø = A$.

2.8.10 Leyes de Dominación

Sea $A \subseteq U$, se verifica que:

i) $A \cap Ø = Ø$ ii) $A \cup U = U$

Demostración

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

$x \in A \cap Ø \Leftrightarrow (x \in A) \wedge (x \in Ø)$ (intersección)

$\Leftrightarrow x \in Ø$ (dado $x \in Ø$ es falso). Luego, $A \cap Ø = Ø$

ii) $A \cup U = U$ se cumple por ser dual de $A \cap Ø = Ø$

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

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

2.9 Partición de un conjunto

Definición

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

1) La unión de todos los subconjuntos da como resultado A,

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

2) Todo par de subconjuntos es disjunto,

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

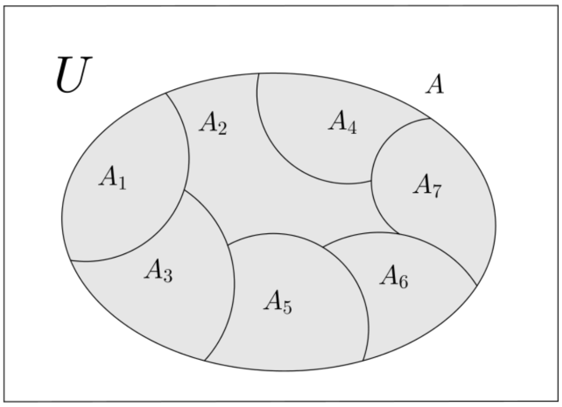


Fig. 2.20. Conjunto A particionado en siete subconjuntos.

Ejemplos 2.13

Si $\mathbb{P} = \{x \in \mathbb{Z} \ / \ x \text{ es par}\}$ e $\mathbb{I} = \{ x \in \mathbb{Z} \ / \ x \text{ es impar} \}$, se tiene que $\{ \mathbb{P}, \mathbb{I} \}$ es una partición de $\mathbb{Z}$, pues: $\mathbb{P} \cap \mathbb{I} = \varnothing$ 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) $\{\{ x \in A \ / \ x = 2k , k \in \mathbb{Z} \} , \{ x \in A \ / \ x = 3k , k \in \mathbb{Z} \} \}$

2.10 Producto Cartesiano

Definición

El producto cartesiano de dos conjuntos A y B , no vacíos, se define como el conjunto de todos los pares ordenados que se pueden formar, donde la primera componente es de A y la segunda componente es de B. Simbólicamente:

$$A \times B = \{(x, y) \ / \ x \in A \ \wedge \ y \in B\}$$

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. El concepto de par ordenado es fundamental en Matemática. 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, etc.

Si $A = B$; $A \times A = \{(x, y) / \ x \in A \wedge y \ \in A\} = A^2$.

Ejemplos 2.14

Sea $\mathbb{R}$: conjunto 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 se representa como:

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

Cada punto P del plano está representado por un par ordenado $(x,\ y)$ de números reales y viceversa. A $\mathbb{R}^2$ se le llama usualmente el Plano Cartesiano.

Teorema

Si A y B son tales que $|A| = n$ y $|B| = m$, entonces $|\ A \times B\ | = n.m$

Ejemplos 2.15

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 determinan por extensión a los conjuntos A y B:

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

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

Entonces $|A \times B| = |A|.|B| = 4.2 = 8$ y definido por extensión se tiene:

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

Actividad 2.9

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

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

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

iii) $(1, a) \in A \times B \ \wedge \ (a, 1) \in A \times B$

iv) $(a, b) \in B \times B$

2.11 Relaciones entre conjuntos

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

Existen algunas estructuras básicas que pueden representarse a través de la relación entre elementos de conjuntos. Aplicaciones numéricas, recuperación de información y problemas de redes son 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, en las estructuras de programas y análisis de algoritmos.

Como ejemplos cotidianos se tiene las 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”; entre otras.

2.12 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.

Definición

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

$R \subseteq (A \times B)$ o $R : A \longrightarrow B$

Notación:

Dado que R es un conjunto de pares ordenados, si (x, y) forma parte de la relación se denotará: $(x, y) \in R$ o $x\ R\ y$

En cualquiera de los casos se dice que x está relacionado con y.

Caso particular:

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

$R \subseteq (A \times A)$ o $R: A \longrightarrow A$

Ejemplos 2.16

i) Sea $R_1 = \{ (a, b) \in \mathbb{Z}^2 \ / \ a > b \}$, entonces (8 , -2) $\in R_1$ y (-2 , 8) $\notin R_1$

ii) Sea $A = \{a, b, c\}$ y R_2 en A definida como $R_2 = \{(a, a); (a, b), (a, c), (c, c)\}$ entonces se tiene que: $a\ R\ a$, $a\ R\ b$, $a\ R\ c$ y $c\ R\ c$.

iii) Cuando un compilador traduce un programa informático construye una tabla 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 $S \longrightarrow A$ y de $S \longrightarrow P$.

2.12.1 Dominio e Imagen

Definiciones

El dominio de una relación R es el conjunto formado por los primeros elementos de los pares ordenados que la componen.

La imagen de R es el conjunto formado por los segundos elementos de los pares ordenados que la componen.

Simbólicamente, si $R: A \rightarrow B$ entonces:

$$\text{Dom } R = \{x \in A \;/\; \exists\, y \in B \wedge (x, y) \in R\}$$

$$\text{Im } R = \{y \in B \;/\; \exists\, x \in A \wedge (x, y) \in R\}$$

Así, en el Ejemplo 2.16 ii) se tiene que Dom $R_2 = \{a, c\}$ e Im $R_2 = \{a, b, c\}$.

2.12.2 Conjunto Relativo de un elemento

Definición

Sea $R: A \rightarrow B$ y sea $a \in A$. Se define conjunto relativo de a, y se denota $R(a)$, 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.

Ejemplos 2.17

Sean $A = \{2, 4, 6\}$ y $B = \{1, 6, 8, 9\}$ y sea $R \subseteq A \times B$ definida por

$$x\, R\, y \;\Leftrightarrow\; x < y$$

Entonces R definida por extensión es:

$$R = \{(2, 6), (2,8), (2, 9), (4, 6), (4, 8), (4, 9), (6, 8), (6, 9)\}$$

$$\text{Dom } R = A \quad \text{e} \quad \text{Im } R = \{6, 8, 9\}$$

Además, los conjuntos relativos a cada elemento son:

$$R(2) = \{y \in B \;/\; (2, y) \in R\} = \{6, 8, 9\}$$

$$R(4) = \{y \in B \;/\; (4, y) \in R\} = \{6, 8, 9\}$$

$$R(6) = \{y \in B \;/\; (6, y) \in R\} = \{8, 9\}$$

2.12.3 Función

Las funciones son relaciones binarias especiales. Una función puede tomarse como una relación de entrada-salida; es decir, para cada entrada o argumento, una función produce una única 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 conjuntos no vacíos. Una función f de A en B es una relación de A en B, en la que para cada $x \in A$, existe un único elemento $y \in B \;/\; (x,y) \in f$.

Notación:

Escribiremos $(x, y) \in f$ o $f(x) = y$ indistintamente, para indicar que al elemento x le corresponde y mediante f, o que y es la imagen de x por f.

Simbólicamente: Una Relación $f : A \to B$ es una función si y solo si

i) Dom $f = A$, esto es, $\forall x \in A, \exists y \in B : f(x) = y$ (Condición de existencia)

ii) $\forall x \in A$, $f(x) = y \;\wedge\; f(x) = z \;\Rightarrow\; y = z$ (Condición de unicidad)

En palabras, diremos que f es una función de A en B si y solo si todo elemento de A tiene imagen y dicha imagen es única.

Observaciones

- Si una de las dos condiciones no se cumple, entonces es suficiente para decir que la relación no es función.
- Las funciones reciben también el nombre de aplicaciones o transformaciones, ya que desde un punto de vista geométrico, se pueden considerar como reglas que transforman a cada elemento de A en un único elemento de B.

Ejemplos 2.18

Sean A = {1, 3, 5} , $B = \{a, b, c, d\}$ y las relaciones siguientes:

R_1 = {(3, a); (5, a)} R_2 = {(3, a); (3, b), (1, b), (5, c)}

R_3 = {(1, a), (3, a); (5, a)} R_4 = {(1, a), (3, b); (5, c)}

Se tiene que:

- R_1 no es función ya que Dom(R_1) = {3, 5} $\neq A$, por lo tanto no cumple la condición de existencia
- R_2 no es función ya que (3, a) $\in R$ y (3, b)$\in R$,   3 tiene dos imágenes distintas, a y b, por lo tanto no cumple la condición de unicidad
- R_3 es función, dado que Dom R_3 = A y a cada elemento de A le corresponde un único elemento de B. En este caso, a todos el mismo, Im R_3= $\{a\}$
- R_4 es función, dado que Dom R_4 = A y a cada elemento de A le corresponde un único elemento de B. En este caso, Im R_4= $\{a , b , c\}$

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 de las relaciones de los apartados a) y b) e indicar cuáles son funciones.

2.13 Matriz Booleana

Una de las maneras de representar una relación entre conjuntos finitos es a través de su matriz booleana.

Definición

Una matriz booleana es una matriz cuyas componentes o entradas son exclusivamente ceros '0' o unos '1'.

Es decir, una 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, relaciones en programas informáticos, modelos de redes de comunicación, sistemas de transporte, etc.

Ejemplos 2.19

Las siguientes son matrices booleanas de tamaño 3x3 y de 3x2

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad ; \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Observe que $a_{21} = 0 \, , a_{21} \neq a_{12} \, , a_{11} = a_{22} = a_{33} = 1 \, , b_{11} \neq b_{22} \; y \; b_{31} = 1$

2.13.1 Operaciones con matrices booleanas

Las operaciones que se pueden realizar entre matrices booleanas son tres: disyunción o suma lógica, conjunción o producto lógico y producto booleano. Además las matrices booleanas pueden compararse. A continuación cada uno de estos conceptos y los requisitos de cada operación.

a) Disyunción o Suma lógica

Definición

Sean A = (a_{ij}) y B= (b_{ij}) matrices booleanas de orden mxn, la disyunción o suma lógica de A y B es la matriz booleana C, del mismo orden, definida como C = A $\vee$ B, tal que su elemento genérico es:

$$c_{\text{ij}} = \begin{cases} 1 & \text{si y solo si } a_{\text{ij}} = 1 \vee b_{\text{ij}} = 1 \\ \\ 0 & \text{en otro caso} \end{cases}$$

Observación

Cada elemento de C se calcula realizando la operación lógica disyunción incluyente entre los elementos de la misma posición de A y B.

Ejemplo 2.20

Si A = $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ y B = $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, entonces

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) Conjunción o Producto Lógico

Definición

Sean A = (a_{ij}) y B= (b_{ij}) matrices booleanas de orden mxn, la conjunción o producto lógico de A y B es la matriz booleana C, del mismo orden, definida como C = A $\wedge$ B, tal que su elemento genérico es

$$c_{\text{ij}} = \begin{cases} 1 & \text{si y solo si } a_{\text{ij}} = 1 \wedge b_{\text{ij}} = 1 \\ \\ 0 & \text{en otro caso} \end{cases}$$

Observación

Cada elemento de C se calcula realizando la operación lógica conjunción entre los elementos de la misma posición de A y B.

🗒 **Ejemplo 2.21**

Si A = $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ y B = $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, entonces

C = A ∧ B = $\begin{pmatrix} 1\wedge1 & 1\wedge0 & 0\wedge1 \\ 0\wedge1 & 1\wedge0 & 0\wedge0 \\ 0\wedge0 & 1\wedge1 & 1\wedge1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

c) Producto booleano

📚 **Definición**

Sean A = (a_{ij}) y B= (b_{ij}) matrices booleanas tales que A es de orden $m \text{ x } r$ y B es de orden $r \text{ x } n$, la matriz producto booleano entre A y B es la matriz booleana C de orden $m \text{ x } n$, definida como C = A ⊙ B cuyo elemento genérico es

$$c_{\mathrm{ij}} = \begin{cases} 1 & \text{si y solo si } \exists \mathrm{k} \,/ a_{\mathrm{ik}} = 1 \;\wedge\; b_{\mathrm{kj}} = 1 \\ \\ 0 & \text{en otro caso} \end{cases}$$

👁 **Observaciones**

El producto booleano es análogo a la multiplicación matricial ordinaria en donde se operan filas de la primera con columnas de la segunda matriz y tal que la adición es sustituida por ∨ y la multiplicación es sustituida por ∧.

🗒 **Ejemplo 2.22**

Si A = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$ y B = $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, entonces

C= A ⊙ B = $\begin{pmatrix} (1\wedge1)\vee(0\wedge0) & (1\wedge1)\vee(0\wedge1) & (1\wedge0)\vee(0\wedge1) \\ (0\wedge1)\vee(1\wedge0) & (0\wedge1)\vee(1\wedge1) & (0\wedge0)\vee(1\wedge1) \\ (1\wedge1)\vee(0\wedge0) & (1\wedge1)\vee(0\wedge1) & (1\wedge0)\vee(0\wedge1) \end{pmatrix}$

= $\begin{pmatrix} 1\vee0 & 1\vee0 & 0\vee0 \\ 0\vee0 & 0\vee1 & 0\vee1 \\ 1\vee0 & 1\vee0 & 0\vee0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

iv) Dominación

Definición

Sean las matrices A = (a_{ij}) y B= (b_{ij}) del mismo orden. Se dice que A domina a B y se simboliza A ≥ B si y sólo si $a_{ij} \geq b_{ij} \quad \forall\ i, j$.

Ejemplo 2.23

Si A= $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$ y B= $\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$, entonces A ≥ B dado que $a_{ij} \geq b_{ij}$, $\forall\ i, j$

Actividad 2.11

Dadas las matrices: $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

a) Calcular A $\vee$ B , A $\wedge$ B , A $\odot$ B y B $\odot$ A

b) Responder : A domina a B , B domina a A?

A partir de aquí y hasta el final del capítulo se trabajarán con las relaciones definidas en un conjunto, o sea, las del tipo $R : A \longrightarrow A$.

2.13.2 Matriz de adyacencia de una relación binaria

Definición

Sea A un conjunto finito y sea $R : A \longrightarrow A$.Se define matriz de adyacencia de R a la matriz M_R (booleana, de orden n) cuyo elemento genérico m_{ij} está dado por

$$M_R = (m_{ij}) : \ m_{ij} = \begin{cases} 1 & \text{si } (a_i , a_j) \in R \\ 0 & \text{si } (a_i , a_j) \notin R \end{cases}$$

📚 **Teorema**

Toda relación definida en un conjunto finito tiene representación matricial booleana y recíprocamente, toda matriz booleana representa a una relación binaria.

🗒 **Ejemplo 2.24**

Sea A = { 1, 2, 4 } y sea $R : A \longrightarrow A$. definida por:

$$x\ R\ y \quad \Leftrightarrow \quad y \geq x$$

Entonces R = {(1,1), (1,2), (1,4), (2,2), (2,4), (4,4)} y su matriz es

$$\mathrm{M_R} = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 4 \end{array} & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

👁 **Observaciones**

- Cada fila y cada columna de $\mathrm{M_R}$ se corresponden con un elemento de A.
- Para determinar el dominio de R bastará ver en que filas hay al menos un 1 y para la imagen bastará con ver en que columnas hay al menos un 1.

2.14 Digrafo

📚 **Definición**

Un digrafo o grafo dirigido es un par ordenado $D = (A, R)$ donde A es un conjunto finito y $R: A \longrightarrow A$

A los elementos de A se les denomina nodos o vértices y a los pares ordenados de R se les denominan arcos, lados o aristas de D.

2.14.1 Representación gráfica de un Digrafo

1. A los nodos o vértices se los representa arbitrariamente por medio de puntos, círculos, etc.
2. A los arcos o aristas se los representa por medio de flechas uniendo los vértices de tal modo que si $(x, y) \in R$ se dibujará una flecha que va desde x hacia y, donde x es el vértice inicial e y es el vértice final de la arista (x, y).
3. Si $(x, x) \in R$, se dibujará una flecha de x a x. Se denomina bucle o lazo.

Ejemplo 2.25

En la Figura 2.21, se tiene una representación gráfica del digrafo D = (A, R), siendo A = {1, 2, 3, 4) y R = {(1,2); (1, 3), (2,1), (2,3), (3,4), (4,3)}.

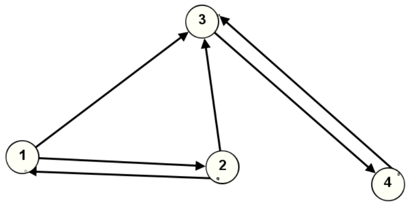


Fig. 2.21. D=(A,R)

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 R, 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 Grafos y Árboles se representará a los dígrafos por medio de la notación D = (V, A,φ) donde V representa al conjunto de vértices, A al conjunto de aristas y φ una función, llamada de incidencia dirigida, que representa φ: $A \longrightarrow$ (V x V).

Actividad 2.12

Encontrar la matriz y el digrafo de las relaciones R_i 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) }

2.15 Composición de Relaciones

Definición

Sean R_1y R_2 relaciones en A, se define $R_2 \circ R_1$, composición de R_1 con R_2 , a la relación definida por:

$$R_2 \circ R_1 = \{(x, y) / \ \exists\, z \in A \text{ tal que } (x, z) \in R_1 \ \wedge \ (z, y) \in R_2 \}$$

De la definición se desprende que $R_1 \circ R_2$, composición de R_2 con R_1 , es la relación definida por:

$$R_1 \circ R_2 = \{(x, y) / \ \exists\, z \in A \text{ tal que } (x, z) \in R_2 \ \wedge \ (z, y) \in R_1 \}$$

Ejemplos 2.26

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

i) $R_2 \circ R_1 =$ {(1, 5), (2, 1), (2, 3), (3, 2), (5, 4), (4, 1), (4,3)}

ii) $R_1 \circ R_2 =$ {(1,4), (3, 1), (4, 2), (4,3), (4, 5), (5,4)}

Observación

La composición de relaciones NO es conmutativa.

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 $R_2 \circ R_1$ y $R_1 \circ R_2$, y realizar los dígrafos de las cuatro nuevas relaciones: R_1 , R_2 , $R_2 \circ R_1$ y $R_1 \circ R_2$

Teorema sobre la matriz de una composición de relaciones

Sea A un conjunto finito y sean R_1 y R_2 definidas en A con sus respectivas matrices de Adyacencia M_{R_1}y M_{R_2}. Entonces la matriz de adyacencia de $R_2 \circ R_1$, $M_{R_2 \circ R_1}$, es el producto booleano entre las matrices M_{R_1}y M_{R_2}.

Simbólicamente $M_{R_2 \circ R_1} = M_{R_1} \odot M_{R_2}$

Actividad 2.14

Considerando R_1 y R_2 definidas en la Actividad 2.13, encontrar las matrices de

i) $R_2 \circ R_1$ ii) $R_1 \circ R_2$ iii) $R_1 \circ R_1$ iv) $R_2 \circ R_2$

2.15.1 Composición de una relación con sí misma

Definición

Sea A finito y sea $R: A \rightarrow A$. Se define R^n como la relación que es la composición de R por si misma n veces. Esto es

$$R^n = R \circ R \circ \ ... \ \circ R$$

Expresado de otro modo se tiene que:

$$R^n = \{ \ (x, y) \ / \ \exists \ z_1 \ , \ z_2, \ldots, z_{n-1} \ \in A, tal \ que \ (x \ , z_1) \ , (\ y_1 \ , z_2), \ldots (\ z_{n-1} \ , y \ ) \in R\}.$$

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:

$$M_{R^n} = \overbrace{M_R \odot M_R \odot \ \ldots\ldots \odot M_R}^{n \ veces}$$

Actividad 2.15

Si A = {1, 2, 3, 4} y sea R dada por la Figura 2.22

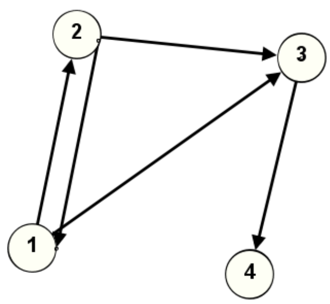


Fig. 2.22 . Digrafo de R.

Demostrar que los dígrafos de R^2, R^3 y R^4 son, respectivamente, los siguientes:

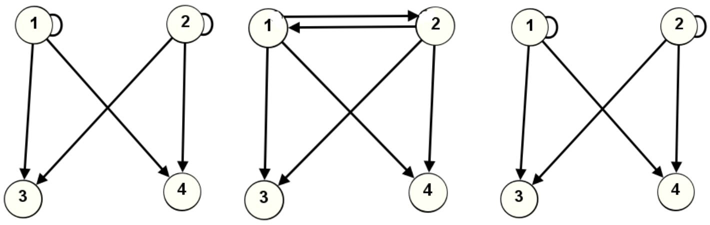


Fig. 2.23. Digrafos de R^2, R^3 y R^4.

2.15.2 Trayectorias en Digrafos

Definición

Sea $R: A \rightarrow A$. Llamamos trayectoria $x - y$ a la sucesión "x, z_1 , $z_2, \dots, z_{n-1}, y$" tal que $(x, z_1), (y_1, z_2), \dots (z_{n-1}, y) \in R$.

Se dice que es de longitud es n dado que los vértices x e y están conectados por medio de n aristas.

2.16 Propiedades de las Relaciones Binarias

En una relación $R : A \rightarrow A$, se pueden dar las siguientes propiedades:

2.16.1 Reflexividad

Definición

R se dice reflexiva si y solo si cada elemento de A está relacionado consigo mismo. Es decir,

$$R \text{ es reflexiva} \quad \Leftrightarrow \quad \forall\, x \in A\,,\ (x, x) \in R$$

De la definición se desprende que:

$$R \text{ no es reflexiva} \ \Leftrightarrow \quad \exists\, x \in A\,,\ (x, x) \notin R$$

Cuando se suceda que ningún elemento se relaciona consigo mismo se dirá arreflexiva. Esto es:

$$R \text{ es arreflexiva} \ \Leftrightarrow \forall x \in A\,,\ (x, x) \notin R$$

👁 **Observaciones**

- Esta propiedad se refleja en un dígrafo, cuando todos los vértices tienen lazos. Si algún elemento no tiene lazos no es reflexiva.
- La matriz de adyacencia de una relación reflexiva se caracteriza por tener todos los elementos de su diagonal principal iguales a uno. Es decir,

  R es reflexiva $\Leftrightarrow$ $m_{ii} = 1, \forall\, i$ y R no es reflexiva $\Leftrightarrow$ $\exists\, i: m_{ii} = 0$
- La matriz de adyacencia de una relación arreflexiva se caracteriza por tener todos los elementos de su diagonal principal iguales a cero. Es decir,

$$R \text{ es arreflexiva } \Leftrightarrow m_{ii} = 0, \forall\, i$$

2.16.2 Simetría

Definición

R es simétrica si y solo si cada vez que x está relacionado con y se cumple que y está relacionado con x. Es decir,

$$R \text{ es simétrica} \Leftrightarrow \forall x, y \in A,\ [\,(x, y) \in R \Rightarrow (y, x) \in R]$$

De la definición se desprende que:

$$R \text{ no es simétrica} \Leftrightarrow \exists\, x, y \in A \,/\, [\,(x, y) \in R \;\wedge\; (y, x) \notin R\,]$$

👁 **Observaciones**

- Si D es el dígrafo de una relación simétrica, entonces entre cada par de vértices distintos de D existen dos aristas con distintos sentidos, o no existe ninguna.
- Los lazos presentes en D cumplen la simetría.
- La matriz de adyacencia M_R de una relación simétrica es tal que todo par de elementos de ella colocados simétricamente respecto de la diagonal principal son iguales. Es decir R es simétrica si y solo si M_R es simétrica. Simbólicamente:

$$R \text{ es simétrica} \Leftrightarrow \forall\, i, j\,,\ m_{ij} = m_{ji}$$

$$R \text{ no es } \textit{simétrica} \Leftrightarrow \exists i, j \,/\, m_{ij} \neq m_{ji}$$

2.16.3 Asimetría

Definición

R se dice asimétrica si y solo 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

- Aplicando la ley lógica $p \to q \;\Leftrightarrow\; \neg p \vee q$, se puede expresar la asimetría del siguiente modo:

  $$R \text{ es asimétrica } \Leftrightarrow \forall x, y \in A,\; [\,(x, y) \notin R \vee (y, x) \notin R]$$

  Esta última dice que para darse cuenta de la asimetría se debe observar que entre cada par de vértices exista un único arco o ninguno.
- Los lazos no pueden existir en una relación asimétrica dado que

  $(x, x) \in R \Rightarrow (x, x) \notin R$ implica que $(x, x) \notin R$.
- Por todo lo dicho se desprende que la matriz de adyacencia M_R de una relación asimétrica es tal que

  $$(m_{ii} = 0\,,\; \forall\, i\,) \;\wedge\; (\,\forall\, i \neq j,\; m_{ij} = 0 \;\vee\; m_{ji} = 0\,)$$

  Esto es en la matriz de una relación asimétrica los elementos de la diagonal son todos ceros y en las posiciones simétricas respecto de la diagonal principal al menos un elemento es cero.

2.16.4 Antisimetría

Definición

R se dice antisimétrica si y solo si cada vez que un elemento x está relacionado con un elemento y e y está relacionado con x solo sea en el caso en que ambos elementos sean iguales. 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**

- Aplicando las leyes lógicas $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$ y $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$, se puede expresar esta definición del siguiente modo

  R es antisimétrica $\Leftrightarrow \forall\, x, y \in A$, $[\, x \neq y \implies (x, y) \notin R \;\vee\; (y, x) \notin R]$

  De esta última afirmación se desprende que para darse cuenta de la antisimetría de R dado su digrafo hay que observar a todos los pares de vértices distintos y corroborar que no exista un arco o ninguno.
- Los lazos pueden existir en una relación antisimétrica dado que

  $$(x, x) \in R \;\wedge\; (x,x) \in R \Rightarrow x = x$$
- La matriz de adyacencia M_R de una relación antisimétrica es tal que:

  $$(\,\exists\, i \,/\; m_{ii} = 1\,) \;\wedge\; (\,\forall\, i \neq j,\; m_{ij} = 0 \;\vee\; m_{ji} = 0\,)$$

  De esta última afirmación se deduce que la matriz de una relación antisimétrica es tal que en su diagonal todo es uno y en las posiciones simétricas respecto de la diagonal principal al menos un elemento es cero.

2.16.5 Transitividad

Definición

Se dice que una relación R definida en A, es transitiva si y solo si cada vez que un elemento cualquiera x está relacionado con un elemento y e y está relacionado con z, se cumple que x está relacionado con z.

Es decir,

R es transitiva $\Leftrightarrow \forall\, x,y,z \in A,\; [\,(x,y) \in R \;\wedge\; (y,z) \in R \Rightarrow (x,z) \in R\,]$

De la definición se desprende que

R no es transitiva $\Leftrightarrow \exists\, x,y,z \in A$ / $[\,(x,y) \in R \wedge (y,z) \in R \;\wedge (x,z) \notin R\,]$

También puede ocurrir que ninguna terna cumpla la transitividad, en cuyo caso:

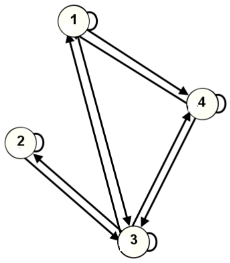
R es atransitiva $\Leftrightarrow \forall\, x,y,z \in A,\; [\,(x,y) \in R \;\wedge\; (y,z) \in R \Rightarrow (x,z) \notin R\,]$

👁 **Observaciones**

- El dígrafo de una relación transitiva es tal que si existe una trayectoria de longitud 2 entre x y z entonces debe existir la trayectoria de longitud 1 entre ellos, entendiendo que x y z son elementos cualesquiera de A.
- Es posible caracterizar la propiedad transitiva por medio de las matrices M_{R} y M_{R^2}. Como la relación R^2 representa a todas las trayectorias de longitud 2 presentes en R , se tendrá que R es transitiva si y solo si $M_{\mathrm{R}} \geq M_{R^2}$ dado que con esto se estaría exigiendo que haya una trayectoria de longitud 1 entre dos elementos entre los cuales hay una trayectoria de longitud 2.

Ejemplos 2.27

Sea R definida en A = {1, 2, 3, 4} cuyo digrafo es la Figura 2.24. Se observa que:



i) R es reflexiva, porque en todos los vértices hay lazos

ii) R es simétrica porque entre dos vértices distintos existen dos aristas con distintos sentidos, o ninguna.

iii) R no es transitiva porque (1,3)$\in R$ y (3,2) $\in R$ pero (1,2) $\notin R$.

Fig.2.24. Digrafo de R.

Actividad 2.16

Dadas las relaciones R_1, R_2 y R_3 mediante sus digrafos D_1,D_2 y D_3, determinar las propiedades que satisfacen cada una.

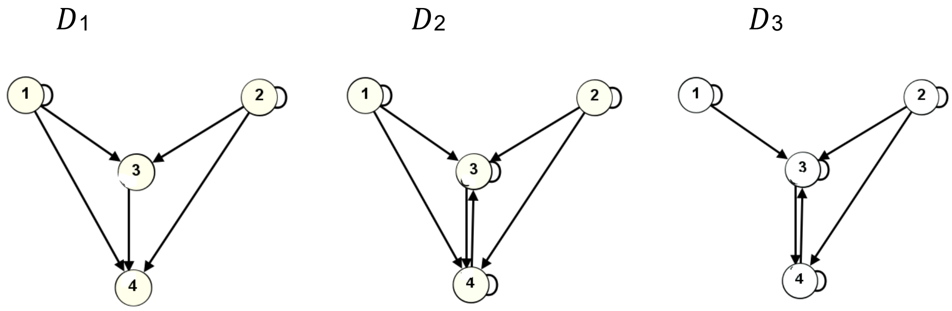


Fig.2.25. Digrafos de R_1 ,R_2 y R_3.

2.17 Relaciones de Equivalencia

Las relaciones de equivalencia 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.

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:

- Reflexividad: $\forall x \in A, (x, x) \in R$
- Simetría: $\forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$
- Transitividad: $\forall x, y, z \in A, (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

Ejemplo 2.28

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,

$$\forall x \ (x \in A \Rightarrow x \, R \, x), \text{ es decir, } R \text{ es reflexiva.}$$

ii) Simetría

En efecto, tomando todos los pares posibles:

(1, 2) $\in R$ y (2, 1) $\in R$

(3, 4) $\in R$ y (4, 3) $\in R$

Luego se cumple $[(x, y) \in R \Rightarrow (y, x) \in R] \ \forall \ x, y \in A$, por lo tanto R es simétrica.

iii) Transitividad

Se deben tomar todas las ternas posibles. En efecto,

(1, 1) $\in R$ y (1, 2) $\in R \Rightarrow$ (1, 2) $\in R$

(1, 2) $\in R$ y (2, 1) $\in R \Rightarrow$ (1, 1) $\in R$

(1, 2) $\in R$ y (2, 2) $\in R \Rightarrow$ (1, 2) $\in R$

(2, 1) $\in R$ y (1, 1) $\in R \Rightarrow$ (2, 1) $\in R$

(2, 1) $\in R$ y (1, 2) $\in R \Rightarrow$ (2, 2) $\in R$

(2, 2) $\in R$ y (2, 1) $\in R \Rightarrow$ (2, 1) $\in R$

(3, 4) $\in R$ y (4, 3) $\in R \Rightarrow$ (3, 3) $\in R$

(3, 4) $\in R$ y (4, 4) $\in R \Rightarrow$ (3, 4) $\in R$

(3, 3) $\in R$ y (3, 4) $\in R \Rightarrow$ (3, 4) $\in R$

(4, 3) $\in R$ y (3, 3) $\in R \Rightarrow$ (4, 3) $\in R$

(4, 3) $\in R$ y (3, 4) $\in R \Rightarrow$ (4, 4) $\in R$

(4, 4) $\in R$ y (4, 3) $\in R \Rightarrow$ (4, 3) $\in R$

Habiendo tomado todas las ternas posibles, se concluye que

$\forall\ x, y, z \in A$, $[(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R]$ y, por tanto, R es transitiva.

Como se demostró que R es reflexiva, simétrica y transitiva se concluye que R es una relación de equivalencia.

Nótese que si en lugar de analizar los pares ordenados se analiza la matriz, la tarea sería más liviana.

En efecto, siendo $M_{\mathrm{R}} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ se observa que

- Es reflexiva dado que todos los elementos de la diagonal son 1.
- Es simétrica dado que la matriz es simétrica.
- Es transitiva dado que

$$\boldsymbol{M}_{R^2} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

de donde se concluye que $M_{\mathrm{R}} \geq M_{R^2}$ cumpliéndose en este caso la igualdad.

Actividad 2.17

Demostrar que la relación R, definida en {1, 2, 3, 4, 5} y dada por el digrafo de la Figura 2.26 es de equivalencia

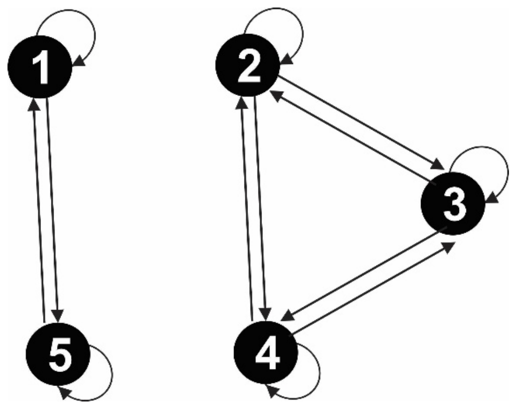


Fig.2.26. Digrafo de R.

Ejemplos 2.29

i) Si R = A x A entonces es una relación de equivalencia.

ii) Si R = ∅ entonces es una relación de equivalencia.

2.17.1 Clase de equivalencia de un elemento

Definición

Sea R una relación de equivalencia definida en A y sea $a \in A$. Se define clase de equivalencia de a al conjunto formado por todos los elementos relacionados con a y se denota $[a]$.

Simbólicamente $[a] = \{y \in A \ / \ (a, y) \in R\}$

Observaciones

- $[a] = R(a)$
- $[a] \neq \emptyset$ dado que por lo menos $(a, a) \in R$

Ejemplo 2.30

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 2.27 se observa su dígrafo, por lo tanto las clases de equivalencia de cada elemento son:

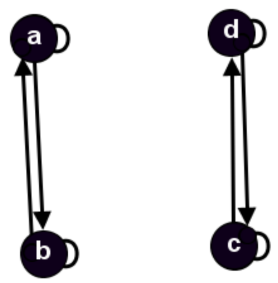


Fig.2.27. Digrafo $D = (A, R)$.

[a] = {a, b} ; [b] = {a, b} ; [c] = {c, d} ; [d] = {c, d}

Nótese que existen solo dos clases de equivalencias distintas y que la relación generó una partición en el conjunto.

Teorema

Sea R una relación de equivalencia en A y sean $a, b \in A$. Entonces se cumple que

$$(a, b) \in R \iff [a] = [b]$$

Es decir, si R es una relación de equivalencia en A entonces dos elementos estarán relacionados si y solo si sus clases de equivalencia son iguales.

2.17.2 Conjunto Cociente de una Relación de Equivalencia

Definición

Llamamos Conjunto Cociente al conjunto formado por todas las clases de equivalencia distintas generadas por la Relación de Equivalencia R en A.

Se denota A/R indicando así que el conjunto A quedó particionado por la relación de equivalencia R.

Ejemplo 2.31

En el Ejemplo 2.30, 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:

$$A/R = \{[a]\,;\,[c]\} = \{\{a, b\}\,;\,\{c, d\}\}$$

Teorema

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 2.32

Sea A = {1, 2, 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 que:

$$[1] = \{1, 2, 3\} \quad \text{y} \quad [4] = \{4\}$$

A partir de las definiciones de relación de equivalencia y de clase de equivalencia se puede ver que:

Como [1] = {1,2,3} entonces los pares (1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2) y (3,3) forman parte de R así como (4 , 4) dado que [4] = {4}

Por lo tanto

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 generada por la partición { {1, 2, 3} , {4} }.

Ejemplos 2.33

i) Para averiguar si la relación R dada por $M_{\mathrm{R}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ es una relación de equivalencia sobre el conjunto A = {a, b, c} se analizan sus propiedades:

- R es reflexiva ya que m_{ii} = 1 $\forall i$, cada elemento de la diagonal es 1

- R es simétrica ya que m_{ij} = m_{ji} $\forall\ i,j$, la matriz es simétrica

- R transitiva dado que $M_{R^2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = M_{\mathrm{R}}$ y por lo tanto se cumple que $M_{\mathrm{R}} \geq M_{R^2}$

Luego R es de equivalencia ya que se cumplen la reflexividad, la simetría y la transitividad, y A/R= { [a] , [b] }, donde [a] = {a} y [b] = {b ,c}.

ii) Si R está definida por la matriz $M_{\mathrm{R}} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ entonces R no es de equivalencia ya que no se cumple la simetría, m_{13} = 1 y m_{31} = 0.

Actividad 2.18

Encontrar el conjunto cociente de R definida en A = {1, 2, 3, 4, 5} de la Actividad 2.17. Realizar un diagrama de Venn de la partición generada.

2.18 Relaciones de Orden

Las nociones de orden son fundamentales tanto en matemáticas como en informática, ya que aparecen en temas de estructuras de datos, clasificación y búsqueda.

Se definen dos tipos de relaciones de orden: orden amplio y orden estricto. Cualesquiera sean los casos, una relación de orden permite ordenar los elementos de un conjunto, permite compararlos.

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:

- Reflexividad: $\forall x \in A, (x,x) \in R$

- Antisimetría: $\forall\, x,y \in A, [\, (x,y) \in R \;\wedge\; (y,x) \in R \Rightarrow x = y \,]$

- Transitividad: $\forall\, x,y,z \in A, [\, (x,y) \in R \;\wedge\; (y,z) \in R \Rightarrow (x,z) \in R \,]$

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:

- Arreflexividad: $\forall x \in A$, $(x,x) \notin R$

- Asimetría: $\forall\, x,y \in A$, $[\, (x,y) \in R \Rightarrow (y,x) \notin R \,]$

- Transitividad: $\forall\, x,y,z \in A$, $[\, (x,y) \in R \;\wedge\; (y,z) \in R \Rightarrow (x,z) \in R \,]$

Ejemplos 2.34

i) Relaciones de orden amplio, se tiene por ejemplo: el orden amplio ($\leq$) usual entre números reales, el orden alfabético de las palabras y la relación de inclusión ($\subseteq$) entre conjuntos.

ii) Relaciones de orden estricto, se tienen: el orden estricto ($<$) usual definido en los números reales, el orden cronológico lineal de los eventos; el orden definido por las magnitudes, por ejemplo ordenaciones por estatura, por longitud, por área, volumen, o cualquier otra magnitud.

iii) En A = {0, 1}, las siguientes relaciones son órdenes estrictos:

$R_0 = \emptyset$, R_1 = {(0, 1)} y R_2 = {(1, 0)}

Y las siguientes son órdenes amplios:

R_3 = {(0, 0), (1,1)} , R_4 = {(0, 0), (1,1)} (0, 1)} y R_5 = {(0, 0), (1,1)} (1, 0)}.

2.18.1 Conjunto Ordenado

Definición

Se denomina Conjunto Ordenado (CO) a todo par (A, R) formado por un conjunto $A \neq \emptyset$ y una relación de orden R definida en A.

Notación

Habitualmente se designan a las relaciones de orden amplio con el símbolo ≤ por analogía con el orden usual en los conjuntos numéricos.

Entonces el par $(A, \leq)$ es un CO y en lugar de "$x\ R\ y$" se escribirá "$x \leq y$".

Si "$x \leq y$" se dice que, "x precede a y" o que "x es menor o igual que y".

Si $(A, \leq)$ es un CO, se representa con " $\geq$ " a la relación inversa de "≤", y es tal que $(A, \geq)$ es también un CO y se dicen dual de (A, ≤).
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".

Ejemplos 2.35

Sea A = { a , b , c } y sea R definida en A como sigue

i) R = {(a, a), (b, b), (c, c), (a, c), (b, c)} entonces (A, R) es un CO donde R es una relación de orden amplio, porque se cumplen las propiedades de reflexividad, antisimetría y transitividad.

ii) R = { (b , a) , (b , c) } entonces (A , R) es un CO donde R es una relación de orden estricto, porque se cumplen las propiedades de arreflexividad, asimetría y transitividad.

Ejemplos 2.36

i) Sea A = {1, 2, 3, 4} y la relación R definida por su matriz

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Luego, R es:

- Reflexiva, en su diagonal todo es uno;
- Antisimétrica, en su diagonal todo es uno y en las posiciones simétricas respecto de la diagonal principal al menos un elemento es cero.
- Transitiva pues $M_R \geq M_{R^2}$. (Se deja para el estudiante la verificación)

Por lo tanto R es una relación de orden amplio y, observando la matriz podemos escribir que: 1 ≤ 1, 1 ≤ 2, 1 ≤ 3, 1 ≤ 4, 2 ≤ 2, 2 ≤ 3, 2 ≤ 4, 3 ≤ 3, 3 ≤ 4 y 4 ≤ 4.

ii) Sea $A = \{ a, b, c, d, e \}$ y sea R dada por su matriz

$$M_R = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Luego R es:

- Arreflexiva, todos los elementos de su diagonal son 0.
- Asimétrica, los elementos de la diagonal son todos ceros y en las posiciones simétricas respecto de la diagonal principal al menos un elemento es cero.
- Transitiva, se cumple que $M_R \geq M_{R^2}$ donde M_{R^2} es
-

$$M_{R^2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \odot \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Por lo tanto R es una relación de orden estricto y, observando la matriz, podemos escribir que $a < e$, $b < e$, $c < a$, $c < b$, $c < d$, $c < e$ y $d < e$.

Actividad 2.19

Sea la relación definida en A = {a, b, c, d , e , f } por el digrafo que se muestra, demostrar que (A , $\leq$) es un CO.

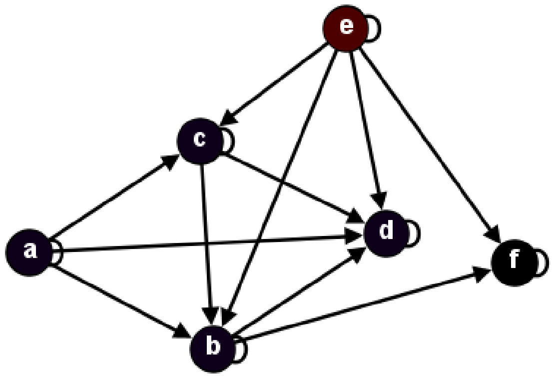


Fig.2.28. Dígrafo D = (A, $\leq$).

2.18.2 Elementos comparables

Definición

Sea (A, ≤) un CO, y sean x, $y \in A$

x e y se dicen comparables si y solo si $x \leq y$ o $y \leq x$

En caso contrario se dice que x e y son "no comparables".

2.18.3 Orden Parcial y Total

Definición

Un Orden se dice que es Total (o Lineal) cuando todos los elementos del conjunto sobre el que está definido son comparables por dicha relación. En caso contrario, si existen elementos no comparables, se dice que el orden es parcial.

Así pues, dado (A, ≤) un CO, se dice que:

" ≤ " es un orden total $\Leftrightarrow$ $\forall\, x, y \in A$, $x \leq y \ \vee\ y \leq x$

" ≤ " es un orden parcial $\Leftrightarrow$ $\exists\, x, y \in A$, $x \nleq y \wedge\ y \nleq x$

Si la relación de orden es lineal o total, se dice que A es una cadena.

Actividad 2.20

Determinar si el CO de la Actividad 2.19 es un orden parcial o total.

2.18.4 Diagrama de Hasse

Definición

Se denomina Diagrama de Hasse a una gráfica que se realiza simplificando el digrafo de las relaciones de orden mediante el siguiente procedimiento:

Paso 1. Se eliminan los lazos o bucles, si el orden es amplio. Si el orden es estricto se pasa directamente al paso 2.

Paso 2. Se eliminan las aristas que son consecuencias de la transitividad.

Paso 3. Se orientan las aristas que quedan hacia arriba e incluso se puede eliminar las orientaciones de las flechas.

Ejemplos 2.37

i) Sea $(A, \leq_1)$ un CO y tal que $A = \{a, b, c, d\}$ con la relación de orden amplio $\leq_1$ dada por:

$a \leq_1 a$, $a \leq_1 b$, $a \leq_1 c$, $a \leq_1 d$, $b \leq_1 b$, $c \leq_1 b$, $b \leq_1 d$, $c \leq_1 c$, $c \leq_1 d$, $d \leq_1 d$.

Entonces su diagrama de Hasse es

Fig.2.29. Diagrama de Hasse de $(A, \leq_1)$.

ii) Sea $(A, \leq_2)$ un CO, tal que $A = \{a, b, c, d, e\}$ y la relación de orden amplio $\leq_2$ 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 y a partir de ellos detectar cuales 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:

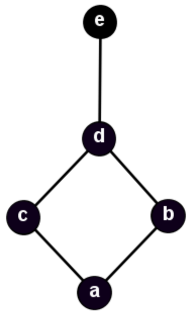


Fig.2.30. Diagrama de Hasse de (A, $\leq_2$).

iii) En el conjunto A= {a, b, c} se define la relación de orden mediante su matriz:

$$M_{\mathrm{R}} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Nótese que la relación de orden es estricta y total, Luego el diagrama de Hasse es:

Fig.2.31. Diagrama de Hasse de (A, R).

Actividad 2.21

Encontrar el diagrama de Hasse de la Actividad 2.20.

2.18.5 Elementos extremos de una Relación de Orden

Definiciones

Sea (A , $\leq$) un CO donde $\leq$ es un orden amplio . Sean a y b elementos de A.

- Se dice que a es el elemento máximo de A si y solo sí $x \leq a$, $\forall x \in A$.
- Se dice que b es el elemento mínimo de A si y solo sí $b \leq x$, $\forall x \in A$.

Sea (A , <) un CO donde < es un orden estricto. Sean a y b elementos de A.

- Se dice que a es el elemento máximo de A si y solo sí $x < a$, $\forall x \in A$.
- Se dice que b es el elemento mínimo de A si y solo sí $b < x$, $\forall x \in A$.

Ejemplos 2.38

i) En los diagramas de Hasse del Ejemplo 2.37

'a' es el máximo y 'd' el elemento mínimo en la Figura 2.29

'e' es el elemento máximo y 'a' es el mínimo en la Figura 2.30

'b' es el elemento máximo y 'a' es el mínimo en la Figura 2.31

iii) Sea la relación de orden amplio sobre el conjunto { a , b , c , d , e } representada por el Diagrama de Hasse de la Figura 2.32

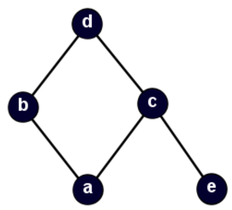


Fig.2.32. Diagrama de Hasse de Actividad 2.21.

El elemento “d” es el máximo, pues todos los elementos preceden a “d”, pero no existe elemento mínimo, ya que no hay un elemento menor a todos; observar que los elementos “a” y “e” no son comparables.

Actividad 2.22

Dadas las siguientes relaciones $\leq_1$ y $\leq_2$ definidas en A = {1, 2, 3, 4, 5} por medio de los digrafos de las Figuras 2.33 y 2.34, 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.

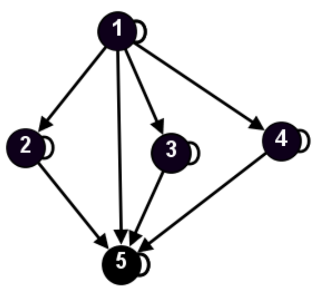


Fig. 2.33. Digrafo de (A, $\leq_1$).

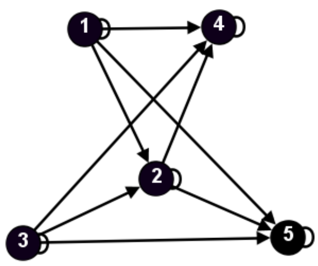


Fig. 2.34. Digrafo de (A, $\leq_2$).

Capítulo 3. TEORIA DE NUMEROS ENTEROS

El conjunto de los Números Enteros.

División en $\mathbb{Z}$.

Divisibilidad: Divisores y Múltiplos.

Números Primos y Compuestos.

Máximo Común Divisor.

Números Coprimos o Primos relativos.

Mínimo Común Múltiplo.

Ecuaciones diofánticas.

Relación de Congruencia en $\mathbb{Z}$.

Introducción

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 solo en $\mathbb{Z}$, 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.

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-x \ / \ x \in \mathbb{N}\}$$

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Con $\mathbb{Z}^+$ se representa al conjunto de los enteros positivos, que son los números naturales; esto es: $\mathbb{Z}^+ = \{1, 2, 3, \ldots\} = \mathbb{N}$

Observación

El número entero 0 no tiene signo, no es ni positivo ni negativo.

El conjunto $\mathbb{Z}$ goza de muchas propiedades que se pueden clasificar en dos categorías:

- 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: ‘·’ las cuales cumplen las siguientes propiedades

1.	$\forall x, y \in \mathbb{Z}$, $x + y \in \mathbb{Z}$	$\forall x, y \in \mathbb{Z}$, $x \cdot y \in \mathbb{Z}$	Leyes de composición internas.
2.	$\forall x, y, z \in \mathbb{Z}$, $(x + y) + z = x + (y + z)$	$\forall x, y, z \in \mathbb{Z}$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$	Leyes asociativas
3.	$\forall x, y \in \mathbb{Z}$, $x + y = y + x$	$\forall x, y \in \mathbb{Z}$, $x \cdot y = y \cdot x$	Leyes conmutativas
4.	$\exists\ 0 \in \mathbb{Z} / \forall x \in \mathbb{Z}$, $x + 0 = 0 + x = x$	$\exists\ 1 \in \mathbb{Z} / \forall x \in \mathbb{Z}$, $x \cdot 1 = 1 \cdot x = x$	Leyes de existencia del neutro aditivo '0' y multiplicativo '1'.
5.	$\forall x \in \mathbb{Z}, \exists (-x) \in \mathbb{Z} \,/\, x + (-x) = (-x) + x = 0$		Ley de existencia del opuesto
6.	$\forall x, y, z \in \mathbb{Z}$, $x.(y + z) = x.y + x.z$	$\forall x, y, z \in \mathbb{Z}$, $(y + z) \cdot x = y \cdot x + z \cdot x$	Ley distributiva de la multiplicación respecto de la adición
7.	$\forall x, y, z \in \mathbb{Z}$, $\text{Si } x \neq 0 \ \wedge\ x \cdot y = x \cdot z, \text{ entonces } y = z$		Ley cancelativa

Tabla 3.1. Propiedades de la adición y multiplicación

Se dice que las operaciones adición: '+' y multiplicación '·' son cerradas en $\mathbb{Z}$

La relación de orden en $\mathbb{Z}$

Definición

Sean x, y $\in \mathbb{Z}$, $x \leq y$ si y solo si $\exists\ k \in \mathbb{N}_0 \,/\, y = x + k$

La relación '≤' es una relación de orden amplio en $\mathbb{Z}$ ya que es:

1. Reflexiva: $x \leq x\ ,\ \forall x \in \mathbb{Z}$
2. Antisimétrica: $x \leq y\ \wedge\ y \leq x \Rightarrow x = z,\ \forall x, y \in \mathbb{Z}$
3. Transitiva: $x \leq y\ \wedge\ y \leq z \Rightarrow x \leq z,\ \forall x, y, z \in \mathbb{Z}$

Además, se cumplen estas otras propiedades:

4. Si $x \leq y \wedge z \in \mathbb{Z}$, entonces $x + z \leq y + z$, $\forall x, y \in \mathbb{Z}$
5. Si $x \leq y$ entonces

i) Si $z \geq 0, \quad x.z \leq y.z$, $\forall x, y \in \mathbb{Z}$

ii) Si $z \leq 0, \quad x.z \geq y.z$, $\forall x, y \in \mathbb{Z}$

que no sólo se verifican en $\mathbb{Z}$, sino también se cumplen en $\mathbb{Q}$ y en $\mathbb{R}$. 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 $X \subset \mathbb{Z}$. Se dice que $c \in \mathbb{Z}$ es una cota inferior del conjunto X si $c \leq x, \forall x \in X$.

Luego se dice que X es un conjunto acotado inferiormente si tiene al menos una cota inferior..

Si además $c \in X$, entonces se dice que c es el primer elemento(o mínimo) de X.

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 tiene al menos una cota superior.

Si además $d \in X$, entonces se dice que d es el último elemento (o máximo) de X

Ejemplos 3.1

i) El conjunto {-17, -15, -5, 5, 15, 19, 100} tiene cotas inferiores y superiores. Así -20, -22, -30 son cotas inferiores, pero -17 es la mayor de las cotas inferiores y como pertenece al conjunto diremos que -17 es el elemento mínimo.

Cotas superiores del conjunto dado podrían ser: 100, 101, 102,…, 170,.., pero 100 es la mínima cota superior y pertenece al conjunto, luego el elemento máximo de este conjunto es 100.

ii) El conjunto de los enteros negativos $\mathbb{Z}^-$ no tienen cotas inferiores; y $\mathbb{Z}^+$ no tienen cotas superiores.

iv) El conjunto de números racionales $\{1/n \ ; \ n \in \mathbb{N}\} \subseteq \mathbb{Q}$ tiene cotas inferiores pero no tiene mínimo. Observar que 0 es la mayor cota inferior, pero no está en el conjunto, luego el conjunto no tiene primer elemento o mínimo.

Principio del Buen Orden

"Todo subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente (o superiormente) posee un primer (o último) elemento"

Lo relevante del Principio del Buen Orden no es sólo el hecho que distingue al conjunto $\mathbb{Z}$ de otros conjuntos numéricos, sino que resulta de gran utilidad desde el punto de vista matemático. Este principio es la base para el método de demostración por Inducción que se verá más adelante.

3.2 División en $\mathbb{Z}$

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, existen q , $r \in \mathbb{Z}$, únicos, tales que:

$$a = b.q + r \quad \text{con} \quad 0 \leq r < |b|.$$

A los números a, b, q y r se les suele llamar, respectivamente, dividendo, divisor, cociente y resto.

Ejemplos 3.2

- **i)** Para $a = 25$ y $b = 3$, se tiene que $25 = 3 \cdot 8 + 1$, entonces el cociente es 8 y el resto es 1, cumpliéndose la condición $0 \leq 1 < |3|$.
- **ii)** Para $a = 3$ y $b = 25$, se tiene que $3 = 25 \cdot 0 + 3$, entonces el cociente es 0 y el resto es 3, cumpliéndose la condición $0 \leq 3 < |25|$.
- **iii)** Para $a = -25$ y $b = 3$, se tiene que $-25 = 3 \cdot (-9) + 2$, entonces el cociente es (-9) y el resto es 2, cumpliéndose la condición $0 \leq 2 < |3|$.
- **iv)** Para $a = 61$ y $b = -7$, se tiene que $61 = (-7) \cdot (-8) + 5$, entonces el cociente es (-8) y el resto es 5, cumpliéndose la condición $0 \leq 5 < |-7|$.
- **v)** Para $a = -21$ y $b = -15$, se tiene que $-21 = (-15) \cdot 2 + 9$, entonces el cociente es 2 y el resto es 9 cumpliéndose la condición $0 \leq 9 < |-15|$.

3.2.1 Operadores binarios div y mod

div y mod son dos operadores matemáticos, usados en Programación, son parte de la división de dos números enteros pues permiten tomar el residuo (o resto) y el cociente.

El operador div

📚 Definición

Sean $a, b\ \in\ \mathbb{Z}$, b ≠ 0, "$a\ div\ b$" es el cociente que se obtiene de dividir a en b.

🗒 Ejemplos 3.3

i) $4\ div\ 2\ =\ 2$; ii) $(-4)\ div\ 2\ =\ -2$;

iii) $79\ div\ 8\ =\ 9$; iv) $3\ div\ 6\ =\ 0$.

El operador mod

📚 Definición

Sean $a, b\ \in \mathbb{Z}$, b ≠ 0, "$a\ mod\ b$" es el resto de la división de a en b.

🗒 Ejemplos 3.4

1) Tomando los mismos valores del Ejemplo 3.3 se tiene que:
$4\ mod\ 2\ =\ 0$, $(-4)\ mod\ 2\ =\ 0$, $79\ mod\ 8\ =\ 7$ y $3\ mod\ 6\ =\ 3$

2) Evaluar $(x+y) mod\ 7 + (3 * x)\ div\ y$ sabiendo que $x = 7$ e $y = 11$

Reemplazando los valores:

$(7+11)\ mod\ 7 + (3*7)\ div\ 1 =\ 18\ mod\ 7\ +\ 21\ div\ 11 =\ 4\ +\ 1\ =\ 5$

El valor de la expresión dada es 5.

👁Observación

De la definición del operador mod se desprende que, $\forall x\ \in\ \mathbb{Z}$ se cumple que

x es par si y solo si $x\ mod\ 2\ =\ 0$

x es impar si y solo si $x\ mod\ 2\ =\ 1$

🛠 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

Se desea hacer un programa que tome un número de tres cifras e indique cuantas unidades, decenas y centenas posee.

Para el número 785, el programa tiene que devolver 7 centenas, 8 decenas y 5 unidades como resultado. Si se aplican los operadores div (DIV) y mod (MOD) se puede hacer el siguiente análisis:

- De $785\ mod\ 10 = 5$ se obtiene la cantidad de unidades.
- De $(785\ div\ 10) mod\ 10 = 8$ se obtiene las decenas.
- Finalmente, de $(785\ div\ 10) div\ 10 = 7$ se obtiene las centenas.

A continuación se muestra el algoritmo en PSeint para el cálculo de unidades, decenas y centenas de un número de tres cifras y su correspondiente diagrama de flujo en la Figura 3.1. En este lenguaje existe la función MOD, pero no existe la función DIV. En su reemplazo se tiene la función TRUNC que devuelve la parte entera del cociente.

```
// Descomposición de un Número de tres cifras en unidades, decenas y centenas
Algoritmo UDC
        Escribir 'Ingresar un número de tres cifras'
        Leer N
        Si N>99 Y N<1000 Entonces
                uni <- N MOD 10
                N <- TRUNC(N/10)
                dec <- N MOD 10
                N <- TRUNC(N/10)
                cen <- N MOD 10
                Escribir 'Las unidades del número ingresado son: ',uni
                Escribir 'Las decenas del número ingresado son: ',dec
```

Escribir 'Las centenas del número ingresado son: ',cen

SiNo

Escribir 'Número ingresado incorrecto'

FinSi

FinAlgoritmo

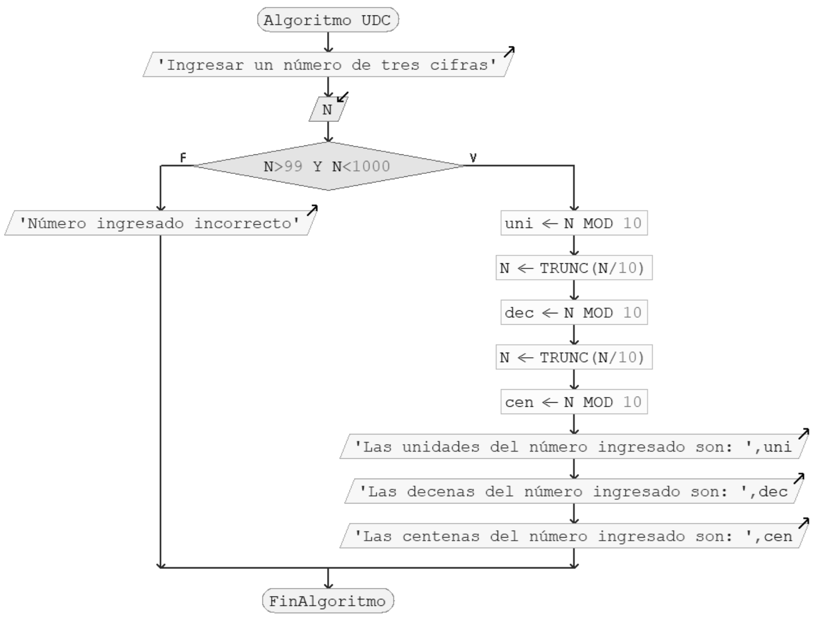


Fig. 3.1. Descomposición de un Número.

Actividad 3.1

i) Decir Verdadero o Falso, y justificar la respuesta:

$a)(-25)\ div\ 5\ =\ -5$ y $(-25)\ mod\ 5\ =\ 0$

$b)(-735)\ div\ (-31)\ =\ 24$ y $(-735)\ mod\ (-31)\ =\ 9$

ii) Si $a = 3,\ b = 10, y\ c = 5$, evaluar $(c^a)\ mod\ 9\ +\ (b\ +\ 2^{a-1})/((7 * c)\ mod\ a)$

3.3 Divisibilidad: Divisores y Múltiplos

La divisibilidad es la base de la Teoría de Números Enteros la cual es una sólida estructura desarrollada por los matemáticos desde la antigüedad, cuya fuerza radica en la facilidad con la que plantea problemas de todo tipo de complejidad.

El concepto de divisibilidad se basa en las **divisiones exactas**, aquellas cuyo **resto es cero**. Por ejemplo la división de 6 en 3 es exacta ya que $6 \; mod \; 3 = 0$.

📚 **Definición**

Sean $a, b \in \mathbb{Z} \; con \; a \neq 0$ se dice que "$a \; divide \; b$" y se denota $a|b$ si existe un entero n tal que $b = a.n$.

Simbólicamente: $a|b \;\; \Leftrightarrow \;\; \exists n \in \mathbb{Z} \; tal \; que \; b = a.n$

Otras formas de decir que "$a \; divide \; b$" son:

"a es un factor de b" , *"a es un divisor de b"* , *"b es múltiplo de a"* o *"b es divisible por a"*

De la definición se desprende que:

$$a \nmid b \quad \Leftrightarrow \neg \exists n \in \mathbb{Z} \; tal \; que \; b = a.n$$

👁 **Observación**

- Sean $x, y \; z \in \mathbb{Z} - \{0\}$, del producto '$x.y = z$', se pueden observar dos divisiones exactas '$z \; mod \; x$' = 0 bien '$z \; mod \; y$' =0 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 entero es múltiplo de sí mismo y de la unidad (1).
- Todo número entero tiene infinitos múltiplos, excepto el 0, que tiene sólo uno (él mismo).
- 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 $2 \in \mathbb{Z}$ tal que $6 = 3.2$

Se dice que 3 divide a 6 o que 6 es múltiplo de 3. Observe que también 2 divide a 6 y 6 es múltiplo de 2

ii) $(-4)\,|12$ pues existe $(-3) \in \mathbb{Z}$ tal que $12 = (-4).(-3)$.

Se dice que (-4) es divisor de 12 y que 12 es múltiplo de (-4). También (-3) es divisor de 12 y 12 es múltiplo de (-3).

iii) $5|(-35)$ pues existe $(-7) \in \mathbb{Z}$ tal que $(-35) = 5.(-7)$. Por lo tanto se tiene que (-35) es múltiplo de 5 y de (-7), y 5 y (-7) son divisores de (-35)

iv) Para demostrar que $n^2 + 3n$ es divisible por 2, basta ver que $n^2 + 3n$ se puede factorizar como $n^2 + 3n = n(n+3)$.

Analizando la expresión factoreada se tiene que: Si n es par, entonces el número resultante es divisible por 2. Si n es impar, entonces $n + 3$ es 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 $0 = a.0$. De lo que se deduce que todo entero no nulo es divisor de cero.
- Un entero a no nulo es un divisor propio de 0 si existe un entero n no nulo tal que 0 = a.n.
- En Z, el elemento 0 no tiene divisores propios pues 0 = a.n si y solo si a = 0 o n = 0.

Algoritmo para determinar si un número divide a otro en lenguaje de Pseint

```
Algoritmo Divisibilidad
        Escribir ("Para determinar si a1b");
        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
```

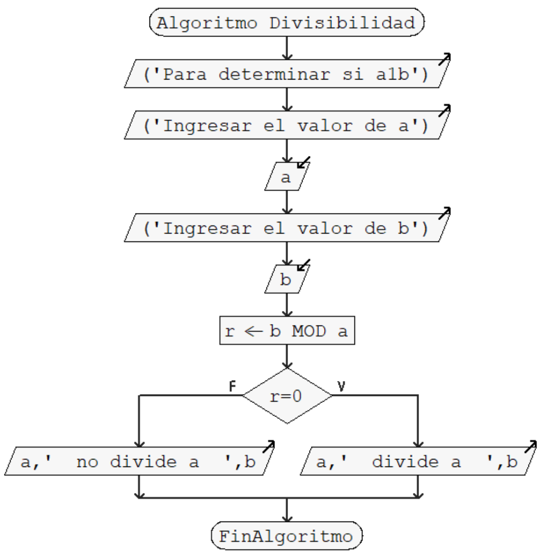


Fig. 3.2. Algoritmo de Divisibilidad.

3.3.1 Propiedades de la divisibilidad

1. Todo número entero a no nulo $(a \in \mathbb{Z} - \{0\})$ posee al menos los siguientes divisores: $1, -1, a, -a$.

Demostración: $Sea\ a \in \mathbb{Z} - \{0\}$,

- $1|a$ pues $\exists\ a \in \mathbb{Z} / a = 1.a$
- $(-1)|a$ pues $\exists\ (-a) \in \mathbb{Z} / a = (-a)(-1)$
- $a|a$ pues $\exists\ 1 \in \mathbb{Z} / a = a.1$
- $(-a)|a$ pues $\exists\ (-1) \in \mathbb{Z} / a = (-a)(-1)$

2. $Si\ a|b \wedge b|a \Rightarrow a = \pm b,\ \forall a, b \in \mathbb{Z} - \{0\}$

Demostración: Sean $a, b \in \mathbb{Z} - \{0\}$, por hipótesis:

$a|b$ entonces $\exists\ k_1 \in \mathbb{Z} / b = a.k_1$ (1)

$b|a$ entonces $\exists\ k_2 \in \mathbb{Z} / a = b.k_2$ (2)

Sustituyendo (1) en (2) se tiene $a = (a.k_1).k_2 \Rightarrow a = a.(k_1.k_2)$, para que esta igualdad se cumpla debe ocurrir que $(k_1.k_2) = 1$ y como $k_1, k_2 \in Z$ 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 $a = \pm b$

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 $a = b$.

3. $Si\ a, b \in \mathbb{Z} - \{0\}\ ,\ a|b \wedge b|c \Rightarrow a\,|c$

Demostración: Por hipótesis, se tiene que:

- $a|b$ entonces $b = a.k_1$, para algún $k_1 \in \mathbb{Z}$ (1)
- $b|c$ entonces $c = b.k_2$, para algún $k_2 \in \mathbb{Z}$ (2)

Si se reemplaza (1) en (2), se tiene que: $c = (a.k_1).k_2 \Rightarrow c = a.(k_1.k_2)$

Como $(k_1.k_2) \in \mathbb{Z}$, se tiene que $k_1.k_2 = k$, con $k \in \mathbb{Z}$ tal que $c = a.k$, luego se concluye que $a|c$.

4. Si $a|b \implies a|(b.x)$, $\forall\ a,\ b,\ x \in \mathbb{Z}$ y $a\ \neq 0$.

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 $b = a.k$ (3), para algún $k \in \mathbb{Z}$

Multiplicando miembro a miembro (3) por x se tendrá: $b.x = (a.k).x$

Como el producto es asociativo se puede escribir: $b.x = a.(k.x)$

Al ser $(k.x) \in \mathbb{Z}$ se concluye que $a|\ (b.x)$

5. Si $a|b$ y $a|c \implies a|(b.x + c.y)$, $\forall\ a, b, c, x\ , y \in \mathbb{Z}$ y $a \neq 0$.

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,

$a|(b.x), \forall x \in \mathbb{Z} \Rightarrow b.x = a.k_1$, para algún $k_1 \in \mathbb{Z}$ (1)

Análogamente, $a|c$, luego por la propiedad,

$a|(c.y), \forall y \in \mathbb{Z} \Rightarrow cy = a.k_2$, para algún $k_2 \in \mathbb{Z}$ (2)

Se desea determinar un entero k tal que $b.x + c.y = a.k$, para ello sumando (1) y (2), miembro a miembro, se tiene: $b.x + c.y = a.k_1 + a.k_2$ (3)

Sacando factor común en (3) $b.x + c.y = a.(k_1 + k_2)$ y como $k_1 + k_2 = k \in \mathbb{Z}$ se concluye que: $a|(b.x + c.y), \forall x, y \in \mathbb{Z}$

Como casos particulares de esta propiedad tenemos que:

- Cuando $x = 1$ e $y = -1$, se tendrá que si $a|b$ y $a|c \implies a|(b - c)$
- Cuando $x = -1$ e $y = 1$, se tendrá que si $a|b$ y $a|c \implies a|(-b + c)$
- Cuando $x = -1$ e $y = -1$, se tendrá que si $a|b$ y $a|c \implies a|(-b - c)$

Actividad 3.2

Indicar si las siguientes afirmaciones son Verdaderas o Falsas, justificando su respuesta:

i) $(-3)|33 \;\wedge\; 33|11$

ii) $a|6 \wedge 6|a \;\rightarrow\; a = 6,\quad$ con $a \in \mathbb{Z}$ y $a \neq 0$

iii) $a|b \wedge c|b \;\rightarrow\; (a.c)|b$, con $a, b, c \in \mathbb{Z}$ y $a, c \neq 0$

iv) $3|(6x - 9y)$, $\forall x, y \in \mathbb{Z}$

v) $8|(16x - 4y)$, $\forall x, y \in \mathbb{Z}$

vi) $\exists\, x, y \in \mathbb{Z}$ tales que $2x + 5y = 1$

vii) $\exists\, x, y, z \in \mathbb{Z}$ 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 positivos son 1 y p.

Todos los demás enteros positivos mayores que 1 que no son primos se llaman compuestos.

Los primeros veinte números primos son:

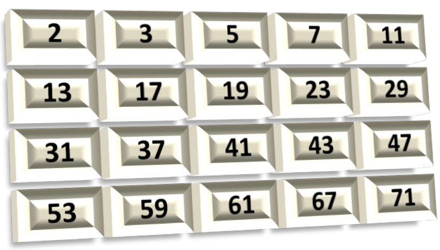


Fig. 3.3. Primeros Números Primos.

Observaciones

- La definición de un número primo se puede extender a los enteros de la siguiente manera: "Un entero p es un número primo si tiene exactamente cuatro divisores: ± 1 y $\pm p$.

- 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. También sirven para asentar las bases de cualquier número, pues sin ellos no se puede elaborar algoritmos y cálculos complejos.

Los números primos muy grandes se obtienen con el algoritmo que busca los números primos de Mersenne (primos que se los escribe como una potencia de dos menos uno), éstos son útiles porque se pueden emplear para codificar cualquier tipo de información de manera segura. Lo utilizan los bancos en los números de seguridad, las transferencias bancarias y otras operaciones.

Teorema: El legado de Euclides

"Existen infinitos números primos"

Demostración:

Supongamos por el contrario que hay una cantidad finita de primos, los cuales ordenados de menor a mayor quedan representados asi: $p_1, p_2, \dots, p_t$.

Sea el número $q = p_1 . p_2 \dots p_t + 1$

- Se observa que q es mayor que el último primo, por lo tanto q es compuesto.
- Además q es tal que da resto 1 al dividirlo por todos los primos. Se tiene pues que q no posee divisores primos y por lo tanto no es compuesto.
- Contradicción!!. Luego existen infinitos primos.

Actividad 3.3

a) Dar al menos un primo que divida 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:

$$n = p_1^{a_1}.p_2^{a_2} \dots p_k^{a_k}.$$

donde los p_i son números primos distintos tal que $p_1 < p_2 < \dots < p_k$ y los $a_i \in \mathbb{Z}^+$

Ejemplos 3.7

La descomposición en factores primos de 30, 64 y 48 es:

$30 = 2.3.5 \qquad 64 = 2^6 \qquad 48 = 2^4.3$

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) Sean a, b enteros y p$\in \mathbb{Z}^+$. Si p es primo y $p|(a.b)$ entonces $p|a \;\; o \;\; p|b$

Demostraciones:

a) Se supone por el contrario, que existe un número n compuesto que no tiene divisores primos. Se define al conjunto de estos números: $S = \{n \in \mathbb{Z}^+ + / \; n$ es un número compuesto y no tiene divisores primos}. Por lo dicho anteriormente $S \neq \varnothing$ 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 '$m = m_1.m_2$', 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 $p|m$ y esto contradice la suposición. Luego $S = \varnothing$ y se concluye que todo número compuesto admite al menos un divisor que es un número primo.

b) Por el Teorema Fundamental de la Aritmética (TFA), como a y b son enteros entonces pueden escribirse como una descomposición única de factores primos.

$$a = \alpha_1^{s_1}.\alpha_2^{s_2}\dots.\alpha_s^{s_s} \quad y \quad b = \beta_1^{r_1}.\beta_2^{r_2}\dots.\beta_r^{r_r}.$$

Entonces sean:

$$a = \alpha_1^{s_1}.\alpha_2^{s_2} \dots \alpha_i^{s_i} \qquad \text{y} \qquad b = \beta_1^{t_1}.\beta_2^{t_2} \dots .\beta_j^{t_j}$$

Por hipótesis $p|(a.b) \quad \Longrightarrow \quad \exists n \in Z \;\; ; \;\; a.b = p.n$ por lo tanto

$$a.b = \alpha_1^{s_1}.\alpha_2^{s_2} \dots \alpha_i^{s_i}.\beta_1^{t_1}.\beta_2^{t_2} \dots .\beta_j^{t_j} = p.n \qquad ,$$

Análogamente como n es un entero cumple con el Teorema Fundamental del Aritmética se puede escribir:

$$a.b = \alpha_1^{s_1}.\alpha_2^{s_2} \dots \alpha_i^{s_i}.\beta_1^{t_1}.\beta_2^{t_2} \dots .\beta_j^{t_j} = p.\eta_1^{u_1}.\eta_2^{u_2} \dots .\eta_k^{u_k}$$

Como estas dos descomposiciones tienen que ser las mismas, entonces los factores deben ser los mismos. Si suponemos que cada factor de la descomposición de a y de b son distintos de p, luego el factor p está en una descomposición y no en la otra, y esto contradeciría al Teorema Fundamental del Algebra. Por lo tanto necesariamente debe existir algún α_i o β_j tal que $\alpha_i = p$ o $\beta_j = p$ de donde se concluye que $p|a$ o $p|b$

Ejemplo 3.8

La afirmación "$Si\ n \mid (a \cdot b) \Rightarrow \ n|a \vee n|b \ , \ \forall n, a, b \in \mathbb{Z}$" es Falsa pues por ejemplo $8|(4 \cdot 10)$ pero no es cierto que $(8|4 \vee 8|10)$.

Algoritmo para la determinación de números primos

Sea n entero mayor que 1, n es primo si ningún primo p tal que $p^2 \leq n$, lo divide.

Paso 1: Verificar si n es 2. Si lo es, n es primo. Caso contrario, seguir con el paso 2.

Paso 2: Verificar si 2 | n. Si es verdadero, n no es primo; de lo contrario, prosiga al paso 3.

Paso 3: Calcular el mayor entero k^2 menor a n. Luego siga con el paso 4.

Paso 4: Verificar si $p \mid n$, donde p es cualquier número primo, tal que 2 < $p \leq k$. Si algún p es tal que $p \mid n$, entonces n no es primo; de lo contrario, n es primo.

🗒 Ejemplos 3.9

Para determinar si 113 es primo, se aplica el algoritmo:

1) 113 no es 2
2) 113 no es par
3) El mayor entero k tal que $k^2 < 113$ es $k=10$
4) Considerando todos los primos p tales que $2 < p \leq 10$
    i) Para $p = 3$, se tiene que 3 no divide a 113
    ii) Para $p = 5$, se tiene que 5 no divide a 113
    iii) Para $p = 7$, 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 nùmero 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
    FinSi
FinProceso
```

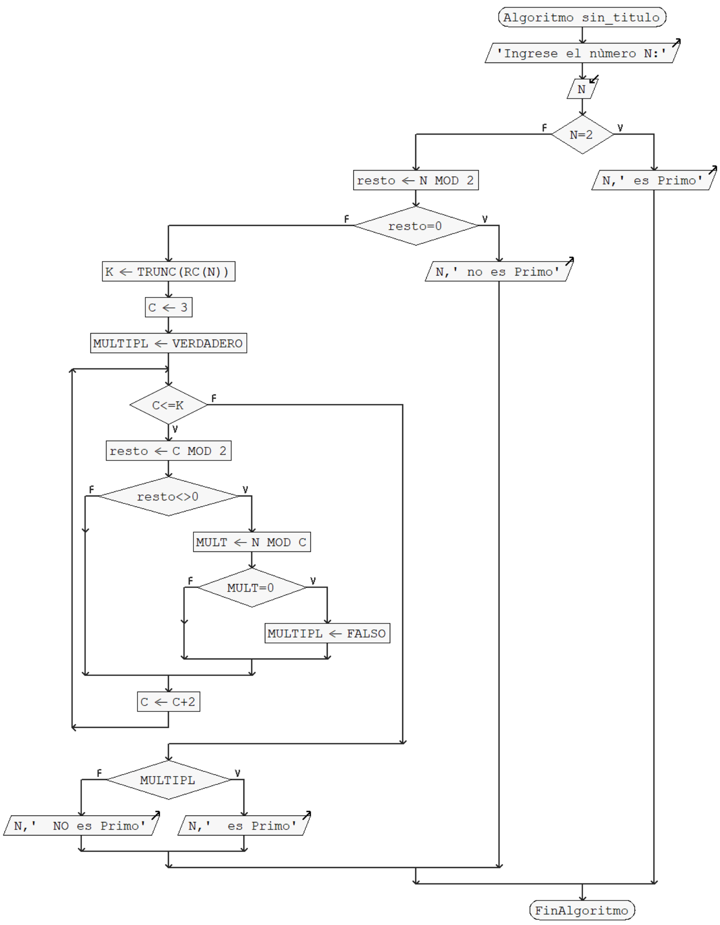


Fig. 3.4. Algoritmo Números Primos.

Actividad 3.4

a) Determinar si los siguientes números son primos: 2317 y 2437.

b) En caso de que alguno de los números del apartado anterior 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 $d \in Z^+$ es el máximo común divisor de a y b, y se denota $d = mcd\,(a, b)$, si y sólo si:

1) $d|a \quad \wedge \quad d|b$ (se lee d es divisor común de $a\ y\ b$)

2) $\forall\ c \in \mathbb{Z}\,,\ c|a \quad \wedge \quad c|b \ \Rightarrow\ c|d$ (d es el mayor común divisor de $a\ y\ b$.)

Observaciones

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 mayor entero positivo del conjunto $D_a \cap D_b$.

Ejemplos 3.10

i) $mcd(12\,,30) \;=\; 6$, pues $D_{12} = \{1, 2, 3, 4, 6, 12\}$ y $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$, $D_{12} \cap D_{30} = \{1, 2, 3, 6\}$, luego $6 = mcd(12{,}30)$

ii) $mcd(13\,,15) = 1$, pues $D_{13} = \{1, 13\}$ y $D_{15} = \{1, 15\}$, y $D_{13} \cap D_{15} = \{1\}$, luego $mcd(13{,}15) = 1$.

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) $mcd\ (a\ ,b) = \ mcd\ (|a|, |b|)$

v) $mcd\ (a\ , k.a)\ = \ |a|\ ,\ \ \forall k \in Z$

vi) $mcd\ (a\ ,b)\ = \ mcd\ (b\ ,r)\ \ siendo\ r\ = \ a\ mod\ b$

Demostraciones:

i) $mcd\ (a\ ,b)\ = \ mcd\ (b, a)$

Si $d\ = \ mcd(a, b)$, entonces d es tal que $d|a$ y $d|b$ y si existe c es tal que $c|a$ y $c|b$. 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 $d = mcd(a, b) = mcd\ (b, a)$.

ii) $mcd\ (a\ ,0)\ = \ |a|$

- 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 $c|\ |a|$ y por lo tanto $|a| = mcd\ (a, 0)$.

iii) $mcd\ (a\ ,b) = \ mcd\ (-a, b)$

Sea $d = mcd\ (a, b)$, entonces $d|a\ y\ d|b$ y $\mathrm{si}\ \ c|a\ y\ c|b$ entonces $c|d$. Como $d|a$ entonces $d|-a$. Luego $d|-\ a\ \ \ y\ \ d|b$, esto es d es divisor común de $-a\ \ \ y\ b$. Además todo entero c tal que $c|-a\ \ \ y\ \ \ c|b$ verifica también que $c|\ a\ \ \ y\ \ \ c|b$, por lo tanto $c|d$ ya que $d = mcd\ (a, b)$. Entonces $d = mcd\ (-a, b)$.

iv) $mcd\ (a\ ,b) = \ mcd\ (|a|, |b|)$

- Si $a \geq 0\ \ y\ \ b \geq 0$ entonces $|a| = a\ \ y\ |b| = b$, luego se verifica que $mcd\ (a, b) = \ mcd\ (|a|, |b|)$.

- Si $a < 0$ y $b \geq 0$ entonces $|a| = -a$ y $|b| = b$, luego por iii) se verifica $mcd\ (a, b) = mcd\ (-a, b) = mcd\ (|a|, |b|)$.

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 $mcd\ (|a|, |b|) = mcd\ (-a, -b) = mcd\ (-a, b) = mcd\ (a, b)$.

v) Cualquiera sea a , se tiene que $|a|\,|a$ y $|a|\,|ka$ (por propiedad 5 de divisibilidad), con lo que se dice que $|a|$ es un divisor común entre $a\ y\ k.a$.

Ahora, si c es cualquier otro entero tal que $c|a$ y $c|k.a$ se tendrá que $c\,\big||a|$ ya que el mayor divisor de a es $|a|$. Entonces $mcd\ (a\ , k.a) = |a|$.

vi) $mcd\ (a\ , b) = mcd\ (b\ , r)$ siendo $r = a\ mod\ b$

Sea $d = mcd(a, b)$. Mostrar que $d = mcd\ (b, r)$, significa probar que $d|b$ y $d|r$ y que si $c|b$ y $c|r$ entonces $c|d$.

Como $a = b.q + r$ y $d|\ a$ y $d|b$ por ser el máximo común divisor entre ellos entonces se tiene que $d|(a - b.q)$ y por lo tanto $d|r$ además de dividir a a y b.

Además si existe otro numero c tal que $c|b\ y\ c|r$ entonces $c|(b.q + r)$ y por lo tanto $c|a$. Pero como d es el máximo común divisor de $a\ y\ b$ entonces $c|d$

Con lo que queda probado que $d = mcd\ (b\ , r)$ siendo $r = a\ mod\ b$.

Corolario

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos, y $n > 0$

$$\mathrm{mcd}\ (na\ , nb) = n.\mathrm{mcd}\ (a, b)$$

3.6 Números Coprimos o Primos relativos

Definición

Sean $a, b \in Z$. Se dice que $a\ y\ b$ son coprimos o primos relativos si y solo si $mcd\ (a, b) = 1$.

Ejemplos 3.11

i) $2\ y\ 3$ son coprimos ya que $mcd(2\ ,3) = 1$

ii) $16\ y\ 15$ son coprimos ya $mcd(16, 15) = 1$

👁 Observación

El concepto de números coprimos no está vinculado al concepto de primos.

📚 Propiedades de los Números Coprimos

Sean $a, b, c \in \mathbb{Z}$

- Si $a\ y\ b$ son coprimos con c, entonces $a.b$ 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 $n \in \mathbb{Z}$, $n|(a.b)\ \wedge\ n$ y a son coprimos entonces $n|b$
- Si $a, b \neq 0\ \ y\ \ d = mcd\ (a, b)$ se verifica que $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos.

Actividad 3.5

a) Encontrar números coprimos con 8

b) Sean los números: 5, 10, 12, 15, 18. Determinar todas las parejas de coprimos que hay entre ellos

c) Decir verdadero o Falso, justificando su respuesta:

i) Si $3|(5.x)$ entonces $3|x$, $\forall x \in \mathbb{Z}$

ii) Si $3|(6.x)$ entonces $3|x$, $\forall x \in \mathbb{Z}$

iii) Si $5 = mcd(10.x, 25.x)$ entonces $2x\ y\ 5x$ son coprimos, $\forall x$

📚 Teorema: Identidad de Bezout

Si $d = mcd(a, b)$ 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 $d = a.x + b.y$

📚Corolario

Dos enteros a y b son coprimos (o primos relativos) si y solo si existen enteros x, y tales que $a.x + b.y = 1$.

Ejemplos 3.12

i) Como $1 = 3.8541 + (-2).12811$ entonces $mcd(8541, 12811) = 1$

ii) Dos enteros consecutivos siempre son coprimos, es decir, mcd(x, x+1)=1, ya que 1.(x+1)+(-1).x=1. Por ejemplo, $mcd(8, 9) = 1$.

Actividad 3.6

Responder Verdadero o Falso, y justificar la respuesta:

i) $mcd(10{,}25) = 5 \wedge mcd(-10, -25) = -5$

ii) $mcd(-5, 5.k) = 5, \forall k \in Z$

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) $mcd(55, 135) = 5.mcd(11, 27) = 5.mcd(11, 6)$

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)

$$a = b.q_1 + r_1, \ \ 0 \leq r_1 < b$$

Por propiedad resulta que $mcd(a,b) = mcd(b,r_1)$

3.1) $Si\ r_1|b$ entonces $mcd(a,b) = mcd(b,r_1) = r_1$

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

$$b = r_1.q_2 + r_2, \ \ 0 \leq r_2 < r_1$$

Al igual que antes se tiene que $mcd(b,r_1) = mcd(r_1,r_2)$

3.2.1) $Si\ r_2|r_1\ entonces\ mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2) = r_2$

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

$$r_1 = r_2.q_3 + r_3, \ \ 0 \leq r_3 < r_2$$

Al igual que antes se tiene que $mcd(r_1,r_2) = mcd(r_2,r_3)$, y así sucesivamente.......

$$r_{n-2} = r_{n-1}.q_n + r_n, \ \ 0 \leq r_n < r_{n-1}$$

Este proceso se repite hasta llegar a un resto igual a cero

$$r_{n-1} = r_n.q_{n+1} + 0$$

Por lo tanto $mcd(r_{n-2},r_{n-1}) = mcd(r_{n-1},r_n) = r_n$

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 a $d = r_k$ en función de los restos anteriores, y finalmente de a y b.

Algoritmo de Euclides en el lenguaje de Pseint

```
Algoritmo CálculoMCD
        Escribir ('Ingresa los números a y b con a>b')
        Leer a,b
        r <- a MOD b
        Si r=0 Entonces
                Escribir 'mcd(a,b)= ',b
        SiNo
                Si r>0 Entonces
                        a <- b
                        b <- r
                        r <- a MOD b
                        Si r=0 Entonces
                            Escribir 'mcd(a,b)= ',b
                        FinSi
                FinSi
        FinSi
FinAlgoritmo
```

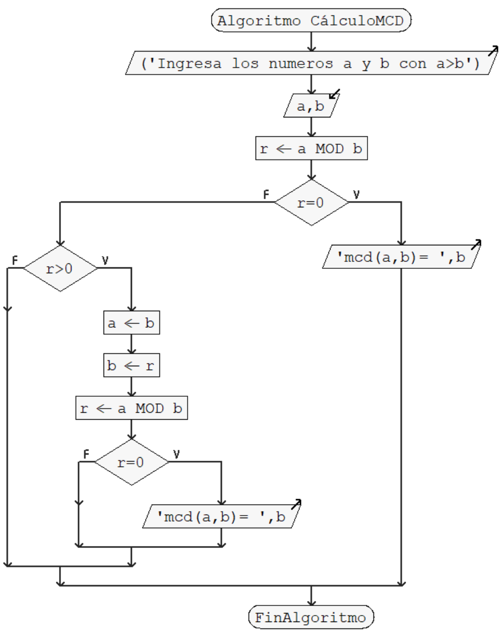


Fig. 3.5. Algoritmo Cálculo mcd.

Ejemplo 3.13

Se muestra a continuación el cálculo de $mcd(250;\ 111)$ y los pasos que se deben dar para expresarlo como combinación lineal de 250 y 111.

Como $111 \nmid 250$ se realizan las divisiones que indica el algoritmo hasta obtener resto nulo.

(1) $\quad 250 = 111.2 + 28 \qquad$ con $\quad 0 < 28 < 111$

(2) $\quad 111 = 28.3 + 27 \qquad$ con $\quad 0 < 27 < 28$

(3) $\quad 28 = 27.1 + \mathbf{1} \qquad$ con $\quad 0 < 1 < 27$

(4) $\quad 27 = 1.27$

Por tanto, $mcd(250; 111) = 1$

Para encontrar la combinación lineal se deben despejar los residuos obtenidos en el algoritmo de Euclides, y se hace una sustitución hacia atrás.

$1 = 28 - 27$	despejando de (3) el mcd
$= 28 - (111 - 28.3)$	despejando de (2) el resto 27
$= 4.28 - 111$	
$= 4.(250 - 111.2) - 111,$	despejando de (1) el resto 28
$1 = \underbrace{4}_{x}.250 + \underbrace{(-9)}_{y}.111$,	luego el $mcd(250,111) = 1$, queda expresado como combinación lineal de 250 y 111.

Actividad 3.7

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:

$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_2 b^2 + r_1 b^1 + r_0$, y de esta forma se indica

$a = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b$ y se dice que es la expresión de a en base b.

Por ejemplo el número entero 4165 en base 7, quedaría aplicando el algoritmo de la división,

$$
\begin{aligned}
4165 &= 7 \cdot 595 + 0 \to r_0 \\
595 &= 7 \cdot 85 + 0 \to r_1 \\
85 &= 7 \cdot 12 + 1 \to r_2 \\
12 &= 7 \cdot 1 + 5 \to r_3 \\
1 &= 7 \cdot 0 + 1 \to r_4
\end{aligned}
$$

Se obtiene $4165 = (15100)_7 = 0 + 0 \cdot 7 + 1 \cdot 7^2 + 5 \cdot 7^3 + 1 \cdot 7^4$

3.7 Mínimo Común Múltiplo

Definición

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos; se dice que $c \in \mathbb{Z}^+$es el mínimo común múltiplo de a y b si y sólo si:

$\boldsymbol{i})\ a|c \quad y \quad b|c$

$\boldsymbol{ii})\ \forall d \in \mathbb{Z},\ a|d \ y \ b|d \Rightarrow c|d$

Para expresar que c es el mínimo común múltiplo de a y b se escribe

$c = mcm\,(a, b)$

Ejemplos 3.14

i) Si $a = 3$ y $b = 8$, los múltiplos comunes a ambos son 24, 48, 72,….

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 60. Luego $mcm(12,15) = 60$.

Teorema

$\forall a, b \in \mathbb{Z}^+$ se verifica que $mcd(a,b).mcm(a,b) = a.b$

Ejemplos 3.15

i) $mcd(250,111) = 1$ luego $mcm(250,111) = \frac{250 \cdot 111}{1} = 27750$

ii) $mcd(250,325) = 25$ luego $mcm(250,325) = \frac{250 \cdot 325}{25} = 3250$

Actividad 3.8

1) Responder Verdadero o Falso, justificando su respuesta:

$i)$ $\forall a, b \in \mathbb{Z}$, $mcd\,(a, b) \,.\, mcm\,(a, b) = |a.b|$

$ii)$ $\forall a, b \in \mathbb{Z}$, si a y b son coprimos entonces $mcm\,(a,b) = a.b$.

2) Tres aviones salen del aeropuerto, uno cada 3 días, otro cada 12 días y el tercero cada 18 días. ¿Cada cuántos días los tres aviones saldrán simultáneamente?

3.8 Ecuación diofántica

Definición

Ecuación diofántica es toda ecuación en una o más variables, con la restricción de que sus coeficientes y sus soluciones sean 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

Toda ecuación diofántica del tipo $ax + by = c$ es compatible si y solo sí $mcd(a, b)|c$.

Además, si una ecuación diofántica $ax + by = c$ es compatible, el conjunto solución es infinito.

Ejemplos 3.16

i) La ecuación diofántica $2x + 3y = 2$ tiene soluciones enteras pues $mcd(2,3) = 1$ y $1|2$.

ii) La ecuación $6x - 3y = 1$ no es compatible pues $mcd(6,3) = 3$ y $3 \nmid 1$. Esto es, $\nexists x, y \in \mathbb{Z}$ que satisfacen la ecuación.

iii) ¿La ecuación diofántica $-8x + 22y = 20$ tiene solución? ¿Cómo se encuentra al menos una de ellas?

Para determinar si una ecuación diofántica tiene solución y para proceder a su encuentro se siguen los siguientes pasos:

1°: Verificación de la condición necesaria y suficiente para la existencia de soluciones: $mcd(a, b)|c$

Se observa que $a = -8$ y $b = 22$, y como $mcd(-8,22) = mcd(22,8)$ se calcula este último:

$22 = 2 \cdot 8 + 6$ (1)

$8 = 6 \cdot 1 + 2$ (2)

$6 = 2 \cdot 3$ (3)

Como $mcd(22{,}8) = 2$ y $2|22$, por el teorema se tiene que la ecuación $-8x + 22y = 20$ es compatible.

2°: Determinación de una solución particular

Despejando los residuos de (2) y (1) y haciendo una sustitución hacia atrás se tendrá:

De (2) $2 = 8 - 6 \cdot 1$ (4)

De (4) y (1) $2 = 8 - (22 - 2 \cdot 8\,)$ (5)

De (5) $2 = 3 \cdot 8 - 22$ (6)

De (6) $2 = \underbrace{(-8)}_{a} . (-3) + \underbrace{22}_{b} . (-1)$ (7)

La igualdad (7) expresa a 2 como combinación lineal de -8 y 22 (Identidad de Bezout).

Ahora, para identificar a (7) con la ecuación a resolver se debe convertir el 2 en 20, lo cual se hace multiplicando por un factor adecuado. Como $20 = 2 \cdot 10$, se multiplica ambos miembros de (7) por 10

$$20 = \underbrace{(-8)}_{a} . \underbrace{(-30)}_{x} + \underbrace{22}_{b} . \underbrace{(-10)}_{y} \qquad (8)$$

Así, una solución de la ecuación diofántica es $x = -30$ e $y = -10$.

Si se quiere encontrar más soluciones de esta ecuación, se tiene el siguiente teorema:

3.8.1 Solución general de una ecuación diofántica

Teorema

Si la ecuación diofántica $ax + by = c$ es compatible y si $(x_0\,, y_0)$ es una solución particular, entonces la solución general está dada por:

$$x = x_0 + \frac{b}{d}.k \quad ; \qquad y = y_0 - \frac{a}{d}.k \quad ; \quad \forall k \in \mathbb{Z}$$

donde d = mcd (a,b)

Demostración:

Sea $ax + by = c$. Como $d = mcd(a, b)|c$ la ecuación tiene solución. Llamando $(x_0\,, y_0)$ a la solución particular y (x, y) a la solución general, dividiendo miembro a miembro por d se tiene que:

$$\begin{cases} \frac{a}{d}x + \frac{b}{d}y = \frac{c}{d} \\ \frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d} \end{cases} \quad \underbrace{\Rightarrow}_{restando\ m.a.m} \quad \frac{a}{d}(x - x_0) + \frac{b}{d}(y - y_0) = 0$$

$$\Rightarrow \quad \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \qquad (*)$$

$$\Rightarrow \quad \frac{b}{d} \,\Big|\, \frac{a}{d}(x - x_0)$$

Pero $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos, por tanto $\frac{b}{d} \,\Big|\, (x - x_0)$, con lo cual existe $k \in \mathbb{Z}$ tal que $(x - x_0) = \frac{b}{d}\,k$, luego $x = x_0 + \frac{b}{d}\,k$.

De manera análoga se tiene a partir de $(*)$

$$\frac{a}{d} \,\Big|\, \frac{b}{d}(y_0 - y)$$

Y , como se dijo, que $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos entonces $\frac{a}{d} \,\Big|\, (y_0 - y)$, con lo cual existe $k \in \mathbb{Z}$ tal que $(y_0 - y) = \frac{a}{d}\,k$, luego $y = y_0 - \frac{a}{d}\,k$.

Por lo tanto, la expresión que representa a las infinitas soluciones (solución general) de la ecuación diofántica, se expresa:

$$\begin{cases} x = x_0 + \frac{b}{d}.k \\ \\ y = y_0 - \frac{a}{d}.k \end{cases} \quad \text{con } k \in \mathbb{Z}$$

Observación

En la práctica, cuando se tiene una solución particular $(x_0\,, y_0)$ y se desea encontrar la solución general se debe sumar y restar un múltiplo entero de $mcm(a,b) = \frac{ab}{d}$; es decir:

$$ax_0 + by_0 + \frac{ab}{d}k - \frac{ab}{d}k = c \quad \Rightarrow \quad a\underbrace{\left(x_0 + \frac{b}{d}k\right)}_{x} + b\underbrace{\left(y_0 - \frac{a}{d}k\right)}_{y} = c \text{ con } k \in \mathbb{Z}$$

Luego se presenta la solución general.

$$\begin{cases} x = x_0 + \dfrac{b}{d}k \\ \\ y = y_0 - \dfrac{a}{d}k \end{cases} \quad , \quad k \in \mathbb{Z}$$

Ejemplos 3.17

i) La ecuación diofántica $4x - 6y = 10$ es compatible, ya que $mcd(4,-6) = mcd\,(4{,}6) = 2 \;y\; 2|10$. En este caso observe que se puede reducir la ecuación original dividiendo ambos miembros por $d = 2$ obteniendo una ecuación equivalente $2x - 3y = 5$ (*) siendo $mcd\,(2,-3) = 1$

Considerando esta última ecuación (*), una solución particular es $(1,-1)$ y la solución general es:

$$\begin{cases} x = 1 + 3k \\ \\ y = (-1) + 2k \end{cases} \quad , \quad \forall k \in \mathbb{Z}$$

Dando valores a k se obtienen otras soluciones: (4, 1), (7, 3),(-2, -3), (-5, -5),…

ii) Si existe, ¿cuál es la solución general de $7x - 11y = 2$?

Dado que $mcd(7,-11) = 1$ y $1|2$ entonces la ecuación es compatible, posee soluciones enteras.

Para encontrar una solución particular se deben seguir los pasos que permiten encontrar la combinación lineal de la que menciona la identidad de Bezout :

$11 = 7.1 + 4$ (1)

$7 = 4.1 + 3$ (2)

$4 = 3.1 + 1$ (3)

$3 = 3.1$

Para encontrar la combinación lineal de 1 respecto de 7 y 11 se despeja el valor del mcd de (3) y se sustituye uno a uno los restos anteriores, del siguiente modo:

De (3) $1 = 4 - 3.1$

Por (2) $1 = 4 - (7 - 4).1 = 2.4 - 7,$

Por (1) $1 = 2.(11 - 7) - 7 = 2.11 - 3.7$

Luego se tiene $1 = (-3).7 + (-2).(-11)$. multiplicando por 2 para identificar esta igualdad con la ecuación a resolver se tiene:

$2 = (-6).7 + (-4).(-11)$, entonces una solución de $7x - 11y = 2$ es $(-6, -4)$.

El resto de las soluciones son: $x = -6 + (-11)k$ e $y = -4 - 7k$; con $k \in \mathbb{Z}$. Luego otra forma de expresar la solución general es:

$$(-6 - 11k, -4 - 7k) \quad \text{, con } k \in \mathbb{Z}$$

Observación

En ocasiones, hay que buscar soluciones que satisfacen otras condiciones adicionales, por ejemplo, soluciones positivas. Para ello, se encuentra en primer lugar la solución general y a continuación se determinan los valores del parámetro k para los cuales se cumplen las condiciones adicionales.

Ejemplo 3.18

Si en el Ejemplo 3.17 (ii) se hubiera pedido las soluciones enteras “no negativas” de la ecuación diofántica $7x - 11y = 2$; se tendría que añadir la condición adicional “no negativas” a la solución general $(-6 - 11k, -4 - 7k)$ y buscar los valores de k que satisfacen tal requerimiento.

$-6-11k \geq 0 \Rightarrow k \leq \frac{-6}{11}$ y $-4-7k \geq 0 \Rightarrow k \leq -4/7$.

Luego $k = -1, -2, -3, \ldots$; para $k = -1$, la solución es $(5,3)$; para $k = -2$, la solución es $(16, 10)$; para $k = -3$, la solución es $(27, 17)$, y así sucesivamente.

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 cierto día se recaudaron $9000 y asistieron más adultos que menores. ¿Cuáles fueron los posibles números de asistentes?

3.9 Congruencia en $\mathbb{Z}$

Al dividir un entero x por un natural $n > 1$ los posibles restos son: $0, 1, 2, \ldots, n-1$. 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: $x \equiv y (mod\ n) \Leftrightarrow x \bmod n = y \bmod n$

Esto significa que x e y tienen el mismo resto al dividirlos en n

Ejemplos 3.19

- $15 \equiv 7\ (mod\ 2)$ pues $15\ mod\ 2 = 7\ mod\ 2 = 1$, pero no es cierto que $15 \equiv 7\ (mod\ 3)$ dado que $15\ mod\ 3 = 0\ y\ 7\ mod\ 3 = 1$.
- $16 \equiv 24\ (mod\ 4)$ y también $-16 \equiv 24\ (mod\ 8)$.

Propiedad

Sean $x, y \in \mathbb{Z}$ y sea $n \in \mathbb{Z}^{+}$. Se cumple que $x\ e\ y$ son congruentes $mod\ n$ si y solo si la diferencia entre ellos es múltiplo de n.

Simbólicamente: $x \equiv y\ (mod\ n) \Leftrightarrow n|(x-y)$

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.

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.

Ejemplos 3.20

i) $21 \equiv 9\ (mod\ 4)$ ya que $4|(21-9)$

ii) $9 \equiv 0\ (mod\ 3)$ porque $9-0=9$ y 3 | 9

iii) $2 \equiv -3\ (mod\ 5)$ porque $2-(-3)=5$ y $5|5$

iv) $-13 \equiv 52\ (mod\ 5)$ pues (-13) - 52 = -65 y 5 |(-65)

Observaciones

A partir de la propiedad: “ $n|(x-y) \Leftrightarrow (x-y)$ es múltiplo de n ” se deduce que $x = y + n.k,\ k \in \mathbb{Z}$, lo que nos dice que para encontrar un valor de x congruente con y basta con sumar cualquier múltiplo de n.

Por ejemplo algunos números congruentes con 0 módulo 4 son:

$0+4;\ \ 0+2.4\ ;\ 0+3.4\ ;\ \ldots$ es decir: $4, 8, 12, 16$ ...

Congruentes con 1 módulo 4:

$1+4\ ;\ \ 1+2.4\ ;\ \ 1+3.4\ ;\ \ldots$ es decir: $5, 9, 13, 17,$ ....

Congruentes con 2 módulo 4:

$2+4\ ;\ \ 2+2.4\ ;\ \ 2+3.4;$ ... es decir: $6,10, 14, 18,$ ....

Congruentes con 3 módulo 4:

$3+4\ ;\ 3+2.4\ ;\ 3+3.4;\ \ldots$ es decir: $7, 11, 15, 19,$ ...

- 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 en el conjunto $\{0, 1, 2, 3, \ldots, n-1\}$, conjunto de los restos posibles al dividir cualquier entero en n, no hay dos números congruentes entre sí $modulo\ n$.

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 ....

3.9.1 Relación de Congruencia módulo n

Definición

En $\mathbb{Z}$, se llama Relación de Congruencia $módulo\ n$ a la relación R definida como

$$R = \{(x, y)/\ x \equiv y(mod\ n)\ , x\ , y \in \mathbb{Z}\ \}$$

📚 **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. Sean $x, y, z \in \mathbb{Z}$

Se cumple que $x \equiv x(mod\ n)$ ya que $n|(x - x)$, $\forall x$. Por lo tanto R es reflexiva.

Se cumple que si $x \equiv y(mod\ n)$ entonces $n|(x - y)$. Por propiedad de la divisibilidad también se cumple que $n|(y - x)$ de donde se deduce que $y \equiv x\ (mod\ n)$. Por lo tanto R es simétrica

Si se cumple que $x \equiv y(mod\ n)\ \wedge\ y \equiv z(mod\ n)$ 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 $x \equiv z(mod\ n)$. Por lo tanto R es transitiva.

Por último se concluye que R es una relación de equivalencia.

3.9.2 Conjunto Cociente de una Relación de Congruencia

Como toda relación de equivalencia, las relaciones de congruencia generan una partición en $\mathbb{Z}$ 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 define $[x]_n$: Clase de equivalencia $mód\ n$ del elemento x al conjunto:

$$[x]_n = \{y \in \mathbb{Z}\ /\ x \equiv y(mod\ n)\ \}$$

Cada clase de equivalencia queda determinada por un resto, por lo tanto hay n clases distintas, $[0]_n, [1]_n, [2]_n, \ldots [n-1]_n$. Se toman los valores $0, 1, 2, \ldots, n-1$ son los representantes de cada clase. Cada clase, expresada por extensión es:

$[0]_n = \{y \in \mathbb{Z} : \ y \equiv 0 \ (mod \ n)\} = \{ \ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots \}$

$[1]_n = \{y \in \mathbb{Z} : \ y \equiv 1 \ (mod \ n)\} = \{\ldots, 1-2n, 1-n, 1, 1+n, 1+2n, 1+3n, \ldots\}$

$[2]_n = \{y \in \mathbb{Z} : \ y \equiv 2 \ (mod \ n)\} = \{\ldots, 2-2n, 2-n, 2, 2+n, 2+2n, 2+3n, \ldots\}$

$$\vdots$$

$[n-1]_n = \{y \in \mathbb{Z} : \ y \equiv n-1 \ (mod \ n)\} = \{\ldots, -2n-1, -n-1, -1, n-1, 2n-1, \ldots\}$

También para el Conjunto Cociente se adopta una notación especial, $\mathbb{Z}_n$ y entonces se tiene que:

$$\mathbb{Z}_n = \{[0]_n , [1]_n , [2]_n , \ldots [n-1]_n \}$$

Ejemplo 3.21

Las clases de equivalencia en $\mathbb{Z}$ módulo 3 son tres: $[0]_3$, $[1]_3$ y $[2]_3$ y entonces el conjunto cociente es $\mathbb{Z}_3 = \{[0]_3 , [1]_3 , [2]_3\}$; donde

$[0]_3 = \{y \in \mathbb{Z} : \ y \equiv 0 \ (mod \ 3)\} = \{y \in \mathbb{Z} \ : \ y = 3k \ , \ k \in \mathbb{Z}\} =$

$= \{\ldots - 9, -6, -3, 0, 3, 6, 9, \ldots\};$

$[1]_3 = \{y \in \mathbb{Z} : \ y \equiv 1 \ (mod \ 3)\} = \{y \in \mathbb{Z} \ : \ y = 1 + 3k \ , \ k \in \mathbb{Z}\} =$

$= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

$[2]_3 = \{y \in \mathbb{Z} : \ y \equiv 2 \ (mod \ 3)\} = \{y \in \mathbb{Z} \ : \ y = 2 + 3k \ , \ k \in \mathbb{Z}\} =$

$= \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$

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 $\mathbb{Z}_5$

Capítulo 4. SUCESIÓN, INDUCCIÓN Y RECURSIVIDAD

Sucesión.

Sucesiones particulares: arreglos, palabras,

Sucesiones Numéricas.

Símbolo Suma.

Inducción Matemática.

Recursión o Recursividad

Clasificación de las relaciones de recurrencia.

Solución de las relaciones de recurrencia lineales de 1° y 2° orden,

homogéneas y de coeficientes constantes.

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 dichos conjuntos de valores se denominan sucesiones.

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 función con la letra S, se tiene $S: \mathbb{N} \longrightarrow A$

y se indica a los valores del Conjunto Imagen (o términos de la sucesión) del siguiente modo:

$S(1) = a_1$; $S(2) = a_2$; $S(3) = a_3$; ....

donde $a_i \in A, \forall i$

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.

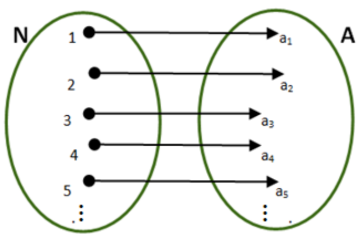


Fig.4.1. Función sucesión.

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) : $a_1, a_2, a_3, \dots$ es una forma abreviada de escribir una función como un conjunto de pares ordenados: $\{(1 . a_1), (2, a_2), (3, a_3), \dots\}$ donde se da por sobreentendido su dominio.
- El dominio de la sucesión también puede ser $\mathbb{N}_0 = \{0,1,2,3,\dots\}$. En este caso, el primer término de la sucesión será a_0, el segundo a_1, etc. Esto es:

$$(a_n) \ : \ a_0, a_1, a_2, \dots \ \text{con} \ n \in \mathbb{N}_0$$

- Los términos de una sucesión pueden o no repetirse.
- Si existe un patrón de comportamiento el término general de una sucesión puede expresarse mediante fórmulas.

Definiciones

• El conjunto correspondiente a una sucesión o conjunto Imagen 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

i) S_1 : 0, 1, 0, 1, 0, 1, ... es la sucesión infinita que alterna ceros y unos. Su conjunto correspondiente (o imagen) es { 0 , 1 }.

ii) S_2 **:** a, b, c, d, e es la sucesión finita de las 5 primeras letras en orden alfabético. Su conjunto imagen es $\{ a, b, c, d, e \}$.

iii) S_3 : 1, 3, 5, 7 es la sucesión finita de los 4 primeros números impares. Su conjunto imagen es { 1 , 3 , 5 , 7 }.

iv) S_4 : 1, 0, 0, 1, 0, 0, 0, 1, 1 es una sucesión finita con elementos repetidos. Su conjunto correspondiente es { 0 , 1 }.

v) S_5 **:** 1, 2, 4, 8, 16, 32, ... 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 $\{a_n \ / \ a_n = 2^{n-1}, n \in \mathbb{N}\}$.

4.1.1 Igualdad de sucesiones

Definición

Dos sucesiones son iguales si y sólo si coinciden sus valores término a término. Simbólicamente:

$$(a_n) = (b_n) \quad \Leftrightarrow \quad a_n = b_n \ , \ \forall n$$

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 $-1 , 1 , -1 , 1 , -1 , ...$

Actividad 4.1

Dar el valor de verdad de las siguientes afirmaciones, justificando su respuesta:

a) El conjunto correspondiente a la sucesión 1 , -1 , 1 , -1 , 1 es {-1,1}

b) $a_n = (-1)^{2n}$ con $n \in \mathbb{N}$ es una sucesión infinita y su conjunto correspondiente es {-1,1}

c) La sucesión 2 , 4 , 6 , ... , 12 es finita y está formada por 6 términos

d) Las sucesiones $a_n = (-2)^{2n}$ y $b_n = 2^{2n}$ con $n \in \mathbb{N}$ no son iguales

4.2 Sucesiones particulares

4.2.1 Arreglos

Definición

Un arreglo es una sucesión de posiciones de memoria o celdas vacías a las que se les puede asignar 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 $S(1)$, $S(2)$, $S(3)$,… se la llamará sucesión de valores del arreglo S. Los arreglos se consideran objetos bien definidos, aun cuando algunas de las posiciones no se les haya asignado valores o si se cambian algunos valores durante la discusión.

Los ejemplos más comunes en matemáticas y en informática son los vectores y las matrices, que son conjuntos de elementos del mismo tipo con tamaños definidos.

4.2.2 Palabras

Para generar palabras se necesita disponer de un Alfabeto que es un conjunto no vacío de símbolos cualesquiera. Se designa con la letra Σ.

Definición

Palabra, cadena o strings es cualquier sucesión de símbolos del alfabeto Σ.

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 λ y su longitud es 0

El conjunto de palabras generadas por símbolos del alfabeto Σ , se denomina Lenguaje y se denota L .

El lenguaje vacío es aquel que no contiene palabras: $\mathrm{L} = \{\,\}$ y no es lo mismo que el lenguaje formado por la palabra vacía , $\mathrm{L}_{\lambda} = \{\lambda\}$.

El conjunto de todas las palabras generadas por Σ, se denomina Lenguaje Universal y se denota con Σ^*

En el contexto de Σ^* , Σ representa el alfabeto como lenguaje unisimbólico, eso significa que las palabas son de un solo símbolo que se corresponden con los símbolos del alfabeto.

Donde $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \ldots .\cup \Sigma^\infty$ (Estrella de Kleene)

Ejemplo 4.3

Sea el alfabeto Σ = {a, b, c} entonces el lenguaje universal generado por Σ es Σ * = { λ , a , b , c , aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, aab, …} y por lo tanto se tiene que w_1= aabccc; w_2= abcc y w_3= ccbacba pertenecen a Σ *.

Actividad 4.2

Sea el alfabeto Σ = {a,b,c}, responder verdadero o falso, y justificar la respuesta

a) aaaa $\in \Sigma$ * $\wedge$ aaa+aabaca$\in \Sigma$ *

b) Si L_1 = {x / x es la palabra vacía o es una palabra de longitud 2 generada por el alfabeto Σ } entonces $|\mathrm{L}_1|$ = 10

c) Si L_2= {x / x es una palabra de long. 3 y de símbolos distintos} entonces $|\mathrm{L}_2|$ = 27.

4.3 Sucesiones Numéricas

Definición

Una sucesión numérica es aquella sucesión cuya imagen es cualquier subconjunto de los Números Reales. Simbólicamente

$$S: \mathbb{N} \longrightarrow \mathbb{R}$$

Ejemplos 4.4

i) $(a_n): 1 , 4 , 9 , 16 , 25 , \ldots$ sucesión de los cuadrados de los números naturales.

ii) $(b_n): 1 , \frac{1}{2} , \frac{1}{3} , \frac{1}{4} , \frac{1}{5} , \ldots$ sucesión de los inversos de los números naturales.

iii) $(c_n): 2 , 4 , 6 , 8 , 10 , \ldots$ sucesión de los números pares positivos.

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.

Ejemplo 4.5

Para encontrar la fórmula explícita de la sucesión dada por: $1 , \frac{1}{2} , \frac{1}{4} , \frac{1}{8} , \frac{1}{16} , \ldots$ una buena sugerencia es asociar a cada valor de la sucesión con el subíndice correspondiente. Entonces si se denota a la sucesión $a_1, a_2, a_3, \ldots$ se tendrá:

$$a_1 = 1 \quad ; \quad a_2 = \frac{1}{2} \quad ; a_3 = \frac{1}{4} \quad ; \quad a_4 = \frac{1}{8} \quad ; \quad \ldots$$

Se observa que el numerador es siempre 1 y en el denominador aparecen las potencias de 2 comenzando con la potencia de exponente cero.

$$a_1 = \frac{1}{2^0} \quad ; \quad a_2 = \frac{1}{2^1} \quad ; a_3 = \frac{1}{2^2} \quad ; \quad a_4 = \frac{1}{2^3} \quad ; \quad \ldots$$

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:

$$a_1 = \frac{1}{2^{1-1}} \quad ; \quad a_2 = \frac{1}{2^{2-1}} \quad ; a_3 = \frac{1}{2^{3-1}} \quad ; \quad a_4 = \frac{1}{2^{4-1}} \quad ; \quad \ldots$$

Por lo tanto se pude escribir el término general del siguiente modo:

$$a_n = \frac{1}{2^{n-1}} \quad , \quad n \in \mathbb{N}$$

También hubiera sido válido representar a la sucesión comenzando en a_0 de tal modo que:

$$a_0 = 1 \quad ; \quad a_1 = \frac{1}{2} \quad ; a_2 = \frac{1}{4} \quad ; \quad a_3 = \frac{1}{8} \quad ; \quad \ldots$$

con lo cual la fórmula del término general seria

$$a_n = \frac{1}{2^n} \quad , \quad n \in \mathbb{N}_0$$

Se puede observar que las fórmulas explicitas no son únicas y que iniciar a n en cero puede llevarnos a una forma más simple en algunos casos.

4.3.1 Progresión Aritmética

Definición

Una progresión aritmética es una sucesión numérica donde cada término, salvo el primero, se obtiene sumando una constante al término anterior. A dicha constante se le llama diferencia de la progresión y se denota d.

El término general de una progresión aritmética es:

$$a_n = a_1 + d(n-1) \quad , \qquad n \in \mathbb{N}$$

donde a_1 es el primer término y d es la diferencia.

Ejemplos 4.6

i) El término general de la progresión aritmética (a_n): 3, 7, 11, 15, ... donde el primer término es 3 y la diferencia 4 es

$$a_n = 3 + 4(n-1) = -1 + 4n \quad , \qquad n \in \mathbb{N}$$

ii) El término general de la progresión aritmética (a_n): -3 , -5, -7 , -9 , ... donde el primer término es -3 y la diferencia - 2 es

$$a_n = -3 - 2(n-1) = -1 - 2n \quad , \qquad n \in \mathbb{N}$$

iii) 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

$$a_n = (-1)^n[3 + 4(n-1)\,] = (-1)^n(-1+4n) \quad , \qquad n \in \mathbb{N}$$

iv) 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?

1° año: $A_1 = 9000$

2° año: $A_2 = 9000 + 500$

3° año: $A_3 = 9000 + 500 + 500 = 9000 + 2\,.500$

4° año: $A_4 = 9000 + 500 + 500 + 500 = 9000 + 3\,.500 = 10500$

Al cabo de n años : $A_n = 9000 + \ (n-1)500 \quad , \ n \in \mathbb{N}$

4.3.2 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 r

El término general de una progresión geométrica es:

$$a_n = a_1.r^{n-1} \quad , \qquad n \in \mathbb{N}$$

donde a_1 es el primer término y r la razón.

Ejemplos 4.7

i) El término general de la progresión geométrica $(a_n): 2\,, 6\,, 18\,, 54\,, \ldots$ donde el primer término es 2 y la razón es 3 es

$$a_\mathrm{n} = 2\,.3^{\mathrm{n}-1}, \qquad \mathrm{n} \in \mathbb{N}$$

ii) El término general de la progresión geométrica $(b_n): 1\ , \ \frac{1}{2}\ , \frac{1}{4}\ , \frac{1}{8}\ , \ldots$ donde el primer término es 1 y la razón es $\frac{1}{2}$ es

$$\mathrm{b_n} = \left(\frac{1}{2}\right)^{\mathrm{n}-1}, \qquad \mathrm{n} \in \mathbb{N}$$

iii) 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 en el 4° año? , ¿Cuánto se pagará al cabo de n años?.

El cálculo sería el siguiente:

1° año: $A_1 = 9000$

2° año: $A_2 = 9000 + 0{,}05\,.\,9000 = 9000.(1 + 0{,}05) = 9000\,.1{,}05$

3° año: $A_3 = 9000\,.1{,}05 + 0{,}05\,.\,9000\,.1{,}05 = 9000\,.\,1{,}05^2$

4° año: $A_4 = 9000\,.\,1{,}05^2 + 0{,}05\,.\,9000\,.\,1{,}05^2 = 9000\,.\,1{,}05^3$

Al cabo de n años : $A_n = 9000\,.\,1{,}05^{n-1}$, $n \in \mathbb{N}$

Actividad 4.3

a) En cada apartado, escribir los seis primeros términos y el término general de las sucesiones que cumplen las condiciones especificadas:

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 en 1

iv) A cada número natural n le corresponde el triple de su anterior.

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) $10\,, 1\,, \frac{1}{10}\,, \frac{1}{100}\,, \frac{1}{1000}, ...$

vi) 3, -9, 27, -81, …

4.4 Símbolo Suma

De ahora en adelante, solo por una cuestión de conveniencia para la notación, se representará a las sucesiones usando al subíndice k .

En algunas situaciones se necesita sumar los términos de una sucesión. Por ejemplo, para 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

$$(3.1-2)+\ (3.2-2)+(3.3-2)+\ \ldots\ +\ (3k-2)\ =$$

$$=\ 1+4+7+10+\ldots+(3n-2)$$

Esta expresión se lee: "Es la suma de los primeros n términos de la sucesión $a_k = 3k - 2$, con $k = 1,2,\ldots,n$" .

Si se tiene una suma con una cantidad de términos demasiado grande, ¿se la puede 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 (Σ), se usa para representar la suma de los n primeros términos de una sucesión cuando se conoce su término general a_k . Se escribe:

$$a_1 + a_2 + a_3 + \ \ldots + a_n \ = \sum_{k=1}^{n} a_k$$

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 no necesariamente tiene que ser 1, puede ser cualquier otro valor m siempre que $m < n$. En cuyo caso, la cantidad de términos de $\sum_{k=m}^{n} a_k$ es $n - m + 1$.

  Por ejemplo, la cantidad de términos de $\sum_{k=0}^{n} a_k$ es $n + 1$.

- El valor de una suma no depende de la letra que se use como índice.

$$\sum_{k=m}^{n} a_k \;=\; \sum_{i=m}^{n} a_i \;=\; \sum_{j=m}^{n} a_j$$

- Se pueden sacar términos de una sumatoria, como consecuencia de la propiedad asociativa de la suma. Entonces, podemos expresarnos así:

$$\sum_{k=1}^{n} a_k = a_1 + \sum_{k=2}^{n} a_k = \sum_{k=1}^{n-1} a_k + a_n$$

❐Ejemplos 4.8

i) La suma de los siete primeros términos de la sucesión $a_k = 3k$, con $k = 1,2,..,7$ se puede expresar de dos maneras:

$$3 + 6 + 9 + 12 + 15 + 18 + 21 \qquad o \qquad \sum_{k=1}^{7} 3k$$

ii) La suma de los seis primeros términos de la sucesión $a_k = \frac{k}{k+1}$, con $k = 1,2,..,6$ se puede expresar de dos maneras:

$$\frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \frac{4}{5} + \frac{5}{6} + \frac{6}{7} \qquad o \qquad \sum_{k=1}^{6} \frac{k}{k+1}$$

iii) La suma de los seis primeros términos de la sucesión $a_k = 5(-1)^k.2^k$ con $k = 0,2,..,5$ se puede expresar de dos maneras:

$$5 - 10 + 20 - 40 + 80 - 160 \qquad o \qquad \sum_{k=0}^{5} 5(-1)^k.2^k$$

Actividad 4.4

a) Decir cuántos términos tienen las siguientes sumas y luego desarrollarlas:

i) $\sum_{j=1}^{n-1} \left(\frac{j}{2}\right)$ ii) $\sum_{k=2}^{n}(3k-2)$ iii) $\sum_{i=3}^{n+1} (-2)^i$

b) Usar el símbolo Σ para representar a cada suma considerando que todas tienen n términos

i) $\frac{5}{4} + \frac{7}{9} + \frac{9}{16} + \frac{11}{25} + \cdots$

ii) $(a+\sqrt{b})+(a+2\sqrt{b})+(a+3\sqrt{b})+(a+4\sqrt{b})+(a+5\sqrt{b})+\cdots$

iii) $(1+\sqrt{b})+(2+3\sqrt{b})+(3+5\sqrt{b})+(4+7\sqrt{b})+(5+9\sqrt{b})+\cdots$

4.5 Inducción Matemática

Peano G. (1858–1932) propuso cinco propiedades fundamentales que caracterizan a los Números Naturales, conocidas 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 como por ejemplo demostrar que un algoritmo con ciclos funciona como se espera.

Principio de Inducción Matemática

Sean $n, n_o \in \mathbb{Z}$ y sea $P(n)$ un predicado en n.

Si se cumplen las siguientes condiciones:

a) $P(n_0)$ es verdadero (Paso básico)

b) $P(k) \Rightarrow P(k+1)$, $\forall k \geq n_0$ (Paso inductivo)

Entonces $P(n)$ es verdadero $\forall n \geq n_o \; con \; n, n_o \in \mathbb{Z}$

¿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. La idea es colocarlas a una distancia tal que, si cae la primera, caen todas.

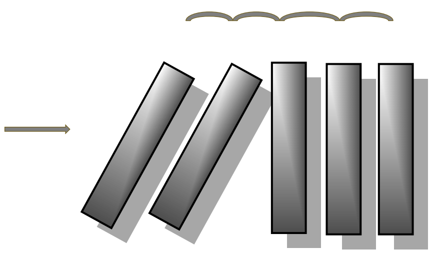


Fig. 4.2. Efecto dominó.

▢Ejemplo 4.9

Para demostrar que la suma de "n" números naturales consecutivos está dada por el semiproducto de "n" por su sucesor, o sea $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $\forall n \in \mathbb{N}$, se procede del siguiente modo:

Paso básico: Se demuestra que la igualdad vale para $n = 1$

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

$$1 = \frac{1.2}{2}$$

$$1 = 1$$

Paso Inductivo: Se demuestra que la igualdad se cumple para el siguiente de cualquier entero. Esto significa probar la implicación lógica:

$$P(k) \quad \Rightarrow P(k+1)\,,\ \forall k \in \mathbb{N}$$

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 $I = II$. Una de las maneras es trabajar con los dos miembros por separado.

$$I = \sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k^2 + k + 2k + 2}{2} = \frac{k^2 + 3k + 2}{2}$$

$$II = \frac{(k+1)(k+2)}{2} = \frac{k^2 + k + 2k + 2}{2} = \frac{k^2 + 3k + 2}{2}$$

Se observa que $I = II$. Por lo tanto queda demostrado que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad , \quad \forall n \in \mathbb{N}$$

Actividad 4.5

Interpretar la siguiente igualdad y demostrarla por medio del Principio de Inducción

$$\sum_{i=1}^{n} (3i-1) = \frac{n(3n+1)}{2} \quad , \quad \forall n \in \mathbb{N}$$

4.6 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

$$n! = n.(n-1)! \ \forall n \in \mathbb{N} \quad \text{con} \quad 0! = 1.$$

Observar que, por ejemplo, en el caso de $6!$ se necesita el valor de $5!$ ya que $6! = 6\,.5!$ lo que nos lleva a necesitar el valor de $4!$, ya que $5! = 5\,.4!$ y asi sucesivamente se tendrá que

$$6! = 6\,.5\,.4\,.3\,.2\,.1\,.0! = 6\,.5\,.4\,.3\,.2\,.1$$

Por lo expuesto se deduce que la función factorial es recursiva.

Definición

Se dice que (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 $f: \mathbb{R}^k \longrightarrow \mathbb{R}$ y k valores iniciales, $a_1, a_2, \dots, a_k$, se define una sucesión en forma recursiva de orden $k \in \mathbb{N}$ de la siguiente manera:

$$\begin{cases} a_1, a_2, \dots, a_k \text{ conocidos} & \text{(condiciones iniciales)} \\ a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-k}), \quad n \geq k+1 & \text{(fórmula de recurrencia)} \end{cases}$$

Observaciones

- La fórmula que define a las sucesiones en forma recursiva recibe también el nombre de ley de recurrencia, ecuación de recurrencia o ecuación en diferencias.
- El número de condiciones iniciales: k, puede ser cualquiera, pero siempre como mínimo debe haber una condición inicial.
- El primer valor puede tener cualquier subíndice, lo más usual es 1 o 0.

Ejemplos 4.11

i) La fórmula recursiva de la sucesión aritmética 2, 4, 6, 8, 10,… es:

$$\begin{cases} a_1 = 2 \\ a_n = a_{n-1} + 2, \; n \geq 2 \end{cases}$$

ii) La fórmula recursiva de la sucesión aritmética 3, 8, 13, 18, 23,… es

$$\begin{cases} b_0 = 3 \\ b_n = b_{n-1} + 5, \; n \geq 1 \end{cases}$$

iii) La fórmula recursiva de la progresión geométrica 3, 9, 27, 81,… es

$$\begin{cases} b_0 = 3 \\ b_n = 3b_{n-1}, \; n \geq 1 \end{cases}$$

iv) Los primeros cinco términos de la sucesión:

$$\begin{cases} c_1 = 1 \\ c_2 = 1 \\ c_n = c_{n-1} + c_{n-2}, \ \ n \geq 3 \end{cases}$$

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, es decir encontrar la fórmula explícita correspondiente.

Actividad 4.6

a) Encontrar los seis primeros términos de la sucesión definida por

$$\begin{cases} c_n = -2c_{n-1} \\ c_0 = 5 \end{cases} \ , \ \ \forall n \in \mathbb{N}$$

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 , …

iii) -1 , 4 , -16 , 64 , -256 , ...

4.6.1 Solución de una Relación de Recurrencia

Definición

Una sucesión recibe el nombre de solución de una relación de recurrencia si su término general, expresado mediante la fórmula explícita, verifica a dicha relación y a sus condiciones iniciales.

Ejemplos 4.12

1) Sean las sucesiones

S_1: 2 , 8 , 32 , 128 , ... y S_2 : 3 , 12 , 48 , 192 , ...

En ambos casos la relación de recurrencia que las identifica es: $a_{n+1} = 4\, a_n$

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:

$$S_1 : \begin{cases} a_1 = 2 \\ a_{n+1} = 4\, a_n \end{cases} \quad \text{y} \quad S_2 : \begin{cases} a_1 = 3 \\ a_{n+1} = 4\, a_n \end{cases} \text{ en ambos casos para } n \in \mathbb{N}$$

Expresando los cuatro primeros términos de cada una se tiene:

Para S_1	Para S_2
$a_1 = 2$	$a_1 = 3$
$a_2 = 2\,.4$	$a_2 = 3\,.4$
$a_3 = 2\,.4\,.4 = 2\,.\,4^2$	$a_3 = 3\,.4\,.4 = 3\,.\,4^2$
$a_4 = 2\,.4\,.4\,.4 = 2\,.\,4^3$	$a_3 = 3\,.4\,.4.4 = 3\,.\,4^3$

De aquí se induce que las soluciones generales de las sucesiones S_1 y S_2 son, respectivamente:

$$a_n = 2\,.\,4^{n-1} \;\; \forall n \in \mathbb{N} \qquad \text{y} \qquad a_n = 3\,.\,4^{n-1} \;\; \forall n \in \mathbb{N}$$

Se observa que difieren solamente en el coeficiente que multiplica a la potencia de 4.

2) Para verificar que $a_n = 3\,n + 6$, $\forall n \in \mathbb{N}_0$ es solución de la relación de recurrencia $a_n = 2a_{n-1} - a_{n-2}$ con las condiciones iniciales $a_0 = 6$ y $a_1 = 9$ se debe comprobar que la formula se verifica para los valores iniciales y por el elemento genérico.

Para los valores iniciales se tiene:

$a_0 = 3\,.0 + 6 = 6$ y $a_1 = 3\,.1 + 6 = 9$

Luego para verificar que $a_n = 3\,n + 6$ 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 en $a_n = 2a_{n-1} - a_{n-2}$ se tiene:

$$3\,n + 6 \;=\; 2\,.(3n+3) \,-\, 3n \;=\; 6n + 6 - 3n \;=\; 3n + 6$$

Queda demostrado que la formula explícita satisface a los valores iniciales y a 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

$$a_n = -\tfrac{1}{2} a_{n-1} \quad , \forall n \in \mathbb{N} \text{ con valor inicial } a_0 = 1$$

2) Determinar cuál de las siguientes fórmulas es solución de la ecuación 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) $a_n = (-2)^n + (-5)^n$, $\forall n \in \mathbb{N}$

4.7 Clasificación de las Relaciones de Recurrencia

Definiciones

■ 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.

■ 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 depende de n. Por el contrario, si alguno depende de n, se dice que es una ecuación de coeficientes variables.

Ejemplos 4.13

i) La relación de recurrencia $b_n = 2b_{n-1} + 3$ es de orden 1 porque la diferencia entre n y $(n-1)$ es 1, es de grado 1 o lineal, es no homogénea pues $b_n = 0$ no satisface la ecuación y de coeficientes constantes.

ii) La relación de recurrencia $a_n = 2a_{n-1} + a_{n-2}$ es de orden 2, lineal, homogénea y de coeficientes constantes.

iii) La relación de recurrencia $a_n^2 = a_{n-1} - 3$ es de orden 1, grado 2, no homogénea y de coeficientes constantes.

iv) La relación de recurrencia $2a_n = n^2 . a_{n-2}$ es de orden 2, lineal, homogénea y de coeficientes variables.

Actividad 4.8

Clasificar las siguientes relaciones de recurrencia:

a) $a_{n+1} = 4 . a_n$

b) $c_n = \frac{1}{2} c_{n-1} - c_{n-2}$

c) $a_n = 4 . a_{n-1} + 5$

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 a dos tipos de relaciones de recurrencia muy frecuentes.

4.7.1 Solución de las Relaciones de Recurrencia Lineales, de Primer Orden, Homogéneas y de coeficientes constantes.

Teorema

Sea (a_n) dada por su relación de recurrencia lineal, homogénea, de primer orden: $a_n = k\,.\,a_{n-1}$, con k constante no nula y con condición inicial a_1. Entonces la solución general está dada por:

$$a_n = a_1\,.\,k^{n-1} \quad , \quad \forall \mathrm{n} \in \mathbb{N}$$

Observación

Si la relación de recurrencia estuviera dada por $a_n = k\,.\,a_{n-1}$ con condición inicial a_0 entonces la solución general estaría dada por:

$$a_n = a_0\, k^n \quad , \quad \forall n \in \mathbb{N}_0$$

Ejemplos 4.14

1) La solución general de $a_{n+1} = 3\,.\,a_n$ con el valor inicial $a_0 = 2$ es

$$a_n = 2\,.\,3^{\mathrm{n}} \;,\; \forall \mathrm{n} \in \mathbb{N}_0$$

2) La relación de recurrencia $3a_{n+1} - 5a_n = 0$ con $a_1 = 4$ es equivalente a $a_{n+1} = \frac{5}{3}a_n$ y tiene por solución general a $a_n = 4\,.\left(\frac{5}{3}\right)^{n-1}$, $\forall n \in \mathbb{N}$.

Actividad 4.9

Resolver las siguientes relaciones de recurrencia:

a) $a_{n+1} = -4\,.\,a_n$ con condición inicial $a_0 = -1$

b) $2b_n + 3\,b_{n-1} = 0$ con condición inicial $b_1 = 4$

c) $c_n = \frac{1}{2}c_{n-1}$ con condición inicial $c_1 = -2$

4.7.2 Solución de las Relaciones de Recurrencia Lineal, de Segundo Orden, Homogéneas y con coeficientes constantes

Teorema

Sea (a_n) dada por su relación de recurrencia lineal, homogénea, de segundo orden, y de coeficientes constantes,

$$a_{n+2} + k_1 a_{n+1} + k_2 a_n = 0 \ , \ \forall n \in \mathbb{N}$$

Si se consideran las raíces de la ecuación: $x^2 + k_1 x + k_2 = 0$, llamada ecuación característica de la relación de recurrencia, se puede demostrar que la solución general será de alguno de los siguientes tipos:

$i)\ a_n = u \,.\, r_1^n + v \,.\, r_2^n \ , \ \forall n$ en el caso de que la ecuación característica tenga dos raíces reales y distintas, r_1 y r_2

$ii)\ a_n = u \,.\, r^n + n \,.\, v \,.\, r^n \ , \ \forall n$ en el caso de que la ecuación característica tenga dos raíces reales e iguales , $r_1 = r_2 = r$.

En ambos casos u y v son constantes a determinar por las condiciones iniciales.

Ejemplos 4.15

1) $a_n - 5\, a_{n-1} + 6\, a_{n-2} = 0$ con $a_0 = 3$ y $a_1 = 5$

Su ecuación característica es $x^2 - 5x + 6 = 0$, cuyas raíces son $r_1 = 2$ y $r_2 = 3$

Entonces, por el teorema, la solución general es del tipo : $a_n = u \,.\, 2^n + v \,.\, 3^n$ y ahora solo queda calcular u y v teniendo en cuenta las condiciones iniciales

$$\begin{array}{lll} a_0 = 3 \ \Rightarrow \ u \,.\, 2^0 + v .\, 3^0 = 3 \ \Rightarrow & \multirow{2}{*}{} \\ a_1 = 5 \ \Rightarrow \ u \,.\, 2^1 + v .\, 3^1 = 5 \ \Rightarrow & \end{array} \begin{cases} u + v = 3 \\ 2u + 3v = 5 \end{cases}$$

La solución del sistema es $u = 4$ y $v = -1$

Por lo tanto, la solución general de la relación de recurrencia propuesta es

$$a_n = 4 \,.\, 2^n - 3^n \ , \ \forall \mathrm{n} \in \mathbb{N}_0$$

2) $a_{n+2} = 4\,a_{n+1} - 4\,a_n = 0$ 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, la solución general es del tipo:

$a_n = u\,.\,2^n + n.v\,.\,2^n$. A continuación se calculan u y v teniendo en cuenta las condiciones iniciales:

$$\begin{array}{lll} a_1 = -3 & \Longrightarrow & u\,.\,2^1 + 1\,.\,v.\,2^1 = -3 \\ a_2 = 2 & \Longrightarrow & u\,.\,2^2 + 2\,.\,v\,.\,2^2 = 2 \end{array} \Longrightarrow \begin{cases} 2u + 2v = -3 \\ 4u + 8v = 2 \end{cases}$$

Resolviendo el sistema se determina que: $u = -\frac{7}{2}$ y $v = 2$

Por lo tanto, la solución general de la relación de recurrencia:

$$a_{n+2} = 4\,a_{n+1} - 4\,a_n = 0 \text{ con } a_1 = -3 \text{ y } a_2 = 2 \text{ es}$$

$$a_n = -\frac{7}{2}\,.\,2^n + 2\,n\,.\,2^n \quad , \quad \forall n \in \mathbb{N}$$

Note que, por medio de las propiedades de la potenciación y del producto, la solución también se la puede escribir como:

$$a_n = -\frac{7}{2}\,.\,2^n + n\,.\,2^{n+1} \quad , \quad \forall n \in \mathbb{N}$$

O bien: $$a_n = 2^n\left(-\frac{7}{2} + 2\,n\right) \quad , \quad \forall n \in \mathbb{N}$$

Actividad 4.10

Encontrar la solución general para las siguientes relaciones de recurrencia:

1) $a_n + a_{n-1} - 6\,a_{n-2} = 0$ con $a_1 = 1$ y $a_2 = 3$

2) $c_n - 6\,c_{n-1} + 9\,c_{n-2} = 0$ con $c_0 = 1$ y $c_1 = 2$

3) $b_{n+2} - \frac{5}{2}b_{n+1} - \frac{3}{2}\,b_n = 0$ con $b_0 = -1$ y $b_1 = 1$

Capítulo 5. GRAFOS Y DIGRAFOS. ÁRBOLES

Grafo no dirigido. Subgrafo.

Caminos en un grafo no dirigido.

Representaciones matriciales de un grafo

Grafos Especiales.

Caminos y Circuitos de Euler.

Caminos y Ciclos de Hamilton.

Isomorfismo de grafos.

Árbol no dirigido.

Digrafo o Grafo dirigido.

Caminos en Digrafos.

Representaciones matriciales de un dígrafo.

Grafo asociado o subyacente a un dígrafo.

Árbol dirigido y Árbol dirigido con raíz.

Árboles binarios posicionales (ABP). Recorridos de ABP.

Introducción

La Teoría de Grafos constituye uno de los temas más importantes de la Matemática Discreta. Esta parte de las matemáticas tiene un claro origen y comienzo en un trabajo publicado en 1736 por el matemático suizo L. Euler (1707-1783) en el problema conocido como “los siete puentes de Königsberg”.

En sus comienzos, la Teoría de Grafos, aparecía bastante insignificante, puesto que se ocupaba principalmente de pasatiempos y rompecabezas. En la actualidad han surgido muchas aplicaciones a cuestiones de carácter práctico, como por ejemplo: emparejamiento, problemas de transporte, flujo de redes (programación), problemas de carácter combinatorio, etc. Pues ante el planteo de una situación problemática, se tiende a hacer un diagrama en el que se representa por medio de puntos las actividades a realizar, o las etapas de un proyecto, localidades o individuos, etc., uniéndolos por medio de líneas o flechas si es que existe alguna relación entre ellos. Por tal motivo, son numerosos los problemas que pueden ser modelados con grafos. Se pueden utilizar también para determinar la implementación o no de un circuito sobre una placa de una sola capa, para diferenciar dos compuestos químicos que tengan la misma fórmula molecular, pero distinta estructura; para estudiar las estructuras de redes en Internet, redes neuronales, análisis de los diferentes algoritmos ya existentes, manejo de las estructuras de datos, creación de los diferentes sistemas operativos manejados hoy en día, entre otras aplicaciones.

Mucho se ha avanzado desde entonces y son varios los resultados importantes que se afianzaron desde el siglo XIX.

A continuación se darán las definiciones, pero se advierte al lector que la terminología utilizada en la teoría de grafos aún no está estandarizada.

5.1 Grafo no dirigido

Definición

Dados dos conjuntos finitos V y A se llama grafo a toda terna $G = (V, A, \varphi)$ tal que: i) $V \neq \emptyset$,

ii) $\varphi : A \to V^{(2)}$, donde $V^{(2)} = \{H \subseteq V\ ,\ |H| = 1\ o\ |H| = 2\}$

A los elementos del conjunto V se les llama vértices o nodos, a los elementos del conjunto A se les llama aristas o lados y φ es llamada 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

Para el diseño del grafo se eligen, en el plano, ubicaciones arbitrarias para los vértices y formas cualesquiera para las aristas. La representación gráfica del mismo consiste en representar: a los elementos del conjunto V, por medio de puntos o círculos; al conjunto A y a la función de incidencia φ 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 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 $\varphi(a_2) = \{ v \}$

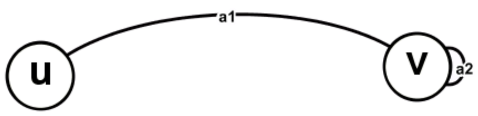


Fig. 5.0. Representación de vértices y aristas

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 φ 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 φ de Ejemplo 5.1.

La Figura 5.1 es la representación de G

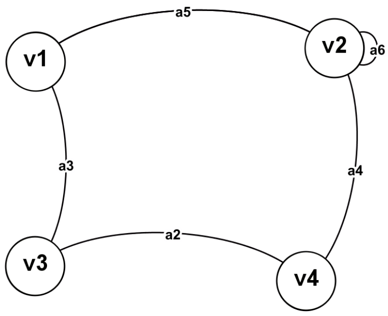


Fig. 5.1. Representación del Grafo de Ejemplo 5.1.

Observación

Los conceptos geométricos como posición, longitud y formas no tienen relevancia 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 φ (a_1) = φ (a_2) entonces a_1 y a_2 se dicen aristas paralelas

■ Si φ (a_1) ≠ φ (a_2) y φ (a_1) ∩ φ (a_2) ≠ ∅ 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 de si mismo. Además 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 $G = (V, A, \varphi)$. Se denomina grado o valencia de un vértice, y se denota $g(v)$, a la función $g: V \rightarrow \mathbb{N}_0$ tal que $g(v)$ es 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, φ) 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 φ 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}
φ(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 φ 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, φ). Se dice que G_1= (V_1, A_1, φ_1) es un subgrafo del grafo G si y solo si: i) $V_1 \subseteq V$; ii) $A_1 \subseteq A$ y iii) $\varphi_1 = \varphi / A_1$ siendo φ_1 es la restricción de la función φ al conjunto A_1

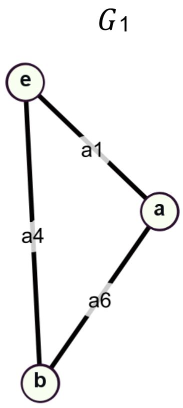
Ejemplo 5.3

Dada la Figura 5.2, observar que G_1 es un subgrafo de G, dado que:

i) $V_1 \subseteq V$ ya que {a, b, e} ⊆ { a , b , c , d , e , f };

ii) $A_1 \subseteq A$ ya que { a_1, a_4, a_6 } ⊆ {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) $\varphi_1 = \varphi / A_1$



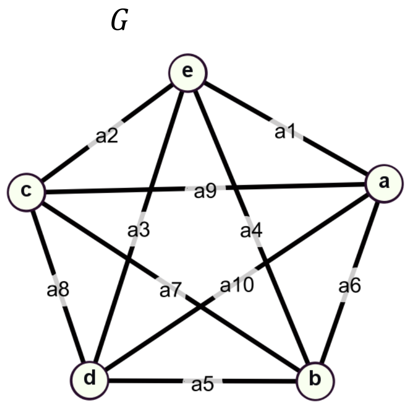


Fig. 5.2. G_1 subgrafo de G

5.2.1 Subgrafos particulares

Definición

Sean $G = (V, A, \varphi)$, $v \in V$ y $a \in A$:

■ Si se suprime v y todas las aristas que inciden en él, el subgrafo resultante se denota $\tilde{G}_v$

■ Si se suprime a, el subgrafo resultante 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 G de la Figura 5.3

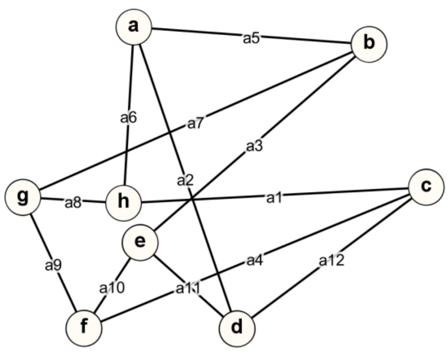


Fig. 5.3. Grafo G

Las Figuras 5.4 a 5.7 representan subgrafos de él:

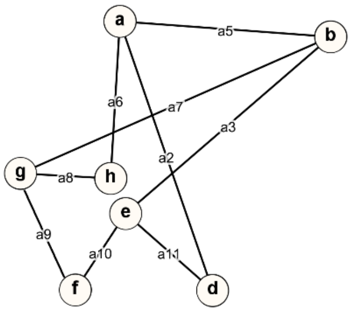


Fig. 5.4. Subgrafo $\tilde{G}_c$.

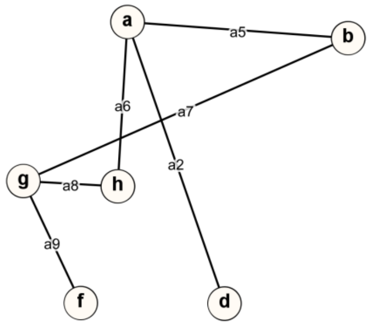


Fig. 5.5. Subgrafo $\tilde{G}_{\{c,e\}}$.

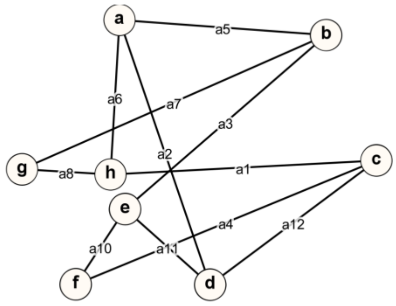


Fig. 5.6. Subgrafo $\tilde{G}_{a_9}$.

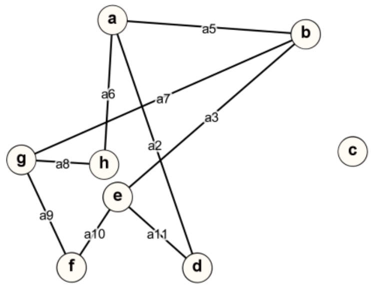


Fig. 5.7. Subgrafo $\tilde{G}_{\{a_1,a_4,a_{12}\}}$.

Actividad 5.2

a) Dado el grafo $G = (V, A, \varphi)$

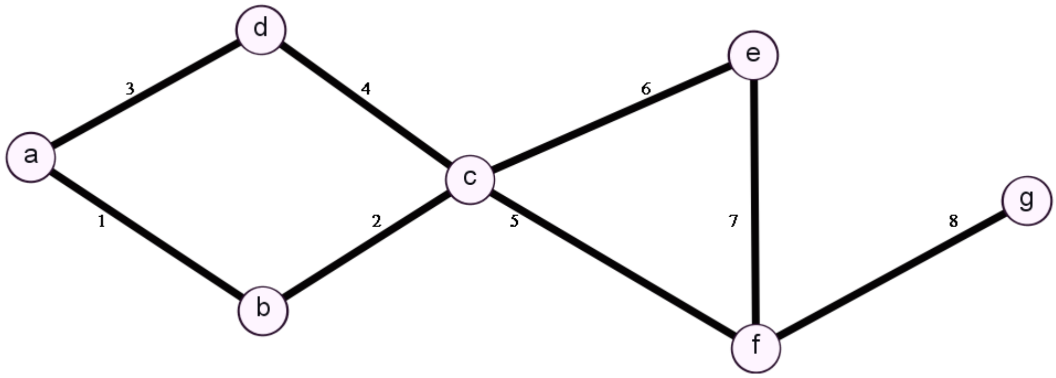


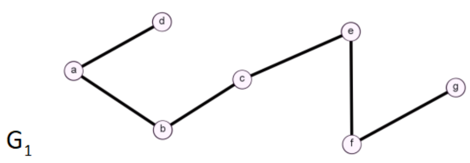
Fig. 5.8. Representación de G.

Obtener los siguientes subgrafos de G

i) $\tilde{G}_{\mathrm{c}}$ ii) $\tilde{G}_8$

iii) $\tilde{G}_{\{\mathrm{a,e,g}\}}$ iv) $\tilde{G}_{\{4,5,6\}}$

b) Indicar si los siguientes grafos son subgrafos de G



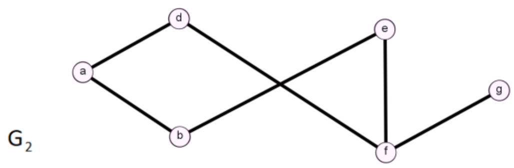


Fig. 5.9. Grafo G_1 .

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.

■ La longitud de un camino es el número de aristas intervinientes.

■ Un camino es cerrado si el último vértice de la secuencia es igual al primero. En caso contrario el camino se dice abierto.

Simbólicamente al camino se lo expresa por medio de la secuencia de aristas involucradas, a_1 , a_2, … , a_n ; o por la secuencia de vértices extremos de dichas aristas v_1, v_2 , v_3 , … , 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:

$$v_1, a_1, v_2, a_2, v_3, \ldots, v_n, a_n, v_{n+1}$$

Ejemplo 5.5

Dado el grafo simple de la 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.

Un problema interesante sería determinar cuántos caminos de longitud 5 que comiencen en el vértice 4 existen en el grafo. Más adelante se verá un teorema que dará la respuesta.

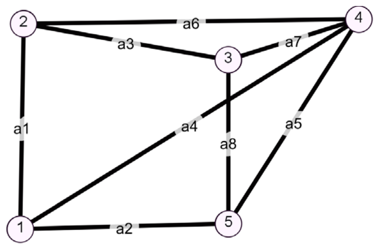


Fig. 5.11. Grafo Ejemplo 5.5.

Definición

Se dice que un camino es simple sí 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 de la Figura 5.12

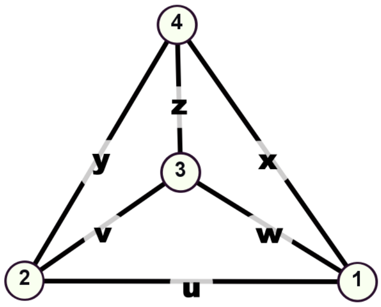


Fig. 5.12. Grafo G.

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 $G = (V, A, \varphi)$

• 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.

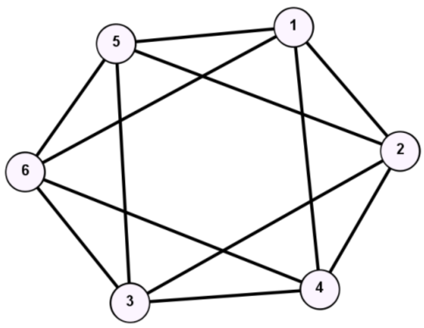


Fig. 5.13. Grafo de la Actividad 5.3.

	Camino	Camino simple abierto	Camino elemental	Circuito	Ciclo	Longitud
1,5,2,3,4	sí	sí	sí	no	no	4
6,3,4,5,3,6						
1,4,2,5,3,2,4,6,1						
5,1,2,5,3,2,4,6						
1,4,6,3,5,2,1						
6,4,3,6,1,2						
2,5,3,6,4,1,5,6,1,2						

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:

$$m_{ij} = \begin{cases} 1 & \text{si } v_i \text{ y } v_j \text{ son adyacentes} \\ 0 & \text{en otro caso} \end{cases}$$

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 1 si los vértices correspondientes a la fila y a la columna de dicho elemento son adyacentes, y 0 en caso contrario.

Observaciones

- La matriz de adyacencia es una matriz booleana, cuadrada y simétrica.
- Los lazos están representados por unos en la diagonal principal. Si un vértice es aislado, tendrá la fila y columna correspondientes llenas de ceros.
- La matriz de adyacencia no permite representar aristas paralelas.
- Si el grafo es simple, el grado de cada vértice estaría dado por la suma de la fila o la columna correspondiente.

Propiedad de la Matriz de Adyacencia

Si M_a es la matriz de adyacencia de un grafo simple, el elemento ij de $M_a^k = M_a$ x M_a x...x M_a (k veces) representa la cantidad de caminos diferentes de longitud "k" del vértice i al vértice j. (x es el producto usual de matrices)

Ejemplo 5.9

Dado el grafo de la Figura 5.14

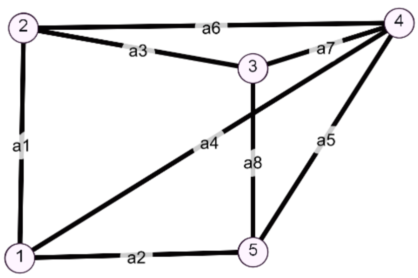


Fig. 5.14. Grafo G.

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 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 x 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 la ideal para representar todo tipo de grafos.

Ejemplo 5.10

Observando el grafo de la Figura 5.14, su 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 φ dada por tabla 5.4

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 φ

i) Representar gráficamente y determinar las correspondientes matrices.
ii) Calcular la cantidad de caminos de longitud 3 del vértice b al e. Expresar las sucesiones que los representan.
iii) Hay circuitos? De que longitud?. Describa al menos dos
iv) Hay ciclos? De que longitud? Describa al menos dos

5.6 Grafos especiales

5.6.1 Grafos conexos

Definición

$G = (V, A, \varphi)$ es conexo si y solo si existe un camino de cualquier longitud entre cualquier par de vértices. Caso contrario, se dice no conexo (o disconexo).

Si V = { v } , de acuerdo a la definición de camino, G es conexo

Ejemplo 5.11

El grafo de la Figura 5.15 es conexo mientras que el de la Figura 5.16 es no conexo

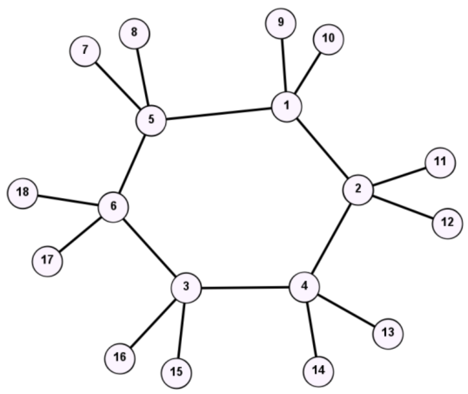


Fig. 5.15. Grafo Conexo.

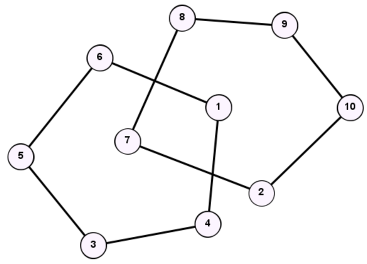


Fig. 5.16. Grafo no conexo.

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 doce 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 G 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) $\tilde{G}_5$ es conexo

iv) $\tilde{G}_d$ no es conexo

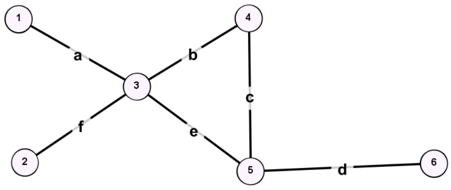


Fig. 5.17. Grafo G

5.6.2 Grafo completo

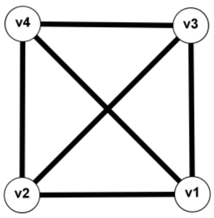
Definición

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

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



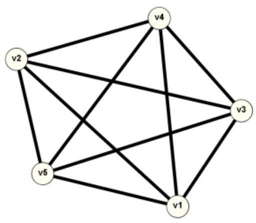


Fig. 5.18. Grafo K4. Fig. 5.19. Grafo K4.

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 conectado con todos los vértices de V_2, entonces G se dice bipartito completo. En este caso, si $|V_1| = n$ y $|V_2| = m$, el grafo se denota por $K_{n,m}$

Cantidad de aristas de $K_{n,m}$: $|A| = n.m$

Ejemplo 5.14

El grafo G de la Figura 5.20 es bipartito no completo mientras que el de la Figura 5.21 es el grafo bipartito completo $K_{3,4}$

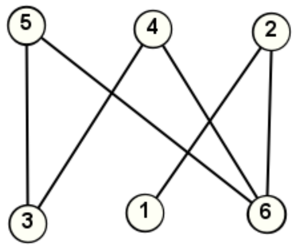


Fig. 5.20. Grafo G.

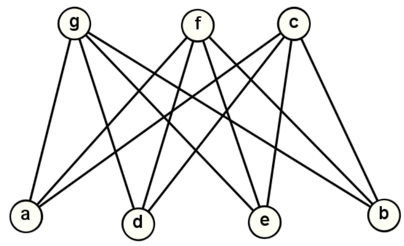


Fig. 5.21. Grafo $K_{3,4}$.

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.

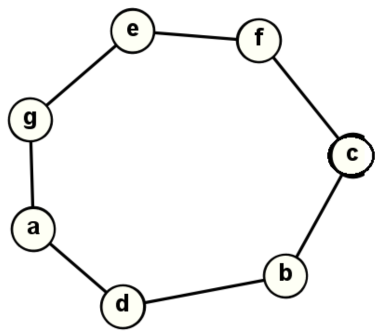


Fig.5.22. Grafo 2-regular.

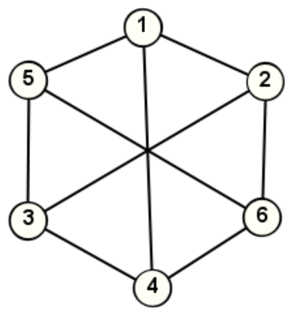


Fig. 5.23. Grafo 3-regular

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 vértices istmos y/o aristas puentes.

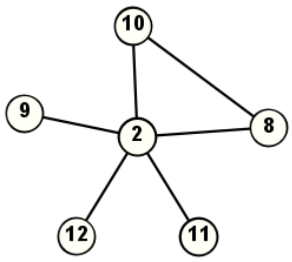


Fig. 5.24. Grafo G_1.

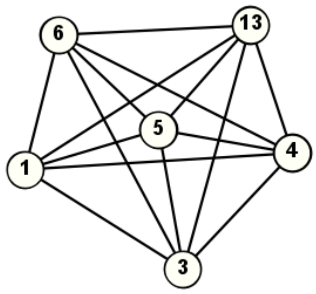


Fig. 5.25. Grafo G_2.

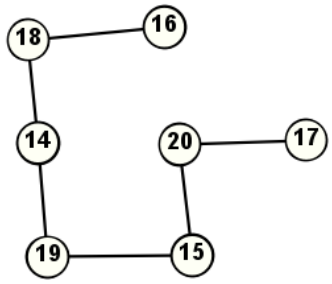


Fig. 5.26. Grafo G_3.

5.7 Caminos y circuitos de Euler

Durante el siglo XVIII, en la ciudad de Königsberg (hoy Kaliningrado) se planteó un famoso problema conocido como el problema de los puentes de Königsberg. 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.

La respuesta al problema 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.

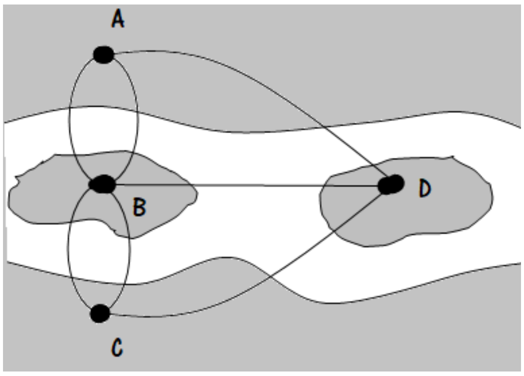


Fig. 5.27. Modelo de los puentes de Königsberg

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 cubre 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 G de la Figura 5.28 posee al menos dos caminos de Euler:

1 , 5 , 2 , 1 , 6 , 2 , 3 , 6 , 4 , 3 , 5 , 4

4 , 6 , 2 , 5 , 1 , 2 , 3 , 5 , 4 , 3 , 6 , 1

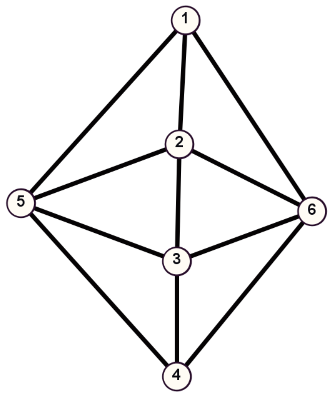


Fig. 5.28. Grafo G

Se puede comprobar que este grafo no posee circuito de Euler, no hay modo de recorrerlo 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 circuitos de Euler.

Teorema

Sea $G = (\mathrm{V}, \mathrm{A}, \varphi)$, se dice que

■ 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

Sean los grafos de las Figuras 5.29 y 5.30

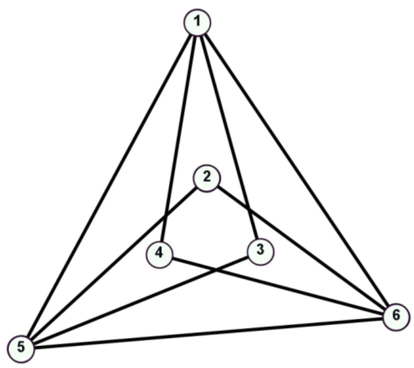


Fig. 5.29. Grafo G_1.

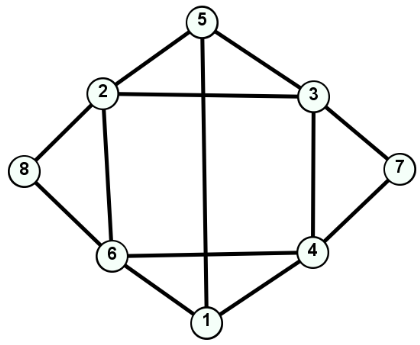


Fig. 5.30. Grafo G_2.

El grafo G_1 (Figura 5.29) posee circuito de Euler, porque todos los vértices tienen grado par, uno de ellos es: 1, 6, 5, 2, 6, 4, 1, 3, 5, 1.

El grafo G_2 (Figura 5.30) posee camino de Euler, porque hay exactamente dos vértices (1, 5) de grado impar; un camino es: 5, 1, 4, 7, 3, 5, 2, 8, 6, 4, 3, 2, 6, 1.

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

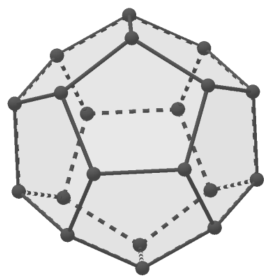


Fig.5.31. Dodecaedro.

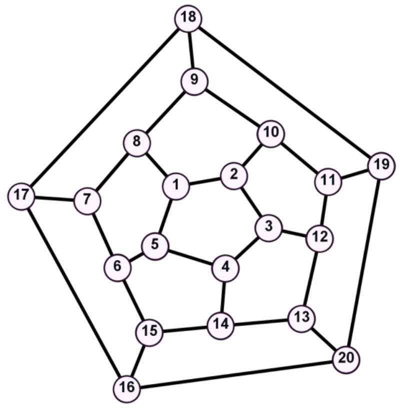
vértices que representaban a importantes ciudades del mundo : Bruselas, Cantón, Delhi, Frankfurt, etc.

El dodecaedro, figura tridimensional, se encuentra plasmado en la Figura 5.31

El juego consistía en encontrar un recorrido que pase exactamente una vez por cada ciudad, y volver a la ciudad de partida.

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 G posee un camino de Hamilton si y solo si posee un camino elemental que contiene todos los vértices de G.

■ Un camino de Hamilton cerrado es un ciclo de Hamilton.

Ejemplos 5.18

i) 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

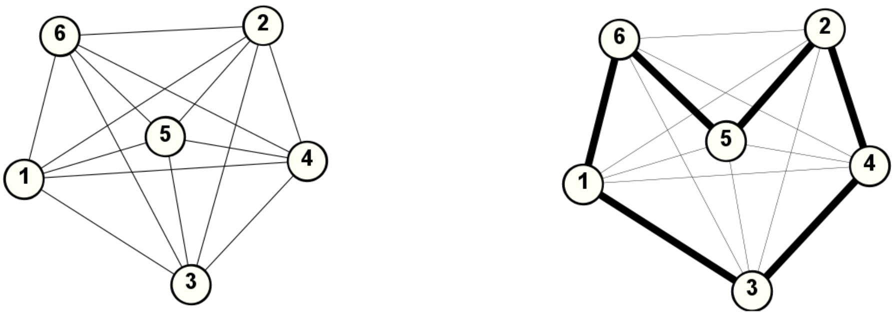


Fig.5.33. Grafo K_6 y un Ciclo de Hamilton

ii) 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

G_1

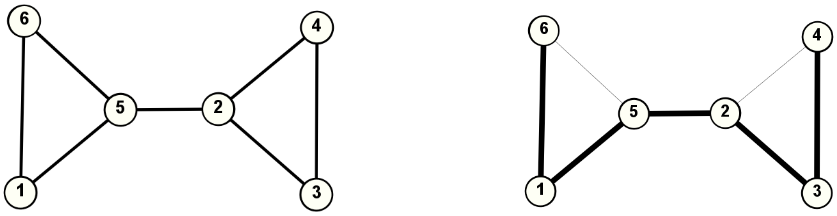


Fig. 5.34. Grafo G_1 y un Camino hamiltoniano en para él

iii) 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

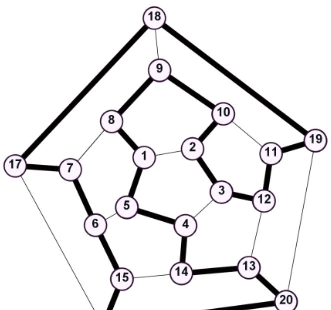


Fig. 5.35. Una solución para el Grafo de Hamilton

5.8.1 Condiciones Suficientes para la existencia de caminos y ciclos de Hamilton

Teorema

Sea $G = (\mathrm{V}, \mathrm{A}, \varphi)$ un grafo simple con tres o mas vértices. Se cumple que

- 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 Circuitos de Euler y Ciclos de Hamilton.
- En cada grafo obtener ambos, siempre que existan.

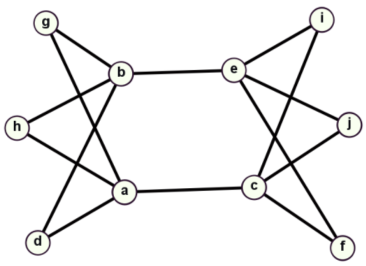


Fig. 5.36. Grafo G_1.

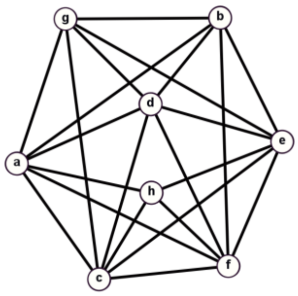


Fig. 5.37. Grafo G_2.

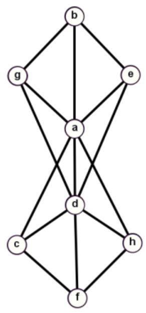


Fig. 5.38. Grafo G_3.

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 $f: V_1 \to V_2$ y $g: A_1 \to A_2$ tales que $\forall\, a \in A_1$, $\varphi_2\big(g(a)\big) = f(\varphi_1(a))$.

Si no hay aristas paralelas, entonces para que G_1 y G_2 sean isomorfos es suficiente que:

$$\forall\, v_1, v_2 \in V_1 \quad , \quad \{v_1,\, v_2\} \in A_1 \quad \Rightarrow \quad \{\, f(v_1)\, , f(v_2)\, \} \in A_2.$$

La definición expresa que hay isomorfismo entre G_1 y G_2 sí y solo si a vértices adyacentes de G_1 le corresponden vértices adyacentes en G_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.

Observaciones

- La correspondencia de vértices de un isomorfismo de grafos mantiene las adyacencias.
- Si los grafos no tienen aristas paralelas, entonces f determina de forma única a la función que se da entre las aristas. De ahí que, para dar un isomorfismo de grafos simples se da únicamente la función f .

5.9.1 Condiciones invariantes bajo isomorfismo

Hay cantidades que mantienen su valor entre grafos isomorfos. Ellas se dicen propiedades invariantes bajo isomorfismo, por ejemplo, “número de vértices y aristas”, “el grado de los vértices”, “caminos de determinada longitud”; “cantidad de ciclos de determinada longitud”, etc. Ellas 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, todo comportamiento que se observe en uno de ellos, en el otro también se debe observar.

Algunas condiciones invariantes bajo isomorfismo son: Tener la misma cantidad de vértices, la misma cantidad de aristas, tener la misma cantidad de vértices de determinado grado, tener la misma cantidad de ciclos de determinada longitud, tener la misma cantidad de aristas que incidan en vértices con determinados grados, etc.

Dado que las incidencias y adyacencias se deben conservar, se pueden usar las matrices de ambos grafos para mostrar que hay isomorfismo. Se tiene entonces el siguiente resultado.

Teorema sobre Isomorfismos

■ Dos grafos son isomorfos si y solo si las matrices de incidencia de ambos, para alguna disposición de sus vértices y aristas, son iguales.

■ En el caso de grafos simples, serán isomorfos si y solo si las matrices de adyacencia son iguales para un determinado orden de los vértices.

¿Cómo trabajar con estos conceptos?

- Se analiza primero si se cumplen las condiciones invariantes (necesarias pero no suficientes)
- Si alguna condición invariante no se cumpliera se deduce que los grafos no son isomorfos.
- Si se cumplen todas las condiciones invariantes analizadas entonces se aplica la definición: Se busca la función f que establece la correspondencia entre los vértices y se demuestra con ella que se preserva la adyacencia o bien se construye la matriz de adyacencia (en el caso de grafos con aristas paralelas) o la matriz de incidencia (en el caso de grafos con aristas paralelas) de ambos, de acuerdo a dicha correspondencia.

Ejemplo 5.19

Para averiguar si los grafos G_1 y G_2 de las Figuras 5.39 y 5.40 son isomorfos:

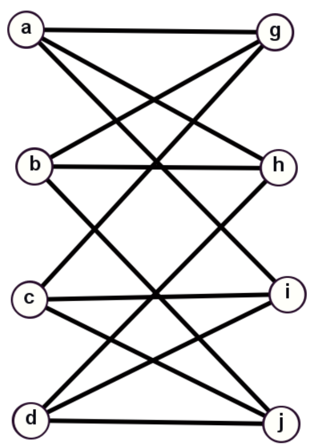


Fig. 5.39. Grafo G_1.

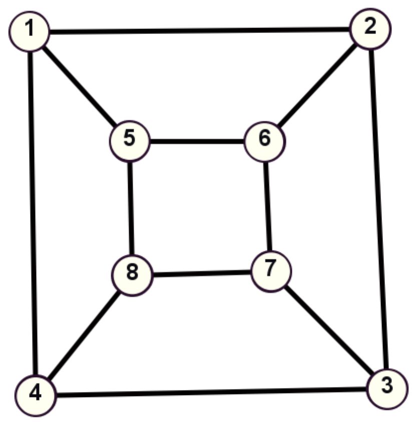


Fig. 5.40. Grafo G_2.

Siguiendo los pasos sugeridos, se observa:

- Igual cantidad de vértices en G_1 y G_2 : 8
- Igual cantidad de aristas en G_1 y G_2 : 12
- Igual cantidad de grados en los vértices de G_1 y G_2. Todos los vértices tienen grado 3.
- No hay lazos ni aristas paralelas en ninguno.
- No hay ciclos de longitud 3 en ninguno
- Ciclos de longitud 4 en G_1 y G_2

Entonces, cabe la posibilidad de que sean isomorfos, y para demostrarlo se busca una correspondencia entre los vértices que respete la adyacencia.

Se observa que, dado que todos los vértices tienen grado 3, la primera asignación seria indistinta por lo que se comienza eligiendo que $f(a) = 1$ por elegir una cualquiera. De allí en más se asigna a los vértices adyacentes al vértice a, vértices adyacentes a 1, por lo tanto se elige $f(g) = 5$, $f(h) = 2$, $f(\mathrm{i}) = 4$. (Observe que no es la única elección posible). Y así se sigue asignado de acuerdo a la adyacencia en cada grafo. Luego una posible función f sería:

$$f: V_1 \to V_2$$

$$f(a) = 1$$

$$f(g) = 5$$

$$f(b) = 6$$

$$f(h) = 2$$

$$f(d) = 3$$

$$f(j) = 7$$

$$f(c) = 8$$

$$f(i) = 4$$

Luego hay que verificar que f preserva la adyacencia, esto es, que se cumple

$$\{v_1,\, v_2\} \in A_1 \quad \Rightarrow \quad \{\, f(v_1)\,,\, f(v_2)\,\} \in A_2.$$

Hay 12 aristas, se deben hacer 12 verificaciones

$$\{a,g\} \in A_1 \quad \Rightarrow \quad \{\,1\,,5\,\} \in A_2$$

$$\{a,h\} \in A_1 \quad \Rightarrow \quad \{\,1\,,2\,\} \in A_2$$

$$\{a,i\} \in A_1 \quad \Rightarrow \quad \{\,1\,,4\,\} \in A_2$$

$$\{b,g\} \in A_1 \quad \Rightarrow \quad \{\,6\,,5\,\} \in A_2$$

$$\{b,h\} \in A_1 \quad \Rightarrow \quad \{\,6\,,2\,\} \in A_2$$

$$\{b,j\} \in A_1 \quad \Rightarrow \quad \{\,6\,,7\,\} \in A_2$$

$$\{c,g\} \in A_1 \quad \Rightarrow \quad \{\,8\,,5\,\} \in A_2$$

$$\{c,i\} \in A_1 \quad \Rightarrow \quad \{\,8\,,4\,\} \in A_2$$

$$\{c,j\} \in A_1 \quad \Rightarrow \quad \{\,8\,,7\,\} \in A_2$$

$$\{d,h\} \in A_1 \quad \Rightarrow \quad \{\,3\,,2\,\} \in A_2$$

$$\{d,i\} \in A_1 \quad \Rightarrow \quad \{\,3\,,4\,\} \in A_2$$

$$\{d,j\} \in A_1 \quad \Rightarrow \quad \{\,3\,,7\,\} \in A_2$$

Con este ejemplo se puede observar la ardua tarea de demostrar que se preserva la adyacencia, y se puede imaginar lo larga de la demostración si existieran cientos de aristas.

Una tarea menos ardua sería comprobar lo anterior usando la matriz de adyacencia de ambas, ordenando convenientemente los vértices de acuerdo a la función f definida entre los vértices.

$$M_{G1} = \begin{array}{c} \\ a \\ g \\ b \\ h \\ d \\ j \\ c \\ i \end{array} \begin{array}{c} \begin{array}{cccccccc} a & g & b & h & d & j & c & i \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \end{array} \qquad M_{G2} = \begin{array}{c} \\ 1 \\ 5 \\ 6 \\ 2 \\ 3 \\ 7 \\ 8 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & 5 & 6 & 2 & 3 & 7 & 8 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Como las matrices de adyacencia, para este orden de sus vértices, son iguales se infiere que los grafos G_1 y G_2 son isomorfos.

👁Observaciones

- Dadas dos matrices de adyacencias correspondientes a dos grafos, si 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: G2

a) G1

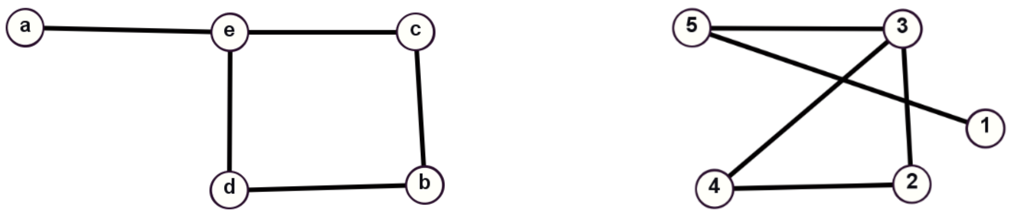


Fig. 5.41. Grafos G1 y G2.

b) G3 G4

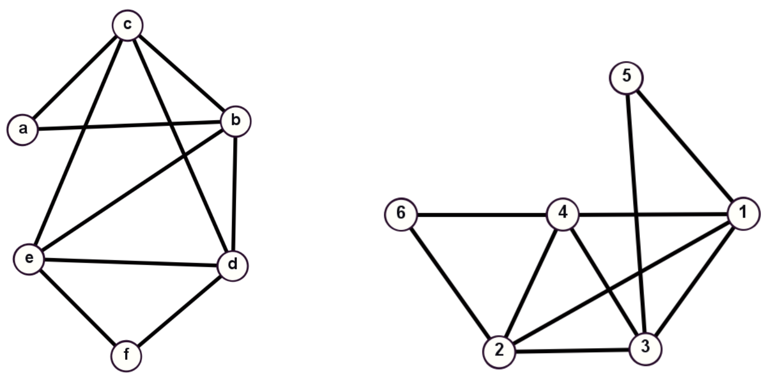


Fig. 5.42. Grafos G3 y G4.

c) G_5 G_6

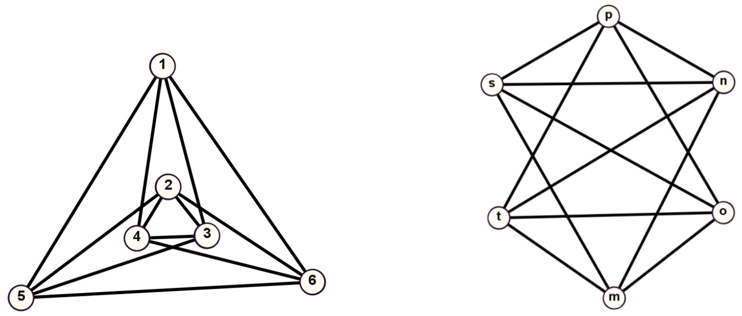


Fig. 5.43. Grafos G_5 y G_6.

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 poseen conexidad y no poseen ciclos.

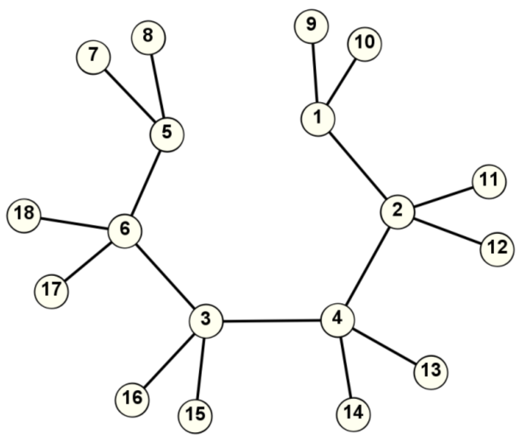


Fig. 5.44. Grafo G_1.

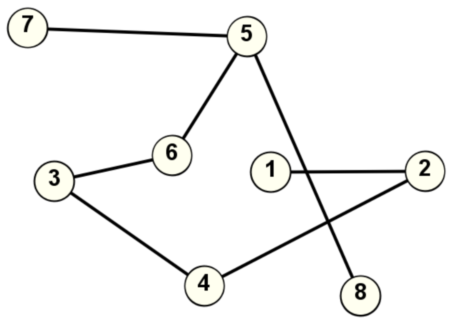


Fig. 5.45. Grafo G_2.

📚 **Definiciones**

■ $G = (V, A, \varphi)$ se dice árbol trivial si y solo si $|V|$=1.

■ Un vértice v se denomina hoja o vértice pendiente si y solo si $g(v) = 1$.

👁 **Propiedades**

Sea $G = (V, A, \varphi)$ un árbol.

- Un árbol es un grafo simple, pero no todo grafo simple es un árbol.
- Si se agrega una arista a un árbol, se genera un ciclo.
- Todas las aristas de un árbol son puentes.
- Todo vértice no pendiente es un istmo y recíprocamente.
- Si G no es el árbol 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

Verificación del cumplimiento del teorema anterior

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.

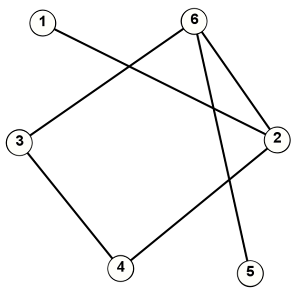


Fig. 5.46. Grafo G_1.

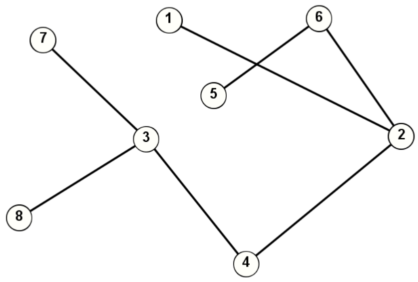


Fig. 5.47. Grafo G_2.

ii) Indicar Verdadero o Falso, justificando su respuesta

a) Existe un árbol de 10 vértices y 10 aristas

b) Si un grafo posee 10 vértices y 9 aristas entonces es un árbol

c) En un árbol todos los vértices son istmos y todas las aristas son puentes.

d) 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 cualesquiera tal que:

i) $V \neq 0$ y ii) $\varphi : A \rightarrow V \text{x} V$

donde a los elementos de V se les llama vértices o nodos, a los elementos de A aristas (lados o arcos) y la función φ 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

La representación de un digrafo es un diagrama que consiste en representar por puntos (o círculos) a los elementos de $\boldsymbol{V}$ y por flechas a los elementos de $\boldsymbol{A}$ de tal manera que si $\varphi(\boldsymbol{a}) = (\boldsymbol{u}, \boldsymbol{v})$ la arista (flecha) $\boldsymbol{a}$ va desde $\boldsymbol{u}$ hacia $\boldsymbol{v}$.

En el caso de presencia de aristas antiparalelas suele graficarse con flechas bidireccionales.

Corresponde hacer recordar que conceptos geométricos como posición, forma, longitud, distancia, etc no tienen importancia en grafos ni en digrafos.

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 φ 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

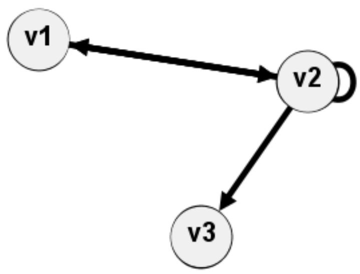


Fig. 5.48. Digrafo D.

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:

- v_1 es 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 incide en él, salvo que sea un lazo

■ 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 algunas de las siguientes opciones:

$$\varphi(a_1) = (v_1, v_2) \text{ y } \varphi(a_2) = (v_2, v_3)\ ,$$

$$\varphi(a_1) = (v_1, v_2) \text{ y } \varphi(a_2) = (v_3, v_2),$$

$$\varphi(a_1) = (v_2, v_1) \text{ y } \varphi(a_2) = (v_2, v_3).$$

■ 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 $D = (\mathrm{V}, \mathrm{A}, \varphi)$ y sea $v \in \mathrm{V}$, se definen las funciones grado positivo y grado negativo de v como sigue:

$$g^+ : \mathrm{V} \to \mathbb{N}_0 \ / \ g^+(v) \text{ es la cantidad de aristas que llegan a } v.$$

$$g^- : \mathrm{V} \to \mathbb{N}_0 \ / \ g^-(v) \text{ es la cantidad de aristas que salen de } v.$$

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 $\boldsymbol{g^+}$ también se le llama grado interno o de entrada.
- A la función $\boldsymbol{g^-}$ también se le llama grado externo o de salida.
- Si $\boldsymbol{v}$ es un vértice aislado y sin lazo entonces $\boldsymbol{g^+(v) = g^-(v) = 0}$

Propiedades de los grados

Dado un dígrafo $\boldsymbol{D = (V, A, \varphi)}$ entonces:

$\boldsymbol{a})\ \sum_{v\in V} \boldsymbol{g^+(v)} = \sum_{v\in V} \boldsymbol{g^-(v)} = |\boldsymbol{A}|$; $\boldsymbol{b})\ \sum_{v\in V} \boldsymbol{g(v)} = \boldsymbol{2|A|}$; $\boldsymbol{c})\ \sum_{v\in V} \boldsymbol{g_n(v)} = \boldsymbol{0}$

Actividad 5.10

Dado el dígrafo $D = (V, A, \varphi)$ de la Figura 5.49

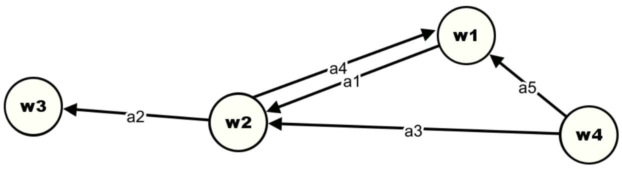


Fig. 5.49. Digrafo D

Se pide:

i) Indicar cuáles son los pares de vértices adyacentes.
ii) Indicar cuáles son las aristas adyacentes a a_5.
iii) Determinar vértices pozos y fuentes, si es que existen.
iv) Encontrar las funciones grado positivo, negativo, total y neto. Presentar a las cuatro funciones en una misma tabla.
v) Verificar las propiedades de los grados de los vértices.

5.11 Caminos, 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: $v_1, a_1, v_2, a_2, \ldots, a_{n-1}, v_n, a_n, v_{n+1}$

Caso contrario basta con indicar la sucesión de vértices involucrados o la sucesión de aristas correspondientes

$$v_1, v_2, \ldots, v_n, v_{n+1} \quad \text{o} \quad a_1, a_2, \ldots, a_{n-1}, a_n$$

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.

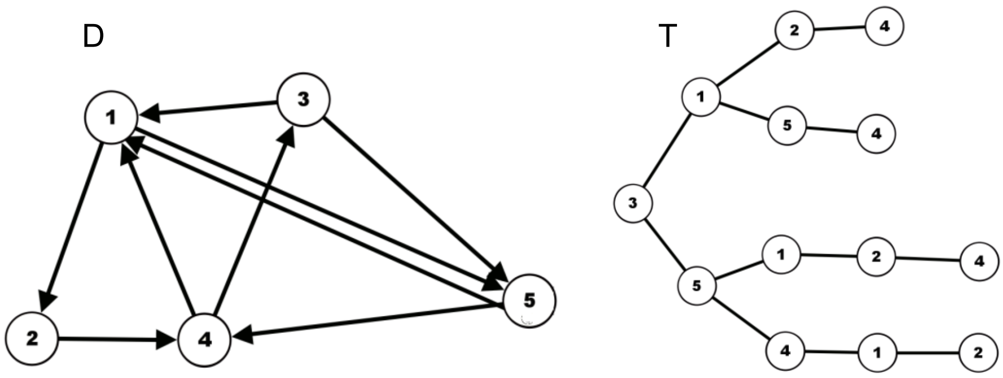


Fig. 5.50. Digrafo D y Árbol T que representa a todos los caminos elementales en D que comienzan en 3.

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

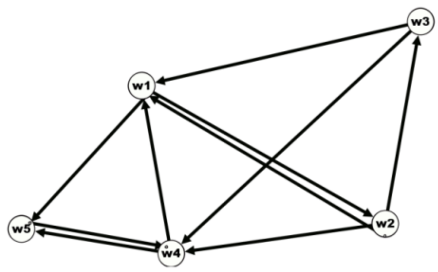


Fig. 5.51. Digrafo D

Responder:

a) ¿Cuáles son todos los caminos simples y circuitos de longitud 6 que comienzan con la secuencia $w_4\ w_1\ w_2$?

b) ¿Cuáles son todos los caminos elementales y ciclos cuyo vértice inicial es w_3? Dar la longitud de cada uno.

c) ¿Existen vértices pozos y vértices fuentes?

5.12 Representaciones matriciales de un digrafo

5.12.1 Matriz de Adyacencia

Definición

Sea $D = (V, A, \varphi)$ un dígrafo sin aristas paralelas y con n vértices, se llama matriz de adyacencia a la matriz $M_a = (m_{ij})$ booleana de orden n tal que:

$$m_{ij} = \begin{cases} 1 & si \ \ \exists a \in A \ \ , \ \varphi\,(a) = (v_i, v_j) \\ 0 & caso\ contrario \end{cases}$$

Observaciones

- M_a fue presentada en el capítulo II como la matriz de una relación binaria.
- La presencia de lazos se manifiesta por unos en la diagonal principal.

Ejemplo 5.24

Dado el dígrafo D de la Figura 5.52:

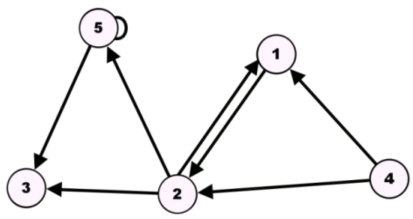


Fig. 5.52. Digrafo D.

Su matriz de adyacencia está dada por:

$$Ma = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

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 la matriz $M_a^k = M_a$ x M_a x…x M_a (k veces) representa la cantidad de caminos diferentes de longitud “k” del vértice i al vértice j.

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 realizan los cálculos correspondientes:

$$M_a^2 = M_a \; x \; M_a = \begin{array}{c} \\ 1\\ 2\\ 3\\ 4\\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array} = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Hay 1(un) 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(un) camino de longitud dos, del vértice 5 al 5.

$$M_a^3 = M_a^2 \; x \; M_a = \begin{array}{c} \\ 1\\ 2\\ 3\\ 4\\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array} = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Hay 2(dos) caminos de longitud $tres$, del vértice 2 al 3.

Hay 1(un) camino de longitud $tres$, del vértice 5 al 3.

$$M_a^4 = M_a^3 \; x \; M_a = \begin{array}{c} \\ 1\\ 2\\ 3\\ 4\\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array} = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 0 & 2 & 0 & 2 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 3 & 0 & 3 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Hay 2(dos) caminos de longitud $cuatro$, del vértice 2 al 3.

Hay 3(tres) caminos de longitud $cuatro$, del vértice 4 al 5.

Hay 1(un) 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 φ 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. Digrafo *D*

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 digrafo sin lazos con n vértices y k aristas, se llama matriz de incidencia a la matriz M_i , de orden $n\text{x}k,$ 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?

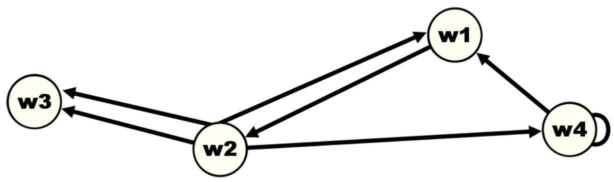


Fig. 5.53. Digrafo D

5.13 Grafo Asociado o subyacente a un digrafo

Definición

Sea $D = (V, A, \varphi)$ un dígrafo y sea $G = (V, A, \gamma)$ un grafo. Se dice que G es el grafo asociado a D si se obtiene a partir de D ignorando el sentido de las aristas y representando a las paralelas o antiparalelas por medio de una única arista.

🗒Ejemplo 5.26

El grafo asociado al digrafo D de la Figura 5.54 es el grafo G, que se muestra en la Figura 5.55

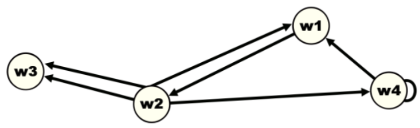


Fig. 5.54. Digrafo D.

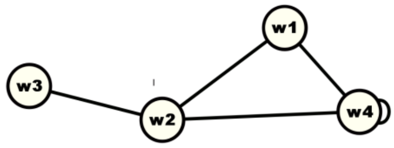


Fig. 5.55. G, grafo asociado de D.

5.14 Digrafo conexo

Definición

Un dígrafo $D = (V, A, \varphi)$ se dice conexo si y solo si su grafo asociado es conexo.

🗒Ejemplo 5.27

El digrafo D de la Figura 5.54 es conexo ya que G, su grafo asociado, lo es.

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 necesarios y suficientes para la existencia de caminos y circuitos de Euler en un digrafo

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:

$$g^{+}(u) = g^{-}(u) - 1 \qquad \text{y} \qquad g^{+}(w) = g^{-}(w) + 1$$

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.

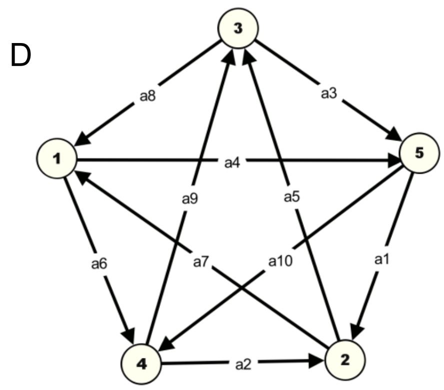


Fig. 5.56. Digrafo con circuito de Euler

Por ejemplo, todos los circuitos cuya secuencia comienza en 4315 estarían representados en el árbol de la Figura 5.57

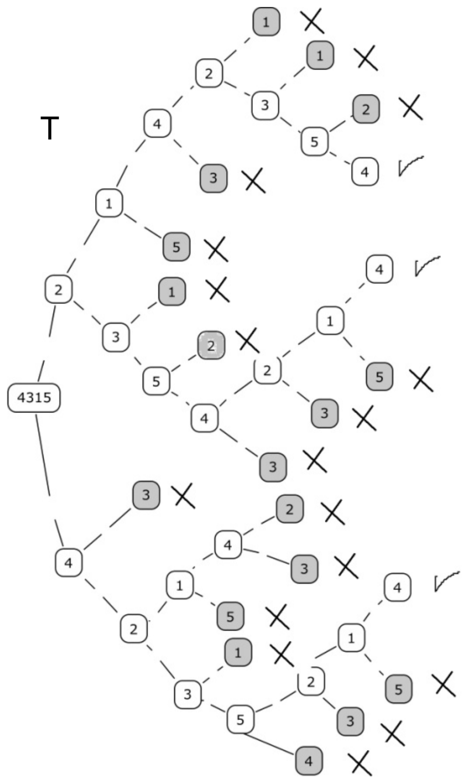


Fig. 5.57. Árbol T.

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 vértices de D sólo una 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.

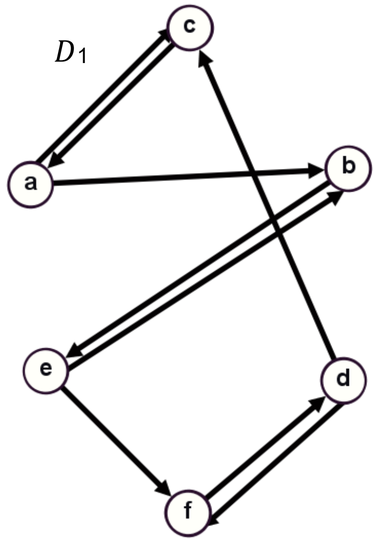


Fig. 5.58. Digrafo D_1.

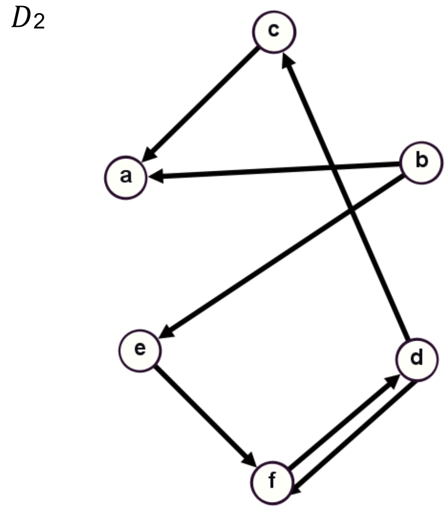


Fig. 5.59. Digrafo D_2.

En D_1 se puede encontrar al menos el ciclo: $\mathrm{b\,e\,f\,d\,c\,a\,b}$ y el camino: $\mathrm{e\,f\,d\,c\,a}$ 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: $\mathrm{b\,e\,f\,d\,c\,a}$.

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 de la figura 5.60 encontrar, si existe, un circuito de Euler y un Ciclo de Hamilton.

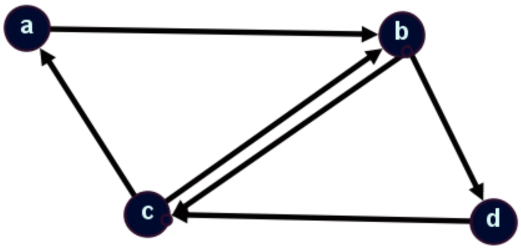


Fig. 5.60. Digrafo D_1.

b) Si es que existen, hallar todos los caminos de Euler del digrafo D_2

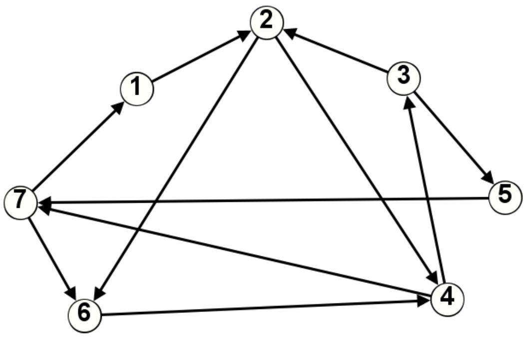


Fig. 5.61. Digrafo D_2.

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 simple. 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 $T = (V, A, \varphi)$ donde $|V| = 1$ y $A = \emptyset$, entonces T se 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 un árbol dirigido, entonces $|V| = |A| + 1$

Ejemplo 5.30

El digrafo 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.

T

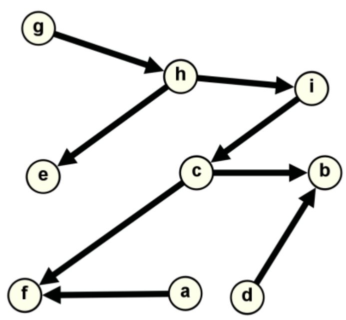


Fig. 5.62. Árbol T.

D

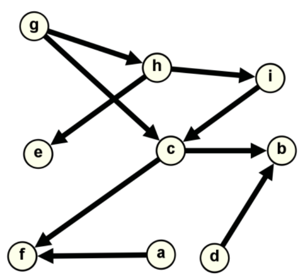


Fig. 5.63. Digrafo D.

5.18 Árbol Dirigido con Raíz

Definición

Sea $D = (V, A, \varphi)$ un digrafo simple, 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 $D = (V, A, \varphi)$ 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 . Para este último, los grados de sus vértices son:

$g^+(i) = 0$ y

$g^+(\mathrm{a}) = g^+(\mathrm{f}) = g^+(\mathrm{g}) = g^+(\mathrm{c}) = g^+(\mathrm{b}) = g^+(\mathrm{h}) = g^+(\mathrm{e}) = g^+(\mathrm{d}) = 1$

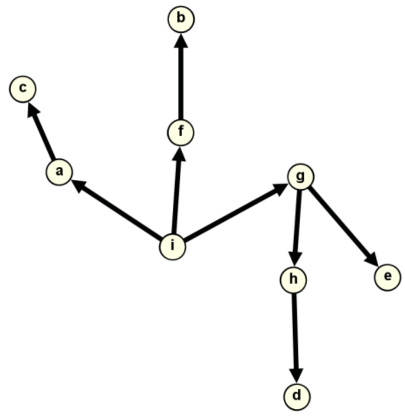


Fig. 5.64. Árbol T.

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 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 sí $v \neq r$ 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 denomina altura de un árbol al mayor número de nivel alcanzado.

■ 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, 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. Se dice que v y w son hermanos si y sólo si tienen el mismo padre.

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 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:

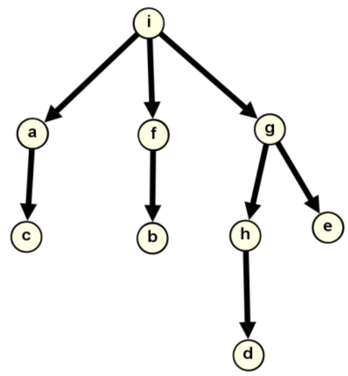


Fig. 5.65. Árbol T(i).

5.18.1 Propiedades de los árboles con raíz

Sea $T = (V, r)$ un árbol con raíz. En T se cumplen las siguientes propiedades:

■ 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 vértice.

D_1

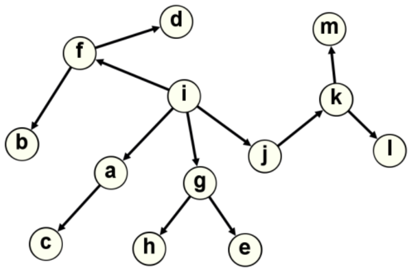


Fig. 5.66. Digrafo D_1.

D_2

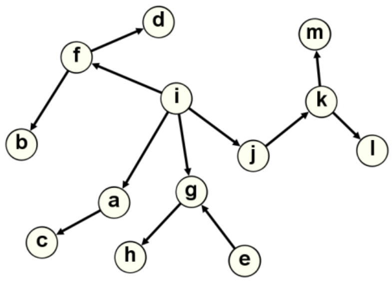


Fig. 5.67. Digrafo D_2.

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) $\Leftrightarrow \quad \forall\, v \in V \quad : g^{-}(v) \leq n$. 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.

T_1

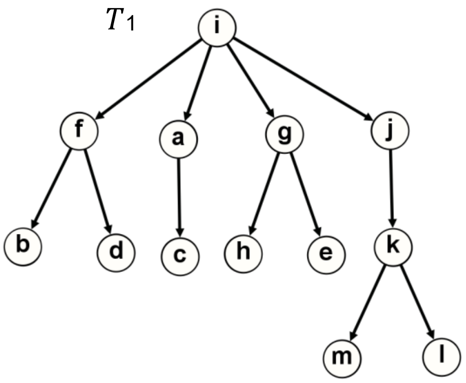


Fig. 5.68. Árbol T_1.

T_2

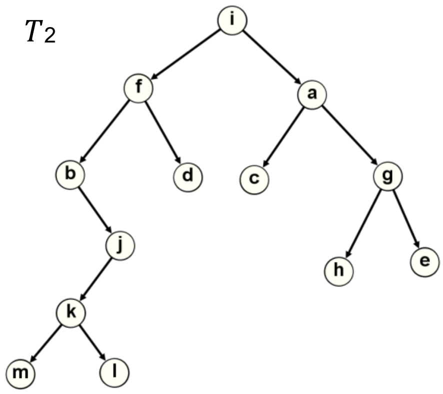


Fig. 5.69. Árbol T_2.

T_3

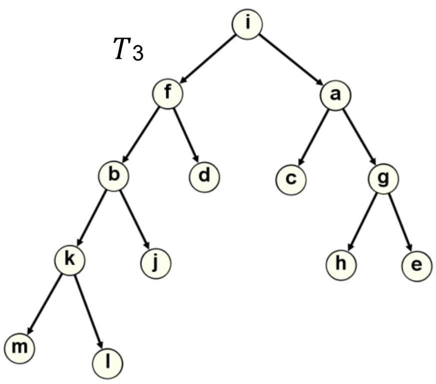


Fig. 5.70. Árbol T_3.

T_4

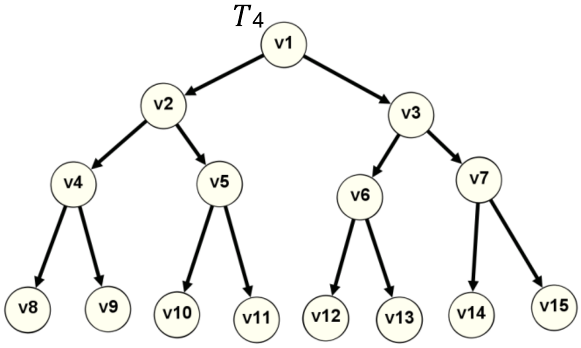


Fig. 5.71. Árbol T_4.

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:

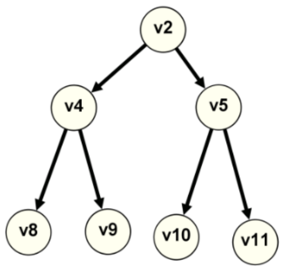


Fig. 5.72. Árbol $T(v_2)$.

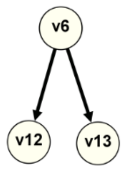


Fig. 5.73. Árbol $T(v_6)$.

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 posicional, sean r_i y r_d ,el hijo izquierdo y derecho de r respectivamente. Entonces, en caso de existir, a $T(r_i)$ se le llama subárbol izquierdo de r y 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 sus respectivos subárboles izquierdo y derecho.

Ejemplos 5.34

Sea el árbol $\mathrm{T} = (\mathrm{V}, v_1)$ 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.

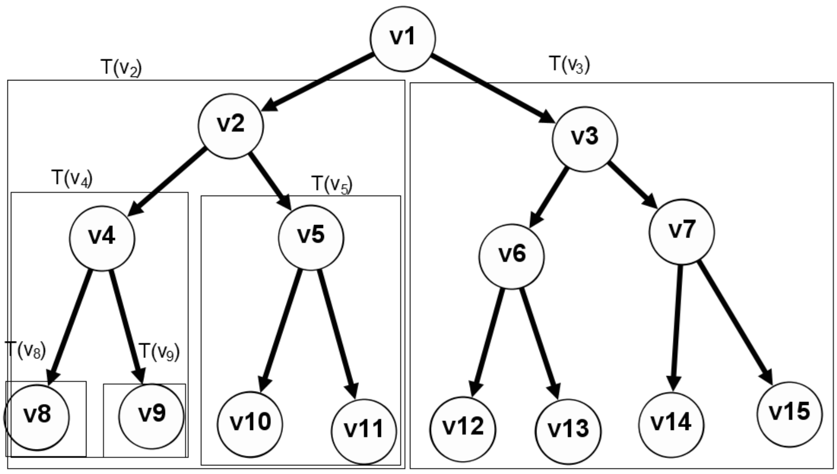


Fig. 5.75. Árbol $T(v_1)$.

5.21 Recorrido de árboles binarios posicionales

Los árboles binarios posicionales son la base de muchas aplicaciones como ser: el acceso a datos almacenados en la memoria de un ordenador, la representación y la evaluación de expresiones algebraicas en las que se incluyen cantidades numéricas, variables y signos de operación, etc. Para todas ellas 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).

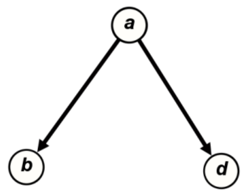
5.21.1 Recorrido o Búsqueda en preorden

Sea $T = (V , r)$ un árbol binario posicional

- Paso 1: Visitar r
- Paso 2: Si existe r_i, entonces volver al paso 1 y aplicar este algoritmo a $T(r_i)$
- Paso 3: Si existe r_d, entonces volver al paso 1 y aplicar este algoritmo a $T(r_d)$
- Paso 4: Fin del algoritmo

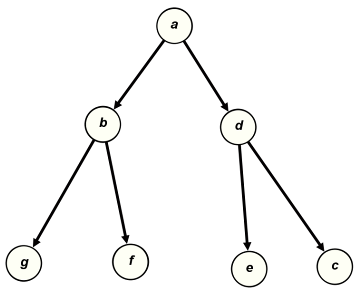
Ejemplos 5.35

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).

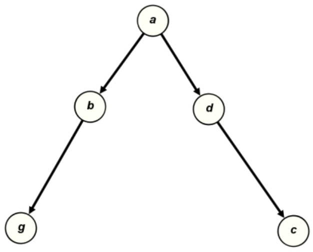


Fig. 5.78. Árbol T_3(a).

Recorrido en preorden de T3: a b g d c

5.21.2 Recorrido o Búsqueda en entreorden

Sea $T = (V, r)$ un árbol binario posicional

- Paso 1: Si existe r_i, aplicar este algoritmo a $T(r_i)$
- Paso 2: Visitar r
- Paso 3: Si existe r_d, entonces volver al paso 1 y aplicar este algoritmo a $T(r_d)$
- Paso 4: Fin del algoritmo

Ejemplos 5.36

El recorrido en entreorden de T_1 de la Figura 5.76 es : b a d

El recorrido en entreorden de T_2 de la Figura 5.77 es: g b f a e d c

El recorrido en entreorden de T_3 de la Figura 5.78 es: 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, aplicar este algoritmo a $T(r_i)$
- Paso 2: Si existe r_d, entonces volver al paso 1 y 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 de la Figura 5.76 es : b d a

El recorrido en posorden de T_2 de la Figura 5.77 es : g f b e c d a

El recorrido en posorden de T_3 de la Figura 5.78 es : g b c d a

Actividad 5.17

Obtener los recorridos de los siguientes árboles enraizados:

$T(6)$

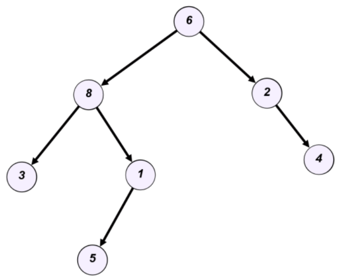


Fig. 5.79. Árbol $T(6)$.

$T(\mathrm{a})$

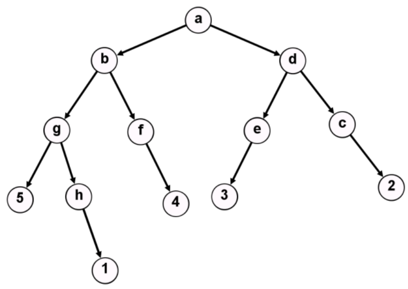


Fig. 5.80. $T(\mathrm{a})$.

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 $p \longrightarrow q$ se representan por medio de los siguientes árboles binarios completos:

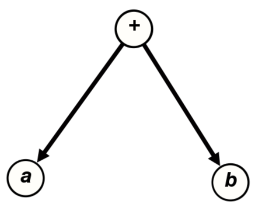


Fig. 5.81. a+b.

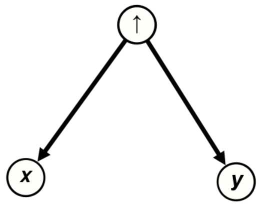


Fig. 5.82. x^y

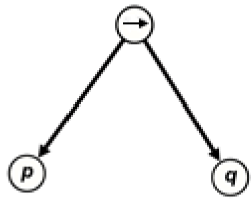


Fig. 5.83. $p \longrightarrow q$

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 $(4 + 5(1 + x)) - (z - 2)/3$ se representa por el árbol de la Figura 5.84

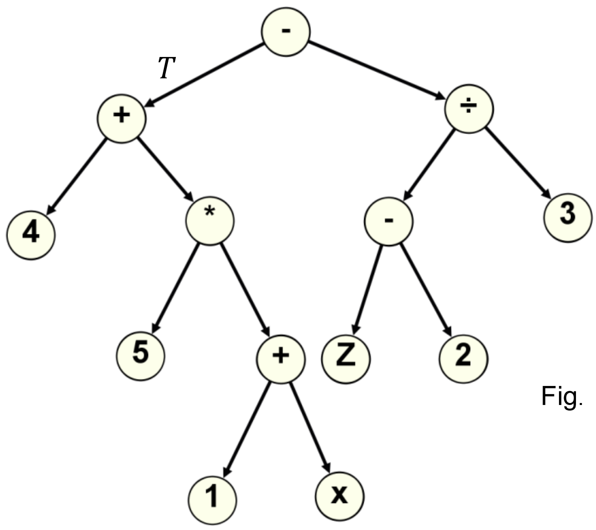


Fig. 5.84. Árbol T.

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) $\frac{(2-3x)^2}{\sqrt{\frac{x}{5}+1}}$

i) ¿Cuál es la altura de cada uno de ellos?
ii) ¿Los vértices hojas pueden estar etiquetados con operadores?
iii) 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 prefija (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 es a la que se está acostumbrado, pero 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
$a \div b$	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 $\left(\frac{a}{2}\right)$ y a sus correspondientes notaciones

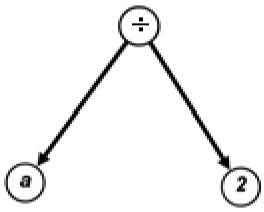


Fig. 5.85.

Notación prefija: ÷ a 2

Notación posfija: a 2 ÷

Notación infija: a ÷ 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

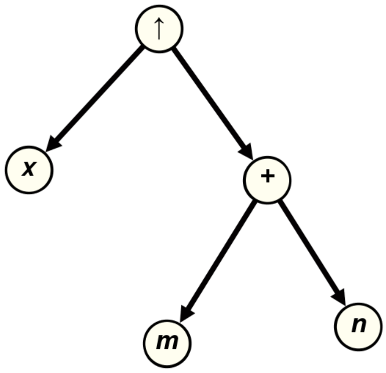


Fig. 5.86.

Notación prefija: $\uparrow \mathbf{x} + \mathbf{m}\ \mathbf{n}$

Notación posfija: $\mathrm{x\ m\ n} + \uparrow$

Notación infija: $\mathrm{x} \uparrow (\mathrm{m} + \mathrm{n})$

Notación usual: $\mathrm{x}^{\mathrm{m+n}}$

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) $+ \uparrow a\ 2 \uparrow \div\ b\ 2\ a$

Capítulo 6. ESTRUCTURAS ALGEBRAICAS FINITAS

Estructuras Algebraicas.

Operaciones.

Propiedades de una Operación Binaria Cerrada.

Principales estructuras algebraicas:

Monoide,

Semigrupo,

Grupo,

Anillo,

Cuerpo.

Álgebra de Boole.

Introducción

Se conocen hasta el nivel inicial de las carreras de ingeniería distintos conjuntos: los numéricos : $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$ y algunos nuevos como $M_{mxn}(\mathbb{R})$, conjunto de las matrices de números reales; $\mathbb{R}^n$, el conjunto de vectores de números reales y C^n, conjunto de funciones continuas hasta la derivada de orden n . En ellos se definen diversas operaciones y se puede observar que, por más que sean de distinta naturaleza, tienen propiedades análogas. Estas analogías permiten clasificar en una misma "categoría" a distintos conjuntos con operaciones diversas. A dichas categorías se las llama Estructuras Algebraicas.

En esta última unidad ampliaremos la diversidad de conjuntos a considerar. En nuestros ejemplos consideraremos muy frecuentemente conjuntos discretos cuyos elementos pueden ser objetos de cualquier naturaleza y las operaciones que se definan en él serán especificadas mediante tablas de resultados.

6.1 Estructuras Algebraicas

Definición

Una Estructura Algebraica es un objeto matemático consistente en uno o más conjuntos no vacíos y una o más operaciones definidas en ellos.

Al representarlas simbólicamente se usa 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:

i) $(\mathbb{N}, -)$, Números Naturales respecto de la operación diferencia usual
ii) $(\mathbb{Z}, +)$, Números Enteros respecto de la operación suma usual
iii) $(\mathbb{R}, +, \bullet)$, Números Reales respecto de la suma y producto usuales.
iv) $(\wp(X), \cup, \cap)$, Potencia de X respecto de la unión e intersección.
v) $(M_{nxn}(\mathbb{R}), +, \bullet)$, Matrices cuadradas de orden n de números reales con la suma y producto usual.

vi) (S , $\vee$, $\wedge$) , Conjunto de todas las proposiciones respecto de las operaciones disyunción y conjunción.

vii) ({0,1}, + , •) , Conjunto de valores booleanos con las operaciones suma y producto lógico.

En particular, si el conjunto es finito se tiene una Estructura Algebraica Finita y son las estructuras en las que pondremos más énfasis en este capítulo.

Según las propiedades de las operaciones, las estructuras algebraicas se clasifican en: Monoides, Semigrupos, Grupos, Anillos, Cuerpos, Algebras booleanas, entre otras. Pero antes de definirlas se debe definir exhaustivamente el concepto de operación y cuáles podrían ser las propiedades de las que goza.

6.2 Operaciones

Las operaciones se clasifican en *binarias* y *unarias*.

6.2.1 Operación binaria

Definición

Sea un conjunto $A \neq \varnothing$, se llama operación binaria sobre A a toda función cuyo dominio es AxA. Se denotará con el símbolo $*$

En particular, se dice que $*$ es una operación binaria cerrada (o ley de composición interna) sobre A si su imagen es A. Simbólicamente, se indica:

$$* : AxA \longrightarrow A$$

$$(a, b) \longrightarrow a*b$$

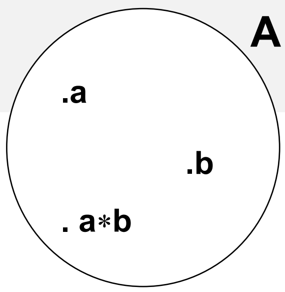


Fig.6.1. Conjunto A.

Observación

No solo el símbolo $*$ está reservado para representar operaciones binarias. Los siguientes símbolos: + , • , $\otimes$, $\oplus$, $\cup$, $\cap$, $\vee$, $\wedge$, ♦, Δ, □, también son usados y son conocidos en su gran mayoría.

Notación

Para indicar que en 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 A es finito, por ejemplo $A = \{ x_1, x_2,\dots, x_n \}$, la operación binaria $* : AxA \to A$ puede definirse por medio de una tabla de doble entrada donde se indicará a los elementos de A en el mismo orden.

$*$	x_1	$\dots$	x_j	$\dots$	x_n
x_1					
$\vdots$					
x_i			$x_i * x_j$		
$\vdots$					
x_n					

elementos de A

La posición (i, j) corresponde al resultado de operar x_i con x_j.

Tabla 6.1

elementos de A

Ejemplos 6.2

a) 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 $\mathbb{C}$

b) La adición usual en A = {1, 2, 3, 4, 5 } no es cerrada ya que $3 + 4 \notin A$.

c) En A = { a , b , c } y la operación $*$ definida por Tabla 6.2 es cerrada.

$*$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Tabla 6.2

Actividad 6.1

Determinar si las siguientes son operaciones cerradas (o leyes de composición interna) en el conjunto indicado:

- Las operaciones resta y división en los conjuntos numéricos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{R} - \{0\}$
- Las operaciones suma y multiplicación usual en el conjunto A donde

$$A = \{ x \in \mathbb{Z} \ / \ x \text{ es un entero impar}\}$$

- La operación $*$: A x A → 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 $A \neq \varnothing$, se dice que una operación es unaria sobre A si es una función con dominio en A.

En particular, se dice que 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:

$$' : A \longrightarrow A$$
$$a \longrightarrow a'$$

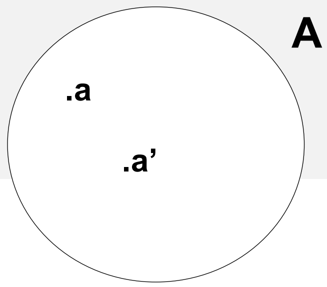


Fig. 6.2. Conjunto A.

Observación

Una operación unaria es aquella operación que sólo necesita un operando.

Ejemplos 6.3

Son operadores unarios:

i) La operación complemento de un conjunto.
ii) La función valor absoluto de un número real.

Actividad 6.2

Determinar si los siguientes son operadores unarios cerrados

a) En S = { p / p es una proposición simple o compuesta } , la operación negación

b) En $M_{2x3}(\mathbb{R})$, la operación transposición

c) En $M_{3x3}(\mathbb{R})$, la operación transposición

6.3 Propiedades de una Operación Binaria Cerrada

6.3.1 Propiedad Conmutativa

Definición

Sea $(A , *)$ con $*$ una operación binaria cerrada.

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 $\otimes$ dada por la tabla 6.4 . Se tiene que $\otimes$ 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**

Se observa que si $\otimes$ es conmutativa hay simetría en la tabla.

6.3.2 Propiedad asociativa

Definición

Sea $(A , *)$ con $*$ una operación binaria cerrada.

Se dice que $*$ es asociativa en A $\Leftrightarrow \forall$ a, b, c $\in$ A : $a*(b*c) = (a*b)*c$

👁**Observación**

- 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.
- Los elementos a, b y c no necesariamente deben ser distintos, por lo que, para probar la asociatividad en conjuntos con menos de 3 elementos se deben tomar elementos iguales.

Ejemplos 6.5

a) La adición y la multiplicación son asociativas en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$

b) La intersección y unión de conjuntos son asociativas, como se mostró en el capítulo 2.

c) La disyunción y la conjunción de proposiciones son operaciones asociativas, como se mostró en el capítulo 1.

Actividad 6.3

Determinar si las siguientes operaciones son conmutativas y asociativas en los conjuntos dados

a) En S = { p / p es una proposición} , las operaciones $\underline{\vee}$ y $\longrightarrow$

b) En A = {a, b} , la operación $*$: AxA $\longrightarrow$ A dada por la Tabla 6.5

$*$	a	b
a	b	b
b	a	b

Tabla 6.5

6.3.3 Existencia del elemento neutro

Definición

Sea (A , $*$) con $*$ una operación binaria cerrada.

Se dice que A posee elemento neutro (o elemento 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 la operación es el elemento original.

Teorema: Unicidad del elemento neutro

Sea (A , $*$) con $*$ una operación binaria cerrada .

Si A posee neutro respecto de $*$, éste es único.

Observación

Cuando el conjunto es finito y la operación se presenta por medio de una tabla, para hallar el elemento neutro se procede de la siguiente forma: Se observa 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

i) En $\mathbb{Z}$, 0 es el neutro respecto de la operación suma pues

$$x + 0 = 0 + x = x \quad , \quad \forall x.$$

ii) En $\mathbb{Z}$, 1 es el neutro respecto de la operación multiplicación pues

$$x \,.\, 1 = 1 \,.\, x = x \quad , \quad \forall x.$$

iii) En el conjunto $\wp(X)$, el neutro respecto de la operación unión es $\varnothing$ 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

$$\varnothing \cup A = A \cup \varnothing = A \qquad \text{y} \qquad A \cap X = X \cap A = A$$

iv) La operación potenciación no posee neutro en ningún conjunto numérico dado que no existe un elemento e tal que $a^e = e^a = a$.

v) 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

Dado que $b \otimes a = a \otimes b = a$, $b \otimes 0 = 0 \otimes b = 0$ y $b \otimes b = b$, entonces el neutro es b.

vi) 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

6.3.4 Existencia de elementos inversos

Definición

Sea (A , $*$) con $*$ una operación binaria cerrada con e como su elemento neutro.

Se dice que a´ es el inverso de a respecto de $*$ sí y solo si $a * a' = a' * a = e$

Y además:

Se dice que A cumple con la propiedad de existencia del inverso si y solo si

$$\forall\, a \in A \,,\, \exists\, a' \in A \;\;/\;\; a * a' = a' * a = e\,.$$

Observaciones

- Si A respecto de la operación $*$ no posee neutro, entonces tampoco posee elementos inversos.
- 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. La fila y la columna donde aparece el neutro están señalando a los elementos que son inversos mutuamente.

Ejemplos 6.7

i) En $\mathbb{Z}$ existe el inverso respecto de la +. Se le llama inverso aditivo (u opuesto). Simbólicamente:

$$\forall\, a \in \mathbb{Z} \,,\, \exists\, a' = -a \in \mathbb{Z} \;\;/\;\; a + (-a) = (-a) + a = 0$$

ii) En $\mathbb{R} - \{0\}$ existe el inverso respecto de la multiplicación, se le llama inverso multiplicativo (o recíproco). Simbólicamente:

$$\forall\, a \in \mathbb{R} - \{0\} \,,\, \exists\, a' = 1 / a \in \mathbb{R} - \{0\} \;\;/\;\; a \,.\, (1/a) = (1/a).\, a = 1$$

iii) En A = { a , 0 , b } y la operación $\otimes$ definida por la tabla 6.8 donde el elemento neutro es b se tiene que a´ = a , 0´ = 0 y b´ = b, luego se puede decir que el conjunto A cumple con la propiedad de existencia del inverso respecto de $\otimes$.

⊗	a	0	b
a	<u>b</u>	0	a
0	0	<u>b</u>	0
b	a	0	<u>b</u>

Tabla 6.8

Actividad 6.4

En cada apartado determinar si el conjunto cumple con la propiedad de existencia del elemento neutro respecto de la operación indicada. En los casos afirmativos investigar si el conjunto cumple con la propiedad de existencia del elemento inverso.

a) En $M_{nxn}(\mathbb{R})$, respecto de la suma y multiplicación usual de matrices

b) En A = {a, 0, b} y la operación binaria $\otimes : AxA \to A$, dada por la Tabla 6.9

c) En A = { a, b, c } con la operación $*$ dada por la Tabla 6.10

⊗	a	0	b
a	a	0	b
0	0	0	a
b	b	a	b

Tabla 6.9

∗	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. En el siguiente ejemplo se mostrará que pueden definirse nuevas operaciones a partir de otras ya conocidas.

Ejemplo 6.8

En $\mathbb{Z}$ se define la operación $*$ por medio de

$$a * b = a + b + 2 , \text{ donde } + \text{ es la suma usual}$$

¿Cuáles son las propiedades de $*$?

i) ¿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 $\mathbb{Z}$.

ii) ¿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:

(I) $a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4$

(II) $(a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4$

Las expresiones finales (I) y (II) son iguales. Por lo tanto, $*$ es asociativa en $\mathbb{Z}$.

iii) ¿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:

(I) $a * b = a + b + 2$

(II) $b * a = b + a + 2 = a + b + 2$ por la propiedad conmutativa de la + en $\mathbb{Z}$.

Las expresiones finales (I) y (II) son iguales. Por lo tanto, $*$ es conmutativa en $\mathbb{Z}$.

iv) ¿Posee $*$ elemento neutro en $\mathbb{Z}$? ¿ $\exists$ e $\in$ Z , $\forall$ a $\in$ 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 $\mathbb{Z}$

v) ¿Existe el elemento inverso respecto de $*$ para cada elemento de $\mathbb{Z}$?

Se debe analizar si $\forall a \in \mathbb{Z}, \ \exists a' \in \mathbb{Z}, \quad a * a' = a' * a = -2$

Como $*$ es conmutativa, se puede buscar el inverso sólo a derecha y el mismo será inverso a izquierda.

$$a * a' = -2 \Rightarrow a + a' + 2 = -2 \Rightarrow a' = -4 - a \in \mathbb{Z}$$

Por ejemplo, $5' = -9$.

La conclusión es que el conjunto $\mathbb{Z}$ posee inverso respecto de la operación $*$.

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 sumas y productos usuales.

Determinar si

i) $\circ$ y $*$ son operaciones conmutativas y asociativas

ii) En $\mathbb{Z}$ existen elementos neutros respecto de $\circ$ y $*$

iii) El conjunto $\mathbb{Z}$ tiene inverso respecto de $\circ$ y $*$

6.3.5 Distributividad

Definición

Sea $(A, *, \circ)$ con $*$ y $\circ$ dos operaciones cerradas en A

Se dice que $\circ$ es distributiva respecto de $*$ en A $\Leftrightarrow$

$\forall a, b, c \in A, \ a \circ (b * c) = (a \circ b) * (a \circ c)$ (distributividad a izquierda) y

$\forall a, b, c \in A, \ (b * c) \circ a = (b \circ a) * (c \circ a)$ (distributividad a derecha)

y, recíprocamente, se dice que $*$ es distributiva respecto de $\circ \Leftrightarrow$

$\forall a, b, c \in A, \ a * (b \circ c) = (a * b) \circ (a * c)$ (distributividad a izquierda) y

$\forall a, b, c \in A, \ (b \circ c) * a = (b * a) \circ (c * a)$ (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

i) En $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ la multiplicación es distributiva respecto de la adición dado que:

$$x \cdot (y + z) = x \cdot y + x \cdot z , \quad \forall x , y , z$$

$$(y + z) \cdot x = y \cdot x + z \cdot x , \quad \forall x , y , z$$

ii) En el conjunto $\wp(X)$ la unión y la intersección son distributivas mutuamente ya que:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad , \quad \forall A , B , C$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad , \quad \forall A , B , C$$

Actividad 6.6

a) En $\mathbb{Z}$ se definen las operaciones "$\circ$" y "$*$" por medio de

$$a \circ b = a + b + a.b \quad y \quad a * b = a + b + 1$$

donde '+' y '.' son las operaciones sumas y productos usuales.

Determinar si $\circ$ y $*$ son distributivas mutuamente.

b) En A = { 0 , 1 } se definen las operaciones "$\circ$" y "$*$" definidas por las tablas 6.11 y 6.12. Determinar si "$\circ$" y "$*$" son distributivas mutuamente.

$\circ$	0	1
0	0	1
1	1	1

Tabla 6.11

$*$	0	1
0	0	0
1	0	1

Tabla 6.12

6.4 Principales Estructuras Algebraicas

Las estructuras algebraicas se clasifican según las propiedades que cumplen las operaciones sobre el conjunto donde están definidas. Las principales son:

6.4.1 Monoide

Definición

Sea $A \neq \varnothing$. Se dice que $M = (A , *)$ es un monoide si y sólo sí "$*$" es una operación cerrada o ley de composición interna, esto es $* : A \times A \longrightarrow A$

Ejemplos 6.10

1) $(\mathbb{N} , +)$ es un monoide mientras que $(\mathbb{N} , -)$ no lo es.

2) $(\mathbb{N} , *)$ donde "$*$" está definido como $a * b = \text{máx}\{a , b\}$ es un monoide.

6.4.2 Semigrupo

Definición

Sea $A \neq \varnothing$. Se dice que $S = (A , *)$ es un Semigrupo si y sólo sí "$*$" cumple las siguientes condiciones:

i) $* : A \times A \longrightarrow A$

ii) $\forall\, a, b, c \in A$: $a*(b*c) = (a*b)*c$

Observaciones

- Si además "$*$" es conmutativa, entonces $S = (A , *)$ se dice semigrupo conmutativo.
- Si existe el elemento neutro en A respecto de "$*$", $S = (A , *)$ se dice que es un semigrupo con unidad

Ejemplos 6.11

i) $(\mathbb{N}, +)$ es un semigrupo conmutativo.

ii) $(\mathbb{N}_0, +)$ es un semigrupo conmutativo con unidad.

iii) $(\mathbb{N}, .)$ es un semigrupo conmutativo con unidad.

iv) $(M_{mxn}(\mathbb{R}) , +)$, $(\wp(X) , \cap)$ 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 sí "∗" cumple las siguientes condiciones:

i) $* : A \times A \longrightarrow A$

ii) $\forall$ a, b, c $\in$ A, $a*(b*c) = (a*b)*c$

iii) $\exists\, e \in A$, $\forall\, a \in A$ / $e * a = a * e = a$

iv) $\forall\, a \in A$, $\exists\, a' \in A$ / $a * a' = a' * a = e$

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 dice orden del grupo.

Ejemplos 6.12

i) $(\mathbb{Q} - \{0\}, \bullet)$ y $(\mathbb{R} - \{0\}, \bullet)$ son grupos, donde "•" es el producto usual.

ii) ($\mathbb{N}$, +) no es grupo, no tiene elemento neutro y por lo tanto tampoco inverso.

iii) ($\mathbb{N}_0$, +) no es grupo, aunque tiene neutro pero no tiene inverso aditivo.

Actividad 6.8

a) ¿Es ($M_{2x3}(\mathbb{R})$, +) grupo abeliano, donde $M_{2x3}(\mathbb{R})$ es el conjunto de todas las matrices de números reales de orden 2x3 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 el tipo de estructura algebraica que es ($\mathbb{Z}_5$, +)

6.4.4 Propiedades de los grupos

Sea (A , $*$) un grupo. Entonces se cumple que:

a) El inverso de cada elemento es único.

b) (x ´) ´ = x

c) (x $*$ y) ´ = y ´ $*$ x ´

d) Si a , b $\in$A, entonces las ecuaciones del tipo x $*$ a = b y a $*$ x = b admiten solución única en A.

Actividad 6.9

a) Demostrar que ($\mathbb{Z}$, $*$) es grupo abeliano, donde "$*$" es la operación definida como a $*$ b = a + b + 3

b) Sea A = { a , b , c } y las operaciones $*_1$ y $*_2$ dadas por las tablas 6.14 y 6.15

$*_1$	a	b	c
a			
b			
c			

Tabla 6.14

$*_2$	a	b	c
a			
b			
c			

Tabla 6.15

i) Completar la tabla 6.14 de tal modo que A tenga estructura de Grupo respecto de $*_1$ con elemento neutro b y a' = c .

ii) Completar la tabla 6.15 para que A sea de grupo abeliano respecto de $*_2$ y además las ecuaciones $a *_2 x = b$ y $c *_2 x = a$ se satisfacen para $x = a$.

6.4.5 Subgrupo

Definición

Sea (A , $*$) un grupo y sea $B \subseteq A$, tal que $B \neq \varnothing$. Se dice que (B ,$*$) es subgrupo de (A , $*$) si y solo sí (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 ($\mathbb{Z}$,+).

Propiedad de los Subgrupos

Sea (A , $*$) un grupo y sea $B \neq \varnothing$ 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:

a) B = { a , b , c } no es subgrupo de A,

b) B = { a , b } es subgrupo de A.

6.4.6 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 $\forall a , b , c \in A$

a) $(a * b) * c = a * (b * c)$

b) $\exists\, e \in A / a * e = e * a = a$

c) $\forall a, \exists a' \in A / a * a' = a' * a = e$

d) $a * b = b * a$

e) $(a \bullet b) \bullet c = a \bullet (b \bullet c)$

f) $a \bullet (b * c) = (a \bullet b) * (a \bullet c)$ y $(b * c) \bullet a = (b \bullet a) * (c \bullet a)$

Resumiendo se tiene que:

$(A , *, \bullet)$ es un Anillo si y solo si

i) $(A , *)$ es un grupo abeliano ;

ii) $(A , \bullet)$ es un semigrupo y

iii) la segunda operación "$\bullet$" se distribuye sobre la primera "$*$".

Observaciones

- Es común escribir $(A , + , \bullet)$ para representar a la estructura algebraica de 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.

Sea A un anillo con identidad. Si todo elemento de A distinto de cero es invertible en A respecto de "$*$" 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

i) ($\mathbb{Z}$, + , $\bullet$) con las operaciones usuales, es un anillo conmutativo con unidad y sin divisores de cero.

ii) ($\mathbb{N}$, + , $\bullet$) con las operaciones conocidas no es un anillo, pues en $\mathbb{N}$ no existe neutro para la adición.

iii) 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 = $\wp(X)$ = { $\varnothing$, {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 6.17 y 6.18

$\oplus$	$\varnothing$	{a}	{b}	{a,b}
$\varnothing$	$\varnothing$	{a}	{b}	{a,b}
{a}	{a}	$\varnothing$	{a,b}	{b}
{b}	{b}	{a,b}	$\varnothing$	{a}
{a,b}	{a,b}	{b}	{a}	$\varnothing$

Tabla 6.17

$\cap$	$\varnothing$	{a}	{b}	{a,b}
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
{a}	$\varnothing$	{a}	$\varnothing$	{a}
{b}	$\varnothing$	$\varnothing$	{b}	{b}
{a,b}	$\varnothing$	{a}	{b}	{a,b}

Tabla 6.18

6.4.7 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

i) $(\mathbb{Z}, +, \bullet)$ con las operaciones suma y producto usual no es cuerpo, pues $\mathbb{Z}$ carece de inversos multiplicativos.

ii) $(\mathbb{Q}, +, \bullet)$, $(\mathbb{R}, +, \bullet)$ 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 "$\bullet$" definidas por las siguientes tablas:

+	0	1
0	0	1
1	1	0

Tabla 6.19

$\bullet$	0	1
0	0	0
1	0	1

Tabla 6.20

6.5 Algebra 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 .

Se dice que (B , + , •) es un Álgebra de Boole si y solo si se satisfacen las siguientes propiedades.

1) $x + (y + z) = (x + y) + z$

$x \bullet (y \bullet z) = (x \bullet y) \bullet z \qquad \forall x, y, z \in B$

2) $x + y = y + x$

$x \bullet y = y \bullet x \qquad \forall x, y \in B$

3) $x + y \bullet z = (x + y) \bullet (x + z)$

$x \bullet (y + z) = x \bullet y + x \bullet z \qquad \forall x, y, z \in B$

4) $\exists\, 0 \in B \,/\, \forall x \in B ,\ x + 0 = 0 + x = x$

$\exists\, 1 \in B \,/\, \forall x \in B ,\ x \bullet 1 = 1 \bullet x = x$

5) $\forall x \in B, \exists\, x' \in B \,/\ x + x' = 1 \quad y \quad x \bullet x' = 0$

Actividad 6.13

Sea B = { 0, 1} y las operaciones “+” y “•” definidas por las tablas 6.21 y 6.22 Demostrar que (B,+ , •) tiene estructura de Algebra de Boole.

+	0	1
0	0	1
1	1	1

Tabla 6.21

•	0	1
0	0	0
1	0	1

Tabla 6.22

6.5.1 Álgebra de Boole del Conjunto Potencia

Teorema

Sea X conjunto finito y sea $\wp(\mathrm{X})$ el conjunto potencia de X . Entonces

$$(\wp(\mathrm{X}), \cup, \cap) \text{ es un Álgebra de Boole para todo conjunto } \mathrm{X}.$$

Demostración

Se demostraron en el capítulo 2 las propiedades de las operaciones unión e intersección. En particular, se vio que:

1) La asociatividad vale para ambas operaciones:

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

2) Se cumple la conmutatividad para ambas operaciones:

$$A \cup B = B \cup A \qquad A \cap B = B \cap A$$

3) Se cumple la distributividad mutua de ambas operaciones:

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

4) Existen los elementos neutros:

$A \cup \emptyset = A$, $\quad A \cap U = A$ (en este caso el universo es X)

5) Existe el conjunto complemento de cada conjunto:

$$\forall\, A \in \wp(\mathbf{X}),\ \exists\, A' \in \wp(\mathbf{X}) \ / \ A' = X - A$$

Por lo tanto $(\wp(\mathrm{X}), \cup, \cap)$ es un Álgebra de Boole , para todo X

Observación:

Todas las propiedades, de 1 a 5 fueron demostradas en la Unidad 2.

Ejemplo 6.16

Si $\mathrm{X} = \{a,\ b,\ c\}$ entonces $\wp(\mathrm{X}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, X\}$ entonces $(\wp(\mathrm{X}), \cup, \cap)$ es un Álgebra de Boole cuyos neutros son $\emptyset$ y X son los neutros respecto de $\cup$ e $\cap$ respectivamente y los complementos son:

$\emptyset' = \mathrm{X}$ y $\mathrm{X}' = \emptyset$ ya que $\emptyset \cup \mathrm{X} = \mathrm{X}$ y $\emptyset \cap \mathrm{X} = \emptyset$

$\{a\}' = \{b,c\}$ y $\{b,c\}' = \{a\}$ ya que $\{a\} \cup \{b,c\} = \mathrm{X}$ y $\{a\} \cap \{b,c\} = \emptyset$

$\{b\}' = \{a,c\}$ y $\{a,c\}' = \{b\}$ ya que $\{b\} \cup \{a,c\} = \mathrm{X}$ y $\{b\} \cap \{a,c\} = \emptyset$

$\{c\}' = \{a,b\}$ y $\{a,b\}' = \{c\}$ ya que $\{c\} \cup \{a,b\} = \mathrm{X}$ y $\{c\} \cap \{a,b\} = \emptyset$

6.5.1 Álgebra de Boole D_n

Sea $n \in \mathbb{N}$ y sea $\mathrm{D}_n = \{\, \mathrm{x} \in \mathbb{N} \,,\ \mathrm{x} \,|n\}$ el conjunto de los divisores positivos de n

Definiendo las operaciones "+" y "$*$ " como sigue

$$x + y = mcm\{x,y\}$$

$$x * y = mcd\{x,y\}$$

Se genera la estructura (D_n , + , $*$) y de allí surge la pregunta ¿Cuáles son las propiedades de las operaciones "+" y "$*$" ? Se puede demostrar que depende del valor de n. El resultado está expresado en el siguiente teorema:

Teorema sobre las Álgebras Booleanas $\boldsymbol{D_n}$

D_n es un Álgebra Booleana si y solo sí $n = p_1.p_2 \ldots\ldots p_k$ donde $p_1, p_2, \ldots\ldots, p_k$ son números primos distintos.

Ejemplos 6.17

i) D_2 es algebra booleana pues 2=2
ii) D_6 es algebra booleana pues 6 = 2.3
iii) D_{20} no es algebra booleana pues 20 = 2.2.5
iv) D_{30} es algebra booleana pues 30 = 2.3.5
v) D_{3003} es algebra booleana pues 3003 = 3.7.11.13
vi) D_{1848} no es algebra booleana pues 1848 = 2^3 .3 . 7.11

Álgebra Booleana $\boldsymbol{D_{30}}$

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 6.23

$*$	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 6.24

Observe que los neutros son: 1 para la operación "+" y 30 para la operación "$*$".

Los complementos son:

$1' = 30$ y $30'=1$ ya que $1 + 30 = 30$ y $1 * 30 = 1$

$2' = 15$ y $15' = 2$ ya que $2 + 15 = 30$ y $2 * 15 = 1$

$3' = 10$ y $10' = 3$ ya que $3 + 10 = 30$ y $3 * 10 = 1$

$5' = 6$ y $6' = 5$ ya que $5 + 6 = 30$ y $5 * 6 = 1$

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.

BIBLIOGRAFIA

Agazzi, E.1990. *La lógica Simbólica*. Ed. Herder, Barcelona.

Alberto, M.; Schwer, I.; Fumero, Y., Llop, P. Chara, M. 2011. *Matemática Discreta*. edUTecNe, Buenos Aires.

Ávila, J. 2005. *Estructuras de matemática discreta para computación*. Costa Rica: UNA.

Copi, I,.2006. *Lógica Simbólica*, Ed. Continental, México.

Countinho, S.C. 2003. Números enteros y Criptografía RSA. Ed. Lima: Instituto de Matemática y Ciencia de Afines. Serie: Texto del Inca, 10.

García Merayo, F. 2001. *Matemática Discreta*. Ed. Paraninfo. Thompson Learning. Madrid

Granado Peralta, S. 2006. *Matemática Discreta*. Ed. CEIT, Bs. As

González Gutiérrez, Francisco J. (2004***)***. Apuntes de matemáticas discretas. Universidad de Cádiz, España. Superior de Ingeniería. Departamento de matemáticas. Disponible en línea en:

http://www2.uca.es/matematicas/Docencia/2005-2006/ESI/1711003/Marco.htm Consultado el 22/07/2014.

Grassmann, W. yTremblay, J.,1988. *Matemática Discreta y Lógica Una perspectiva desde la ciencia de la computación*. Ed. Prentice Hall, Madrid.

Grimaldi, R. 2007. *Matemáticas Discretas y Combinatoria*. Ed. Addison-Wesley Iberoamericana. Estados Unidos.

Hortalá González, M.T., Leach Albert, J., Rodríguez Artalejo, M. 2008. *Matemática Discreta y Lógica Matemática*. España, Editorial Complutense, S.A.

Johnsonbaugh, R. 2005. *Matemáticas Discretas*. 6ª edición. Editorial Pearson Educación. México.

Kolman, B., Busby, R. y Ross, S. 1995. *Estructuras de matemáticas discretas para computación*. México: Prentice-Hall Hispanoamericana.

Lipschutz, S. 1966. *Matemáticas Finitas.* McGraw-Hill. México.

Lipschutz, S. y Lipson, M. 2004. 2000 problemas resueltos de matemática discreta. España: Mc.Graw-Hill.

Lipschutz, S. 1991. *Teoría de conjuntos y temas afines*. Traducido por Jesus Maria Castaño. 1a. Ed. México: Mc Graw-Hill (Serie de compendios Schaum).

Liu, C.L. 1995. *Elementos de matemáticas discretas*. 2 ed. México: McGraw-Hill.

Mora Flores, W. 2010. Introducción a la Teoría de Números. Ejemplos y algoritmos. *Revista digital Matemáticas, Educación e Internet p.1-219*.1ra ed. Escuela de Matemática, Instituto Tecnológico de Costa Rica.

Zamorano Soriano, T. 2011. Cuadernillo de Apuntes de Matemáticas Discretas. TESOEM Tecnológico de Estudios Superiores del Oriente del estado de Mexico.

Indice

Gladys Mónica Romano

Licenciada en Matemática de la Universidad Nacional de Tucumán (UNT), año 1988.
Profesora adjunta de Matemática Discreta de la Universidad Tecnológica Nacional – Facultad Regional Tucumán (UTN-FRT).

Jefe de Trabajos Prácticos de Probabilidades y Estadísticas de la UTN-FRT.
Profesora adjunta de Álgebra de la Universidad del Norte Santo Tomas de Aquino (UNSA)

Profesora adjunta de Métodos Numéricos de la UNSA.

Integrante del grupo de Investigación de Robótica Educativa de la UTN-FRT.

Lidia Beatriz Esper

Licenciada en Matemática, Especialista en Investigación Educativa y Magíster en Enseñanza de la Matemática Superior, egresada de la UNT.

Profesora Asociada en Matemática, Matemática I y Matemática II, de la carrera de Geología de la Facultad de Ciencias Naturales e IML - UNT.

Profesora Adjunta en Matemática Discreta de la carrera en Ingeniería en Sistema de Información de la UTN- FRT y en Matemática I de la Facultad de Cs. Económicas de la UNSTA.

Posee Categoría Investigador Equivalente “II” del Programa de Incentivos a Docentes Investigadores de la UNT, MEd, SPU, y categoría “B” otorgada por Rectorado de la UTN.

Desde 2013 directora de diversos proyectos relacionados con la Ciencia de la Educación y Tecnologías.

Autora de libros y artículos científicos y pedagógicos, producidos en las áreas de investigación, extensión y docencia en Matemática.

edUTecNe

CiN REUN
Red de Editoriales de Universidades Nacionales de la Argentina

LUA Libro Universitario Argentino

UTN FACULTAD REGIONAL TUCUMÁN