MATEMATICA DISCRETA

Versión preliminar

Departamento de Matemática
Universidad Nacional del Sur

Material elaborado por

- **Estela Bianco**
- **Aldo V. Figallo**
- **Claudia Sanza**
- **Alicia N. Ziliani**

Bahía Blanca 2004

Índice General

1 Introducción informal a la lógica matemática

En este capítulo describiremos, de manera intuitiva, algunos conceptos importantes de la lógica matemática. Como creador de esta disciplina debemos considerar al filósofo y matemático alemán del siglo XVII, G. W. Leibniz (1646–1716), pero quien la redescubre y desarrolla es el matemático inglés G. Boole (1815–1864). Entre los que hicieron un aporte decisivo se encuentran el lógico alemán G. Frege (1848-1925) y el lógico y filósofo norteamericano Ch. S. Peirce (1839–1914).

1.1 El lenguaje coloquial

Oraciones declarativas y proposiciones

De los múltiples usos del lenguaje, los que interesan a la lógica son aquellos que cumplen una *función informativa*, esto es, cuando se lo utiliza para suministrar información mediante oraciones declarativas o para presentar argumentos.

Además, lo que interesa de las oraciones declarativas es su *significado*.

Recordemos que en Gramática se indican las siguientes definiciones:

(i) Oración: Palabra o conjunto de ellas, con sentido completo (plano semántico) y autonomía sintáctica (plano sintáctico). No necesita de ningún elemento extraoracional para completar su significación.

(ii) Oraciones declarativas: Son las oraciones que cumplen una *función informativa*, es decir, las que afirman o niegan algo y a las cuales se les puede asignar un *valor de verdad* verdadero o falso.

Por otra parte, en Lógica y en Matemática es frecuente usar la siguiente definición:

(iii) Oraciones equivalentes: Son aquellas que tienen *el mismo significado*.

Cuando admitimos la noción de equivalencia entre las oraciones declarativas, a las *clases* de oraciones equivalentes las llamaremos proposiciones.[1]

[1] El uso que se le da en Lógica a la palabra `proposición´ no coincide con el que se le da en Gramática. En Matemática también se utiliza `enunciado´ como sinónimo de `proposición´.

Ejemplos

(1) *El Dr. Pérez estudia el contrato de locación.*

(2) *El contrato de locación es estudiado por el Dr. Pérez.*

(3) *Rodríguez aborrece las obligaciones.*

(4) *Rodríguez detesta las obligaciones.*

(5) *Si* $6 > 4$, *entonces* $6 > 2$.

(6) *De* $6 > 4$ *resulta* $6 > 2$.

(7) $6 > 2$ *es consecuencia de* $6 > 4$.

(8) *De* $6 > 4$ *se deduce* $6 > 2$.

Las oraciones declarativas indicadas en (1) y (2) tienen el mismo significado y por lo tanto representan a la misma proposición.

Las enunciadas en (3) y (4) representan la misma proposición siempre que aceptemos a la palabra \`detestar´ como sinónimo de la palabra \`aborrecer´.

Las enunciadas en (5), ...,(8) están referidas a propiedades de los números reales y en Matemática se acepta que representan a la misma proposición.

Otros ejemplos

(9) *Siete es mayor que doce.*

(10) *¿Quién es?.*

(11) *Ella es inteligente.*

(12) *En otros planetas del sistema solar hay diversos tipos de seres vivos.*

La oración indicada en (9) es una proposición, y más precisamente una proposición falsa.

La oración del ejemplo (10) es interrogativa y no cumple una función informativa, entonces no puede considerarse ni verdadera ni falsa. Por lo tanto no es una proposición.

En (11) la palabra *ella* es variable, la oración no es ni verdadera ni falsa ya que *ella* no está especificada, luego no es una proposición. La oración de (12) es una proposición ya que es verdadera o falsa, aunque nosotros no estamos en condiciones de decidir cómo es.

Proposiciones simples y compuestas

Las proposiciones se pueden dividir en proposiciones simples y proposiciones compuestas.

Proposiciones simples

Llamaremos proposiciones simples a aquellas que no contienen propiamente a otra proposición.

Ejemplo

El gobernador de Mendoza presentó la renuncia.

Proposiciones compuestas

Diremos que una proposición es compuesta si no es simple.

Ejemplo

Si García aprueba el examen es porque ha estudiado.

Podemos reemplazar la proposición anterior por la siguiente,

Si García ha estudiado, entonces aprueba el examen

la cual contiene propiamente a las proposiciones

García ha estudiado,

aprueba el examen, [*García*]

y por lo tanto es compuesta.

Las conectivas

Son palabras, frases o expresiones lingüísticas que ligan a dos proposiciones llamadas componentes, y tales que la expresión así obtenida es una proposición cuyo valor de verdad queda definido en términos de los valores de verdad de sus componentes.

***La conjunción de proposiciones y la conectiva* y**

La proposición compuesta que obtenemos al unir dos proposiciones por la palabra **y** se denomina conjunción de dichas proposiciones.

Ejemplo

2 *es un número positivo y* 2 *no divide a* 15.

***La disyunción de proposiciones y la conectiva* o**

La proposición compuesta que resulta al unir dos proposiciones por la palabra **o** se denomina disyunción de dichas proposiciones.

Observemos que en el lenguaje coloquial la palabra **o** tiene al menos dos significaciones distintas.

Ejemplos

(i) *Los clientes que sean estudiantes universitarios o jubilados serán favorecidos con un* 20% *de descuento.*

(ii) *Juan acepta ser el candidato a intendente por la lista blanca o renuncia al partido.*

El ejemplo (i) puede ser reformulado del siguiente modo:

Los clientes que sean estudiantes universitarios serán favorecidos con un 20% *de descuento o los clientes que sean jubilados serán favorecidos con un* 20% *de descuento.*

En este caso, la palabra **o** se usa en sentido no excluyente puesto que no se niega la posibilidad de descuento a los jubilados que estudien en la universidad. En cambio en (ii), **o** está usada en un sentido excluyente ya que, o es el candidato a intendente o renuncia, y no se pueden dar las dos posibilidades simultáneamente.

En general, es difícil determinar el sentido en que está usada la conectiva **o**.

En Latín se usan 'aut' y 'vel' para el **o** excluyente y el no excluyente respectivamente.

En Lógica y en Matemática la palabra **o** se usa siempre en el sentido no excluyente.

Ejemplos

(i) *Estudiaré música o canto coral.*

(ii) *El gobierno argentino establece un control sobre la caza del zorro colorado, o esas especies se extinguirán en un futuro muy próximo.*

(iii) 13 *es un número primo, o es divisible por un número distinto de* 1 *y* 13*.*

(iv) *Barcos japoneses o rusos pescan en aguas argentinas.*

En las proposiciones dadas en (i) y (iv) el sentido del **o** es no excluyente, en cambio en (ii) y (iii) es excluyente.

***Proposiciones condicionales y la conectiva* si ... entonces ...**

Dadas dos proposiciones que denominaremos *antecedente* y *consecuente*, llamaremos proposición condicional a la que obtenemos al anteponer la palabra **si** al antecedente y unirla al consecuente por medio de la palabra **entonces**.

Ejemplo

Si Marta fue al museo, entonces vió esa famosa escultura.

tiene por antecedente a

Marta fue al museo

y por consecuente a

vió esa famosa escultura. [*Marta*]

A las conectivas que acabamos de ver las llamaremos conectivas binarias porque siempre ligan a dos proposiciones dando origen a una nueva proposición.

Ahora consideraremos una conectiva unaria, es decir una conectiva que aplicada a una proposición *produce* una nueva proposición.

***La negación de una proposición y la conectiva* no**

Llamaremos negación de una proposición a la proposición que tiene *significado* opuesto a la dada.

En algunos casos es posible obtener la negación de una proposición, colocando la palabra **no** delante del verbo de la proposición dada.

Ejemplo

Si la proposición es

1 *es un número par*,

su negación es

1 *no es un número par.*

También podemos obtener *la negación* anteponiendo a la proposición dada la conectiva **no es el caso que**.

Ejemplo

La negación de

1 *es un número par*,

puede obtenerse escribiendo

no es el caso que 1 *es un número par.*

Observemos que la negación de una proposición simple es compuesta.

Constantes y variables

Hay disciplinas como la Matemática que desarrollan su propio lenguaje coloquial. A veces se hace necesario distinguir en él dos tipos de términos, las *constantes* y las *variables*.

Constantes

Son términos que tienen un significado fijo que permanece invariable en el curso de las consideraciones. Por ejemplo, en la aritmética intervienen constantes tales como *uno* (1), *cero* (0), *suma* (+), *producto* (·), etc.

Variables

No poseen significado propio. Es frecuente designar a las variables con letras $a, b, c \ldots$, x, y, $z \ldots$.

Usaremos variables para construir funciones proposicionales, fórmulas y funciones designativas.[2]

Funciones proposicionales

Dado que las variables no poseen significado propio, la expresión:

[2]En esta introducción, la palabra función no tiene el significado que se le da en Matemática

x es un número natural,

no es una proposición. Se transformará en una proposición si reemplazamos la variable x por alguna constante adecuada.

Las frases que contienen variables y que tienen *la forma* de una proposición las llamaremos funciones proposicionales.

Entonces las funciones proposicionales son tales que al reemplazar las variables por constantes (variables iguales por constantes iguales) se convierten en proposiciones.

Si al efectuar el reemplazo indicado, la proposición obtenida es verdadera, diremos que los objetos designados por esas constantes *satisfacen* la función proposicional.

Ejemplos

Si consideramos nuevamente la función proposicional

x es un número natural,

y reemplazamos x por 3 y posteriormente x por $\frac{1}{2}$ obtenemos las proposiciones:

3 *es un número natural*, [proposición verdadera]

$\frac{1}{2}$ *es un número natural.* [proposición falsa]

Fórmulas

Son funciones proposicionales o proposiciones formadas exclusivamente por símbolos matemáticos.

Ejemplos

(i) $2x < 5$, [fórmula]

(ii) $x + y = 9$, [fórmula]

(iii) *x más y es igual a* 9, [no es una fórmula]

(iv) $4 > -1$. [fórmula]

Funciones designativas

Son aquellas expresiones en las cuales al reemplazar las variables por constantes se transforman en constantes.

Ejemplos

(i) $x + 2$, [si $x = 2$, designa a 4]

(ii) $x < y$. [no es función designativa]

Cuantificadores

Son expresiones del tipo:

(i) para todo x, para todo y, ...

(ii) existen $x, y, \ldots$ tales que ....

La primera recibe el nombre de *cuantificador universal* y la segunda se llama *cuantificador existencial*. Se suelen simbolizar,

(i′) $(\forall x)(\forall y) \ldots,$

(ii′) $(\exists x)(\exists y) \ldots.$

respectivamente.

Ejemplos

(i) *Todos los hombres son mortales.*

(ii) *Algunos hombres son necios.*

Podemos usar variables y cuantificadores para escribir oraciones equivalentes a las anteriores, del siguiente modo:

(i′) *Para todo x, si x es hombre, entonces x es mortal.*

(ii′) *Existe x tal que x es hombre y x es necio.*

Estos ejemplos ilustran que existen casos en que si anteponemos cuantificadores a las funciones proposicionales obtenemos proposiciones, aunque no siempre es así.

Ejemplos

(i) $x + z > y$, [es función proposicional]

(ii) $(\exists x)(\exists y)(\exists z)(x + z > y)$, [es proposición verdadera]

(iii) $(\forall x)(x + z > y)$. [es función proposicional en y, z]

Variables libres y ligadas

Si al anteponer cuantificadores a una función proposicional obtenemos una proposición diremos que las *variables* están *ligadas* (o que son *variables aparentes*), en caso contrario diremos que hay *variables libres* (o *variables efectivas*).

Ejemplos

(i) $(\forall x)(\forall y)(\exists z)(x + y = z)$, [$x, y, z$ son ligadas]

(ii) $(\exists y)(x < y)$. [y es ligada, x es libre]

1.2 El lenguaje simbólico

Desde ahora en adelante supondremos que a cada proposición le podemos hacer corresponder un *nombre*, por ejemplo una letra latina mayúscula: P, Q, R[3]$, \ldots$, y en algunos casos usaremos letras con subíndices: $P_1, P_2, P_3, \ldots$.

Variables proposicionales

Llamaremos variables proposicionales (v.p.) a los símbolos utilizados para designar a las proposiciones simples.

Observemos que las variables proposicionales no son *variables* en el sentido del párrafo ***Constantes y variables***.

[3]Es decir, el símbolo P *representa* a todos los miembros de la colección de oraciones declarativas que tienen el mismo significado.

Meta-variables

Llamaremos variables sintácticas (o meta-variables) a las utilizadas para designar proposiciones arbitrarias y habitualmente las simbolizaremos con letras latinas minúsculas $a, b, c, \ldots, p$, $q, r, \ldots$.

La diferencia entre las letras $P, Q, R, \ldots$ y las letras $a, b, c, \ldots$ consiste en que las primeras son meras *etiquetas* que designan ciertas proposiciones particulares, en cambio las últimas son *variables* que pueden ser sustituídas por dichas *etiquetas.*

El álgebra de las formas proposicionales

Indicaremos a continuación de qué modo podemos describir al conjunto de las proposiciones en términos de las proposiciones simples y las conectivas mencionadas anteriormente.

Sea X el conjunto de las v.p. y consideremos los símbolos $\wedge, \vee, \rightarrow, \sim$. Con $For[X]$ designaremos al conjunto cuyos elementos llamaremos *formas proposicionales* (f.p.), *formas enunciativas* o simplemente *polinomios* y que se construyen por medio de las siguientes reglas:

(R1) si $x \in X$, entonces x es f.p.,

(R2) si p y q son f.p., entonces $p \wedge q$, $p \vee q$, $p \rightarrow q$ son f.p., [p, q variables sintácticas]

(R3) si p es una f.p., entonces $\sim p$ es una f.p., [p variable sintáctica]

(R4) (de cierre) las únicas f.p. son las determinadas por R1, R2 y R3.

Diremos que el *sistema* $\mathcal{F} = \langle For[X], \wedge, \vee, \rightarrow, \sim\rangle$ es el álgebra de las formas proposicionales.

Interpretación de los símbolos

Si p y q son f.p. que designan a ciertas proposiciones del lenguaje coloquial, entonces

$$p \wedge q, \;\; p \vee q, \quad p \rightarrow q,$$

representan a la conjunción, disyunción y condicional de dichas proposiciones, respectivamente. Además,

$$\sim p$$

representa a la negación de la proposición que designa p.

Así por ejemplo, si p y q designan respectivamente las proposiciones

El sol es una estrella,

La luna es un satélite de la Tierra,

entonces $p \wedge q$ designa

El sol es una estrella y la luna es un satélite de la Tierra.

De lo expuesto anteriormente resulta que el conjunto de las proposiciones coincide con $For[X]$.

Tablas de verdad

Ahora bien, como toda proposición es verdadera o falsa, podemos pensar que cualquier f.p. dada toma el *valor de verdad* verdadero o el *valor de verdad* falso.

Consideremos el conjunto $\mathbb{B} = \{\mathrm{F}, \mathrm{V}\}$, donde F y V son símbolos arbitrarios para designar las nociones falso y verdadero respectivamente. Entonces, dada una f.p. p tendrá sentido hablar del *valor de verdad* de p o de la *valuación* de p, que notaremos con $v(p)$, y escribiremos $v(p) = \mathrm{F}$ ó $v(p) = \mathrm{V}$, si p designa una proposición falsa o verdadera, respectivamente.

En este apartado indicaremos de qué modo se puede definir el valor de verdad de una f.p. a partir de los valores de verdad de las v.p. que la constituyen.

En cada caso, lo haremos por medio de una tabla llamada *tabla de verdad* asociada a la f.p..

El producto lógico

Dadas dos proposiciones parece adecuado considerar que la conjunción de ellas sea verdadera cuando ambas lo sean. Luego si $p, q \in X$, la valuación de $p \wedge q$ queda definida a partir de la valuación de p y la valuación de q según se indica en la tabla 1.2.1:

$v(p)$	$v(q)$	$v(p \wedge q)$
F	F	F
F	V	F
V	F	F
V	V	V

tabla 1.2.1

La tabla anterior nos permite definir sobre $\mathbb{B}$, lo que llamaremos producto lógico y notaremos con $\cdot$, del siguiente modo:

$\cdot$	F	V
F	F	F
V	F	V

tabla 1.2.2

Tenemos así que $v(p \wedge q) = v(p) \cdot v(q)$.

La suma lógica

Dadas dos proposiciones y teniendo en cuenta que la disyunción de ellas corresponde al *o* no excluyente (*o débil*) del lenguaje coloquial, resulta natural aceptar que es verdadera cuando al menos una de ellas lo sea. Entonces si $p, q \in X$, la valuación de $p \vee q$ queda determinada por la tabla 1.2.3:

$v(p)$	$v(q)$	$v(p \vee q)$
F	F	F
F	V	V
V	F	V
V	V	V

tabla 1.2.3

Ella induce una operación binaria sobre $\mathbb{B}$, lo que llamaremos suma lógica y que notaremos con $+$, de la siguiente manera:

$+$	F	V
F	F	V
V	V	V

tabla 1.2.4

Entonces se verifica $v(p \vee q) = v(p) + v(q)$.

Observemos que aun cuando nos hemos limitado a considerar el *o* en sentido no excluyente, hay grandes diferencias entre el uso del *o* en el lenguaje diario y en la lógica.

Ejemplos

(i) En el lenguaje coloquial unimos dos proposiciones simples con la letra *o* cuando ellas tienen alguna relación; jamás podríamos considerar la siguiente proposición:

El aeropuerto de Buenos Aires está inoperable o cinco es un número primo.

Y menos aún tomarla como verdadera.

(ii) En el lenguaje coloquial el *o* se halla influído de ciertos factores de carácter sicológico. En efecto

> *"Imaginemos, por ejemplo, que un amigo nuestro, después de habérsele preguntado cuándo dejará la ciudad, contesta que lo hará hoy, mañana o pasado. Si más tarde comprobamos que en aquel momento nuestro amigo ya había decidido partir ese mismo día, tendremos probablemente la impresión de haber sido confundidos ex profeso y que nuestro amigo nos dijo una mentira".*
> (A. Tarski, Introducción a la Lógica, Espasa Calpe, 1968).

La implicación lógica

En el caso de la implicación, el lenguaje coloquial no nos ayuda demasiado. La tabla que vamos a definir se aparta algo de nuestra intuición y estará basada en el uso que se le da en matemática a la noción de implicación.

Nosotros aceptaremos que la frase

si P, *entonces* Q,

tiene el mismo significado que las frases

P *implica* Q,

de P *se deduce* Q,

P *tiene por consecuencia a* Q,

Q *es consecuencia de* P.

Entonces, dadas las v.p. p y q tenemos que completar la tabla siguiente:

$v(p)$	$v(q)$	$v(p \to q)$
F	F	
F	V	
V	F	
V	V	

tabla 1.2.5

Observemos que, como en los casos anteriores, una vez construída la tabla 1.2.5, podremos definir sobre $\mathbb{B}$, lo que llamaremos implicación lógica, y que designaremos con $\mapsto$, de modo tal que se verifique:

$$v(p \to q) = v(p) \mapsto v(q).$$

Entonces podemos modificar la tabla 1.2.5 y escribir

$v(p)$	$v(q)$	$v(p) \mapsto v(q)$
F	F	
F	V	
V	F	
V	V	

tabla 1.2.6

Por lo tanto debemos definir

(i) F $\mapsto$ F,

(ii) F $\mapsto$ V,

(iii) V $\mapsto$ F,

(iv) V $\mapsto$ V.

Teniendo en cuenta que en matemática no se hacen deducciones a partir de hipótesis falsas, sólo deberíamos ocuparnos de los casos (iii) y (iv), pero a los efectos de completar la tabla 1.2.6 también indicaremos los valores de (i) y (ii).

Definimos

(i) F $\mapsto$ F = V,

(ii) F $\mapsto$ V = V,

(iii) V $\mapsto$ F = F,

(iv) V $\mapsto$ V = V.

Estas *igualdades* pueden interpretarse como sigue:

(i) *Es verdadero* (2*do. miembro*) *que de algo falso* (*antecedente*) *se puede deducir algo falso* (*consecuente*).

(ii) *Es verdadero* (2*do. miembro*)*que de algo falso* (*antecedente*) *se puede deducir algo verdadero* (*consecuente*).

(iii) *Es falso* (2*do. miembro*)*que de algo verdadero* (*antecedente*) *se puede deducir algo falso* (*consecuente*).

(iv) *Es verdadero* (2*do. miembro*) *que de algo verdadero* (*antecedente*) *se puede deducir algo verdadero* (*consecuente*).

Indicaremos a continuación ejemplos dados por E. Gentile en "Notas de Algebra", (Eudeba, Bs. As., 1988) que justifican las definiciones (i) y (ii).

(i) De

$$1 = -1, \qquad \text{[proposición falsa]}$$

se deduce, sumando 1 a ambos miembros,

$$2 = 0. \qquad \text{[proposición falsa]}$$

(ii) De

$$1 = -1, \qquad \text{[proposición falsa]}$$

se deduce, elevando ambos miembros al cuadrado,

$$1 = 1. \qquad \text{[proposición verdadera]}$$

Por otra parte, dado que la Matemática no es una ciencia contradictoria, jamás probaremos a partir de una hipótesis verdadera una conclusión falsa. Esto motiva la definición (iii).

Finalmente, resulta adecuado considerar como verdaderas las conclusiones obtenidas de hipótesis verdaderas lo que justifica la definición de (iv).

Resumiendo, la tabla 1.2.5 se completa como sigue:

$v(p)$	$v(q)$	$v(p \to q)$
F	F	V
F	V	V
V	F	F
V	V	V

tabla 1.2.7

Luego, la tabla 1.2.7 nos permite definir la implicación lógica del siguiente modo:

$\mapsto$	F	V
F	V	V
V	F	V

tabla 1.2.8

La negación lógica

Dada una proposición, su negación será verdadera si ella es falsa y será falsa si ella es verdadera. Luego, la tabla de verdad es:

$v(p)$	$v(\sim p)$
F	V
V	F

tabla 1.2.9

En $\mathbb{B}$ queda definida la llamada negación lógica, que notaremos con $-$, como sigue:

x	$-x$
F	V
V	F

tabla 1.2.10

Entonces se verifica $v(\sim p) = -v(p)$.

A partir de las tablas anteriores podemos construir la tabla de verdad de cualquier f.p..

Ejemplos

Para simplificar, cuando no haya lugar a confusión al calcular las tablas de verdad, escribiremos p en lugar $v(p)$.

(i) $p \wedge (\sim q)$

p	q	$\sim q$	$p \wedge (\sim q)$
F	F	V	F
F	V	F	F
V	F	V	V
V	V	F	F

(ii) $p \to (q \vee r)$

p	q	r	$q \vee r$	$p \to (q \vee r)$
F	F	F	F	V
F	F	V	V	V
F	V	F	V	V
F	V	V	V	V
V	F	F	F	F
V	F	V	V	V
V	V	F	V	V
V	V	V	V	V

El álgebra de prueba

Llamaremos álgebra de prueba al *sistema* $\langle \mathbb{B}, \cdot, +, \mapsto, -, \mathrm{F}, \mathrm{V} \rangle$, donde $\cdot$, $+$, $\mapsto$ y $-$ son las definidas por las tablas 1.2.2, 1.2.4, 1.2.8 y 1.2.10 respectivamente.

En lo que sigue cambiaremos los símbolos F, V por los símbolos 0 y 1, respectivamente.

1.3 Tautologías, contradicciones y contingencias

Sea $p \in For[X]$, diremos que

(i) p es una *tautología* si la tabla de verdad de p toma siempre el valor 1,

(ii) p es una *contradicción* si la tabla de verdad de p toma siempre el valor 0,

(iii) p es una *contingencia* si no es una tautología ni una contradicción.

Ejemplos

Hallar la tabla de verdad de

(i) $(p \to q) \to ((p \to r) \to (p \to (q \wedge r)))$.

Para simplificar, escribiremos

$$\alpha = (p \to r) \to (p \to (q \wedge r)),$$

$$\beta = (p \to q) \to ((p \to r) \to (p \to (q \wedge r))).$$

p	q	r	$p \to q$	$p \to r$	$q \wedge r$	$p \to (q \wedge r)$	α	β
0	0	0	1	1	0	1	1	1
0	0	1	1	1	0	1	1	1
0	1	0	1	1	0	1	1	1
0	1	1	1	1	1	1	1	1
1	0	0	0	0	0	0	1	1
1	0	1	0	1	0	0	0	1
1	1	0	1	0	0	0	1	1
1	1	1	1	1	1	1	1	1

Por lo tanto β es una tautología.

(ii) $p \wedge \sim p$

p	$\sim p$	$p \wedge \sim p$
0	1	0
1	0	0

Por lo tanto $p \wedge \sim p$ es una contradicción.

Tautologías importantes

(1) $p \to p$, [ley de identidad]

(2) $(p \wedge q) \to p$,

$(p \wedge q) \to q$, [leyes de simplificación del producto lógico]

(3) $p \to (p \vee q)$,

$q \to (p \vee q)$, [leyes de simplificación de la suma lógica]

(4) $(p \to q) \to ((q \to r) \to (p \to r))$, [ley del silogismo hipotético]

(5) $\sim (p \wedge \sim p)$, [ley de contradicción]

(6) $p \vee \sim p$, [ley del tercero excluído]

(7) $p \to (q \to p)$, [ley de absorción]

(8) $\sim p \to (p \to q)$, [ley de Duns Scoto]

(9) $(p \to q) \vee (q \to p)$. [ley de linealidad]

Ya sabemos que podemos interpretar a las fórmulas como representaciones simbólicas de frases del lenguaje coloquial, así por ejemplo pensaremos que las tautologías (1) a (9) pueden ser simbolizaciones de las frases

(1) *de p se deduce p*,

(2) *p y q implican p*,

p y q implican q,

(3) *de p se deduce p o q*,

de q se deduce p o q,

(4) *si p implica q, entonces p implica r es consecuencia de q implica r*,

(5) *no es el caso que p y no p*,

(6) *p o no p*,

(7) *de p se deduce que q implica p*,

(8) *la negación de p implica que q es consecuencia de p*,

(9) *de p se deduce q o de q se deduce p.*

1.4 Equivalencia semántica

Dadas $p, q \in For[X]$, diremos que p es semánticamente equivalente a q y escribiremos $p \approx q$, si ambas tienen la misma tabla de verdad.

Ejemplos

(i) $p \to q \approx \sim p \vee q$,

p	q	$\sim p$	$p \to q$	$\sim p \vee q$
0	0	1	**1**	**1**
0	1	1	**1**	**1**
1	0	0	**0**	**0**
1	1	0	**1**	**1**

(ii) $p \vee q \approx (p \to q) \to q$,

p	q	$p \to q$	$p \vee q$	$(p \to q) \to q$
0	0	1	**0**	**0**
0	1	1	**1**	**1**
1	0	0	**1**	**1**
1	1	1	**1**	**1**

Equivalencias importantes

Sean $p, q, r \in For[X]$. Entonces

(1) $p \vee q \approx q \vee p$,

(2) $p \wedge q \approx q \wedge p$,

(3) $p \vee (q \vee r) \approx (p \vee q) \vee r$,

(4) $p \wedge (q \wedge r) \approx (p \wedge q) \wedge r$,

(5) $p \wedge (q \vee r) \approx (p \wedge q) \vee (p \wedge r)$,

(6) $p \vee (q \wedge r) \approx (p \vee q) \wedge (p \vee r)$,

(7) $p \wedge q \approx \sim (\sim p \vee \sim q)$,

(8) $p \vee q \approx \sim (\sim p \wedge \sim q)$,

(9) $p \approx p \vee p$,

(10) $p \approx p \wedge p$.

Como consecuencia de (3) de ahora en más escribiremos $p \vee q \vee r$ para indicar indistintamente $p \vee (q \vee r)$ ó $(p \vee q) \vee r$. Análogamente, de (4) escribiremos $p \wedge q \wedge r$ para indicar $p \wedge (q \wedge r)$ ó $(p \wedge q) \wedge r$.

1.5 Conjunto adecuado de conectivas

Un conjunto $\{c_1, \ldots, c_n\}$ de conectivas se dice *adecuado* si toda tabla de verdad puede ser obtenida en términos de esas conectivas.

Ejemplos

Los siguientes son conjuntos adecuados de conectivas:

(i) $\{\wedge, \vee, \rightarrow, \sim\}$,

(ii) $\{\sim, \vee\}$.

1.6 Formas argumentativas

Llamaremos forma argumentativa a una sucesión finita $p_1, p_2, \ldots, p_n, p$ de f.p., y diremos que p es *la conclusión* de las *premisas* $p_1, p_2, \ldots, p_n$. A veces representaremos a una forma argumentativa de alguna de las siguientes maneras:

(i) $p_1, p_2, \ldots, p_n, \ \therefore \ p$,

(ii)
$$\begin{array}{ll} & p_1, \\ & p_2, \\ & \vdots \\ & p_n, \\ \therefore & p. \end{array}$$

Ejemplos

(i) modus ponens:

$$\begin{array}{ll} & p \rightarrow q, \\ & p, \\ \therefore & q. \end{array}$$

(ii) modus tollens:

$$\begin{array}{ll} & p, \\ & \sim q \to \sim p, \\ \therefore & q. \end{array}$$

Validez de una forma argumentativa

Una forma argumentativa $p_1, p_2, \ldots, p_n, \therefore p$ es válida si, para toda asignación de valores de verdad a las v.p. que aparecen en ellas que verifique $v(p_1) = \ldots = v(p_n) = 1$, también se verifica que $v(p) = 1$.

Ejemplos

Analizar si las siguientes formas argumentativas son válidas o no:

(i)
$$\begin{array}{ll} & p, \\ & \sim q \to p, \\ \therefore & q. \end{array}$$

p	q	$\sim q$	$\sim q \to p$	$\boldsymbol{p}$	$\boldsymbol{\sim q \to p}$	$\boldsymbol{q}$
0	0	1	0	0	0	0
0	1	0	1	0	1	1
1	0	1	1	**1**	**1**	**0**
1	1	0	1	1	1	1

Por lo tanto no es válida.

(ii)
$$\begin{array}{ll} & p, \\ & \sim q \to \sim p, \\ \therefore & q. \end{array}$$

p	q	$\sim q$	$\sim p$	$\sim q \to \sim p$	p	$\sim q \to \sim p$	q
0	0	1	1	1	0	1	0
0	1	0	1	1	0	1	1
1	0	1	0	0	1	0	0
1	1	0	0	1	**1**	**1**	**1**

Por lo tanto es válida.

1.7 Consecuencias semánticas

Si una forma argumentativa

$$p_1, p_2, \ldots, p_n, \ \therefore \ p$$

es válida, diremos que p *es consecuencia semántica* de $p_1, p_2, \ldots, p_n$ y escribiremos:

$$\{p_1, p_2, \ldots, p_n\} \models p.$$

Más generalmente, si A es un conjunto cualquiera de f.p., diremos que p es *consecuencia semántica* de A y escribiremos $A \models p$, si existen $p_1, \ldots, p_n \in A$ tales que $\{p_1, \ldots, p_n\} \models p$.

La correspondencia que a cada $A \subseteq For[X]$ le asigna el conjunto $C(A) = \{p : A \models p\}$ recibe el nombre de operador de consecuencia semántico.

Teoremas semánticos

Si p es consecuencia semántica de $\emptyset$, diremos que p es un *teorema semántico* y escribiremos $\models p$.

Observemos que $\models p$ si, y sólo si, p es una tautología.

Versión semántica del Teorema de la Deducción

Las siguientes condiciones son equivalentes:

(i) $\{p_1, p_2, \ldots, p_n\} \models p$,

(ii) $\models (p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow p$.

Ejemplo

Verificar que $\models ((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$.

Aplicando el teorema de la deducción probaremos que $\{p \rightarrow q, q \rightarrow r\} \models p \rightarrow r$

p	q	r	$p \to q$	$q \to r$	$p \to r$
0	0	0	**1**	**1**	**1**
0	0	1	**1**	**1**	**1**
0	1	0	1	0	1
0	1	1	**1**	**1**	**1**
1	0	0	0	1	0
1	0	1	0	1	1
1	1	0	1	0	0
1	1	1	**1**	**1**	**1**

1.8 Formas proposicionales normales disyuntivas y conjuntivas

Si en la construcción de la f.p. α intervienen las variables $x_1, x_2, \ldots, x_n$, en los casos necesarios, escribiremos $\alpha = \alpha(x_1, x_2, \ldots, x_n)$.

Formas normales disyuntivas

Llamaremos *forma normal disyuntiva* (f.n.d.) a toda f.p. $\alpha = \alpha(x_1, x_2, \ldots, x_n)$ tal que

$$\alpha = \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} x_{ij}^{*}, \text{ donde } x_{ij}^{*} = x_t \quad \text{ó} \quad x_{ij}^{*} = \sim x_t.$$

Se puede probar que

Toda $\alpha \in For[X]$ que no es una contradicción es semánticamente equivalente a una forma normal disyuntiva β.

Método para calcular una f.n.d. equivalente a una f.p. α

Sea $\alpha = \alpha(x_1, \ldots, x_n) \in For[X]$.

Paso 1

Calculamos la tabla de verdad de α.

Paso 2

Hallamos todas las n–uplas $t = (t_1, \ldots, t_n)$ de las valuaciones de las variables, para cuales α toma el valor 1.

Paso 3

Para cada uno de los t obtenidos en el paso 2, consideramos la fórmula $\alpha_t = x_1^* \wedge \ldots \wedge x_n^*$, donde $x_i^* = x_i$, si $t_i = 1$ ó $x_i^* = \sim x_i$, si $t_i = 0$.

Paso 4

La fórmula buscada es: $\beta = \alpha_{t_1} \vee \alpha_{t_2} \vee \ldots \vee \alpha_{t_k}$.

Ejemplo

Hallar la f.n.d. de $p \to (\sim q \wedge r)$.

p	q	r	$\sim q$	$\sim q \wedge r$	$p \to (\sim q \wedge r)$
0	**0**	**0**	1	0	**1**
0	**0**	**1**	1	1	**1**
0	**1**	**0**	0	0	**1**
0	**1**	**1**	0	0	**1**
1	0	0	1	0	0
1	**0**	**1**	1	1	**1**
1	1	0	0	0	0
1	1	1	0	0	0

$t_1 = (0, 0, 0), \quad \alpha_{t_1} = \sim p \wedge \sim q \wedge \sim r,$

$t_2 = (0, 0, 1), \quad \alpha_{t_2} = \sim p \wedge \sim q \wedge r,$

$t_3 = (0, 1, 0), \quad \alpha_{t_3} = \sim p \wedge q \wedge \sim r,$

$t_4 = (0, 1, 1), \quad \alpha_{t_4} = \sim p \wedge q \wedge r,$

$t_5 = (1, 0, 1), \quad \alpha_{t_5} = p \wedge \sim q \wedge r,$

$(\sim p \wedge \sim q \wedge \sim r) \vee (\sim p \wedge \sim q \wedge r) \vee (\sim p \wedge q \wedge \sim r) \vee (\sim p \wedge q \wedge r) \vee (p \wedge \sim q \wedge r).$

Formas normales conjuntivas

Llamaremos *forma normal conjuntiva* (f.n.c.) a toda f.p. $\alpha(x_1, \ldots, x_n)$ de la forma

$\bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} x_{ij}^*$, donde $x_{ij}^* = x_t$ ó $x_{ij}^* = \sim x_t$.

Se puede probar que

Toda $\alpha \in For[X]$ que no es una tautología es semánticamente equivalente a una forma normal conjuntiva β.

Método para calcular una f.n.c. equivalente a una f.p. α

Sea $\alpha = \alpha(x_1, \ldots, x_n) \in For[X]$.

Paso 1

Calculamos la tabla de verdad de α.

Paso 2

Hallamos todas las n–uplas $t = (t_1, \ldots, t_n)$ de las valuaciones de las variables, para cuales α toma el valor 0.

Paso 3

Para cada uno de los t obtenidos en el paso 2, consideramos la fórmula
$\alpha_t = x_1^* \vee \ldots \vee x_n^*$, donde $x_i^* = x_i$, si $t_i = 0$ ó $x_i^* = \sim x_i$, si $t_i = 1$.

Paso 4

La fórmula buscada es: $\beta = \alpha_{t_1} \wedge \alpha_{t_2} \wedge \ldots \wedge \alpha_{t_k}$.

Ejemplo

Hallar la f.n.c. de $(\sim p \to q) \wedge r$.

p	q	r	$\sim p$	$\sim p \to q$	$(\sim p \to q) \wedge r$
0	**0**	**0**	1	0	**0**
0	**0**	**1**	1	0	**0**
0	**1**	**0**	1	1	**0**
0	1	1	1	1	1
1	**0**	**0**	0	1	**0**
1	0	1	0	1	1
1	**1**	**0**	0	1	**0**
1	1	1	0	1	1

$t_1 = (0,0,0), \quad \alpha_{t_1} = p \vee q \vee r,$

$t_2 = (0,0,1), \quad \alpha_{t_2} = p \vee q \vee \sim r,$

$t_3 = (0,1,0), \quad \alpha_{t_3} = p \vee \sim q \vee r,$

$t_4 = (1,0,0), \quad \alpha_{t_4} = \sim p \vee q \vee r,$

$t_5 = (1,1,0), \quad \alpha_{t_5} = \sim p \vee \sim q \vee r,$

$(p \vee q \vee r) \wedge (p \vee q \vee \sim r) \wedge (p \vee \sim q \vee r) \wedge (\sim p \vee q \vee r) \wedge (\sim p \vee \sim q \vee r).$

1.9 Ejercicios

E 1.9.1

(i) ¿Cuáles de las siguientes expresiones son proposiciones?

(a) 7 es un número par.

(b) ¿Qué hora es?

(c) $3^2 - 5$ es un número impar.

(d) El río Colorado provee de agua a todas las quintas linderas.

(e) Ella ganó la Lotería.

(ii) Indicar cuáles de las siguientes proposiciones son compuestas:

(a) En la Argentina no se han producido epidemias de viruela en los últimos diez años.

(b) Juan no está bien informado o no quiere aceptar las noticias.

(c) Comprendo los puntos de vista de Marta, pero no los comparto.

(d) Si me levanto temprano, tomo el tren de las ocho.

(e) En los días feriados el centro de Bahía Blanca permanece desierto.

E 1.9.2

¿Cuáles de las siguientes expresiones son funciones proposicionales, funciones designativas y fórmulas?

(i) x es hermano de Juan.

(ii) $\sqrt{x^2} = |x|$.

(iii) $2x^2 - 3y + 1$.

(iv) el máximo común divisor de x, y y z.

(v) y es el máximo común divisor de x y z.

E 1.9.3

Las funciones proposicionales que aparecen en la aritmética y que sólo contienen una variable (aunque ésta puede intervenir, como es natural, en varios lugares de la función dada) se pueden dividir en tres categorías:

(a) funciones que se satisfacen para todo número,

(b) funciones que no se satisfacen para ningún número,

(c) funciones que se satisfacen para algunos números y no se satisfacen para otros.

¿A cuál de estas categorías pertenecen las siguientes funciones proposicionales considerando como dominio de interpretación al conjunto de los números reales?.

(i) $\dfrac{x}{3} = 4 + x$.

(ii) $x^2 < 0$.

(iii) $x^2 + 2x + 1 = 0$.

(iv) $x \leq |x|$.

(v) $x + 10 = x + 1$.

(vi) $x + 10 > 1 + x$.

E 1.9.4

(i) Si a la función proposicional $x + y = x$ se le anteponen cuantificadores, se podrán formar con ella seis proposiciones distintas; por ejemplo:

(a) para números cualesquiera x e y, $x + y = x$,

(b) para un número cualequiera x, existe un número y tal que $x + y = x$,

(c) existe un número y tal que para todo número x, $x + y = x$.

Formular las retantes proposiciones y estudiar cuáles de ellas son verdaderas, considerando como dominio de interpretación al conjunto de los números reales.

(ii) Idem inciso (i) para la función proposicional $x^2 < y$.

E 1.9.5

Indicar en cada caso una proposición del lenguaje coloquial que no contenga cuantificadores ni variables y con significado equivalente a:

(i) Para todo x, si x es país inexplorado, entonces x es fascinante.

(ii) Existe x tal que x es político y x es honesto.

E 1.9.6

Sustituir cada una de las siguientes proposiciones por otra con significado equivalente formulada con cuantificadores y variables:

(i) Algunos trabajos son insalubres.

(ii) Todos los comerciantes aumentarán sus precios.

(iii) Ciertas avenidas tienen doble circulación.

(iv) Cualquier rectángulo tiene cuatro lados.

E 1.9.7

Escribir las siguiente expresiones en lenguaje simbólico y distinguir variables libres y ligadas:

(i) para todo x, $x \cdot (-y) = -(x \cdot y)$,

(ii) para números cualesquiera x e y, si $x < y$ y $z < 0$, entonces $x \cdot z > y \cdot z$,

(iii) existe un número x tal que $x + y = x$,

(iv) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$,

(vi) para todo x, $x^2 \geq 0$.

E 1.9.8

¿Qué números reales satisfacen cada una de las siguientes funciones proposicionales?

(i) para todo número x, $x^2 > y$,

(ii) existe un número y tal que $\dfrac{1}{y} = x$.

E 1.9.9

(i) Traducir las siguientes fórmulas al lenguaje coloquial:

(a) $(\forall x)(x < 0 \to (\exists y)(y > 0 \ \wedge \ x + y = 0))$,

(b) $(\exists x)(y < x \ \wedge \ x < 2 \wedge \ \sim (x \cdot y > 0))$,

(c) $(\forall y)(x^2 = y \to (\exists z)(x \cdot z = -y \ \vee \ x \cdot z = y))$.

(ii) Recíprocamente, escribir las siguientes expresiones en lenguaje simbólico:

(d) existen números y y z tales que para todo número x, $z < x + y$ y $z > y$,

(e) para números cualesquiera x e y, si $(x + y)^2 = z$, entonces $x^2 + 2xy + y^2 = z$,

(f) para números cualesquiera y y z, existe un número x tal que si $y < x$ y $z < x$, entonces no es el caso que $y + z \geq x$.

Señalar en cada una de las expresiones (a), ... , (f) cuáles son variables libres y cuáles ligadas. Si alguna variable es libre, dar ejemplos siempre que sea posible, de números reales que satisfacen y que no satisfacen las funciones proposicionales. Para aquellas expresiones que son proposiciones, determinar si son verdaderas o falsas considerando como dominio de interpretación al conjunto de los números reales.

E 1.9.10

Dadas las siguientes proposiciones:

A: 15 es múltiplo de 5,

B: 4 es divisible por 2,

C: 9 es divisible por 7,

traducir al lenguaje coloquial

(i)	$B \vee \sim C$,	(ii)	$\sim B \vee (A \to C)$,
(iii)	$(C \wedge \sim A) \to B$,	(iv)	$C \wedge (\sim A \to B)$.

E 1.9.11

Escribir en lenguaje simbólico e indicar el valor de verdad de cada una de las siguientes proposiciones:

(i) 8 es par o 6 es impar,

(ii) 8 es par y 6 es impar,

(iii) 8 es impar o 6 es impar,

(iv) 8 es impar y 6 es impar,

(v) si 8 es impar, entonces 6 es impar,

(vi) si 8 es par, entonces 6 es impar,

(vii) si 8 es impar, entonces 6 es par,

(viii) si 8 es impar y 6 es impar, entonces $8 < 6$.

E 1.9.12

Indicar en cada caso, cuál es la forma correcta de negar las siguientes proposiciones:

(i) $2 < 5$ y 3 es impar.

(a) $2 > 5$ y 3 es par,

(b) $2 \geq 5$ y 3 es par,

(c) $2 \geq 5$ o 3 es impar,

(d) $2 \geq 5$ o 3 es par.

(ii) Llueve o voy al cine.

(a) no llueve o no voy al cine,

(b) ni llueve ni voy al cine,

(c) no es cierto que llueve y no voy al cine.

(iii) 6 es múltiplo de 2 y 3.

(a) 6 no es múltiplo de 2 y no es múltiplo de 3,

(b) 6 no es múltiplo de 2 o no es múltiplo de 3,

(c) 6 es múltiplo de 2 y no es múltiplo de 3,

(d) 6 no es múltiplo de 2 ni de 3.

E 1.9.13

Dados p, $q \in For[X]$, consideremos la conectiva $\leftrightarrow$ cuya tabla de verdad es la siguiente:

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

Sean r, s, $t \in For[X]$ tales que $v(s) = v(r) = 1$ y $v(t) = 0$. Calcular el valor de verdad de las siguientes f.p.:

(i) $(s \wedge t) \leftrightarrow t$,

(ii) $(r \leftrightarrow t) \wedge \sim r$,

(iii) $\sim (r \leftrightarrow \sim t)$,

(iv) $(t \vee \sim r) \leftrightarrow (t \wedge s)$.

E 1.9.14

Construir las tablas de verdad de las siguientes f.p. y clasificarlas en tautologías, contradicciones y contingencias:

(i) $\sim p \to (q \vee \sim p)$,

(ii) $((p \wedge q) \to p) \to q$,

(iii) $(p \wedge q) \rightarrow \sim p$,

(iv) $(\sim p \rightarrow q) \rightarrow (\sim q \rightarrow p)$,

(v) $p \wedge \sim (p \vee q)$,

(vi) $((p \wedge q) \vee (r \wedge \sim q)) \leftrightarrow ((\sim p \wedge q) \vee (\sim r \wedge \sim q))$.

E 1.9.15

Determinar, en cada caso, α, $\beta \in For[X]$ tales que las siguientes f.p. sean tautologías:

(i) $\sim \alpha \rightarrow \alpha$,

(ii) $\alpha \vee \beta$,

(iii) $\alpha \wedge (\sim \alpha \rightarrow \beta)$.

E 1.9.16

Demostrar que los siguientes pares de f.p. son semánticamente equivalentes:

(i)	$\sim\sim p$,	p,
(ii)	$p \leftrightarrow q$,	$(p \wedge q) \vee (\sim p \wedge \sim q)$,
(iii)	$(p \wedge q) \rightarrow r$,	$p \rightarrow (q \rightarrow r)$,
(iv)	$p \rightarrow q$,	$\sim q \rightarrow \sim p$,
(v)	$p \rightarrow q$,	$\sim p \vee q$,
(vi)	$\sim (p \vee q)$,	$\sim p \wedge \sim q$,
(vii)	$(p \rightarrow q) \rightarrow q$,	$p \vee q$,
(viii)	$p \rightarrow (q \rightarrow r)$,	$q \rightarrow (p \rightarrow r)$,
(ix)	$(p \rightarrow q) \wedge (q \rightarrow p)$,	$(p \wedge q) \vee (\sim p \wedge \sim q)$.

E 1.9.17

Probar que $\{\sim, \wedge\}$, $\{\sim, \vee\}$ y $\{\sim, \rightarrow\}$ son conjuntos adecuados de conectivas.

E 1.9.18

Investigar la validez de las siguientes formas argumentativas:

(i) $p \to q$

$\sim q \vee r$

$\therefore\ p \to r$

(ii) $q \wedge r$

$p \to q$

r

$\therefore\ p$

(iii) $(p \wedge q) \to (r \vee s)$

$\sim r \wedge \sim s$

$\therefore\ \sim p \vee \sim q$

(ii) $p \vee (q \wedge r)$

$s \to \sim (p \vee q)$

$s \vee t$

$\therefore\ t$

E 1.9.19

Para cada una de las siguientes argumentaciones escribir una forma argumentativa que se corresponda con ella y determinar si es válida o si es no válida.

(i) Si Marta ha ido al museo, entonces conoce esa famosa escultura. Marta no conoce esa famosa escultura. Luego, Marta no ha ido al museo.

(ii) Los soldados encontraron cerrado el paso, o si temieron un ataque enemigo, se refugiaron en las montañas. Pero los soldados no se refugiaron en las montañas. Luego, los soldados encontraron cerrado el paso o no temieron un ataque enemigo.

(iii) Pedro no fue debidamente defendido o es realmente culpable. Si Carlos fue su abogado, fue debidamente defendido. Por lo tanto, si Carlos fue su abogado, Pedro es realmente culpable.

(iv) Si Carlos aumenta de peso, entonces abusó de dulces o abusó de pastas. Si Carlos no abusó de dulces, entonces está mintiendo. Si Carlos está mintiendo y aumenta de peso, entonces no abusó de pastas. Por lo tanto, Carlos abusó de dulces.

E 1.9.20

Demostrar que cualesquiera sean p, q, $r \in For[X]$

(i) $\{\sim p\} \models (p \to q)$,

(ii) $\models (p \to p)$,

(iii) $\{p \wedge \sim p\} \models q$,

(iv) $\{p \vee q, \sim p\} \models q$,

(v) $\{p \to q, \sim q\} \models \sim p$,

(vi) $\{p \to q\} \models (r \to p) \to (r \to q)$.

E 1.9.21

Demostrar aplicando la versión semántica del teorema de la deducción.

(i) $\models ((p \to q) \wedge (q \to r)) \to (p \to r)$,

(ii) $\models ((p \to q) \wedge (p \wedge r)) \to (q \wedge r)$,

(iii) $\models ((p \to q) \wedge (p \to (q \to r))) \to (p \to r)$.

E 1.9.22

Encontrar en cada caso una f.p. en

(i) forma normal disyuntiva semánticamente equivalente a

  (a) $(p \vee q) \to \sim q$,

  (b) $\sim (p \wedge q) \leftrightarrow (p \vee q)$,

  (c) $(p \to q) \vee (p \wedge \sim r)$.

(ii) forma normal conjuntiva semánticamente equivalente a

  (a) $(p \vee q) \to (\sim q \to \sim p)$,

  (b) $(p \to q) \wedge r$,

  (c) $p \to (q \leftrightarrow r)$.

2 Conjuntos

2.1 Introducción

La siguiente es una exposición de la teoría de conjuntos de naturaleza intuitiva. Tomaremos como conceptos primitivos, es decir no definidos, a las nociones de elemento y de conjunto. También utilizaremos una relación primitiva que notaremos $\in$ y que llamaremos relación de pertenencia.

Habitualmente designaremos a los elementos y a los conjuntos con letras latinas minúsculas y mayúsculas respectivamente, aunque a veces no es posible o no es conveniente respetar estas convenciones.

Un conjunto está determinado cuando disponemos de *un criterio* para establecer si un elemento pertenece o no a dicho conjunto.

A las fórmulas $a \in A$, $a \notin A$ las leeremos: *el elemento a pertenece al conjunto A* y *el elemento a no pertenece al conjunto A*, respectivamente.

Igualdad de conjuntos

A la fórmula $A = B$ la leeremos: *el conjunto A es igual al conjunto B*, o *A es igual a B*. Y admite la siguiente interpretación:

> A y B son dos conjuntos que tienen los mismos elementos y por lo tanto deben ser idénticos.

A la fórmula $A \neq B$ la leeremos: *los conjuntos A y B son distintos*. Y significa que A y B no son idénticos, es decir, que no tienen los mismos elementos.

Representaciones de conjuntos

Representación por extensión

Comenzaremos analizando un ejemplo. Para indicar al conjunto E cuyos elementos son las estaciones del año, escribiremos

$E = \{\text{verano, otoño, invierno, primavera}\}$.

Entonces diremos que el segundo miembro de esta igualdad es una *representación por extensión* de E.

Generalizando lo anterior, para designar conjuntos por extensión, con respecto a sus elementos, tendremos en cuenta las siguientes reglas:

(R1) Los escribiremos separados por comas y encerrados por una llave inicial y otra final.

(R2) No repetiremos ninguno de ellos.

(R3) Los denotaremos en cualquier orden.

Aplicando R3 al conjunto E, también escribiremos:

$$E = \{\text{otoño, verano, primavera, invierno}\}.$$

Es claro que los conjuntos que no tienen un número finito de elementos, a los que llamaremos conjuntos infinitos, no admiten representaciones por extensión. Sin embargo, en algunos casos de conjuntos infinitos, es frecuente utilizar representaciones similares a ellas, así por ejemplo se suele designar al conjunto $I\!N$ de los números naturales con $\{1, 2, 3, \dots\}$.

Representación por comprensión

Si D es el conjunto de los días del año 1994, para representarlo por extensión deberemos escribir sus 365 elementos, utilizando símbolos de algún tipo, por ejemplo

$$D = \{1/1, 2/1, \dots, 31/1, 1/2, \dots, 28/2, \dots, 1/12, \dots, 31/12\},$$

donde los puntos suspensivos significan que hemos omitido escribir algunos de sus elementos. La siguiente, es una manera más sencilla de describir a D:

$$D = \{x : x \text{ es día del año 1994}\}.$$

Diremos que el segundo miembro de esta igualdad es una *representación por comprensión* de D y la leeremos: *D es el conjunto de los elementos x tales que x es día del año 1994.*

Consideremos ahora el conjunto H de los habitantes de la República Argentina (R.A.). Aun cuando pudiésemos contar a sus elementos, es prácticamente imposible precisar cuales son, y por lo tanto, no podríamos representarlo por extensión. Luego, es imprescindible hacerlo por comprensión. Entonces escribiremos:

$H = \{x : x \text{ es habitante de la R.A.}\}$.

El esquema general para representar un conjunto A por comprensión es el siguiente:

(C1) Determinaremos *una cláusula* que notaremos con P y tal que la verifiquen únicamente los elementos de A.

(C2) Escribiremos $A = \{x : x \text{ verifica P}\}$, y leeremos: *$A$ es el conjunto de los elementos x que verifican P.*

En general, existe más de una cláusula para definir a un conjunto. En efecto, si consideramos

$A = \{3, 4, 5, 6, 7\}$

y las cláusulas

P1: $x \in I\!N$, x es mayor que 2 y menor que 8,

P2: $x \in I\!N$, x es mayor o igual que 3 y menor que 8,

resulta claro que vale

$A = \{x : x \text{ verifica P1}\} = \{x : x \text{ verifica P2}\}$.

Observemos que existen expresiones lingüísticas con apariencia de cláusulas, que no pueden ser utilizadas como tales. Así por ejemplo,

P3: Un número natural par.

Por otra parte, hay expresiones de naturaleza subjetiva que no definen a un conjunto; una de ellas es:

P4: Los alumnos inteligentes de segundo grado.

Algunas observaciones sobre las representaciones

Si S es el conjunto de los días de la semana, aceptaremos que podemos escribir:

$$\begin{aligned}
S &= \{x : x \text{ es día de la semana}\} \\
&= \{\text{lunes, martes, miércoles, jueves, viernes, sábado, domingo}\} \\
&= \{\text{monday, tuesday, wednesday, thursday, friday, saturday, sunday}\} \\
&= \{\text{lu, ma, mi, ju, vi, sa, do}\}.
\end{aligned}$$

En la tercera representación de S, los días de la semana están escritos en inglés, y en la cuarta hemos usado abreviaturas de los nombres de los días de la semana escritos en castellano. Es decir, como siempre se trata del mismo conjunto S, no podemos cambiar sus elementos, y por lo tanto estamos admitiendo que podemos cambiar los nombres de dichos elementos.

2.2 El conjunto vacío

Necesariamente debemos admitir que todo elemento es igual a si mismo, esto es, debemos aceptar que a la cláusula,

P: los x tales que $x = x$,

la verifican todos los elementos que consideremos.

En oposición, aceptaremos que la cláusula

$\overline{\text{P}}$: los x tales que $x \neq x$,

no es verificada por ningún elemento.

D 2.2.1 *Denotaremos con* $\emptyset$ *al conjunto* $\{x : x \neq x\}$ *y lo llamaremos conjunto vacío.*

2.3 Descripción gráfica de conjuntos

Hacer dibujos para simbolizar conjuntos es un recurso didáctico de gran utilidad. El procedimiento que detallaremos a continuación, tiene limitaciones y deberemos tener siempre presente que se trata, como lo manifestamos al comienzo, de un buen recurso didáctico.

Las reglas que utilizaremos para realizar el diagrama de un conjunto A son las siguientes:

(R1) Si $A = \emptyset$, entonces A no tiene diagrama.

(R2) Si $A \neq \emptyset$, dibujaremos una curva cerrada que no se entrecruce, como la de la figura 2.3.1 y representaremos a A con la región sombreada y sin la curva, como la de la figura 2.3.2.

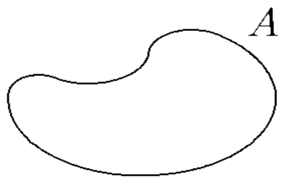


figura 2.3.1

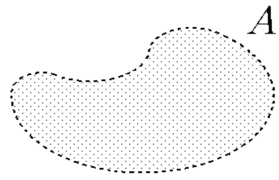


figura 2.3.2

En lo sucesivo al sombreado lo haremos solamente en los casos necesarios.

(R3) Si A es un conjunto finito y queremos representar todos sus elementos, para cada uno de ellos, dibujaremos un punto o una señal cualquiera en la zona que representa a A.

Observación importante

Sea $A \neq \emptyset$ y supongamos que la figura 2.3.2 es un diagrama de dicho conjunto, por R3 todos los elementos de A están en el interior de la zona acotada, pero no tenemos porqué suponer que todos los puntos de la misma representan elementos de A.

Más aun, si A es un conjunto finito seguramente hay puntos de dicha zona que no representan elementos de A.

Así por ejemplo si $A = \{1, 2, 3, 4, 5\}$, la figura 2.3.3 será un diagrama de A.

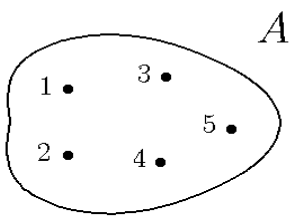


figura 2.3.3

En este caso solamente cinco puntos de la zona acotada designan elementos de A.

2.4 Subconjuntos de un conjunto

La relación de inclusión

D 2.4.1 *Llamaremos relación de inclusión y la denotaremos por $\subseteq$, a la relación determinada por las siguientes propiedades:*

(C1) $\emptyset \subseteq A$, *para todo conjunto* A.

(C2) *Si* A *y* B *son conjuntos y* $A \neq \emptyset$, *entonces* $A \subseteq B$ *si, y sólo si, todo elemento de* A *es también elemento de* B.

A la fórmula $A \subseteq B$ la leeremos: A *es subconjunto de* B.

También es usual leerla de las siguientes maneras: A *está incluído en* B, A *está contenido en* B, A *es parte de* B, etc.. Nosotros usaremos indistintamente cualquiera de ellas.

A la fórmula $A \nsubseteq B$ la leeremos: A *no está contenido en* B. Y significa que no se verifica $A \subseteq B$.

De C2 resulta que para comprobar que $A \subseteq B$ tenemos que ejecutar el siguiente esquema de trabajo:

Paso 1:

Haremos la hipótesis H: Sea $x \in A$ un elemento cualquiera.

Paso 2:

A partir de H, utilizando *razonamientos válidos*, demostramos la tesis T: $x \in B$.

En este contexto, es trivial demostrar que para todo conjunto A, se verifica $A \subseteq A$. En efecto,

de la hipótesis

H: $x \in A$,

resulta la tesis

T: $x \in A$.

Nota. Si queremos representar a A por comprensión por medio de la cláusula P y sabemos que $A \subseteq B$, entonces en algunos casos por ser conveniente, escribiremos $A = \{x \in B : x \text{ verifica P}\}$.

Propiedades de $\subseteq$

Las propiedades que indicaremos a continuación, son las más importantes de la relación $\subseteq$. Cualquiera sean los conjuntos A, B y C se verifican:

(O1) $A \subseteq A$. [propiedad reflexiva]

(O2) Si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$. [propiedad antisimétrica]

(O3) Si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$. [propiedad transitiva]

Observación

La propiedad O2 nos suministra un método para determinar cuando dos conjuntos A y B son iguales:

Paso 1:

Verificamos que $A \subseteq B$.

Paso 2:

Verificamos que $B \subseteq A$.

Paso 3:

Del paso 1, paso 2 y O2 concluímos que $A = B$.

La relación inclusión estricta

D 2.4.2 *Llamaremos relación de inclusión estricta y la denotaremos por $\subset$, a la relación definida de la siguiente manera:*

$A \subset B$ *si, y sólo si,* $A \subseteq B$ *y* $A \neq B$.

A la fórmula $A \subset B$ la leeremos: A *es subconjunto propio de* B o A *está estrictamente contenido en* B.

Ejemplos

(i) Los conjuntos $A = \{4, 5, 7, 10, 24\}$, $B = \{5, 10\}$, $C = \{3, 10, 24\}$ y $D = \{1, 4\}$ son tales que $B \subseteq A$, $C \nsubseteq A$, $D \nsubseteq A$.

(ii) Consideremos los conjuntos: $A = \{x : x$ es letra de la palabra *durazno* $\}$,

$B = \{x : x$ es letra de la palabra *zorra* $\}$, $C = \{x : x$ es letra de la palabra *aro*$\}$.

Entonces $A = \{d,u,r,a,z,n,o\}$, $B = \{z,o,r,a\}$, $C = \{a,r,o\}$ y se cumple $C \subset B$, $B \subset A$.

En algunos textos se utiliza el símbolo $\subset$ para la relación $\subseteq$. Pero no nos parece adecuado.

2.5 El conjunto de las partes de un conjunto

D 2.5.1 *Llamaremos familia de conjuntos a un conjunto cuyos elementos son a su vez conjuntos.*

El siguiente es un ejemplo muy importante de familia de conjuntos:

D 2.5.2 *Dado un conjunto A, llamaremos partes de A a la familia* $\mathcal{P}(A) = \{X : X \subseteq A\}$.

Ejemplos

(i) $\mathcal{P}(\emptyset) = \{\emptyset\}$.

(ii) $B = \{\text{luna, sol}\} \Rightarrow \mathcal{P}(B) = \{\emptyset, \{\text{luna}\}, \{\text{sol}\}, B\}$.

2.6 Operaciones con conjuntos

En lo que sigue, aunque no lo digamos explicítamente, todos los conjuntos que consideraremos serán subconjuntos de un conjunto fijo R llamado referencial (o universal), es decir, serán elementos de $\mathcal{P}(R)$.

La intersección

D 2.6.1 *Llamaremos intersección de A con B al conjunto*

$$A \cap B = \{x \in R : x \in A \ y \ x \in B\}.$$

Es frecuente simbolizar a la cláusula que define la intersección con

$$x \in A \wedge x \in B.$$

D 2.6.2 *Si A y B son tales que $A \cap B = \emptyset$, diremos que son disjuntos.*

Observemos que es aquí donde aparece la necesidad de contar con el conjunto vacío.

La unión

D 2.6.3 *Llamaremos unión de* A *con* B *al conjunto*

$$A \cup B = \{x \in R : x \text{ pertenece al menos a uno de los conjuntos } A,\ B\}.$$

Tenemos así que $x \in A \cup B$ si, y sólo si, x satisface alguna de las tres condiciones siguientes:

$$(1)\ x \in A, \quad (2)\ \ x \in B, \quad (3)\ \ x \in A \cap B.$$

Para abreviar la escritura de la cláusula anterior, la simbolizaremos con:

$$x \in A \vee x \in B.$$

El símbolo $\vee$, llamado *alternación*, desempeña el papel del o débil del castellano.
Entonces

$$A \cup B = \{x \in R : x \in A \vee x \in B\}.$$

La diferencia

D 2.6.4 *Llamaremos diferencia de* A *y* B *al conjunto*

$$A \setminus B = \{x \in R : x \in A \ \text{ y } \ x \notin B\}.$$

La complementación

D 2.6.5 *Llamaremos complemento de* A *(relativo a* R*) al conjunto* $R \setminus A$.

Es frecuente usar también, alguno de los siguientes símbolos para designar al complemento de A: $\mathfrak{C}_R A$, $\mathfrak{C}A$, A', $\overline{A}$. Luego,

$$A' = \{x \in R : x \notin A\}.$$

La noción de complemento depende del conjunto referencial R elegido, esto es, si variamos el referencial varía el complemento.

Ejemplos

(i) Sean $R = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$,

$A = \{1, 2, 5, 6, 7, 9\}$,

$B = \{1, 3, 4, 5, 9, 10\}$,

$C = \{2, 7\}$.

Entonces

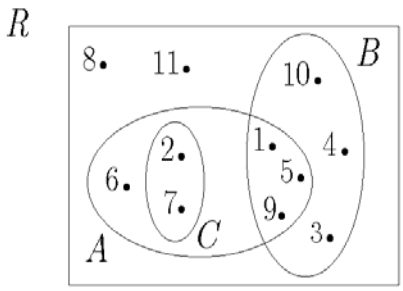
$A \cap C = C$,

$A \cap B = \{1, 5, 9\}$,

$A \cup C = A$,

$B \setminus A = \{3, 4, 10\}$,

$B' = \{2, 6, 7, 8, 11\}$.



(ii) Sean $R = \{2, 4, 7\}$, $A = \{2, 7\}$, $B = \{4\}$. Luego $A \cap B = \emptyset$.

(iii) Sean $R = \{x : x$ es letra de la palabra *murciélago*$\}$,

$A = \{x : x$ es letra de la palabra *cielo*$\}$,

$B = \{x : x$ es letra de la palabra *olor*$\}$.

Entonces

$A \cap B = \{l, o\}$,

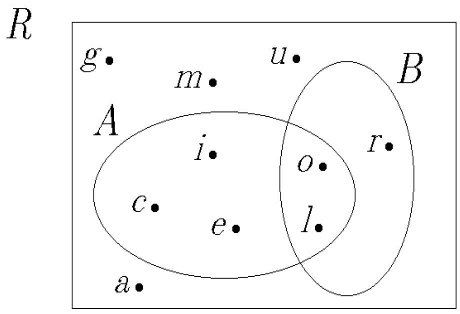
$A \setminus B = \{e,i,c\}$,

$A \cup B = \{e,i,c,l,o,r\}$,

$B \setminus A = \{r\}$,

$R \setminus A = \{m,u,a,g,r\}$,

$B \setminus R = \emptyset$.



2.7 Diagramas

Sean A y B conjuntos no vacíos. Entonces se pueden presentar las siguientes situaciones:

(i) $A \not\subseteq B$, $B \not\subseteq A$ y $A \cap B \neq \emptyset$,

(ii) $A \not\subseteq B$, $B \not\subseteq A$ y $A \cap B = \emptyset$,

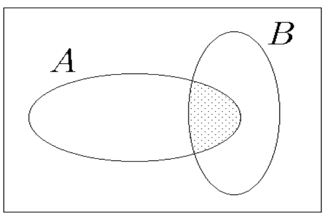
(iii) $A \not\subseteq B$ y $B \subseteq A$,

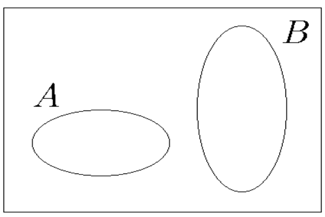
(iv) $A \subseteq B$ y $B \not\subseteq A$,

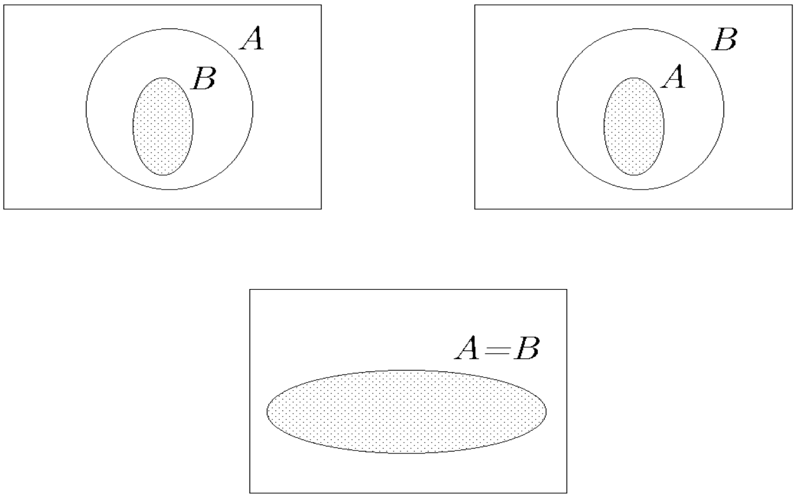
(v) $A = B$.

La intersección

La zona sombreada indica $A \cap B$.

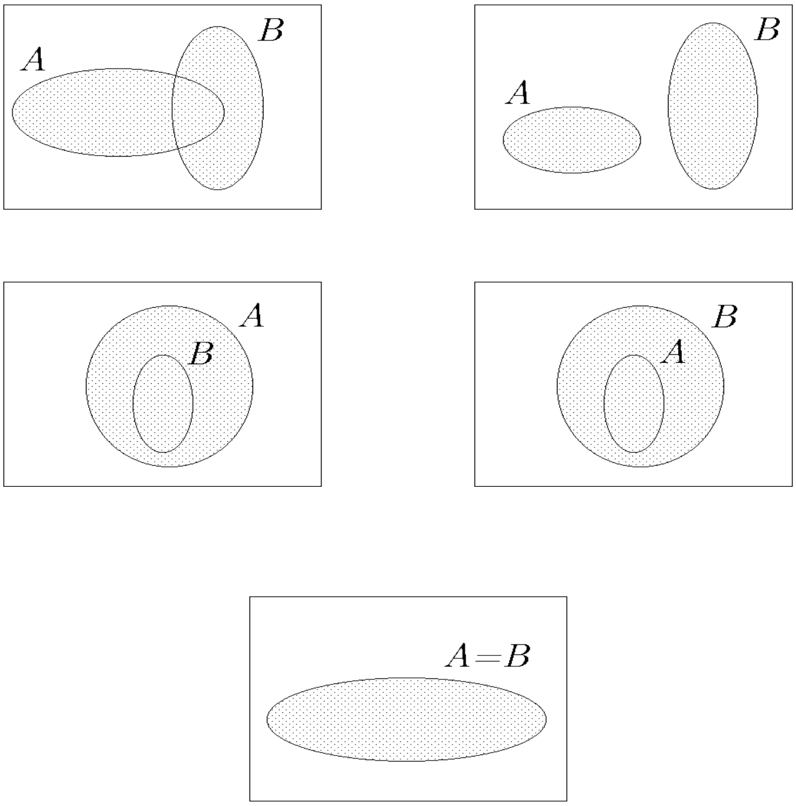






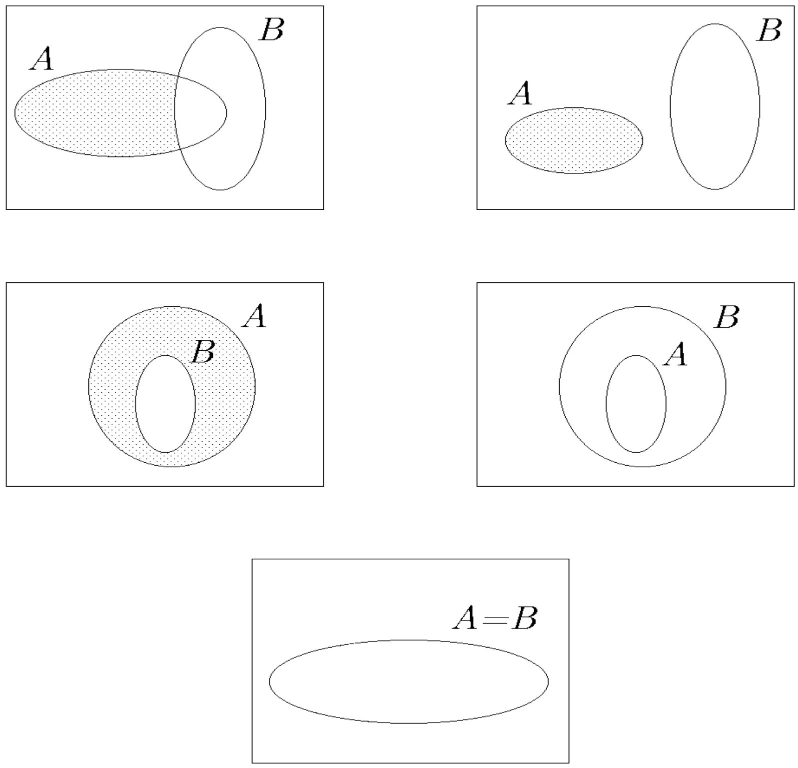
La unión

La zona sombreada indica $A \cup B$.



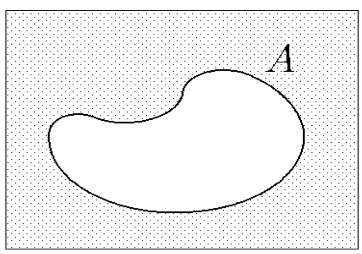
La diferencia

La zona sombreada indica $A \setminus B$.



La complementación

La zona sombreada indica A'



2.8 Propiedades de las operaciones conjuntistas

Las propiedades fundamentales de las operaciones indicadas anteriormente son:

(P1) $A \cap (B \cap C) = (A \cap B) \cap C$, [asociativa]

(P2) $A \cap A = A$, [idempotencia]

(P3) $A \cap B = B \cap A$, [conmutativa]

(P4) $A \cup (B \cup C) = (A \cup B) \cup C$, [asociativa]

(P5) $A \cup A = A$, [idempotencia]

(P6) $A \cup B = B \cup A$, [conmutativa]

(P7) $A \cap (A \cup B) = A$, [absorción]

(P8) $A \cup (A \cap B) = A$, [absorción]

(P9) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, [distributiva]

(P10) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, [distributiva]

(P11) $(A \cap B)' = A' \cup B'$,

$(A \cup B)' = A' \cap B'$. [leyes de De Morgan]

Si A es un conjunto finito, indicaremos con $|A|$ el número de elementos de A.

2.9 Principio de inclusión y exclusión

T 2.9.1 *Sean A y B dos conjuntos finitos, entonces*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Dem.

(i) Si $A \cap B = \emptyset$, entonces $|A \cap B| = 0$ y en este caso es claro que

$$|A \cup B| = |A| + |B|.$$

Luego,

$$|A \cup B| = |A| + |B| - 0 = |A| + |B| - |A \cap B|.$$

(ii) Si $A \cap B \neq \emptyset$, entonces $A \cup B = (A \setminus B) \cup B$. Como $A \setminus B$ y B son disjuntos, entonces

$$\begin{aligned} |A \cup B| &= |(A \setminus B)| + |B| && \text{[por (i)]} \\ &= |A \setminus B| + |B| + |A \cap B| - |A \cap B| \\ &= |A| + |B| - |A \cap B|. && [(A \setminus B) \cup (A \cap B) = A] \ \blacksquare \end{aligned}$$

2.10 Ejercicios

E 2.10.1

Dados los siguientes conjuntos representados por comprensión, representarlos por extensión:

(a) $A = \{x : x \in \mathbb{N},\ x^2 < 25\}$,

(b) $B = \{x : x \in \mathbb{R},\ x^2 = -1\}$,

(c) $C = \{x : x \in \mathbb{N},\ x^2 - 2x - 3 = 0\}$,

(d) $D = \{x : x \in \mathbb{Z},\ |x| < 4\}$,

(e) $F = \{x : x = y^3,\ y \in \{0, 1, 2\}\}$.

E 2.10.2

Representar por comprensión, de dos maneras distintas, cada uno de los siguientes conjuntos:

(a) conjunto vacío,

(b) de los números enteros cuyo cubo es menor que 27,

(c) $\{1, 2, 3, 4, 5\}$,

(d) de los números reales positivos cuyo cuadrado es menor que 4.

E 2.10.3

Sean $A = \{\emptyset, \{1, 2, 3\}, \{4\}, 4, \{5, 6\}\}$, $B = \{\{\emptyset\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}$ y $C = \{\{\emptyset\}, 1, 2, 3, 4, 5, 6\}$.

(a) ¿Es $A = B = C$? Justificar la respuesta.

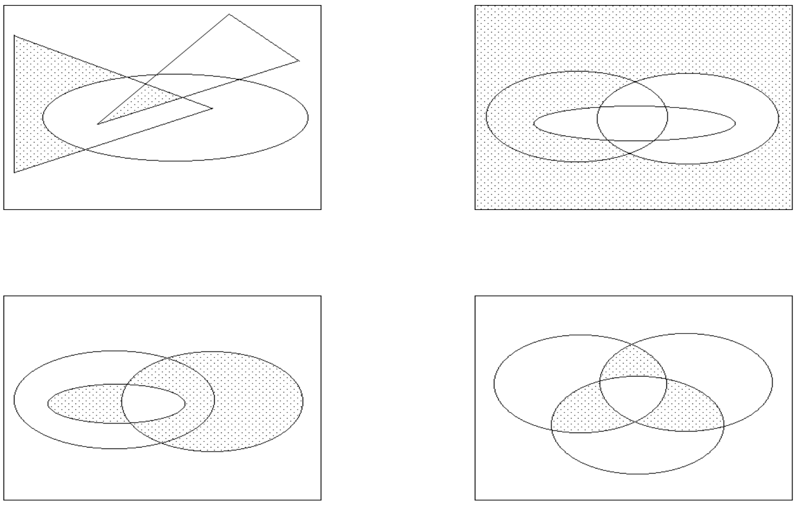
(b) ¿Cuáles de las siguientes expresiones son correctas?

$\emptyset \in A$,	$\emptyset \in B$,	$\emptyset \in C$,
$\emptyset \subseteq A$,	$\emptyset \subseteq B$,	$\emptyset \subseteq C$,
$\{\emptyset\} \subseteq A$,	$\{\emptyset\} \subseteq B$,	$\{\emptyset\} \subseteq C$,
$\{1,2,3\} \in A$,	$\{1,2,3\} \in B$,	$\{1,2,3\} \in C$,
$\{\{4\}\} \subseteq A$,	$\{\{4\}\} \subseteq B$,	$\{\{4\}\} \subseteq C$,
$4 \in A$,	$4 \in B$,	$4 \in C$,
$\{1,2,3\} \subseteq A$,	$\{1,2,3\} \subseteq B$,	$\{1,2,3\} \subseteq C$,
$\{\{\emptyset\},4\} \subseteq A$,	$\{\{\emptyset\},4\} \subseteq B$,	$\{\{\emptyset\},4\} \subseteq C$.

(c) Hallar $A \cap B$, $A \cap C$, $B \cap C$, $B \cap C \cap A$, $A \setminus B$, $C \setminus B$, $B \setminus C$ y $A \cup (B \setminus C)$.

E 2.10.4

(a) Escribir las operaciones que dan por resultado la zona sombreada.



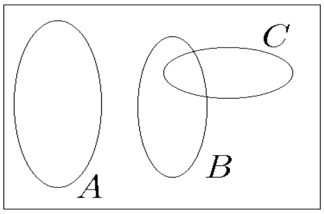
(b) Sombrear en cada diagrama la zona correspondiente a los conjuntos

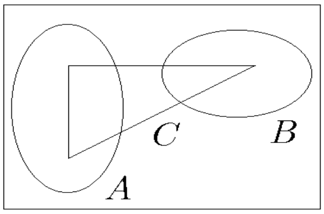
(i) $(A \cap B) \cup C$,

(ii) $(A \cup B) \setminus C$,

(iii) $(A \setminus B) \cap C'$,

(iv) $(B \cap C)' \cup A$.





E 2.10.5

Dar un ejemplo de tres conjuntos W, X e Y tales que $W \in X$, $X \in Y$ y $W \notin Y$.

E 2.10.6

Sean A, B y C subconjuntos de un conjunto U. Probar que

(a) $A \cap A = A$,

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

(c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

(d) $(A')' = A$,

(e) $(A \cap B)' = A' \cup B'$,

(f) $A \cup A' = U$,

(g) $A \cap A' = \emptyset$,

(h) $\emptyset' = U$,

(i) $U' = \emptyset$.

E 2.10.7

Sea U el conjunto de las letras del alfabeto y sean $A = \{a, b, c\}$ y $C = \{a, b, d, e\}$. Si $|A \cap B| = 2$ y $A \cap B \subset B \subset C$, hallar B.

E 2.10.8

Usando un diagrama de Venn determinar, si existen, conjuntos A, B y C que verifiquen simultáneamente las siguientes condiciones:

(i) $A \cap B = \emptyset$,

(ii) $(C \cap B) \setminus A = \emptyset$,

(iii) $(C \cap A) \setminus B = \emptyset$,

(iv) $(C \cap A) \cup (C \cap B) \cup (A \cap B) \neq \emptyset$.

E 2.10.9

Sea $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Demostrar que

(a) $A \triangle B = (A \cup B) \setminus (B \cap A)$,

(b) $A \triangle B = B \triangle A$,

(c) $A \triangle \emptyset = A$,

(d) si $A \triangle B = A \triangle C$, entonces $B = C$.

(Sugerencia: Usar que $A \triangle (B \triangle C) = (A \triangle B) \triangle C$).

E 2.10.10

Determinar la validez de las siguientes afirmaciones:

(a) si $A \cup B = A \cup C$, entonces $B = C$,

(b) si $A \cap B = A \cap C$, entonces $B = C$,

(c) si $A \triangle B = A \triangle C$, entonces $B = C$.

E 2.10.11

Probar que

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

(b) $A \subseteq B$ si, y sólo si, $A \cap B' = \emptyset$,

(c) $(A \cup B) \cap B' = A$ si, y sólo si, $A \cap B = \emptyset$,

(d) $A \triangle B = A \cup B$ si, y sólo si, $A \cap B = \emptyset$.

E 2.10.12

Simplificar las siguientes expresiones:

(a) $(A \cap B')' \cup (B \cap C)$,

(b) $(A \cup B \cup C) \cap (A \cap B' \cap C')' \cap C'$,

(c) $(((A \cap B) \cup C)' \cap B')'$,

(d) $((A \cup B) \cap A') \cup (B \cap A)'$.

E 2.10.13

Sean $A = \{1, 2, 3, 4\}$, $B = \{\emptyset, \{\emptyset\}\}$ y $C = \{a, b\}$. Hallar

(a) todos los subconjuntos de A con tres elementos,

(b) $\mathcal{P}(A)$,

(c) $\mathcal{P}(B)$,

(d) $\mathcal{P}(A) \cap \mathcal{P}(B)$,

(e) $\mathcal{P}(\mathcal{P}(C))$.

E 2.10.14

Probar que $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$. ¿Es esta igualdad válida para la unión?. Justificar la respuesta.

E 2.10.15

(a) En vísperas de un triatlón se realiza una encuesta entre 80 personas obteniéndose la siguiente información: 30 practican ciclismo, 39 natación, 32 atletismo, 10 ciclismo y natación, 15 natación y atletismo, 17 ciclismo y atletismo, y 11 ningún deporte. ¿Cuántas personas están en condiciones de participar en el triatlón?

(b) Los dueños de un video club desean conocer las preferencias de sus 1049 asociados para los fines de semana. Realizada una encuesta se obtienen los siguientes resultados:

- 444 personas desean ver una película de suspenso.
- 347 personas prefieren ver una comedia.
- 502 personas están a sacar una película de acción.
- 139 personas quieren ver de acción y suspenso.
- 154 personas están dispuestas a sacar una película de acción y comedias.
- 604 personas eligen ver películas de suspenso o comedias.
- 124 personas no desean ver ninguno de estos géneros.

Determinar

(i) ¿Cuántas personas desean ver los tres géneros?

(ii) ¿Cuántas personas manifestaron su deseo de ver únicamente comedias?.

3 Relaciones y funciones

3.1 Producto cartesiano

Pares ordenados

Tomaremos a la noción de par ordenado como concepto primitivo.

Diremos que (u, v) es un par ordenado que tiene a u como primera componente y a v como segunda componente.

Igualdad de pares ordenados

D 3.1.1 *Dos pares ordenados (a, b) y (c, d) son iguales si, y sólo si, $a = c$ y $b = d$.*

Producto cartesiano de dos conjuntos

D 3.1.2 *Sean A y B dos conjuntos dados. Llamaremos producto cartesiano de A por B, y lo representaremos con $A \times B$ (que leeremos A* por *B), al conjunto*

$$A \times B = \{(a, b) : a \in A,\ b \in B\}.$$

Si $A = B$, entonces notaremos con A^2 a $A \times A$.

Ejemplo

Sean $A = \{1, 2\}$ y $B = \{a, b\}$, entonces

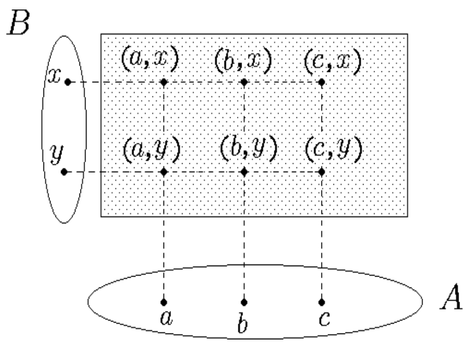
$$A \times B = \{(1, a), (1, b), (2, a), (2, b)\}.$$

Representaciones gráficas del producto cartesiano

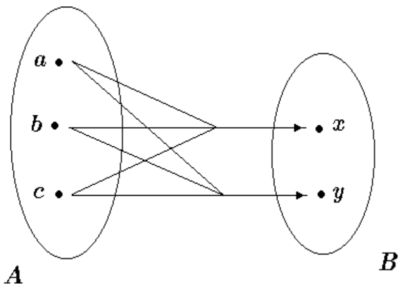
Sean $A = \{a, b, c\}$ y $B = \{x, y\}$, entonces

$$A \times B = \{(a, x), (a, y), (b, x), (b, y), (c, x), (c, y)\}.$$

Un gráfico cómodo de $A \times B$ es el siguiente:



También se lo puede representar por medio del siguiente diagrama:



En este caso, cada flecha distingue un par ordenado.

3.2 Relaciones

Relaciones binarias

D 3.2.1 *Sean A y B dos conjuntos. Llamaremos relación binaria entre los elementos de A y los de B a cualquier subconjunto R de $A \times B$.*

Es claro que $\emptyset$ y $A \times B$ son relaciones binarias entre los elementos de A y los de B. Representaremos con $Rel(A, B)$ al conjunto de las relaciones binarias entre los elementos de A y B. Entonces

$$Rel(A, B) = \{X : X \subseteq A \times B\} = \mathcal{P}(A \times B).$$

Notaciones útiles

A continuación vamos a introducir las siguientes notaciones:

(i) Frecuentemente escribiremos aRb (que leeremos: *a está en relación R con b*) para indicar que $(a,b) \in R$.

(ii) Si aRb, diremos que b es un correspondiente de a por R, o que b es una imagen directa de a por R. Al conjunto de todas las imágenes de a por R lo notaremos $R(a)$, esto es

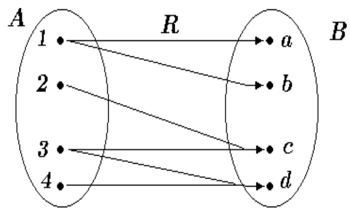
$$R(a) = \{b \in B : (a,b) \in R\}.$$

(iii) Si aRb, diremos que a es una preimagen de b, o que a es una imagen inversa de b. Al conjunto de todas las imágenes inversas de b lo notaremos $R^{-1}(b)$, esto es

$$R^{-1}(b) = \{a \in A : (a,b) \in R\}.$$

Ejemplo

Sean $A = \{1,2,3,4\}$, $B = \{a,b,c,d\}$ y $R = \{(1,a),(1,b),(2,c),(3,c),(3,d),(4,d)\}$,



entonces

$$R(1) = \{a,b\},\ R(2) = \{c\},\ R(3) = \{c,d\},\ R(4) = \{d\},$$

$$R^{-1}(a) = \{1\},\ R^{-1}(b) = \{1\},\ R^{-1}(c) = \{2,3\},\ R^{-1}(d) = \{3,4\}.$$

Dominio, imagen y rango de una relación binaria

D 3.2.2 *Sea $R \subseteq A \times B$. Diremos que*

(i) *$\{a \in A :$ existe $b \in B$ tal que $(a,b) \in R\}$ es el dominio de R,*

(ii) *$\{b \in B :$ existe $a \in A$ tal que $(a,b) \in R\}$ es la imagen de R,*

(iii) *B es el rango de R,*

y los simbolizaremos con $Dom(R)$, $Im(R)$ y $\mathcal{R}(R)$ respectivamente.

Ejemplo

Sean $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ y $R = \{(1, a), (1, b), (1, c), (3, b)\}$, entonces

$Dom(R) = \{1, 3\}$, $Im(R) = \{a, b, c\}$ y $\mathcal{R}(R) = B$.

Relación opuesta de una relación binaria

D 3.2.3 *Si R es una relación binaria, entonces llamaremos relación opuesta de R (o relación inversa de R), y la representaremos con R^{op}, a la relación*

$$R^{op} = \{(y, x) : (x, y) \in R\}.$$

Ejemplo

Si $R = \{(a, b), (a, c)\}$, entonces $R^{op} = \{(b, a), (c, a)\}$.

Composición de dos relaciones

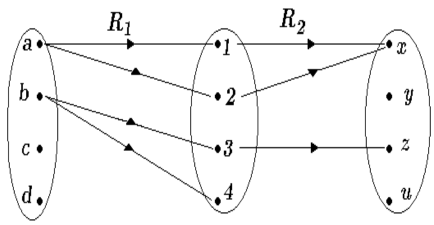
D 3.2.4 *Sean R_1 y R_2 dos relaciones, llamaremos composición de R_1 con R_2 y la representaremos con $R_2 \circ R_1$, a la relación definida del siguiente modo:*

$$R_2 \circ R_1 = \{(x, z) : \text{ existe } y \text{ que verifica } (x, y) \in R_1, (y, z) \in R_2\}.$$

Observemos que el símbolo $R_2 \circ R_1$ se lee en forma inversa a como está escrito: R_1 *compuesto con* R_2.

Ejemplo

Si las relaciones están definidas sobre conjuntos finitos, la forma más sencilla de hallar la composición es mediante diagramas.



$R_2 \circ R_1 = \{(a, x), (b, z)\}$.

Algunas propiedades de la composición

(i) La composición de dos relaciones se puede realizar siempre, y en algunos casos es el conjunto vacío.

(ii) Cualesquiera sean las relaciones R_1, R_2 y R_3 se verifica

$$R_3 \circ (R_2 \circ R_1) = (R_3 \circ R_2) \circ R_1.$$

Matriz asociada a una relación binaria

Toda relación binaria finita puede ser representada por una matriz del siguiente modo:

D 3.2.5 *Sea R una relación binaria entre los elementos de los conjuntos $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$. Llamaremos matriz asociada a R, y la indicaremos con $M(R)$, a $M(R) = (r_{ij})_{n\times m}$ donde*

$$r_{ij} = \begin{cases} 1 & \text{si } (a_i, b_j) \in R \\ 0 & \text{en caso contrario} \end{cases}.$$

Ejemplo

Si $A = \{a, b, c\}$, $B = \{1, 2, 7, 10\}$ y $R = \{(a, 7), (a, 10), (b, 2), (c, 1), (c, 7)\}$, entonces

$$M(R) = \begin{array}{c c} & \begin{array}{cccc} 1 & 2 & 7 & 10 \end{array} \\ \begin{array}{c} a \\ b \\ c \end{array} & \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \end{array}.$$

Algunas propiedades de la matriz asociada a una relación binaria

(i) La suma de los números de la i–ésima fila representa la cantidad de correspondientes que tiene a_i por R.

(ii) La suma de los números de la $j-$ésima columna representa la cantidad de preimágenes que tiene b_j por R.

(iii) A partir de los datos A, B y $M(R)$ podemos obtener R.

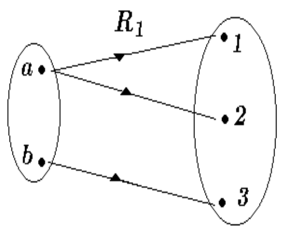
(iv) Dada una matriz $M = (r_{ij})_{n\times m}$ existe una relación R tal que $M = M(R)$. Dicha relación no es única.

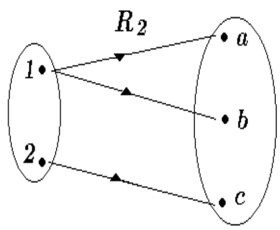
Ejemplo

Sea $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

entonces $R_1 = \{(a,1),(a,2),(b,3)\}$ y $R_2 = \{(1,a),(1,b),(2,c)\}$ son tales que $M(R_1) = M(R_2)$ pero $R_1 \neq R_2$.

Este ejemplo muestra que la correspondencia que a cada relación binaria le asigna su matriz asociada no es inyectiva. Si $R_1 \neq R_2$ con $M(R_1) = M(R_2)$, tenemos que los gráficos de dichas relaciones coinciden (y esto es lo que importa).





3.3 Relaciones $n-$arias

$n-$uplas

Diremos que $(a_1, a_2, \ldots, a_n)$ es una $n-$upla que tiene a a_j como $j-$ésima coordenada, $j = 1, 2, \ldots, n$.

Igualdad de $n-$uplas

D 3.3.1 *Dos $n-$uplas $(a_1, a_2, \ldots, a_n)$ y $(b_1, b_2, \ldots, b_n)$ son iguales si, y sólo si, se verifica $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$.*

Producto cartesiano de varios conjuntos

D 3.3.2 *Sean A_1, A_2, $\ldots$, A_n, n conjuntos dados. Llamaremos producto cartesiano de estos n conjuntos, y lo representaremos con $A_1 \times A_2 \times \cdots \times A_n$ ó $\prod_{i=1}^{n} A_i$, al conjunto*

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Si $A_1 = A_2 = \ldots = A_n = A$, a $\prod_{i=1}^{n} A_i$ lo representaremos con A^n.

Ejemplo

Sean $A_1 = \{a, b, c\}$, $A_2 = \{x, y\}$ y $A_3 = \{1\}$, entonces

$$A_1 \times A_2 \times A_3 = \{(a, x, 1), (a, y, 1), (b, x, 1), (b, y, 1), (c, x, 1), (c, y, 1)\}.$$

Relaciones n−arias

D 3.3.3 *Llamaremos relación $n-$aria entre los elementos de los conjuntos A_1, A_2, $\ldots$, A_n a cualquier subconjunto de $A_1 \times A_2 \times \cdots \times A_n$.*

Al conjunto de todas las relaciones $n-$arias entre los elementos de los conjuntos A_1, A_2, $\ldots$, A_n lo representaremos con $Rel(A_1, A_2, \ldots, A_n)$. Entonces

$$Rel(A_1, A_2, \ldots, A_n) = \{X : X \subseteq A_1 \times A_2 \times \cdots \times A_n\} = \mathcal{P}(\prod_{i=1}^{n} A_i).$$

Dominio, imagen y rango de una relación n−aria

D 3.3.4 *Dada $X \in Rel(A_1, \ldots, A_n)$, llamaremos dominio, imagen y rango de X respectivamente a los conjuntos*

$$Dom(X) = \{(a_1, \ldots, a_{n-1}) \in A_1 \times \cdots \times A_{n-1} : \text{existe } b \in A_n \text{ y } (a_1, \ldots, a_{n-1}, b) \in X\},$$

$$Im(X) = \{b \in A_n : \text{existe } (a_1, \ldots, a_{n-1}) \in A_1 \times \cdots \times A_{n-1} \text{ y } (a_1, \ldots, a_{n-1}, b) \in X\},$$

$$\mathcal{R}(X) = A_n.$$

Ejemplo

Sean $A_1 = A_2 = \{0, 1, 2\}$, $A_3 = \{1, 3, 4\}$ y $X = \{(0, 0, 1), (0, 1, 1), (2, 1, 1)\}$, entonces

$Dom(X) = \{(0,0),(0,1),(2,1)\}$,

$Im(X) = \{1\}$,

$\mathcal{R}(X) = \{1,3,4\}$.

j-ésima proyección de una relación n−aria

D 3.3.5 *Sea $X \subseteq A_1 \times \cdots \times A_n$, llamaremos $j-$ésima proyección de X al conjunto*

$$P_j = \{a \in A_j : (a_1, \ldots, a_{j-1}, a, a_{j+1}, \ldots, a_n) \in X\}.$$

Ejemplo

Sea $X = \{(a,1,1),(b,2,1),(c,0,-1),(d,1,1)\} \subseteq A_1 \times A_2 \times A_3$.

En este caso, aun cuando no conocemos a los conjuntos A_1, A_2, A_3, podemos determinar las tres proyecciones de X

$P_1 = \{a,b,c,d\}$, $P_2 = \{1,2,0\}$ y $P_3 = \{1,-1\}$.

Algunas propiedades de las proyecciones

(i) Si $X \subseteq A_1 \times A_2$, entonces $P_1 = Dom(X)$ y $P_2 = Im(X)$. Esto no sucede si $n > 2$.

(ii) Sea $X \subseteq A_1 \times A_2 \times \ldots \times A_n$ y sean $P_1, P_2, \ldots, P_n$ todas las proyecciones de X, entonces es fácil verificar que

$$X \subseteq P_1 \times P_2 \times \ldots \times P_n.$$

Es decir, podemos considerar que X es una relación entre los conjuntos proyecciones de la relación.

Si llamamos coordenada superflua a cualquier elemento $a \in A_j$ que no es $j-$ésima coordenada de ninguna de las $n-$uplas de X, y tomamos a X como una relación entre los elementos de los conjuntos proyecciones en lugar de los conjuntos $A_1, A_2, \ldots, A_n$, eliminaremos las coordenadas superfluas.

Ejemplo

Sean $A_1 = \{a,b,c,d,e\}$, $A_2 = \{0,1,2,3\}$, $A_3 = \{1,-1\}$ y $X \subseteq A_1 \times A_2 \times A_3$ tal que

$X = \{(a, 1, 1), (b, 0, 1), (c, 0, 1), (c, 1, 1)\}.$

Entonces tenemos que $d, e, 2, 3, -1$ son coordenadas superfluas. En cambio, considerando las proyecciones $P_1 = \{a, b, c\}$, $P_2 = \{0, 1\}$, $P_3 = \{1\}$ y $X \subseteq P_1 \times P_2 \times P_3$, no tenemos coordenadas superfluas.

Se puede demostrar que si la relación $n-$aria $X \subseteq A_1 \times A_2 \times \ldots \times A_n$ es tal que $X \subseteq B_1 \times B_2 \times \ldots \times B_n$, entonces $P_1 \times P_2 \times \ldots \times P_n \subseteq B_1 \times B_2 \times \ldots \times B_n$.

3.4 Funciones

Ahora veremos un tipo especial de relación binaria particularmente importante.

Relaciones funcionales

D 3.4.1 *Llamaremos relación funcional o función a toda $f \in Rel(A \times B)$ que verifica*

$(a, b) \in f$ *y* $(a, c) \in f \Rightarrow b = c.$

Ejemplo

Sean $A = \{a, b, c\}$, $B = \{1, 2, 3\}$ y

$f_1 = \{(a, 1), (b, 1), (c, 2)\},$

$f_2 = \{(a, 1), (b, 1)\},$

$f_3 = \{(c, 2)\},$

$f_4 = \{(a, 1), (a, 2), (b, 3)\},$

entonces f_1, f_2, f_3 son funciones pero f_4 no lo es pues $(a, 1), (a, 2) \in f_4$ y $1 \neq 2$.

Observaciones

(i) Siendo que las funciones son relaciones especiales, podemos determinar dominio de f, imagen de f y rango de f de la manera ya vista.

Si f_1 y f_3 son las del ejemplo anterior, tenemos que

$$Dom(f_1) = \{a, b, c\} = A,\ Im(f_1) = \{1, 2\},\ \mathcal{R}(f_1) = B,$$

$$Dom(f_3) = \{c\},\ Im(f_3) = \{2\},\ \mathcal{R}(f_3) = B.$$

(ii) Si f es una relación funcional, entonces para cada $a \in Dom(f)$ el conjunto $f(a)$ tiene un solo elemento.

Para abreviar escribiremos $b = f(a)$ en lugar de $f(a) = \{b\}$, y diremos que b es el correspondiente de a por f.

(iii) Cuando el dominio de f es finito, en lugar de definir a f por extensión se suele hacer por medio de una tabla.

x	$f_1(x)$
a	1
b	1
c	2

o

x	a	b	c
$f_1(x)$	1	1	2

(iv) En casi todos los textos se suele escribir: *sea $y = f(x)$ una función dada*, que es una expresión incorrecta pues una función es un conjunto y $f(x)$ es solamente el correspondiente de x por f. A pesar de ello cuando nos sea conveniente también la utilizaremos.

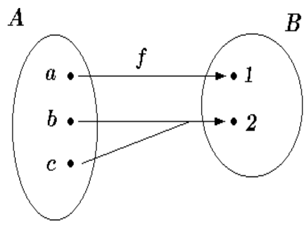
Funciones totales y parciales

Funciones totales

D 3.4.2 *Si $f \subseteq A \times B$ es una relación funcional y $Dom(f) = A$, entonces diremos que f es una función total de A en B o que es una función de A en B, y escribiremos $f : A \longrightarrow B$ o $A \xrightarrow{f} B$.*

Ejemplo

Sea $f = \{(a, 1), (b, 2), (c, 2)\}$, entonces si elegimos $A = Dom(f) = \{a, b, c\}$ y $B = \{1, 2\}$, tenemos que $f : A \longrightarrow B$.



Funciones parciales

D 3.4.3 *Si $f \subseteq A \times B$ es una relación funcional y $Dom(f) \neq A$, entonces diremos que f es una función parcial de A en B.*

Toda función parcial f puede ser transformada en una función total. En efecto, basta considerar a f como un subconjunto de $Dom(f) \times B$.

Funciones especiales

(i) **Función constante**: Diremos que f es constante si

$$f = \{(x, b) : x \in A, \, b \in B \text{ fijo } \}.$$

Es decir, tenemos que $f : A \longrightarrow B$ es constante si se verifica $f(x) = b$ para todo $x \in A$, siendo b un elemento fijo de B.

También podemos decir que f es constante si todos los elementos del dominio de f tienen el mismo correspondiente.

(ii) **Función identidad**: Llamaremos identidad de A, y la indicaremos I_A, a la función

$$I_A = \{(x, x) : x \in A\}.$$

Esto es, $I_A : A \longrightarrow A$ está definida por $I_A(x) = x$ para todo $x \in A$.

(iii) **Función inclusión**: Si $A \subseteq B$, llamaremos función inclusión de A en B y la simbolizaremos con i, a la función

$$i = \{(x, x) : x \in A\}.$$

Es decir, la función inclusión es un subconjunto de la función identidad. Esto es, tenemos que $i : A \longrightarrow B$ está definida por $i(x) = x$, para todo $x \in A$.

(iv) **Funciones proyecciones**: Sean A y B conjuntos no vacíos. Las funciones

$$p_1 : A \times B \longrightarrow A,$$
$$p_2 : A \times B \longrightarrow B,$$

tales que para cada $(a, b) \in A \times B$

$$p_1((a, b)) = a,$$
$$p_2((a, b)) = b,$$

se denominan primera proyección y segunda proyección, respectivamente.

En general, dados n conjuntos $A_1, \dots, A_n$ tenemos n funciones $p_j, j = 1, 2, \dots, n$, llamadas funciones proyecciones, las cuales están definidas como sigue:

$$p_j : A_1 \times \ldots \times A_j \times \ldots \times A_n \longrightarrow A_j,$$

donde para cada $(a_1, \dots, a_j, \dots, a_n) \in A_1 \times \ldots \times A_j \times \ldots \times A_n$,

$$p_j((a_1, \dots, a_j, \dots, a_n)) = a_j.$$

Todas las funciones que acabamos de definir, desempeñan un papel importante en la teoría de funciones como veremos más adelante.

Imagen y preimagen de un subconjunto por medio de una función

D 3.4.4 *Sea $f \subseteq A \times B$ una función dada, entonces*

(i) *para cada subconjunto $X \subseteq A$, llamaremos imagen de X por f al conjunto*

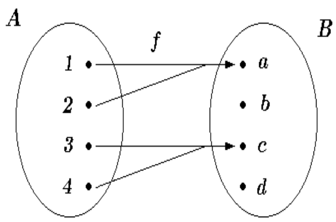
$$f(X) = \{f(x) : x \in X\}.$$

(ii) *para cada subconjunto $Y \subseteq B$, llamaremos preimagen o imagen completa inversa de Y por f al conjunto*

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

Ejemplo

Sea f la función dada por el siguiente diagrama:



y consideremos

$X_1 = \{2, 4\}$, $X_2 = \{1, 2, 3\}$,

$Y_1 = \{a, b\}$, $Y_2 = \{d\}$,

entonces tenemos

$f(X_1) = \{a, b\}$, $f(X_2) = \{a, b\}$,

$f^{-1}(Y_1) = \{1, 2, 3, 4\}$, $f^{-1}(Y_2) = \emptyset$.

Funciones de conjuntos asociadas a una función

D 3.4.5 *Dada $f : A \longrightarrow B$ podemos considerar dos nuevas funciones*

$F : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$,

$F^* : \mathcal{P}(B) \longrightarrow \mathcal{P}(A)$,

definidas por

$F(X) = f(X)$, *para todo* $X \in \mathcal{P}(A)$,

$F^*(Y) = f^{-1}(Y)$, *para todo* $Y \in \mathcal{P}(B)$,

respectivamente.
Estas dos funciones se denominan las funciones de conjuntos asociadas a la función f.

Ejemplo

Sean $A = \{1, 2, 3\}$, $B = \{a, b\}$ y $f : A \longrightarrow B$ la función indicada en la siguiente tabla:

x	1	2	3
$f(x)$	a	b	b

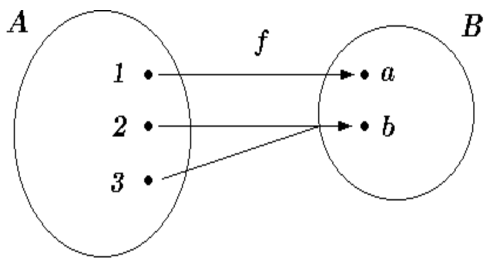
Entonces tenemos

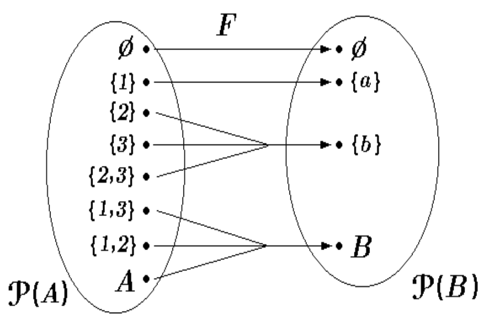
$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, A\},$$

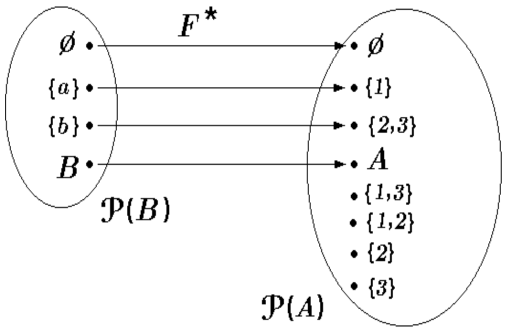
$$\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, B\},$$

X	$\emptyset$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	A
$F(X)$	$\emptyset$	$\{a\}$	$\{b\}$	$\{b\}$	B	B	$\{b\}$	B

Y	$\emptyset$	$\{a\}$	$\{b\}$	B
$F^*(Y)$	$\emptyset$	$\{1\}$	$\{2,3\}$	A







Propiedades importantes de las funciones de conjuntos asociadas a una función

Para todo $X_1, X_2 \in \mathcal{P}(A)$ se verifican las siguientes propiedades:

(i) $F(\emptyset) = \emptyset$,

(ii) $X_1 \subseteq X_2 \Rightarrow F(X_1) \subseteq F(X_2)$,

(iii) $F(X_1 \cup X_2) = F(X_1) \cup F(X_2)$,

(iv) $F(X_1 \cap X_2) \subseteq F(X_1) \cap F(X_2)$. [en general no se verifica la igualdad]

Para todo $Y_1, Y_2 \in \mathcal{P}(B)$ se verifican las siguientes propiedades:

(v) $F^*(\emptyset) = \emptyset$,

(vi) $Y_1 \subseteq Y_2 \Rightarrow F^*(Y_1) \subseteq F^*(Y_2)$,

(vii) $F^*(Y_1 \cup Y_2) = F^*(Y_1) \cup F^*(Y_2)$,

(viii) $F^*(Y_1 \cap Y_2) = F^*(Y_1) \cap F^*(Y_2)$.

Restricción y extensión de funciones

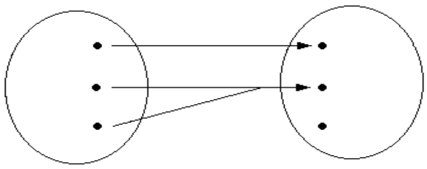
D 3.4.6 *Diremos que la función g es una extensión de f o que f es una restricción de g, si se verifican:*

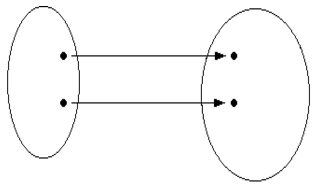
(i) $Dom(f) \subseteq Dom(g)$,

(ii) $f(x) = g(x)$, *para todo* $x \in Dom(f)$.

Para indicar que f es una restricción de g a veces usaremos el símbolo $f = g|_{Dom(f)}$ que leeremos f *es igual a* g *restringida a* $Dom(f)$.

Ejemplo





entonces

$Dom(f) = \{1, 2, 3\}$,

$Dom(g) = \{1, 2\}$.

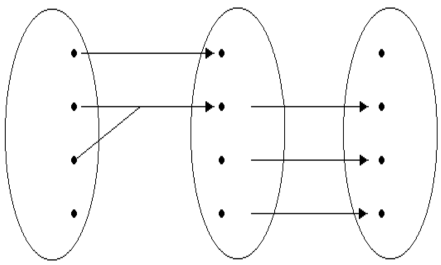
Como $Dom(g) \subseteq Dom(f)$ y vale $g(x) = f(x)$ para todo $x \in Dom(g)$, tenemos que $g = f|_{Dom(g)}$. Es decir, f extiende a g y también decimos que g restringe a f.

Composición de funciones

D 3.4.7 *Dadas las relaciones funcionales f y g, la composición de f con g es la relación*

$$g \circ f = \{(x, z) : \text{ existe } y \text{ tal que } (x, y) \in f, (y, z) \in g\}.$$

Ejemplo



$g \circ f = \{(b, y), (c, y)\}$.

Algunas propiedades de la composición de funciones

T 3.4.1 *Sean f y g dos funciones, entonces*

(i) $g \circ f$ *es una función,*

(ii) $Dom(g \circ f) = \{x \in Dom(f) : f(x) \in Dom(g)\}$,

(iii) $Dom(g \circ f) = f^{-1}(Im(f) \cap Dom(g))$.

Dem.

(i) Caso 1. Si $g \circ f = \emptyset$ ó $g \circ f$ tiene un solo elemento, entonces es una función.

Caso 2. Si $g \circ f$ tiene más de un elemento,

(1) sea $(x, y) \in g \circ f$, [existe por hipótesis]

(2) sea $(x, z) \in g \circ f$. [existe por hipótesis]

Entonces existen w y t tales que

(3) $(x, w) \in f$, [(1)]

(4) $(w, y) \in g$, [(1)]

(5) $(x, t) \in f$, [(2)]

(6) $(t, z) \in g$. [(2)]

Entonces

(7) $t = w$, [(3),(5) y f función]

(8) $y = z$. [(4),(6),(7) y g función]

(ii) $z \in Dom(g \circ f) \Leftrightarrow$

existe y tal que $(z, y) \in g \circ f \Leftrightarrow$

existe w tal que $(z, w) \in f, (w, y) \in g \Leftrightarrow$

$w = f(z)$ y $(f(z), y) \in g \Leftrightarrow$

$z \in Dom(f)$ y $f(z) \in Dom(g) \Leftrightarrow$

$z \in \{x \in Dom(f) : f(x) \in Dom(g)\}$.

(iii) $x \in Dom(g \circ f) \Leftrightarrow$

$x \in Dom(f)$ y $f(x) \in Dom(g) \Leftrightarrow$ [(ii)]

$f(x) \in Im(f)$ y $f(x) \in Dom(g) \Leftrightarrow$

$f(x) \in Im(f) \cap Dom(g) \Leftrightarrow$

$x \in f^{-1}(Im(f) \cap Dom(g))$. ■

Clasificación de funciones

Funciones inyectivas

D 3.4.8 *Diremos que una función $f \subseteq A \times B$ es inyectiva si se verifica*

$(x, y) \in f$ *y* $(z, y) \in f \Rightarrow x = z$.

Observaciones

(i) Si nos dan la función por medio de una expresión de la forma $y = f(x)$ y nos piden que demostremos que f es inyectiva procedemos de la siguiente manera:

(1) suponemos que $a, b \in Dom(f)$ son tales que $f(a) = f(b)$,

(2) a partir de $f(a) = f(b)$, utilizando propiedades conocidas,
demostramos que $a = b$.

Consideremos el siguiente ejemplo: Sea $\mathbb{R}^- = \{x \in \mathbb{R} : x < 0\}$ y $f : \mathbb{R}^- \longrightarrow \mathbb{R}$ la función definida por $f(x) = x^2 + 1$. Entonces f es inyectiva. En efecto,

(1) sean $a, b \in \mathbb{R}^-$ tales que $f(a) = f(b)$,

luego

(2) $a^2 + 1 = b^2 + 1$, [(1) y definición de f]

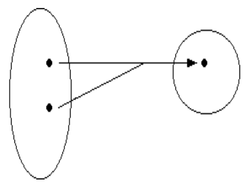
(3) $\sqrt{a^2} = \sqrt{b^2}$, [(2)]

(4) $|a| = |b|$, [(3)]

(5) $-a = -b$, [(4), def. de valor absoluto y $a, b \in I\!R^-$]

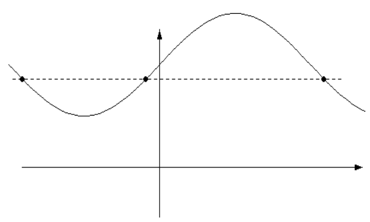
(6) $a = b$. [(5)]

(ii) Un gráfico de f del tipo



[dos puntos del dominio tienen la misma imagen]

o un gráfico del tipo



[una recta paralela al eje $\boldsymbol{x}$ corta al gráfico en más de un punto]

es el de una función que no es inyectiva.

Funciones epiyectivas

D 3.4.9 *Diremos que la función $f \subseteq A \times B$ es epiyectiva o sobreyectiva si*

$Im(f) = B$.

Observación

Es claro que siempre vale $Im(f) \subseteq B$, luego para probar que f es sobreyectiva, solamente debemos probar que $B \subseteq Im(f)$.

Entonces si debemos demostrar que f es sobreyectiva procedemos de la siguiente manera:

(1) suponemos $b \in B$,

(2) a partir de (1), hallamos $a \in A$ que verifique $f(a) = b$.

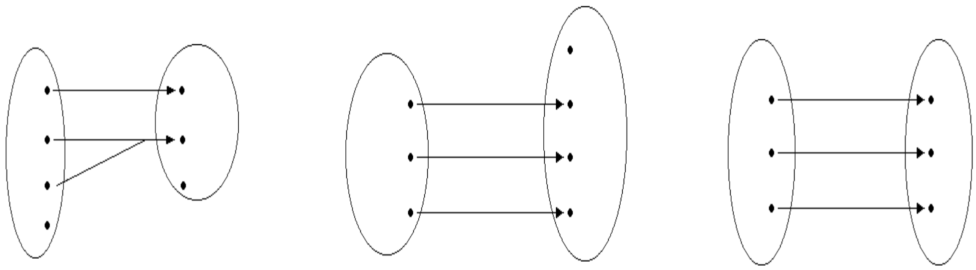
Funciones biyectivas

D 3.4.10 *Diremos que $f : A \longrightarrow B$ es biyectiva o que es una biyección de A en B si es inyectiva y sobreyectiva.*

Observemos que hablamos de funciones biyectivas solamente en el caso de funciones totales.

Ejemplos

Consideremos las siguientes funciones:



Entonces

f no es inyectiva ni sobreyectiva,

g es inyectiva y no es sobreyectiva,

h es biyectiva.

Relación opuesta de una relación funcional

A continuación vamos a calcular en algunos ejemplos la relación opuesta de una relación funcional.

(i) Si $f = \{(a,1),(b,1),(c,2)\}$, entonces $f^{op} = \{(1,a),(1,b),(2,c)\}$ no es función.

(ii) Si $f = \{(a,1),(b,2),(c,4)\}$, entonces $f^{op} = \{(1,a),(2,b),(4,c)\}$ es función.

Algunas propiedades de la relación opuesta de una función

T 3.4.2 *Las siguientes condiciones son equivalentes:*

(i) f^{op} *es una función,*

(ii) *f es inyectiva.*

Dem.
(i) $\Longrightarrow$ (ii): Caso 1. Si $f = \emptyset$ ó f tiene un solo elemento, entonces es inyectiva.

Caso 2. Si f tiene más de un elemento, entonces sean

(1) $(x, y) \in f$,

(2) $(z, y) \in f$.

Luego,

(3) $(y, x) \in f^{op}$, [(1)]

(4) $(y, z) \in f^{op}$, [(2)]

(5) $x = z$, [(i),(3),(4)]

(6) f es inyectiva. [(1),(2),(5)]

(ii) $\Longrightarrow$ (i): Caso 1. Si $f^{op} = \emptyset$ ó f^{op} tiene un solo elemento, entonces f^{op} es función.

Caso 2. Si f^{op} tiene más de un elemento, entonces sean

(1) $(x, u) \in f^{op}$,

(2) $(x, v) \in f^{op}$.

Luego,

(3) $(u, x) \in f$, [(1)]

(4) $(v, x) \in f$, [(2)]

(5) $u = v$, [(ii),(3),(4)]

(6) f^{op} es función. [(1),(2),(5)] ■

T 3.4.3 *Sea $f : A \longrightarrow B$ una función. Las siguientes condiciones son equivalentes:*

(i) *f^{op} es función total de B en A,*

(ii) *f es biyectiva,*

(iii) *existe $g : B \longrightarrow A$ tal que*

(a) $g \circ f = I_A$,

(b) $f \circ g = I_B$.

Dem.

(i) $\Longrightarrow$ (ii): Sea

(1) $b \in B$,

entonces

(2) $f^{op}(b) = a \in A$, [por (i), a es único]

(3) $(b, a) \in f^{op}$, [(2)]

(4) $(a, b) \in f$, [(3)]

(5) $b \in Im(f)$, [(4)]

(6) f es epiyectiva. [(1),(5)]

Además

(7) f es inyectiva, [(i),T 3.4.2]

(8) f es biyectiva. [(6),(7)]

(ii) $\Longrightarrow$ (iii):Por la hipótesis resulta

(1) f es inyectiva,

(2) f es sobreyectiva.

Luego

(3) f^{op} es función, [(1),T 3.4.2]

(4) $Dom(f^{op}) = B$, [(2)]

(5) $f^{op} : B \longrightarrow A$. [(4),(3)]

Tomando $g = f^{op}$ resulta (iii).

(iii) $\Longrightarrow$ (i): Dejaremos como ejercicio probar que $Dom(f^{op}) = B$ y sólo demostraremos que f^{op} es función.

Caso 1. Si f^{op} tiene un solo elemento, entonces f^{op} es función total.

Caso 2. Si f^{op} tiene más de un elemento, entonces sean

(1) $(x, y) \in f^{op}$

y

(2) $(x, z) \in f^{op}$.

Entonces

(3) $(y, x) \in f$, [(1)]

(4) $(z, x) \in f$, [(2)]

(5) $f(y) = x$, [(3)]

(6) $f(z) = x$, [(4)]

(7) $f(y) = f(z)$, [(5),(6)]

(8) $g(f(y)) = g(f(z))$, [(7)]

(9) $y = z$, [(8),(iii)(a)]

(10) f^{op} es función. [(1),(2),(9)] ■

Nota: Si f^{op} es función, es habitual llamarla *la inversa* de f.

3.5 Producto directo de conjuntos

D 3.5.1 *Sea I un conjunto no vacío y sea $\{A_i\}_{i\in I}$ una familia de conjuntos. Llamaremos producto directo de los conjuntos A_i y lo indicaremos con $\prod_{i\in I} A_i$, al conjunto*

$$\prod_{i\in I} A_i = \{f : I \longrightarrow \bigcup_{i\in I} A_i : f(i) \in A_i,\ \textit{para cada}\ i \in I\}.$$

Ejemplo

Sean $I = \{1,2,3\}$, $A_1 = \{a,b\}$, $A_2 = \{x,y,z\}$ y $A_3 = \{z,t\}$. Entonces

$$\bigcup_{i\in I} A_i = \{a,b,x,y,z,t\}.$$

Los elementos de $\prod_{i\in I} A_i$ están indicados en la tabla siguiente:

I	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}
1	a	a	a	a	a	a	b	b	b	b	b	b
2	x	x	y	y	z	z	x	x	y	y	z	z
3	z	t	z	t	z	t	z	t	z	t	z	t

Cualquier función f_j anterior es el conjunto

$$f_j = \{(1, f_j(1)), (2, f_j(2)), (3, f_j(3)\}.$$

Es claro que f_j queda determinada por las segundas coordenadas de los pares ordenados, es decir, podemos reconocerla por medio de la terna $(f_j(1), f_j(2), f_j(3))$.

Más precisamente, podemos establecer la correspondencia

$$f_j \longrightarrow (f_j(1), f_j(2), f_j(3)).$$

La observación anterior nos conduce al siguiente resultado:

T 3.5.1 *Si $\{A_i\}_{i\in I}$ es una familia de conjuntos con $I = \{1,2,\ldots,n\}$, entonces la función Ψ que a cada $f \in \prod_{i\in I} A_i$ le hace corresponder $\Psi(f) = (f(1), f(2), \ldots, f(n))$ es una biyección de $\prod_{i\in I} A_i$ en $\prod_{i=1}^{n} A_i$.*

Dem.

(i) Ψ es inyectiva:

Sean $f, g \in \prod_{i\in I} A_i$ tales que

(1) $\Psi(f) = \Psi(g)$,

entonces

(2) $(f(1), f(2), \dots, f(n)) = (g(1), g(2), \dots, g(n))$, [def. de Ψ]

(3) $f(i) = g(i)$, para todo $i \in I$, [(2)]

(4) $f = g$. [(3)]

(ii) Ψ es sobreyectiva:

Sea $(a_1, \dots, a_n) \in \prod_{i=1}^{n} A_i$ y sea $f : I \longrightarrow \bigcup_{i\in I} A_i$ la función tal que para cada $i \in I$, $f(i) = a_i$. Entonces es fácil verificar que $\Psi(f) = (a_1, \dots, a_n)$. ■

Este último teorema es muy importante pues nos permite identificar las nociones de producto directo y producto cartesiano de conjuntos, esto es, podemos trabajar con n–uplas o funciones según nos sea más cómodo.

Por otra parte, el producto cartesiano se puede definir solamente para un número finito de conjuntos en cambio el producto directo se puede definir para familias arbitrarias de conjuntos.

3.6 Conjuntos coordinables

D 3.6.1 *Dados los conjuntos A y B diremos que:*

(i) *el cardinal de A es menor o igual que el cardinal de B, y escribiremos $\overline{\overline{A}} \preceq \overline{\overline{B}}$, si existe $f : A \longrightarrow B$ inyectiva,*

(ii) *el cardinal de A es menor que el cardinal de B, y escribiremos $\overline{\overline{A}} \prec \overline{\overline{B}}$, si ninguna función inyectiva $f : A \longrightarrow B$ es sobreyectiva,*

(iii) *tienen el mismo cardinal, o que son conjuntos coordinables, y escribiremos $\overline{\overline{A}} \approx \overline{\overline{B}}$ si $\overline{\overline{A}} \preceq \overline{\overline{B}}$ y $\overline{\overline{B}} \preceq \overline{\overline{A}}$.*

Observaciones

(i) $\overline{\overline{A}} \approx \overline{\overline{B}}$ si, y sólo si, existe $f : A \longrightarrow B$ biyectiva.

(ii) Es fácil verificar que $\overline{\overline{A}} \prec \overline{\overline{B}}$ si, y sólo si, $\overline{\overline{A}} \preceq \overline{\overline{B}}$ y $\overline{\overline{A}} \not\approx \overline{\overline{B}}$.

(iii) Si A y B son conjuntos finitos entonces las siguientes condiciones son equivalentes:

(a) $\overline{\overline{A}} \approx \overline{\overline{B}}$,

(b) $|A| = |B|$, es decir A y B tienen la misma cantidad de elementos.

(iv) En adelante, teniendo en cuenta (iii), dados los conjuntos A y B finitos o no, escribiremos en los casos que no haya lugar a confusión, $|A|$ y $|A| = |B|$ en lugar de $\overline{\overline{A}}$ y $\overline{\overline{A}} \approx \overline{\overline{B}}$ respectivamente. En el caso que A sea finito también seguiremos escribiendo $|A| = n$ para indicar que A tiene n elementos.

(v) Se puede demostrar que para todo par de conjuntos A y B se verifica una y sólo una de las tres condiciones siguientes:

(1) $|A| \prec |B|$, (2) $|A| = |B|$, (3) $|B| \prec |A|$.

(vi) En la sección 5, veremos que la relación de coordinabilidad $\preceq$ es una relación de equivalencia sobre la familia $\mathcal{P}(X)$ de subconjuntos de un conjunto X no vacío.

3.7 Ejercicios

E 3.7.1

Sean $A = \{a, b, c\}$, $B = \{1, 2\}$ y $C = \{d\}$.

(a) Calcular $A \times C$, $C \times A$, $A \times B$, $B \times A$, $A \times B \times C$ y $C \times A \times B$.

(b) Representar gráficamente

(b.1) $A \times C$ y $B \times A$ del inciso (a),

(b.2) $D \times E$, donde

(i) $D = \{x : x \in \mathbb{N}\}$, $E = \{y : y \in \mathbb{R},\ 1 \leq y \leq 2\}$,

(ii) $D = \{x : x \in \mathbb{R},\ x \leq 0\}$, $E = \{y : y \in \mathbb{N},\ y^2 = 4\}$,

(iii) $D = \{x : x \in \mathbb{Z},\ -3 \leq x \leq 4\}$, $E = \{y : y \in \mathbb{R},\ y \leq 0\}$.

E 3.7.2

(a) Dados los conjuntos A, B y C, probar que

(i) $A \times (B \cap C) = (A \times B) \cap (A \times C)$,

(ii) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

(b) Sean A y B conjuntos, ¿cuándo es válida la igualdad $A \times B = B \times A$?

E 3.7.3

Sea $A = \{1, 2\}$. Hallar $\mathcal{P}(A) \times \mathcal{P}(A)$.

E 3.7.4

Sean $A = \{1, 2, 3\}$ y $B = \{2, 3, 4, 5\}$. Dar ejemplos, en cada caso, de dos relaciones binarias no vacías

(a) entre A y B,

(b) entre B y A,

(c) sobre A,

(d) que sean simultáneamente relaciones binarias entre A y B, y entre B y A.

E 3.7.5

(a) Para los conjuntos A y B del ejercicio 3.7.4, determinar

(i) $|A \times B|$,

(ii) el número de relaciones binarias entre A y B,

(iii) el número de relaciones binarias sobre A,

(iv) el número de relaciones binarias entre A y B que contienen los pares $(1, 2)$,$(2, 3)$, $(2, 4)$ y $(1, 5)$,

(v) el número de relaciones binarias entre A y B que contienen exactamente 5 pares ordenados,

(vi) el número de relaciones binarias sobre A que contienen al menos 7 elementos.

(b) Si A y B son conjuntos finitos, hallar el número de relaciones binarias entre A y B y el número de relaciones binarias sobre A.

(c) Sean A y B conjuntos con $|B| = 3$. Si existen 4096 relaciones binarias entre A y B, hallar $|A|$.

E 3.7.6

En el conjunto de números naturales, decidir cuáles de los siguientes pares ordenados pertenecen a la relación R:

(a) xRy si, y sólo si, x divide a y, $\quad (2,4), (2,5), (2,6)$,

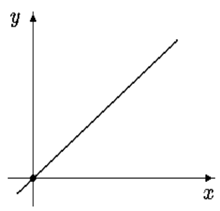
(b) xRy si, y sólo si, $x > y^2$, $\quad (1,2), (2,1), (5,2), (6,4), (4,3)$,

(c) xRy si, y sólo si, $2x + 3y = 10$, $\quad (5,0), (2,2), (3,1), (1,3)$.

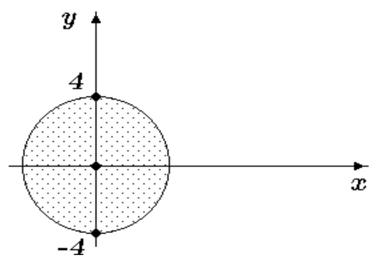
E 3.7.7

Para cada una de las siguientes figuras indicar la relación binaria sobre el conjunto $\mathbb{R}$ que determina la zona marcada:

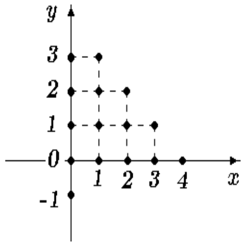
(a)



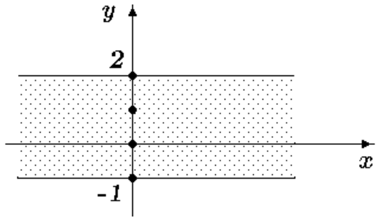
(b)



(c)



(d)



E 3.7.8

Sean $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d, e, f\}$ y $C = \{x, y, w\}$. Dadas las siguientes relaciones indicar, en cada caso, dominio, imagen, rango, P_1 y P_2:

(a) $R = \{(1, x), (2, x), (3, x), (4, y)\}$,

(b) $S = \{(a, 1, x), (c, 1, w), (e, 3, w)\}$. ¿Es $P_1(S) = Dom(S)$ y $P_2(S) = Im(S)$?

(c) $T = \{(x, a), (x, b), (y, b), (x, c), (y, f), (y, c)\}$,

(d) $W = \{(x, f, 1), (x, f, 2), (y, e, 3), (w, b, 3)\}$. ¿Es $P_3(W) = \mathcal{R}(\mathcal{W})$?

E 3.7.9

Sean R, S y T tres relaciones binarias. Probar que

(a) $(S^{op})^{op} = S$,

(b) $(R \cup S)^{op} = R^{op} \cup S^{op}$,

(c) $(R \cap S)^{op} = R^{op} \cap S^{op}$,

(d) $(R \circ S)^{op} = S^{op} \circ R^{op}$,

(e) $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$,

(f) $(R \cup S) \circ T = (R \circ T) \cup (S \circ T)$.

E 3.7.10

Hallar R^{op}, S^{op}, $R \circ S$, $S \circ R$, $(S \circ R)^{op}$, $R \circ S^{op}$ en cada uno de los siguientes casos

(a) $R = \{(1, 2), (3, 4), (1, 8), (2, 9), (2, 2)\}$,

$S = \{(2, 7), (4, 10), (4, 6), (8, 5)\}$,

(b) $R = \{(x, y) : x \in \mathbb{R},\ y = |x + 1|\}$,

$S = \{(x, y) : x \in \mathbb{R},\ y = 1 + 2x\}$,

(c) $R = \{(x, y) : x \in [0, \infty),\ y = \sqrt{x} + 1\} \cup \{(x, y) : x \in [0, \infty),\ y = -\sqrt{x} + 1\}$,

$S = \{(x, y) : x \in \mathbb{R} \setminus \{0\},\ y = \dfrac{1}{2x}\}$.

E 3.7.11

Hallar en cada caso dos relaciones S y T tales que $S \circ T = R$ siendo

(a) $R = \{(a,x),(b,y),(a,z),(c,x)\}$,

(b) $R = \{(x,y) : x \in \mathbb{N},\ y = 2x+1\} \cup \{(1,8),(1,7)\}$.

E 3.7.12

(a) Hallar una matriz asociada a las relaciones R y T del ejercicio 3.7.8. ¿Qué interpretación puede darse a la suma de los números de una fila? ¿Y a los de una columna?

(b) Dados los conjuntos $A = \{x,y,z\}$, $B = \{1,2\}$ y las relaciones

$R = \{(x,1),(x,2),(z,2)\}$,

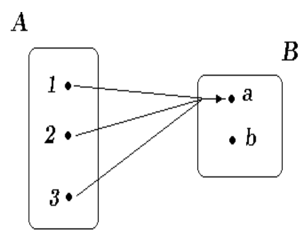
$S = \{(1,y),(2,y),(1,x),(2,z)\}$,

verificar que la matriz asociada a $S \circ R$ se obtiene del producto $M(R) \cdot M(S)$ cambiando por 1 todos los números mayores que 1 y dejando invariante los restantes.

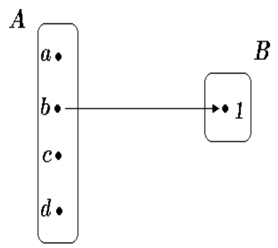
E 3.7.13

Dadas las siguientes relaciones entre los elementos de A y B:

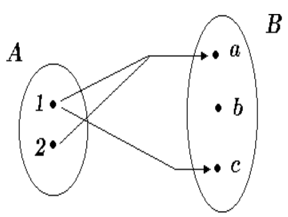
(i)



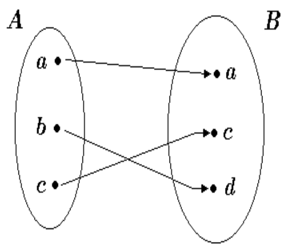
(ii)



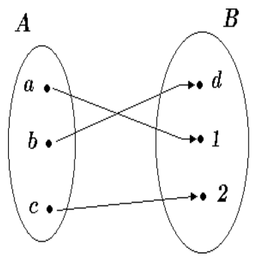
(iii)



(iv)



(v)



(vi)

x	$R(x)$
1	$\{2\}$
3	$\{4\}$
5	$\{6\}$
7	$\{8\}$

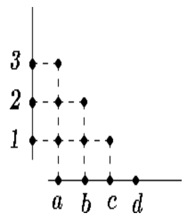
(vii)

x	$R(x)$
a	$\{1,4\}$
b	$\{2\}$
c	$\{3\}$

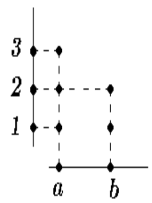
(viii)

x	$R(x)$
1	$\{2\}$
2	$\{2\}$
3	$\{3,2\}$

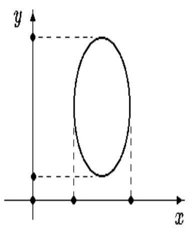
(ix) $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$,



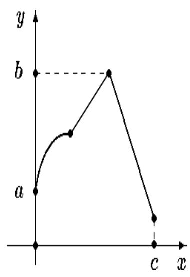
(x) $A = \{a, b\}$, $B = \{1, 2, 3\}$,



(xi) $A = [a, b] \subseteq I\!R$, $B = [c, d] \subseteq I\!R$,



(xii) $A = [0, c] \subseteq I\!R$, $B = [0, b] \subseteq I\!R$,



(xiii) $A = B = I\!N$, $R = \{(x, y) : x \in A,\ x = y\} \cup \{(1, 4)\}$.

Indicar

(a) cuáles son funcionales,

(b) dominio e imagen de cada una de las funciones,

(c) cuáles definen funciones totales de A en B.

E 3.7.14

Indicar dominio e imagen de cada una de las siguientes funciones $f \subseteq A \times B$:

(a) $A = B = \mathbb{Z}$, $f(x) = x + 4$,

(b) $A = B = \mathbb{N}$, $f(x) = x - 5$,

(c) $A = \mathbb{N}$, $B = \mathbb{R}$, $f(x) = \frac{2}{x}$,

(d) $A = \mathbb{R}$, $B = \mathbb{N}$, $f(x) = \frac{2}{x}$,

(e) $A = B = \mathbb{R}$, $f(x) = \sqrt{x} - 5$.

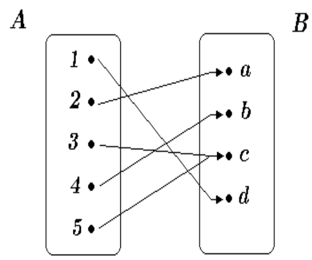
E 3.7.15

Hallar, en los casos posibles, una matriz asociada a las funciones del ejercicio 3.7.13 ¿Qué características especiales tiene la matriz asociada a una relación cuando ésta es funcional?

E 3.7.16

Dada $f : A \longrightarrow B$ calcular, en cada caso, $F(X)$ y $F^*(Y)$

(a)



$X = \{2, 4\}$, $Y = \{a, c\}$.

(b) $A = \{a, b, c, d, e, s, g\}$, $B = \{1, 2, 3, 4, 5\}$,

x	a	b	c	d	e	s	g
$f(x)$	1	1	1	2	2	1	3

$X = \{a, g\}$, $Y = \{1, 5\}$.

(c) $f : [-2, +\infty) \longrightarrow I\!R$,

$$f(x) = \begin{cases} x^2 & \text{si } -2 \leq x \leq 2 \\ x+1 & \text{si } x > 2 \end{cases},$$

$X = \{-2, 0, 1, \sqrt{2}, 2, 5\}$, $Y = (-7, -2]$.

(d) $f : I\!R \setminus \{0\} \longrightarrow I\!R$, $f(x) = \dfrac{1}{x^2}$,
$X = [3, 5)$, $Y = [-3, 2)$.

E 3.7.17

Dada $f : A \longrightarrow B$ y $X_1, X_2 \subseteq A$, $Y_1, Y_2 \subseteq B$, probar que

(a) si $X_1 \subseteq X_2$, entonces $F(X_1) \subseteq F(X_2)$,

(b) $F(X_1 \cap X_2) \subseteq F(X_1) \cap F(X_2)$ ¿es válida la igualdad?,

(c) $F^*(Y_1 \cup Y_2) = F^*(Y_1) \cup F^*(Y_2)$,

(d) $F^*(\mathcal{C}Y_1) = \mathcal{C}F^*(Y_1)$.

E 3.7.18

Determinar si f es una restricción de g en cada uno de los siguientes casos:

(a) $f = \{(1, 6), (7, 0), (15, -8), (6, 1)\}$,

$$g : I\!N \longrightarrow Z\!\!Z, \quad g(x) = \begin{cases} -x+7 & \text{si } x \text{ es impar} \\ 3x & \text{en otro caso} \end{cases}.$$

(b) $I\!P$ es el conjunto de los números naturales pares y

$$f : I\!P \times I\!P \longrightarrow I\!P, \quad f((x, y)) = x + y,$$

$$g : I\!N \times I\!N \longrightarrow Z\!\!Z, \quad g((x, y)) = \begin{cases} x+y & \text{si } x,\ y \text{ son pares} \\ x-y & \text{en otro caso} \end{cases}.$$

(c) $f : I\!R^- \longrightarrow I\!R$, $f(x) = -2x$ y $g : I\!R \longrightarrow I\!R$, $g(x) = 2|x|$.

(d) $A = B = \mathbb{N}$, f es la función parcial de A en B definida por $f(x) = \dfrac{x}{2}$

y $\quad g : \mathbb{N} \longrightarrow \mathbb{Q}, \quad g(x) = \dfrac{x}{2}$.

E 3.7.19

Sean $Y = \{(0, y) : y \in \mathbb{N}\}$ y $f : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Z}$ tal que $f((x, y)) = x + y$. Si $p_2 : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{N}$ es la segunda proyección, probar que $p_2|_Y$ es una restricción de f.

E 3.7.20

(a) Sean $S = \{1, 2, 3, 4\}$, $T = \{1, 2, 3, 4, 5, 6\}$ y $U = \{6, 7, 8, 9, 10\}$.

Sean $f = \{(1, 2), (2, 4), (3, 3), (4, 6)\} \subseteq S \times T$ y $g \subseteq T \times U$ definida por

x	1	2	3	4	5	6
$g(x)$	7	6	9	7	8	9

.

Hallar $g \circ f$ y $f \circ g$.

(b) Dadas las funciones

$$f_1(x) = -x^2, \qquad f_2(x) = 3 + x,$$

$$f_3(x) = \sqrt{x} - 3, \qquad f_4(x) = -\frac{1}{x^2},$$

$$f_5(x) = \frac{3}{x + 2}, \qquad f_6(x) = -\sqrt{x},$$

$$f_7 = \{(x, y) : x \in \mathbb{R},\ y = -x^2 + 9\}.$$

Calcular las siguientes funciones y determinar el dominio de cada una de ellas:

(i) $f_1 \circ f_2$, (ii) $f_2 \circ f_1$,

(iii) $f_3 \circ f_1$, (iv) $f_1 \circ f_3$,

(v) $f_5 \circ f_4$, (vi) $f_1 \circ f_5$,

(vii) $f_5 \circ f_3$, (viii) $f_3 \circ f_4$,

(ix) $f_6 \circ f_7$, (x) $f_5 \circ f_7$.

Determinar, si es posible, $(f_5 \circ f_7)(\sqrt{11})$ y $(f_5 \circ f_7)(3)$.

E 3.7.21

Clasificar las funciones del ejercicio 3.7.13, inciso (c) en inyectivas, epiyectivas y/o biyectivas.

E 3.7.22

(a) Sean $S = \{a, b, c, d\}$ y $T = \{x, y, z\}$. Hallar en cada caso, si es posible, una función $f : S \longrightarrow T$ tal que

  (i) f no sea inyectiva ni epiyectiva,

  (ii) f sea epiyectiva y no sea inyectiva,

  (iii) f sea inyectiva.

(b) Hallar, en cada caso, una función

  (i) $f : \mathbb{N} \times \mathbb{Q} \longrightarrow \mathbb{Q}$ epiyectiva,

  (ii) $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ inyectiva,

  (iii) total epiyectiva, del conjunto de los números naturales pares en el conjunto de los números naturales múltiplos de 3.

E 3.7.23

Hallar una restricción biyectiva de cada una de las siguientes funciones reales de variable real:

(a) $f(x) = \dfrac{1}{x^2}$,

(b) $f(x) = 2x^2$,

(c) $f(x) = |x^2 - 1|$.

E 3.7.24

Dadas las siguientes funciones:

$$f_1 : \mathbb{R} \longrightarrow \mathbb{R},\ f_1(x) = 2x + 1,$$

$f_2 = \{(x, y) : x \in \mathbb{N} \cup \{0\},\ y = 2x + 1\},$

$f_3 : \mathbb{Z} \longrightarrow \mathbb{Z},\ f_3(x) = |x|,$

$f_4 : \mathbb{R} \longrightarrow \mathbb{R},\ f_4(x) = |x|,$

$f_5 = \{(x, y) : x \in \mathbb{R},\ y = x^2 - 4\},$

$f_6 = \{(x, y) : x \in \mathbb{N},\ y = x^2 - 4\},$

$f_7 : [\frac{1}{2}, 3) \longrightarrow (\frac{1}{3}, 2],\ f_7(x) = \frac{1}{x},$

$f_8 : \mathbb{R}^2 \longrightarrow \mathbb{R}^2,\ f_8((x, y)) = (y + 1, x + 1).$

(a) Determinar si son inyectivas, epiyectivas o biyectivas.

(b) Calcular, cuando sea posible, la función inversa, indicando dominio e imagen de la misma.

(c) ¿Es f_2 una restricción de f_1?, ¿es f_5 una extensión de f_6? Justificar.

E 3.7.25

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$.

(a) Probar que

(i) si f y g son inyectivas, entonces $g \circ f$ es inyectiva,

(ii) si f y g son epiyectivas, entonces $g \circ f$ es epiyectiva,

(iii) si $g \circ f$ es epiyectiva, entonces g también lo es,

(iv) si $g \circ f$ es inyectiva, entonces f también lo es.

(b) Encontrar ejemplos donde

(i) $g \circ f$ sea epiyectiva y f no,

(ii) $g \circ f$ sea inyectiva y g no.

4 Multigrafos y multidigrafos

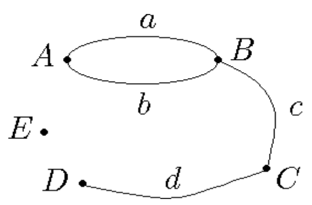
Muchas situaciones de la vida real pueden ser esquematizadas por medio de diagramas construídos por puntos (vértices o nodos) y líneas que conectan algunos pares de vértices, eventualmente alguna línea puede unir un vértice consigo mismo.

Estos esquemas, que facilitan la comprensión del problema a resolver, aparecen frecuentemente en disciplinas dispares y bajo nombres diversos, a saber: redes (en ingeniería, economía), sociogramas (en sicología), organigramas (en economía y planificación), diagramas de flujo (en programación).

La teoría que se ocupa del estudio de estos diagramas se conoce con el nombre de Teoría de Grafos.

En esta Teoría se estudian dos tipos de nociones: dirigidas u orientadas y no dirigidas. Nosotros comenzaremos por esta última.

Consideremos por ejemplo un mapa de ciudades y rutas que unen dichas ciudades.



Ciudades: A, B, C, D, E, rutas: a, b, c, d.

De este diagrama podemos obtener cierta información. Por ejemplo:

(1) hay dos rutas que unen las ciudades A y B,

(2) no existe una ruta directa entre A y D,

(3) la ciudad E está aislada.

4.1 Multigrafos

La noción matemática con que se pueden abordar este tipo de problemas es la siguiente:

D 4.1.1 *Llamaremos multigrafo G a una terna (V, A, φ) formada por*

(i) *un conjunto V no vacío cuyos elementos denominaremos vértices o nodos,*

(ii) *un conjunto A, disjunto con V, cuyos elementos llamaremos aristas,*

(iii) *una función $\varphi : A \longrightarrow \mathcal{P}(V)$ tal que $1 \leq |\varphi(a)| \leq 2$, para todo $a \in A$.*

A los elementos del conjunto $\varphi(a)$ los denominaremos extremos de la arista a.

Nosotros trabajaremos siempre con multigrafos cuyo conjunto de vértices y de aristas es finito.

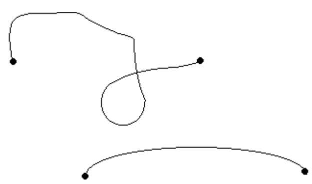
Habitualmente indicaremos los vértices con números: $1, 2, \ldots, n$ y las aristas con letras minúsculas: $a, b, \ldots$.

Ejemplo

Sea $G = (V, A, \varphi)$ donde $V = \{1, 2, 3, 4\}$, $A = \{a, b, c, d\}$ y φ está dada por

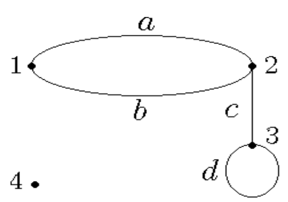
x	a	b	c	d
$\varphi(x)$	$\{1,2\}$	$\{1,2\}$	$\{2,3\}$	$\{3\}$

Los vértices se representan por puntos y las aristas por líneas continuas que unen dichos puntos. Como no se especifica la forma de la línea podríamos utilizar

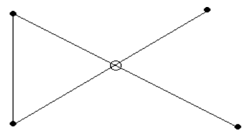


se elige la más simple de ellas, en este caso la segunda.

Luego, para el ejemplo anterior tenemos



Observemos que dos aristas pueden intersectarse en puntos que no son vértices, por ejemplo

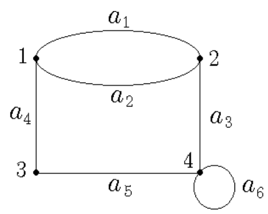


$\otimes$ no es vértice.

Nociones elementales

Vamos a indicar a continuación algunos conceptos elementales de la teoría de multigrafos. Para ejemplificar vamos a considerar el multigrafo $G = (V, A, \varphi)$ donde $V = \{1, 2, 3, 4, 5\}$, $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ y φ está dada por

x	a_1	a_2	a_3	a_4	a_5	a_6
$\varphi(x)$	$\{1, 2\}$	$\{1, 2\}$	$\{2, 4\}$	$\{1, 3\}$	$\{3, 4\}$	$\{4\}$



D 4.1.2 *Dos vértices son adyacentes si son extremos de una misma arista.*

1 y 2 son adyacentes,

2 y 3 no lo son,

4 es adyacente consigo mismo.

D 4.1.3 *Una arista que une un vértice consigo mismo se denomina un bucle.*

a_6 es un bucle.

Si un multigrafo no tiene bucles diremos que es libre de bucles.

D 4.1.4 *Se llama grado de un vértice v y se nota $gr(v)$ al número de aristas que se apoyan en él.*

Adoptaremos la siguiente convención: los bucles cuentan doble.

$gr(4) = 4$, $gr(5) = 0$.

D 4.1.5 *Un vértice es aislado si su grado es nulo.*

5 es vértice aislado.

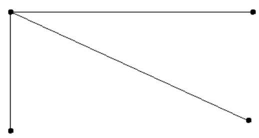
D 4.1.6 *Dos aristas son paralelas si tienen los mismos extremos.*

a_1 y a_2 son aristas paralelas.

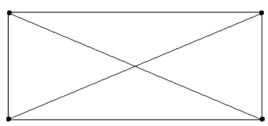
D 4.1.7 *Llamaremos grafo a todo multigrafo sin aristas paralelas.*

Si tenemos en cuenta la definición de multigrafo, dos aristas p y q son paralelas si $\varphi(p) = \varphi(q)$. Por lo tanto si φ es una función inyectiva, G es un grafo.

D 4.1.8 *Se denomina grafo simple a un grafo sin bucles.*



D 4.1.9 *Un grafo simple se dice completo si cualquier par de vértices distintos son adyacentes.*



D 4.1.10 *Una cadena entre v_1 y v_k es una sucesión de vértices y aristas del tipo*
$v_1\, a_1\, v_2\, a_2 \cdots v_{k-1}\, a_{k-1}\, v_k$,
donde para cada i, a_i es la arista de extremos v_i, v_{i+1}.

c_1: $1\, a_4\, 3\, a_5\, 4\, a_6\, 4\, a_3\, 2$,

c_2: $1\, a_4\, 3\, a_5\, 4\, a_5\, 3\, a_4\, 1$,

c_3: $1\, a_1\, 2\, a_2\, 1$,

c_4: $1\, a_1\, 2\, a_3\, 4\, a_3\, 2\, a_2\, 1$.

D 4.1.11 *Llamaremos longitud de una cadena al número de aristas que intervienen en ella, contando cada arista tantas veces como figure en la sucesión que la define.*

$long(c_1) = 4$,

$long(c_2) = 4$.

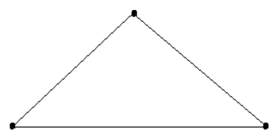
D 4.1.12 *Llamaremos ciclo a toda cadena que comienza y termina en un mismo vértice v, sin aristas ni vértices repetidos excepto v (en los extremos).*

$1\, a_1\, 2\, a_2\, 1$,

$1\, a_1\, 2\, a_3\, 4\, a_5\, 3\, a_4\, 1$.

Si un multigrafo no tiene ciclos se dice acíclico.

Observemos que si G es acíclico es simple. La recíproca no es válida, basta considerar



D 4.1.13 *Un multigrafo se dice conexo si es un único vértice o si cualquier par de vértices pueden unirse por una cadena. En caso contrario se llama disconexo.*

Muchas veces deseamos que los vértices de un multigrafo G lleven cierta información, por ejemplo si se trata de un mapa de rutas, los nombres de las ciudades. En este caso diremos que G es un multigrafo etiquetado.

Otras veces podemos necesitar adosar cierta información a las aristas, por ejemplo la distancia entre dos ciudades, en este caso diremos que G es un multigrafo valuado.

Submultigrafos

D 4.1.14 $G' = (V', A', \varphi')$ *es un submultigrafo de* $G = (V, A, \varphi)$ *si se verifican*

(i) $V' \subseteq V$,

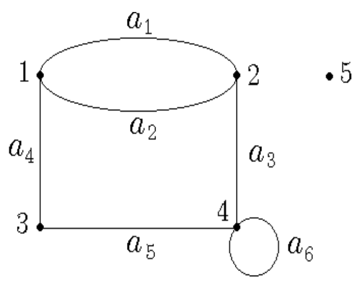
(ii) $A' \subseteq A$,

(iii) $\varphi' = \varphi|_{A'}$.

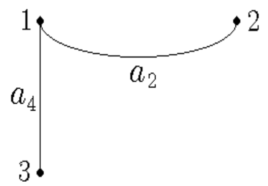
Ejemplos

(i) Todo multigrafo es un submultigrafo de sí mismo.

(ii) Si consideramos el multigrafo G



un submultigrafo de G es

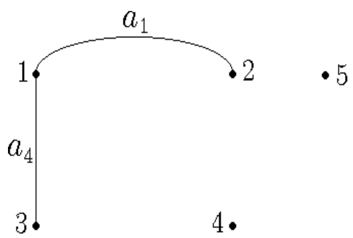


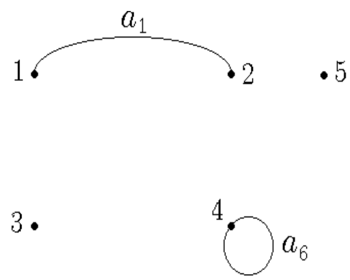
Submultigrafos cubrientes

D 4.1.15 $G' = (V', A', \varphi')$ *es un submultigrafo cubriente de* $G = (V, A, \varphi)$, *si* $V = V'$.

Ejemplos

Si G es el multigrafo del ejemplo (ii) anterior, entonces





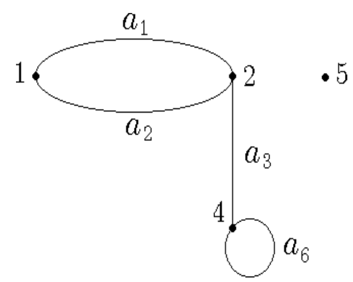
G' y G'' son submultigrafos cubrientes de G.

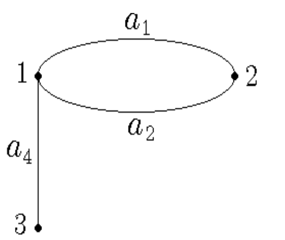
Submultigrafos inducidos o generados

D 4.1.16 *$G' = (V', A', \varphi')$ es el submultigrafo inducido por V' en $G = (V, A, \varphi)$ si conserva todas las aristas de G cuyos extremos pertenecen a V'.*

Ejemplos

Si G es el multigrafo del ejemplo (ii) anterior, entonces





G' y G'' son submultigrafos inducidos por $\{1, 2, 4, 5\}$ y $\{1, 2, 3\}$ respectivamente en G.

Representación computacional de los multigrafos

Hemos dicho que la mayor ventaja de los multigrafos es la representación visual de la información, sin embargo para utilizar la computadora debemos representar esta información de otras formas. Consideraremos dos maneras distintas de hacerlo:

(i) la matriz de adyacencia,

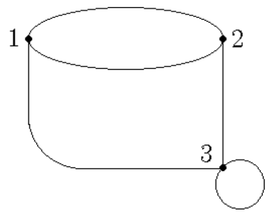
(ii) la lista de adyacencia.

Matriz de adyacencia

D 4.1.17 *Sea G un multigrafo con n vértices $v_1, v_2, \ldots, v_n$. La matriz de adyacencia de G es la matriz $M(G) = (a_{ij})_{n\times n}$, donde a_{ij} es el número de aristas de extremos v_i y v_j, $1 \leq i, j \leq n$.*

Ejemplo

Sea G



entonces,

$$M(G) = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{pmatrix} 0 & 2 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \end{array}.$$

Observemos que la matriz de adyacencia es simétrica, ya que el número de aristas de extremos v_i, v_j es igual al número de aristas de extremos v_j, v_i.

La matriz de adyacencia nos permite determinar el número de cadenas de una cierta longitud dada que hay entre dos vértices arbitrarios de G del siguiente modo:

T 4.1.1 *Sean G un multigrafo con n vértices, $M(G) = (a_{ij})_{n\times n}$ su matriz de adyacencia y $M^2(G) = (b_{ij})_{n\times n}$. Entonces b_{ij} es el número de cadenas de longitud 2 entre el vértice v_i y el v_j.*

Dem. Sabemos que $b_{ij} = a_{i1}a_{1j} + a_{i2}a_{2j} + \cdots + a_{in}a_{nj}$, $1 \leq i, j \leq n$. Si consideramos un término cualquiera de esta suma, por ejemplo $a_{i1} \cdot a_{1j}$, se pueden presentar los siguientes casos:

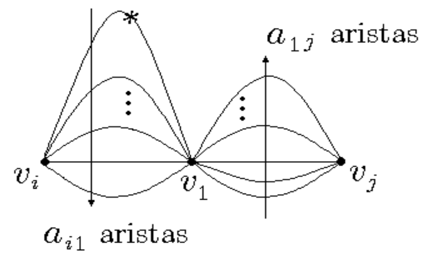
(i) $a_{i1} \cdot a_{1j} = 0$, de donde

(i.1) $a_{i1} = 0$, es decir, no hay ninguna arista de extremos v_i, v_1, ó

(i.2) $a_{1j} = 0$, es decir, no hay ninguna arista de extremos v_1, v_j.

Luego, no puede haber ninguna cadena de longitud 2 entre v_i y v_j pasando por v_1.

(ii) $a_{i1} \cdot a_{1j} \neq 0$, entonces tendremos una situación como la indicada en la siguiente figura:



Si consideramos una arista fija que une v_i con v_1, a partir de ella tenemos a_{1j} cadenas de longitud 2 que unen v_i con v_j pasando por v_1.

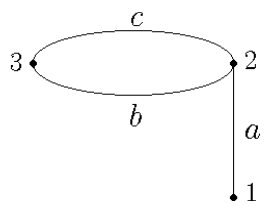
Reemplazando esta arista por otra arista fija tenemos nuevamente a_{1j} cadenas de longitud 2 entre v_i y v_j pasando por v_1.

Repitiendo el proceso a_{i1} veces obtenemos $a_{i1} \cdot a_{1j}$ cadenas de longitud 2 entre v_i y v_j pasando por v_1.

De manera análoga se prueba que $a_{it} \cdot a_{tj}$ es el número de cadenas de longitud 2 entre v_i y v_j pasando por v_t. Luego b_{ij} es el número total de cadenas de longitud 2 entre v_i y v_j. ■

Ejemplo

Sea G



entonces

$$M(G) = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix} \end{array} \text{ y } M^2(G) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 5 & 0 \\ 2 & 0 & 4 \end{pmatrix}.$$

En particular, hay cinco cadenas de longitud 2 que unen el vértice 2 con sí mismo, que son:

$2\,b\,3\,b\,2$,

$2\,b\,3\,c\,2$,

$2\,c\,3\,c\,2$,

$2\,a\,1\,a\,2$,

$2\,c\,3\,b\,2$.

Usando el principio de inducción se puede demostrar el siguiente teorema:

T 4.1.2 *Sean G un multigrafo con n vértices, $M(G) = (a_{ij})_{n\times n}$ su matriz de adyacencia y $M^m(G) = (d_{ij})_{n\times n}$. Entonces d_{ij} es el número de cadenas de longitud m entre el vértice v_i y el v_j.*

Lista de adyacencia

Existe un tipo de multigrafos G para el cual la matriz de adyacencia es rala, es decir contiene muchos ceros y es el caso en que G tiene pocas aristas. De todas maneras si G tiene n vértices, para informar $M(G)$ a la máquina debemos introducir $\dfrac{n^2+n}{2}$ números.

Este hecho nos conduce a buscar un procedimiento donde no haya que informar los ceros.

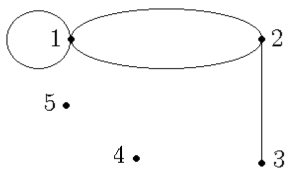
El método más eficiente es el llamado lista de adyacencia de un multigrafo y consiste en lo siguiente:

(i) hacemos una lista con todos los vértices del multigrafo,

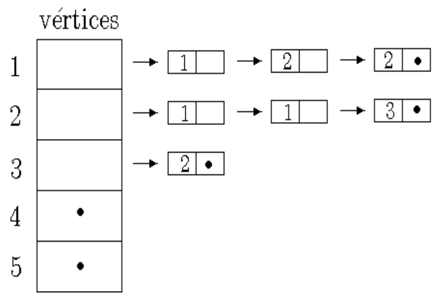
(ii) para cada vértice indicamos todos los vértices adyacentes a él, colocándose un punto al finalizar la lista de cada vértice.

Ejemplo

Dado el multigrafo G



la lista de adyacencia de G es



La ventaja de este procedimiento con respecto a la matriz de adyacencia es que debemos entrar menos datos y por lo tanto ocupamos menos lugar de memoria.

La desventaja, es que para saber si un vértice v_i está es adyacente con v_j debemos leer toda la lista de los adyacentes con v_i, en cambio en la matriz de adyacencia leemos sólo el lugar ij.

4.2 *Arboles*

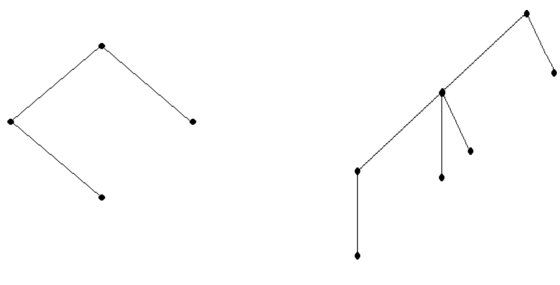
Hay un tipo de grafos, llamados árboles, de particular importancia en computación. Ellos son usados por ejemplo:

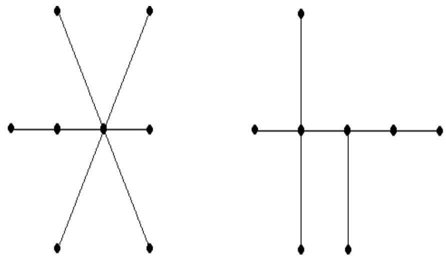
(i) en compiladores o traductores, para determinar si un lenguaje de alto nivel es sintácticamente correcto,

(ii) en estructura de datos para la representación de archivos. Allí se emplean los llamados árboles de búsqueda.

D 4.2.1 *Un árbol es un grafo conexo y sin ciclos.*

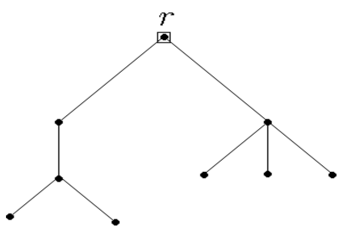
Ejemplos





En computación, los de mayor aplicación son los árboles con raíz, es decir árboles en los cuales hay un vértice distinguido r que se denomina la raíz del árbol.

Es usual tomar como raíz al vértice que se encuentra en la parte superior del dibujo.

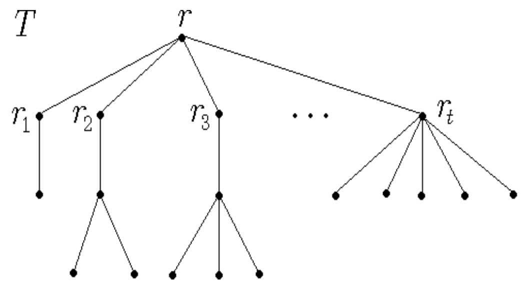


Un árbol T con raíz puede ser definido recursivamente como sigue:

(1) un único vértice es un árbol con raíz,

(2) si un árbol T tiene más de un vértice, entonces un único vértice r es la raíz del árbol, y los vértices $r_1, r_2, \ldots, r_t$ unidos a r por una única arista son raíces de árboles disjuntos.

Los vértices $r_1, r_2, \ldots, r_t$ se denominan los hijos de r y r se llama el padre de $r_1, r_2, \ldots, r_t$.



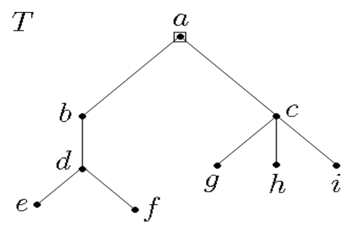
Como un árbol con raíz es un grafo conexo, existe siempre una cadena que une la raíz con cualquier vértice del árbol y como es acíclico dicha cadena es única.

Esto nos permite introducir la siguiente noción:

D 4.2.2 *La profundidad de un vértice v en un árbol con raíz r, que notaremos $pr(v)$, es la longitud de la cadena que une v con r. Aceptaremos que $pr(r) = 0$.*

D 4.2.3 *Se denomina altura de un árbol T con raíz, y la notaremos $h(T)$, al máximo de las profundidades de los vértices.*

Ejemplo



$pr(g) = 2$, $pr(e) = 3$, $h(T) = 3$.

D 4.2.4 *Se denomina hoja a todo vértice de T sin hijos, en caso contrario, diremos que es un vértice interno.*

T 4.2.1 *Todo árbol finito T tiene hojas.*

Dem. Sea v_1 un vértice de T,

(i) si v_1 es una hoja, está demostrado. En caso contrario

(ii) sea v_2 un hijo de v_1,

- (ii.1) si v_2 es una hoja, está demostrado. En caso contrario
- (ii.2) sea v_3 un hijo de v_2.

Como el árbol es finito este proceso finaliza y el vértice en el que para, es una hoja. ■

T 4.2.2 *Todo árbol T con m vértices tiene $m - 1$ aristas.*

Dem. Haremos la demostración por inducción sobre m.

Si $m = 1$, T tiene un sólo vértice, entonces si hay alguna arista debe ser un bucle por lo tanto T tiene un ciclo, absurdo. Luego, hay 0 aristas.

Supongamos que el teorema se verifica para $m = k$. Probémoslo para $m = k + 1$.

Sean x una hoja de T, y el padre de x y c la arista de extremos x e y. Si en T suprimimos c y llamamos T' al árbol resultante, el número de vértices de T' es k y aplicando la hipótesis inductiva, T' tiene $k - 1$ aristas, de donde T tiene k aristas. ■

Arbol cubriente minimal

Un problema que se presenta en el diseño de redes es como conectar todos los vértices eficientemente, donde los vértices pueden ser computadoras, teléfonos, etc. Un árbol cubriente minimal puede proveernos una solución económica.

Arbol cubriente de un grafo

D 4.2.5 *Dado un grafo conexo G, un árbol cubriente de G es un subgrafo cubriente conexo y sin ciclos.*

Es decir, es un subgrafo cubriente de G que es un árbol.

Dado un grafo conexo y valuado G, indicaremos cómo construir un árbol cubriente de G de valuación mínima.

Algoritmo para obtener un árbol cubriente minimal

Sea G un grafo conexo y valuado, con n vértices. El algoritmo consiste en lo siguiente:

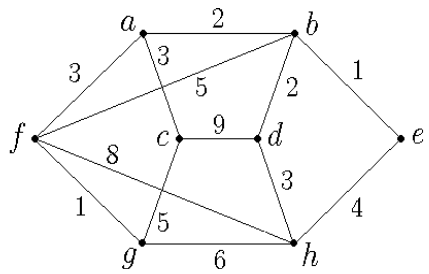
(i) se elige un vértice arbitrario de G como primer elemento de un conjunto que notaremos IN,

(ii) de todos los vértices z de G tales que $z \notin IN$ y son adyacentes a los vértices del conjunto, se selecciona uno cuya arista tenga valuación mínima. Dicho vértice se agrega a IN y la arista en cuestión forma parte del árbol cubriente buscado,

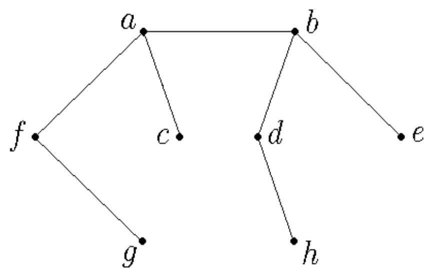
(iii) se repite el paso (ii) hasta que $|IN| = n$, esto es, hasta que todos los vértices de G estén en el conjunto IN.

Observemos que en (ii) puede haber más de un vértice en las condiciones pedidas, de donde resulta que el árbol cubriente minimal hallado no es único. Lo que es única es la valuación mínima.

Ejemplo



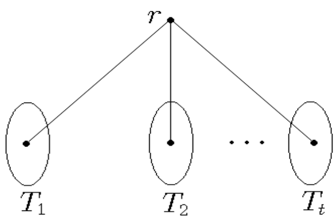
En este caso $IN = \{d, b, e, a, h, c, f, g\}$ y el árbol cubriente minimal correspondiente es



Recorrido de árboles

Indicaremos tres algoritmos muy útiles para recorrer un árbol, ellos nos permitirán recorrerlo en pre–orden, orden simétrico y post–orden, respectivamente.

En estos métodos es conveniente emplear la definición recursiva de árbol con raíz, donde de la raíz parten las aristas que sostienen las raíces de los subárboles.



Sea T un árbol con raíz r, tal que todos los subárboles de T están etiquetados de izquierda a derecha con $T_1, T_2, \ldots, T_t$.

Pre–orden

Si lo recorremos en pre–orden, la raíz del árbol es visitada primero y luego los subárboles son procesados de izquierda a derecha en pre–orden.

Algoritmo

La entrada es un árbol T con raíz r y subárboles etiquetados de izquierda a derecha $T_1, T_2, \ldots, T_t$; la salida es la lista de vértices en preorden:

(1) escribir r,

(2) para $i = 1$ hasta t hacer pre–orden en T_i.

Orden simétrico

Se comienza recorriendo el árbol izquierdo en orden simétrico, luego se visita la raíz y a continuación los restantes subárboles son procesados de izquierda a derecha en orden simétrico.

Algoritmo

La entrada es un árbol T con raíz r y subárboles etiquetados de izquierda a derecha $T_1, T_2, \ldots, T_t$; la salida es la lista de vértices en orden simétrico:

(1) orden simétrico en T_1,

(2) escribir r,

(3) para $i = 2$ hasta t hacer orden simétrico en T_i.

Post–orden

En este caso la raíz es visitada al final, después que todos los subárboles han sido procesados de izquierda a derecha en post–orden.

Algoritmo

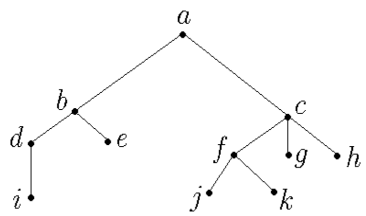
La entrada es un árbol T con raíz r y subárboles etiquetados de izquierda a derecha $T_1, T_2, \ldots, T_t$; la salida es la lista de vértices en post-orden:

(1) para $i = 1$ hasta t hacer post–orden en T_i,

(2) escribir r.

Ejemplo

Si consideramos el árbol T



La lista de vértices en

(i) pre–orden es: $a\,b\,d\,i\,e\,c\,f\,j\,k\,g\,h$,

(ii) orden simétrico es: $i\,d\,b\,e\,a\,j\,f\,k\,c\,g\,h$,

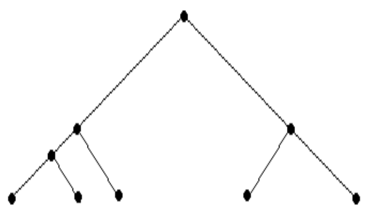
(iii) post–orden es: $i\,d\,e\,b\,j\,k\,f\,g\,h\,c\,a$.

4.3 *Arboles binarios*

D 4.3.1 *Un árbol se dice binario si cada vértice tiene a lo sumo dos hijos, que llamaremos hijo izquierdo e hijo derecho, respectivamente.*

Ejemplo

El arbol indicado en la figura es binario

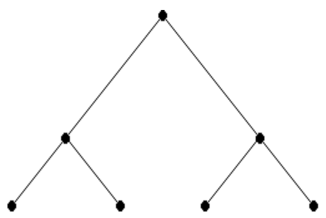


Arbol binario lleno

D 4.3.2 *Un árbol binario se dice lleno cuando todos los vértices internos tienen dos hijos y todas las hojas tienen la misma profundidad.*

Ejemplo

El arbol binario indicado en la figura es lleno



Aplicaciones

Recordemos que si X es el conjunto de las variables proposicionales (v.p.) y consideramos los símbolos de las operaciones binarias $\wedge, \vee, \rightarrow$, y el de la operación unaria $\sim$, con $For[X]$ designamos al conjunto de las formas proposicionales (f.p.), que se construyen por medio de las siguientes reglas:

(R1) si $x \in X$, entonces x es f.p.,

(R2) si p y q son f.p., entonces $(p \wedge q), (p \vee q), (p \rightarrow q)$ son f.p.,

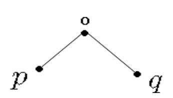
(R3) si p es una f.p., entonces $\sim p$ es una f.p.,

(R4) (de cierre) las únicas f.p. son las determinadas por R1, R2 y R3.

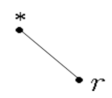
Entonces, cualquier $p \in For[X]$ puede representarse por medio de un árbol binario etiquetado del siguiente modo:

Paso 1:

Si $\alpha = p \circ q$, donde $\circ$ es una operación binaria, dibujamos



Si $\alpha = *r$, donde $*$ es una operación unaria, dibujamos

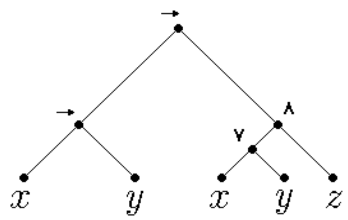


Paso 2:

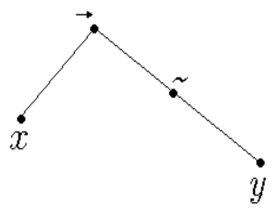
Aplicar el Paso 1 a p, q y r hasta que p, q y $r \in X$.

Ejemplos

(1) $\alpha = (x \to y) \to ((x \vee y) \wedge z)$



(2) $\beta = x \to \sim y$



Si en los ejemplos anteriores recorremos los vértices en

(i) orden simétrico,

 (1) $(x \to y) \to ((x \vee y) \wedge z)$,

 (2) $x \to \sim y$,

(ii) pre–orden,

 (1) $\to \to xy \wedge \vee xyz$,

 (2) $\to x \sim y$,

(iii) post–orden,

(1) $xy \to xy \vee z\wedge \to$,

(2) $xy \sim\to$.

Es decir,

(a) en (i) obtenemos la expresión de partida, donde los paréntesis se colocan al terminar de procesar cada subárbol. Esta manera de escribir a las fórmulas se denomina notación infija,

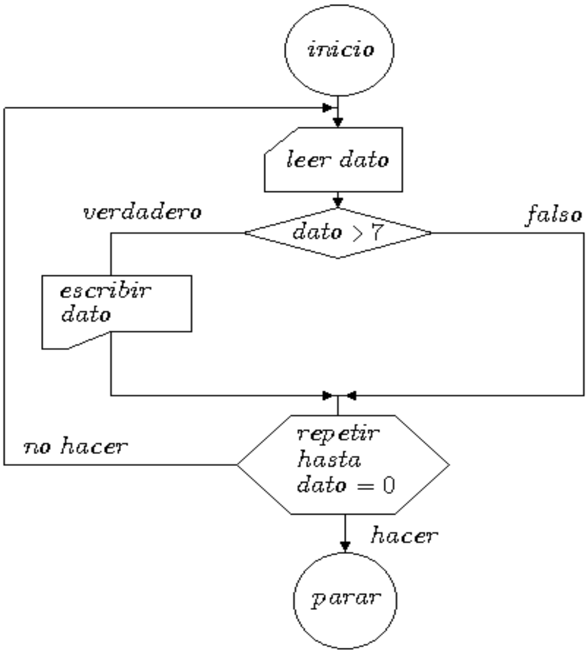
(b) en (ii) los símbolos de las operaciones preceden a los operandos. Esta manera de escribir a las fórmulas se denomina notación polaca a derecha o prefija,

(c) en (iii) los símbolos de las operaciones se escriben a continuación de los operandos. Esta manera de escribir a las fórmulas se denomina notación polaca a izquierda o postfija.

Observemos que ni la notación prefija ni la postfija requieren paréntesis, luego estas notaciones son más eficientes, aunque menos familiares que la infija. Los compiladores a menudo cambian la notación infija en los programas de computación por la prefija o la postfija para hacer más eficiente el proceso.

4.4 Multidigrafos

Antes de indicar la definición de multidigrafo veamos un ejemplo de tal noción. Consideremos el diagrama de flujo correspondiente a un programa de computación que lee una sucesión de enteros no negativos, imprime aquellos enteros mayores que 7 y para cuando ingresa como dato a 0.



D 4.4.1 *Llamaremos multidigrafo* $\overrightarrow{\mathrm{G}}$ *a una terna* (V, A, φ) *formada por*

(i) *un conjunto no vacío* V*, cuyos elementos denominaremos vértices o nodos,*

(ii) *un conjunto* A*, disjunto con* V*, cuyos elementos llamaremos arcos,*

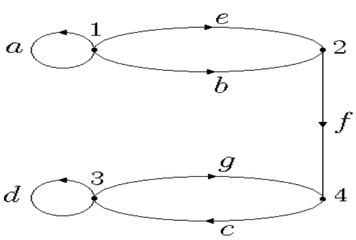
(iii) *una función* $\varphi : A \longrightarrow V \times V$ *tal que* $\varphi(a) = (v_1,\, v_2)$*,* v_1 *se llama vértice inicial u origen y* v_2 *se denomina vértice final o extremo del arco* a*.*

Nota. Para indicar que $\varphi(a) = (v_1,\, v_2)$, escribiremos $\overrightarrow{v_1 v_2}$.

Ejemplo

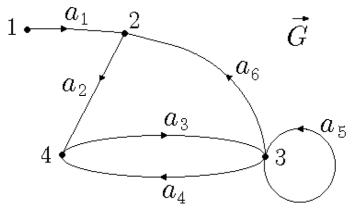
Sea $\overrightarrow{\mathrm{G}} = (V, A, \varphi)$, donde $V = \{1, 2, 3, 4\}$ y $A = \{a, b, c, d, e, f, g\}$ y φ está dada por la tabla

x	a	b	c	d	e	f	g
$\varphi(x)$	$(1,1)$	$(1,2)$	$(4,3)$	$(3,3)$	$(1,2)$	$(2,4)$	$(3,4)$



Nociones elementales

Vamos a indicar a continuación algunos conceptos elementales de la teoría de multidigrafos. Para ejemplificar, vamos a considerar el multidigrafo $\overrightarrow{\mathrm{G}} = (V, A, \varphi)$ indicado en la figura



D 4.4.2 *Llamaremos grado positivo (negativo) de un vértice v, y lo denotaremos con $gr^+(v)$ $(gr^-(v))$, al número de arcos con origen (extremo) en v.*

En el ejemplo anterior, $gr^-(1) = 0$ y $gr^+(3) = 3$.

D 4.4.3 *Un vértice v es aislado, si $gr^+(v) = gr^-(v) = 0$.*

D 4.4.4 *Un arco que une un vértice consigo mismo se denomina un bucle.*

En el ejemplo anterior, a_5 es un bucle.

D 4.4.5 *Dos arcos u y w son paralelos si $\varphi(u) = \varphi(w)$.*

D 4.4.6 *Llamaremos digrafo a todo multidigrafo sin arcos paralelos.*

D 4.4.7 *Un camino de v_1 a v_k es una sucesión de vértices y arcos del tipo*

$$v_1\, a_1\, v_2\, a_2 \ldots\, v_{k-1}\, a_{k-1}\, v_k,$$

donde para cada i, a_i es el arco con origen v_i y extremo v_{i+1}.

En el ejemplo anterior,

$$c_1 :\ 2\, a_2\, 4\, a_3\, 3\, a_5\, 3,$$

$$c_2 :\ 4\, a_3\, 3\, a_4\, 4\, a_3\, 3,$$

$$c_3 :\ 1\, a_1\, 2.$$

D 4.4.8 *Llamaremos longitud de un camino al número de arcos que intervienen en él, contando cada arco tantas veces como figure en la sucesión que lo define.*

En el ejemplo anterior,

$long(c_1) = 3, \quad long(c_3) = 1.$

D 4.4.9 *Diremos que el vértice v_k es alcanzable desde v_j, $v_k \neq v_j$ si en $\overrightarrow{\mathrm{G}}$ existe un camino de v_j a v_k.*

En el ejemplo anterior,

3 es alcanzable desde 2,

2 es alcanzable desde 1.

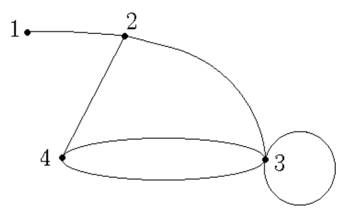
D 4.4.10 *Llamaremos circuito a todo camino que comienza y termina en un mismo vértice v sin arcos y sin vértices repetidos excepto v (en los extremos).*

En el ejemplo anterior,

$3\, a_5\, 3$,

$4\, a_3\, 3\, a_4\, 4$.

D 4.4.11 *Dado un multidigrafo $\overrightarrow{\mathrm{G}}$, llamaremos multigrafo subyacente o soporte de $\overrightarrow{\mathrm{G}}$, al que se obtiene a partir de $\overrightarrow{\mathrm{G}}$ suprimiendo las orientaciones.*



D 4.4.12 *Un multidigrafo es conexo, si su soporte lo es.*

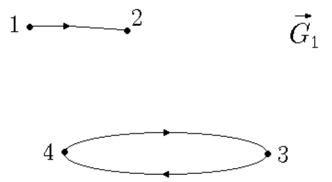
D 4.4.13 *Un multidigrafo es fuertemente conexo, si todo par de vértices distintos puede unirse por un camino.*

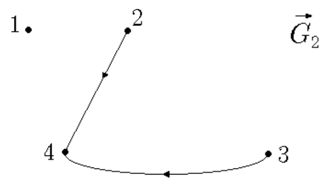
El multidigrafo $\overrightarrow{\mathrm{G}}$ no es fuertemente conexo pues no hay un camino de 2 a 1.

Las nociones de submultidigrafos, submultidigrafos cubrientes e inducidos se definen de manera análoga al caso no dirigido.

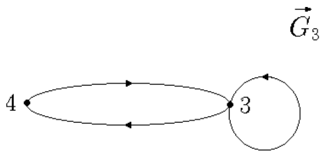
Ejemplos

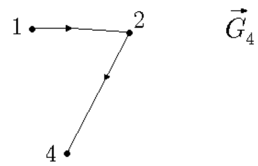
(i) G_1 y G_2 son submultidigrafos cubrientes de $\overrightarrow{G}$.





(ii) $\overrightarrow{\mathrm{G}}_3$ es inducido por $\{3, 4\}$ y $\overrightarrow{\mathrm{G}}_4$ es inducido por $\{1, 2, 4\}$.





Representación computacional de los multidigrafos

De manera análoga a lo visto para multigrafos, indicaremos dos formas distintas de informar un multidigrafo a una computadora, por medio de

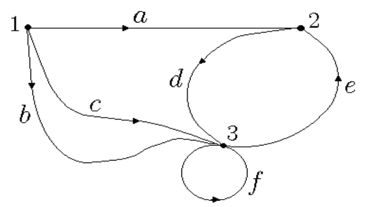
(i) la matriz de precedencia,

(ii) la lista de precedencia.

Matriz de precedencia

Sea $\overrightarrow{\mathrm{G}}$ un multidigrafo con n vértices $v_1, v_2, \dots, v_n$. La matriz de precedencia de $\overrightarrow{\mathrm{G}}$ es la matriz $M(\overrightarrow{\mathrm{G}}) = (a_{ij})_{n \times n}$, donde a_{ij} es el número de arcos con origen v_i y extremo v_j, $1 \leq i, j \leq n$.

Ejemplo



$$M(\overrightarrow{\mathrm{G}}) = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array}$$

Observemos que la matriz de precedencia no tiene por que ser simétrica.

De manera análoga a lo visto para el caso no dirigido, se prueba que

T 4.4.1 *Sean* $\overrightarrow{\mathrm{G}}$ *un multidigrafo con* n *vértices,* $M(\overrightarrow{\mathrm{G}}) = (a_{ij})_{n\times n}$ *su matriz de precedencia,* $m \in \mathbb{N}$ *y* $M^m(\overrightarrow{\mathrm{G}}) = (d_{ij})_{n\times n}$*. Entonces* d_{ij} *es el número de caminos de longitud* m *del vértice* v_i *al* v_j*.*

Ejemplo

Si $\overrightarrow{\mathrm{G}}$ es el multidigrafo del ejemplo anterior, entonces

$$M^2(\overrightarrow{\mathrm{G}}) = \begin{pmatrix} 0 & 2 & 3 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Luego, hay 3 caminos de longitud 2 del vértice 1 al 3, que son

$1\,a\,2\,d\,3$,

$1\,b\,3\,f\,3$,

$1\,c\,3\,f\,3$.

Un problema que se presenta con frecuencia es, dado un multidigrafo, saber si un vértice puede ser alcanzado o no desde otro. Recordemos que un vértice v_j es alcanzable desde v_i, $v_i \neq v_j$, si existe algún camino de v_i a v_j. Si consideramos la matriz $M(\overrightarrow{\mathrm{G}})$ y calculamos $M^2(\overrightarrow{\mathrm{G}})$, $M^3(\overrightarrow{\mathrm{G}}), \ldots$, entonces para que haya cualquier camino de v_i a v_j el lugar ij de alguna de estas matrices debe ser no nulo.

Se puede demostrar que en un multidigrafo $\overrightarrow{\mathrm{G}}$ con m vértices, cualquier camino que no tenga vértices repetidos puede tener a lo sumo $m-1$ arcos (y m vértices) antes que un vértice se repita. Además, en todo camino de longitud mayor que $m-1$, cualquier sección entre dos vértices repetidos es un circuito y por lo tanto puede eliminarse, luego la longitud del camino disminuye. Entonces si existe un camino desde v_i a v_j deberá ser de longitud a lo sumo $m-1$. Luego, sólo debemos calcular $M(\overrightarrow{\mathrm{G}})$, $M^2(\overrightarrow{\mathrm{G}})$, $M^3(\overrightarrow{\mathrm{G}}), \ldots,$ $M^{m-1}(\overrightarrow{\mathrm{G}})$, para decidir si v_i es alcanzable desde v_j.

Otra manera más eficiente de hacerlo, pues se ocupa menos lugar de memoria, consiste en calcular las matrices:

$$M(\overrightarrow{\mathrm{G}}),\ M^2(\overrightarrow{\mathrm{G}}),\ M^3(\overrightarrow{\mathrm{G}}), \ldots,\ M^{m-1}(\overrightarrow{\mathrm{G}})$$

y guardar solamente la matriz

$$R = M(\overrightarrow{\mathrm{G}}) + M^2(\overrightarrow{\mathrm{G}}) + M^3(\overrightarrow{\mathrm{G}}) + \ldots + M^{m-1}(\overrightarrow{\mathrm{G}}) = (r_{ij}).$$

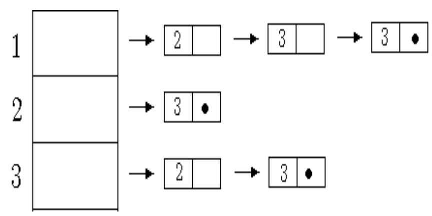
Si $r_{ij} > 0$, entonces se tiene que v_i es alcanzable desde v_j.

Lista de precedencia

Se construye de manera análoga al caso no dirigido.

Ejemplo

Si consideramos el multidigrafo del ejemplo anterior, la lista de precedencia correspondiente es



4.5 Ejercicios

E 4.5.1

Suponiendo que

A habla español, francés e inglés,

B habla español, inglés y alemán,

C habla español y alemán,

D habla francés,

esquematizar las distintas formas de comunicación directa entre ellos.

E 4.5.2

Dados los siguientes multigrafos:

(i) $G_1 = (V_1, A_1, \varphi_1)$, donde $V_1 = \{1, 2, 3, 4\}$, $A_1 = \{a, b, c, d, e, f, g\}$ y φ_1 está dada por la siguiente tabla:

x	a	b	c	d	e	f	g
$\varphi_1(x)$	$\{1, 2\}$	$\{1, 4\}$	$\{1\}$	$\{1, 3\}$	$\{2, 4\}$	$\{4, 3\}$	$\{2, 3\}$

(ii) $G_2 = (V_2, A_2, \varphi_2)$, donde $V_2 = \{1, 2, 3, 4, 5, 6\}$, $A_2 = \{a, b, c, d, e, f, g\}$ y φ_2 está dada por la siguiente tabla:

x	a	b	c	d	e	f	g
$\varphi_2(x)$	$\{1, 2\}$	$\{1, 4\}$	$\{2, 4\}$	$\{2, 3\}$	$\{2, 3\}$	$\{4, 5\}$	$\{4, 5\}$

(a) hacer el diagrama de cada uno de ellos,

(b) indicar cuáles de ellos son grafos, cuáles son conexos y cuáles son completos,

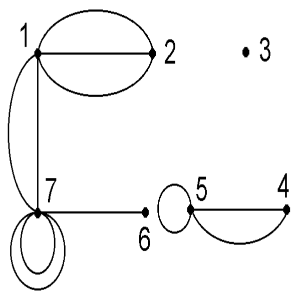
(c) hallar $gr(1)$ en G_1 y en G_2,

(d) hallar en G_2 una cadena que comience y termine en un mismo vértice que contenga todas las aristas de G_2 sin repetirlas. ¿Es esto siempre posible cualquiera sea el multigrafo?. Justifique,

(e) hallar en G_1 un ciclo de longitud 4 que contenga la arista d.

E 4.5.3

Dado el multigrafo G



(i) hallar, en cada caso, el multigrafo inducido por cada uno de los siguientes conjuntos de vértices:

(a) $\{7, 3\}$,

(b) $\{5, 2, 6\}$,

(c) $\{1, 2, 4, 5, 7\}$.

(ii) hallar un subgrafo cubriente de G que contenga ciclos,

(iii) hallar la suma de los grados de todos los vértices de G y verificar que dicha suma es dos veces el número de aristas de G.

E 4.5.4

Para cada uno de los multigrafos del Ejercicio 4.5.2, hallar

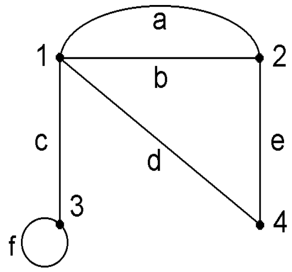
(i) la matriz de adyacencia asociada,

(ii) la lista de adyacencia asociada.

E 4.5.5

Sea G un multigrafo con n vértices $v_1, \ldots, v_n$ y m aristas $e_1, \ldots, e_m$. La matriz de incidencia de G es la matriz $C(G) = (c_{ij})_{n\times m}$, donde c_{ij} es el número de veces $(0, 1$ o $2)$ que v_i es extremo de e_j.

Dado el siguiente multigrafo G, hallar $C(G)$:



E 4.5.6

Sea $G = (V, A, \varphi)$ un multigrafo, probar que

(i) $\sum_{v \in V} gr(v) = 2|A|$,

(ii) el número de vértices de G de grado impar es par.

E 4.5.7

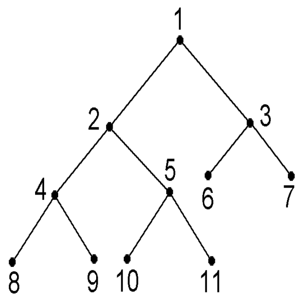
(i) Si G tiene 21 aristas con 7 vértices de grado 1, 3 de grado 2, 7 de grado 3 y el resto de grado 4, determinar el número total de vértices de G.

(ii) Idem inciso (i), sabiendo además que tiene 6 vértices aislados.

(iii) Un multigrafo donde todos los vértices tienen el mismo grado se dice regular. ¿Existen multigrafos regulares con 10 aristas en el que cada vértice tiene grado 4?. ¿Existen multigrafos regulares con 15 aristas en el que cada vértice tiene grado 4?. En caso de ser posible, dar ejemplos.

E 4.5.8

(i) Dado el árbol binario

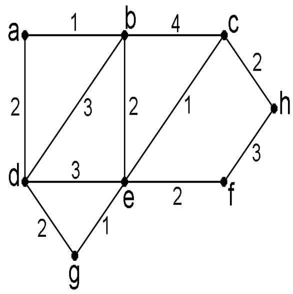


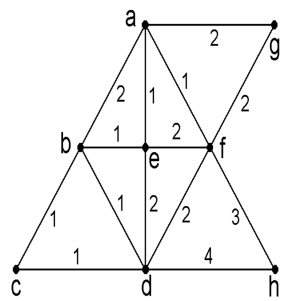
Determinar su raíz y su altura. ¿Es binario lleno?. ¿Cuál es el hijo izquierdo de 9?. ¿Qué profundidad tiene 4?

(ii) Hallar un árbol binario de altura 4 con cuatro hojas, una de ellas de profundidad 2, otra de profundidad 3 y tal que su raíz no tenga hijo derecho.

E 4.5.9

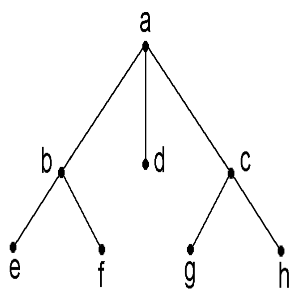
Hallar dos árboles minimales cubrientes para cada uno de los siguientes grafos:

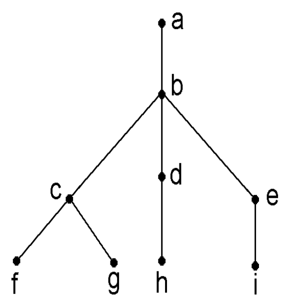


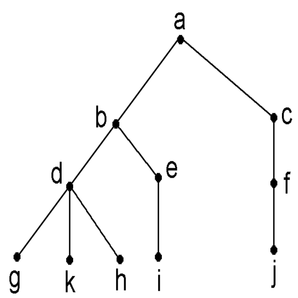


E 4.5.10

Escribir la lista de vértices en preorden, orden simétrico y post-orden para cada uno de los siguientes árboles:

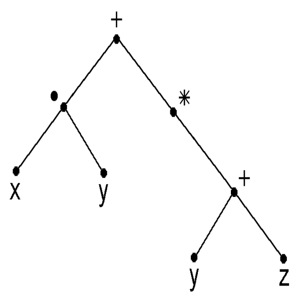


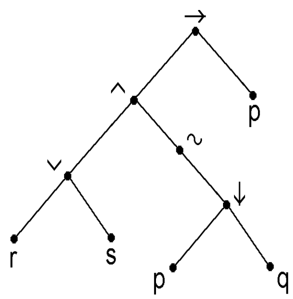




E 4.5.11

Hallar la fórmula asociada a cada uno de los siguientes árboles binarios en notación prefija, infija y post-fija:





E 4.5.12

Escribir las siguientes fórmulas en notación

(i) prefija y post-fija. Hallar el árbol binario asociado.

(a) $x + (((y + z) \cdot t) \cdot z)$,

(b) $((((p \vee q) \wedge r) \rightarrow s) \downarrow p) \wedge \sim q$,

(c) $(((\sim (p \wedge q)) \rightarrow r) \wedge (r \vee q)) \rightarrow s$.

(ii) infija.

(a) $\cdot\ + \cdot\ 2\ x\ y\ t$,

(b) $\rightarrow\ \wedge\ \rightarrow \rightarrow\ p\ q\ \sim \sim\ r\ \sim\ s\ \downarrow\ t\ r$,

(c) $x\ y\ \cdot\ z\ t\ \cdot\ + x\ y\ +\ \cdot$,

(d) $p\ q\ r \wedge \downarrow\ s\ \wedge\ p\ q \wedge\ \sim\ r \wedge\ \rightarrow$.

E 4.5.13

Existen cuatro tipos básicos de sangre: A, B, AB y O. El tipo O puede donar a cualquiera de los cuatros tipos, A y B pueden donar a AB, lo mismo que a su propio tipo, pero el tipo AB sólo puede donar a AB. Dibujar un digrafo que represente esta situación.

E 4.5.14

Dado el multidigrafo $\vec{G} = (V, A, \varphi)$, donde $V = \{1, 2, 3, 4, 5\}$, $A = \{a, b, c, d, e, f, g, h, i, j\}$ y φ está dada por la tabla

x	a	b	c	d	e	f	g	h	i	j
$\varphi(x)$	$(1,2)$	$(2,3)$	$(2,5)$	$(4,2)$	$(1,3)$	$(5,1)$	$(4,5)$	$(5,3)$	$(1,4)$	$(3,4)$

a) hacer el diagrama asociado a $\vec{G}$. ¿Es $\vec{G}$ digrafo?.

b) hallar $gr^+(1)$ y $gr^-(4)$,

c) hallar dos caminos que no repitan vértices desde el vértice 3 hasta el 2,

d) hallar un camino que repita vértices desde el vértice 1 hasta el 2,

e) hallar el multigrafo soporte,

f) ¿es $\vec{G}$ fuertemente conexo?,

g) hallar el subdigrafo inducido por el conjunto de vértices $\{1, 3, 4, 5\}$.

E 4.5.15

Sean u y v dos vértices distintos de un multidigrafo $\vec{G}$. Si existe un camino en $\vec{G}$ desde u hasta v, probar que existe un camino desde u hasta v que no repite vértices.

E 4.5.16

Sea $\vec{G}$ un multidigrafo finito. Si $\vec{G}$ no contiene circuitos, probar que existe al menos un vértice v tal que $gr^+(v) = 0$.

E 4.5.17

Hallar la matriz de precedencia y la lista de precedencia para los multidigrafos de los ejercicios 4.5.13 y 4.5.14.

5 Relaciones binarias especiales

5.1 Relaciones binarias entre los elementos de un conjunto

D 5.1.1 *Llamaremos relación binaria entre los elementos de A, a cualquier subconjunto de $A \times A$.*

Al conjunto de todas las relaciones binarias entre los elementos de A, lo representaremos con el símbolo $Rel(A)$.

Es claro que se verifica que

$$Rel(A) = \{B : B \subseteq A \times A\} = \mathcal{P}(A \times A).$$

En toda esta sección, cuando no digamos lo contrario, las relaciones consideradas serán entre los elementos de un conjunto.

Relaciones con ciertas propiedades particulares

D 5.1.2 *Sea $R \in Rel(A)$. Diremos que R es*

(i) *reflexiva si:* $(a,a) \in R$, *para todo* $a \in A$, $[aRa]$

(ii) *simétrica si:* $(x,y) \in R \Rightarrow (y,x) \in R$, $[xRy \Rightarrow yRx]$

(iii) *antisimétrica si:* $(x,y) \in R, (y,x) \in R \Rightarrow x = y$, $[xRy, yRx \Rightarrow x = y]$

(iv) *transitiva si:* $(x,y),(y,z) \in R \Rightarrow (x,z) \in R$. $[xRy, yRz \Rightarrow xRz]$

Nota. Otra forma de definir la propiedad antisimétrica es: si $(x,y) \in R$ y $x \neq y$, entonces $(y,x) \notin R$.

Ejemplos

Consideremos el conjunto $A = \{a,b,c,d,e\}$ y las relaciones binarias

$$R_1 = \{(a,b),(b,c),(a,c)\},$$

$$R_2 = \{(a,a),(b,b),(c,c),(d,d),(e,e)\},$$

$$R_3 = R_2 \cup \{(a,b),(b,a)\}.$$

Entonces

R_1: no es reflexiva, $[(a,a) \notin R_1]$

no es simétrica $[(a,b) \in R_1 \text{ y } (b,a) \notin R_1]$

es transitiva y antisimétrica.

R_2: es reflexiva, simétrica, transitiva y antisimétrica.

R_3: es reflexiva, simétrica y transitiva,

no es antisimétrica. $[(a,b),(b,a) \in R_3 \text{ y } a \neq b]$

Nota. La relación R_2 del ejemplo muestra que una relación puede ser simétrica y antisimétrica a la vez.

Relaciones especiales

Para todo conjunto $X \neq \emptyset$, $Rel(X)$ siempre contiene tres elementos muy importantes:

(i) la relación vacía: $\emptyset \in Rel(X)$, $[\emptyset \subseteq X^2]$

(ii) la relación identidad: $I_X = \{(x,x) : x \in X\}$,

(iii) la relación plena: $\tau_X = X^2$. $[X^2 \subseteq X^2]$

5.2 Digrafos y relaciones binarias

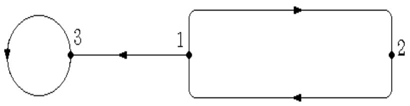
Relación binaria asociada a un digrafo

Dado un digrafo $\overrightarrow{G}$, podemos considerar la relación binaria $R(\overrightarrow{G})$ sobre el conjunto V de vértices de $\overrightarrow{G}$ definida del siguiente modo:

$$R(\overrightarrow{G}) = \{(x,y) : \text{ existe un arco con origen } x \text{ y extremo } y\}.$$

Ejemplo

Sea $\overrightarrow{G}$ el digrafo indicado en la figura



entonces $R(\overrightarrow{G}) = \{(1,2),(1,3),(2,1),(3,3)\}$.

Digrafo asociado a una relación binaria

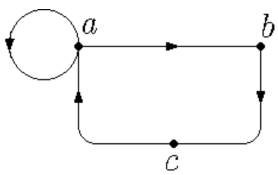
A toda $R \in Rel(X)$, $R \neq \emptyset$ podemos asociarle un digrafo $\overrightarrow{G}(R)$ del siguiente modo:

(i) el conjunto V de vértices de $\overrightarrow{G}$ es X,

(ii) si $(x,y) \in R$, entonces hay un arco con origen x y extremo y.

Ejemplo

Sean $X = \{a,b,c\}$ y $R = \{(a,a),(a,b),(b,c),(c,a)\}$, entonces
$V = \{a,b,c\}$ y $\overrightarrow{G}(R)$ es el indicado en la figura siguiente

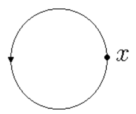


Nota. La correspondencia que a cada $R \in Rel(X)$, $R \neq \emptyset$ le asigna el digrafo $R(\overrightarrow{G})$, establece una biyección entre el conjunto de relaciones no vacías sobre el conjunto X y el conjunto de digrafos que tienen como conjunto de vértices al conjunto X.

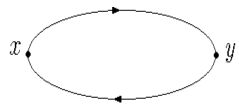
Determinación de propiedades de una relación por medio de su digrafo asociado

Sean $R \in Rel(X)$ y $\overrightarrow{G}(R)$ su digrafo asociado, entonces R es

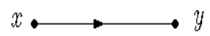
(i) reflexiva: si en cada vértice hay un bucle.



(ii) simétrica: si para cada arco existe su opuesto.



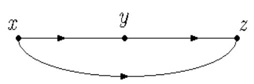
(iii) antisimétrica: si para cada par de vértices x, y, $x \neq y$ se verifica una y sólo una de las siguientes condiciones:



o

o

(iv) transitiva: si toda vez que existen los arcos $\overrightarrow{xy}$, $\overrightarrow{yz}$, también existe el arco $\overrightarrow{xz}$.



5.3 $P-$clausura de una relación binaria

D 5.3.1 *Si $R \in Rel(X)$ y P es una propiedad (por ejemplo la propiedad transitiva), llamaremos $P-$clausura de R, y la indicaremos con R^P, a la relación binaria sobre X que tiene las siguientes propiedades:*

(P1) $R \subseteq R^P$,

(P2) R^P *tiene la propiedad* P,

(P3) *si* $R^* \in Rel(X)$ *verifica:*

(i) $R \subseteq R^*$,

(ii) R^* *tiene la propiedad* P,

entonces $R^P \subseteq R^*$.

Observaciones

(i) R^P es la menor relación que contiene a R verificando la propiedad P.

(ii) Dada $R \in Rel(X)$ y una propiedad P, no siempre existe la $P-$clausura de R. En efecto, si $R = \{(a, b), (b, a)\}$, entonces es claro que no existe la clausura antisimétrica de R.

Propiedades útiles para la determinación de las P−clausuras

Vamos a ver ahora un resultado que nos será de utilidad para determinar las clausuras reflexiva, simétrica y transitiva de una relación.

T 5.3.1 *Sea* $R \in Rel(X)$, *entonces*

(i) *las siguientes condiciones son equivalentes:*

(i.1) R *es reflexiva,*

(i.2) $I_X \subseteq R$.

(ii) *las siguientes condiciones son equivalentes:*

(ii.1) R *es simétrica,*

(ii.2) $R^{op} = R$.

(iii) *las siguientes condiciones son equivalentes:*

(iii.1) R *es transitiva,*

(iii.2) $R^2 \subseteq R$, *donde* $R^2 = R \circ R$.

Dem.

(i) La demostración es trivial.

(ii) (ii.1) $\Longrightarrow$ (ii.2):

(1) $(x, y) \in R \Leftrightarrow$ [ii.1)]

$(y, x) \in R \Leftrightarrow$ [definición de R^{op}]

$(x, y) \in R^{op}$,

(2) $R = R^{op}$. [(1)]

(ii.2) $\Longrightarrow$ (ii.1):

Sea

(1) $(x, y) \in R$, [hipótesis]

entonces

(2) $(x, y) \in R^{op}$, [(1) y (ii.2)]

(3) $(y, x) \in R$, [definición de R^{op}]

(4) R es simétrica. [(1) y (3)]

(iii) (iii.1) $\Longrightarrow$ (iii.2):

Sea

(1) $(x, y) \in R^2$, [hipótesis]

entonces existe $z \in X$ tal que

(2) $(x, z) \in R$, [(1)]

(3) $(z, y) \in R$. [(1)]

Luego,

(4) $(x, y) \in R$, [(2), (3) y (iii.1)]

(5) $R^2 \subseteq R$. [(1) y (4)]

(iii.2) $\Rightarrow$ (iii.1):

Sean

(1) $(x, y) \in R$, [hipótesis]

(2) $(y, z) \in R$, [hipótesis]

entonces

(3) $(x, z) \in R \circ R = R^2$, [(1), (2) y definición de composición]

(4) $(x, z) \in R$. [(3) y (iii.2)] ■

Determinación de las $P-$clausuras de una relación por medio de su digrafo asociado

A veces para determinar la $P-$clausura de una relación R es útil emplear el digrafo $\overrightarrow{G}(R)$, asociado a R. En efecto, si R^P es la clausura

reflexiva: cada vértice debe tener un bucle,

simétrica: para cada arco de $\overrightarrow{G}(R^P)$ debe estar su opuesto,

transitiva: para cada par de arcos $\overrightarrow{ac}$ y $\overrightarrow{cb}$ de $\overrightarrow{G}(R^P)$, debe estar el arco $\overrightarrow{ab}$.

Dada $R \in Rel(X)$, indicaremos con R^{RF}, R^{SIM}, R^{TR} las clausuras reflexiva, simétrica y transitiva de R, respectivamente.

Ejemplo

Sea $X = \{a, b, c, d\}$ y $R = \{(a, a), (b, c), (b, d), (c, b), (c, a)\}$.

Para determinar la clausura reflexiva, incorporamos a R los pares (x, x) que le faltan para que contenga a I_X. Luego,

$$R^{RF} = R \cup \{(b, b), (c, c), (d, d)\}.$$

Para determinar la clausura simétrica, incorporamos a R los pares (x, y) que le faltan cuando (y, x) está en R. Luego,

$$R^{SIM} = R \cup \{(d, b), (a, c)\}.$$

Para determinar la clausura transitiva, incorporamos los pares (x, z) que le faltan a R cuando los pares (x, y), (y, z) están en R

$$(b, c), (c, b) \in R \Rightarrow (b, b) \in R,$$

$$(b, c), (c, a) \in R \Rightarrow (b, a) \in R,$$

$$(c, b), (b, c) \in R \Rightarrow (c, c) \in R,$$

$$(c, b), (b, d) \in R \Rightarrow (c, d) \in R,$$

$$R^{TR} = R \cup \{(b, b), (c, c), (b, a), (c, d)\}.$$

5.4 Clausuras: reflexiva, simétrica, transitiva

Las clausuras anteriores se pueden determinar del siguiente modo:

T 5.4.1 *Si $R \in Rel(X)$, entonces se verifican*

(i) $R^{RF} = R \cup I_X$,

(ii) $R^{SIM} = R \cup R^{op}$,

(iii) $R^{TR} = \{(x, y) \in X^2 :$ existe un camino de longitud finita del vértice x al vértice y en $\overrightarrow{G}(R)\}$.

Dem. Solamente probaremos (iii).
Sea $B = \{(x, y) \in X^2 :$ existe un camino de longitud finita del vértice x al vértice y en $\overrightarrow{G}(R)\}$, entonces se verifican

(P1) $R \subseteq B$: Sea $(x, y) \in R$, entonces en $\overrightarrow{G}(R)$ existe un camino de longitud uno que une el vértice x con el vértice y. Luego, $(x, y) \in B$.

(P2) B es transitiva:

Sean

(1) $(u, v) \in B$,

(2) $(v, w) \in B$,

entonces en $\overrightarrow{G}(R)$

(3) existe un camino de longitud l_1 del vértice u al v, [(1)]

(4) existe un camino de longitud l_2 del vértice v al w, [(2)]

(5) existe un camino de longitud finita del vértice u al w, [(3) y (4)]

(6) $(u, w) \in B$. [(5) y definición de B]

(P3) Si $R \subseteq R^*$ y R^* es transitiva, entonces $B \subseteq R^*$:

Supongamos que

(1) $R \subseteq R^*$,

(2) R^* es transitiva,

y sea

(3) $(u, v) \in B$,

entonces

(4) $(u, w_1) \in R, (w_1, w_2) \in R, \ldots, (w_{n-1}, w_n) \in R, (w_n, v) \in R$ [(3) y definición de B]

(5) $(u, w_1) \in R^*, (w_1, w_2) \in R^*, \ldots, (w_{n-1}, w_n) \in R^*, (w_n, v) \in R^*$ [(4) y (1)]

(6) $(u, v) \in R^*$, [(5) y (2)]

(7) $B \subseteq R^*$. [(3) y (6)] ■

5.5 Relaciones de equivalencia

D 5.5.1 *Sea $R \in Rel(X)$, $R \neq \emptyset$. Diremos que R es una relación de equivalencia si es reflexiva, simétrica y transitiva. Esto es, si R verifica:*

(E1) $(x, x) \in R$ *para todo* $x \in X$,

(E2) $(x, y) \in R \Rightarrow (y, x) \in R$,

(E3) $(x, y) \in R, (y, z) \in R \Rightarrow (x, z) \in R$.

Notaciones

(i) Denotaremos con $Ref(X)$, $Sim(X)$, $Tran(X)$ y $EQ(X)$ al conjunto de todas las relaciones reflexivas, simétricas, transitivas y de equivalencia definidas sobre un conjunto X respectivamente.

(ii) Es habitual representar a una relación de equivalencia con alguno de los símbolos $\sim$, $\simeq$, $\equiv$.

Entonces si (x, y) pertenece a la relación se escribe $x \sim y$, $x \simeq y$, ó $x \equiv y$ y se lee x *e* y *son equivalentes.*

Ejemplo

Dado un conjunto A, no vacío, las relaciones

$$I_A = \{(x, x) : x \in A\} \quad \text{y} \quad \tau_A = A^2,$$

llamadas las relaciones triviales, son de equivalencia.

5.6 Relación de equivalencia asociada a una función

D 5.6.1 *Sea $f : X \longrightarrow Y$ una función arbitraria. Llamaremos relación asociada con f a la relación*

$$R_f = \{(a, b) \in X \times X : f(a) = f(b)\}.$$

Es fácil ver que $R_f \in EQ(X)$.

Ejemplo

Si $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4\}$ y $f : X \longrightarrow Y$ es la función indicada en la siguiente tabla:

x	a	b	c	d
$f(x)$	1	2	2	1

entonces $R_f = I_X \cup \{(a, d), (d, a), (b, c), (c, b)\}$.

5.7 Relación de equivalencia asociada a una partición

D 5.7.1 *Una partición de un conjunto X no vacío, es una familia $\mathcal{F}$ de subconjuntos de X con las siguientes propiedades:*

(Pa1) *si $A \in \mathcal{F}$, entonces $A \neq \emptyset$,*

(Pa2) *si $A, B \in \mathcal{F}$ y $A \cap B \neq \emptyset$, entonces $A = B$,*

(Pa3) $\bigcup\limits_{A \in \mathcal{F}} A = X$.

A los elementos de $\mathcal{F}$ los llamaremos $\mathcal{F}$–conjuntos.

Nota. La condición Pa2 es equivalente a la siguiente: si $A, B \in \mathcal{F}$ y $A \neq B$, entonces $A \cap B = \emptyset$.

Al conjunto de todas las particiones de un conjunto X lo representaremos con $Part(X)$.

D 5.7.2 *Sea X un conjunto no vacío y $\mathcal{F} \in Part(X)$. Llamaremos relación asociada con $\mathcal{F}$ a la relación*

$$R_{\mathcal{F}} = \{(x, y) \in X \times X : \text{ existe } A \in \mathcal{F} \text{ tal que } x, y \in A\}.$$

Es decir, $(x, y) \in R_{\mathcal{F}}$ si, y sólo si, x e y pertenecen al mismo $\mathcal{F}$–conjunto.

T 5.7.1 *Si $\mathcal{F} \in Part(X)$, entonces $R_{\mathcal{F}} \in EQ(X)$.*

Dem.

(E1) $R_{\mathcal{F}}$ es reflexiva:

(1) Sea $x \in X$, [hipótesis]

(2) $X = \bigcup\limits_{A \in \mathcal{F}} A$, [$\mathcal{F} \in Part(X)$]

(3) existe $B \in \mathcal{F}$ tal que $x \in B$, [(1),(2)]

(4) $(x, x) \in R_{\mathcal{F}}$. [(3)]

(E2) $R_{\mathcal{F}}$ es simétrica: Inmediata.

(E3) $R_{\mathcal{F}}$ es transitiva:

Sean

(1) $(x, y) \in R_{\mathcal{F}}$, [hipótesis]

(2) $(y, z) \in R_{\mathcal{F}}$, [hipótesis]

entonces,

(3) existe $A \in \mathcal{F}$ tal que $x, y \in A$, [(1)]

(4) existe $B \in \mathcal{F}$ tal que $y, z \in B$, [(2)]

(5) $y \in A \cap B$, [(3),(4)]

(6) $A \cap B \neq \emptyset$, [(5)]

(7) $A = B$, [Pa2]

(8) existe $A \in \mathcal{F}$ tal que $x, z \in A$, [(3),(4),(7)]

(9) $(x, z) \in R_{\mathcal{F}}$. [(8)] ■

Ejemplo

Si $X = \{a, b, c, d, e, f\}$ y $\mathcal{F} = \{\{a, d\}, \{c\}, \{b, e, f\}\}$, entonces

$$R_{\mathcal{F}} = I_X \cup \{(a, d), (d, a), (b, e), (e, b), (b, f), (f, b), (e, f), (f, e)\}.$$

5.8 Clases de equivalencia y conjunto cociente

Clases de equivalencia

D 5.8.1 *Sea $R \in EQ(X)$ y $x \in X$. Llamaremos R–clase (o simplemente clase) de equivalencia que contiene a x al conjunto $R(x) = \{y \in X : (x, y) \in R\}$.*

También usaremos las notaciones x_R, $\overline{x}$ o $|x|$, para designar a la clase de equivalencia que contiene a x. En general, las dos últimas se emplean cuando la relación R es una relación de equivalencia fija.

Propiedades de las clases de equivalencia

T 5.8.1 *Si $R \in EQ(X)$, entonces se verifican las siguientes propiedades:*

(C1) $x \in x_R$, *cualquiera sea* $x \in X$,

(C2) *las siguientes condiciones son equivalentes:*

(a) $(x, y) \in R$,

(b) $x_R = y_R$.

Dem.

(C1) La demostración es inmediata ya que $x_R = \{u \in X : (u, x) \in R\}$ y $(x, x) \in R$.

(C2) (a) $\Longrightarrow$ (b):

(i) $x_R \subseteq y_R$:

Sean

(1) $(x, y) \in R$, [hipótesis]

(2) $u \in x_R$, [hipótesis]

entonces

(3) $(u, x) \in R$, [(2)]

(4) $(u, y) \in R$, [(3),(1)]

(5) $u \in y_R$, [(4)]

(6) $x_R \subseteq y_R$. [(2),(5)]

(ii) $y_R \subseteq x_R$: se demuestra en forma análoga a (i).

De (i) y (ii) resulta $x_R = y_R$.

(b) $\Longrightarrow$ (a):

(1) $x_R = y_R$, [hipótesis]

(2) $y \in x_R$, [(C1),(1)]

(3) $(x, y) \in R$. [(2)] ■

Nota. Si C es la clase de equivalencia que contiene a x, esto es si $C = x_R$, entonces diremos que x es un representante de la clase C.

Conjunto cociente

D 5.8.2 *Sea $R \in EQ(A)$. Denominaremos conjunto cociente de A por R y lo denotaremos con A/R, al conjunto de todas las clases de equivalencia de A determinadas por R.*

Es usual emplear la notación $A/R = \{x_R\}_{x \in A}$.

Nosotros también la usaremos, aunque tiene defectos, pues sugiere que A puede ser utilizado como conjunto de índices para A/R, lo cual en general no es cierto, como lo muestra el siguiente ejemplo:

Si $A = \{a, b, c\}$ y $R = I_A \cup \{(a, b), (b, a)\}$, entonces $a_R = \{a, b\}$, $c_R = \{c\}$ y $A/R = \{a_R, c_R\}$.

En cambio, $\{x_R\}_{x \in A} = \{a_R, b_R, c_R\}$ y es claro que $A/R \neq \{x_R\}_{x \in A}$.

Ejemplos

(i) Sean A un conjunto no vacío arbitrario y $R = I_A = \{(x, x) : x \in A\}$. Entonces $x_R = \{x\}$ y $A/R = \{\{x\} : x \in A\}$.

(ii) Sea $A = \{a, b, c, d, e, g\}$, $B = \{1, 2, 3\}$ y $f : A \longrightarrow B$ la función indicada en la siguiente tabla:

x	a	b	c	d	e	g
$f(x)$	1	1	2	2	2	3

Si consideramos la relación R_f, entonces:

$a_{R_f} = \{x \in A : (x, a) \in R_f\} = \{x \in A : f(x) = f(a)\} = \{a, b\}$,

$c_{R_f} = \{c, d, e\}$,

$g_{R_f} = \{g\}$.

Luego $A/R_f = \{a_{R_f}, c_{R_f}, g_{R_f}\} = \{\{a, b\}, \{c, d, e\}, \{g\}\}$.

5.9 Partición asociada a una relación de equivalencia

T 5.9.1 *Sea X un conjunto no vacío y $R \in EQ(X)$. Entonces el conjunto cociente X/R es una partición de X.*

Dem.

(Pa1) $x_R \neq \emptyset$ para todo $x_R \in X/R$, [$x \in x_R$]

(Pa2) $x_R \cap y_R \neq \emptyset \Rightarrow x_R = y_R$:

Sean

(1) $x_R, y_R \in X/R$ tales que $x_R \cap y_R \neq \emptyset$, [hipótesis]

entonces,

(2) $c \in x_R \cap y_R$, [(1)]

(3) $(x, c) \in R$, [(2)]

(4) $(c, y) \in R$, [(2)]

(5) $(x, y) \in R$, [(3),(4)]

(6) $x_R = y_R$. [(5),(C2)]

(Pa3) $\bigcup\limits_{x \in X} x_R = X$:

(i) $\bigcup\limits_{x \in X} x_R \subseteq X$:

(1) $x_R = \{u \in X : (u, x) \in R\}$,

(2) $x_R \subseteq X$, [(1)]

(3) $\bigcup\limits_{x \in X} x_R \subseteq X$. [(2)]

(ii) $X \subseteq \bigcup\limits_{x \in X} x_R$:

Sea

(1) $z \in X$, [hipótesis]

(2) $z \in z_R$, [(C1)]

(3) $z \in \bigcup\limits_{x \in X} x_R$, [(2)]

(4) $X \subseteq \bigcup\limits_{x \in X} x_R$, [(1),(3)]

De (i) y (ii) resulta Pa3. ■

Las nociones de partición y relación de equivalencia sobre un conjunto están conectadas de la siguiente manera:

T 5.9.2 *Sea A un conjunto dado, entonces se verifican:*

(i) *Si $R \in EQ(A)$, existe $\mathcal{F} \in Part(A)$ tal que $R_{\mathcal{F}} = R$.*

(ii) *Si $\mathcal{F} \in Part(A)$, existe $R \in EQ(A)$ tal que $\mathcal{F} = A/R$.*

De T 5.9.2 resulta que para hallar las relaciones de equivalencia sobre un conjunto A basta hallar las particiones de A y recíprocamente.

El número p_n de particiones de un conjunto con n elementos puede calcularse por medio de la fórmula recursiva:

(i) $p_0 = 1$,

(ii) $p_n = \sum\limits_{j=1}^{n} \binom{n-1}{j-1} p_{n-j}$.

5.10 Funciones canónicas

D 5.10.1 *Sea A un conjunto no vacío y $R \in EQ(A)$. La función $q_R : A \longrightarrow A/R$ definida por $q_R(x) = x_R$ (o $q(x) = x_R$) se denomina aplicación canónica asociada con R.*

Observemos que q_R es una función pues cada $x \in A$ pertenece a una y sólo una clase de equivalencia. Por otra parte, es claro que q_R es sobreyectiva.

El siguiente resultado expresa la conexión existente entre las nociones de función y relación de equivalencia.

T 5.10.1 (teorema del triángulo) *Sean $f : A \longrightarrow B$ una función arbitraria, $R = R_f$ la relación de equivalencia asociada a f y $q_R : A \longrightarrow A/R$ la aplicación canónica asociada con R. Entonces existe una única función $f^* : A/R \longrightarrow B$ tal que $f^* \circ q_R = f$.*

Además se verifican:

(i) f^* *es inyectiva,*

(ii) f^* *es sobreyectiva si, y sólo si, f lo es.*

$$\begin{tikzcd}
A \arrow[r, "f = f^* \circ q_R"] \arrow[d, "q_R"'] & B \\
A/R \arrow[ur, "f^*"'] &
\end{tikzcd}$$

Dem. Sea $f^* = \{(C, f(x)) : C \in A/R, x \in C\}$, entonces

(a) f^* es funcional:

Sean

(1) $(C, f(x)), (C, f(y)) \in f^*$, con $x, y \in C$, [hipótesis]

entonces,

(2) $(x, y) \in R$, [(1)]

(3) $f(x) = f(y)$. [(2) y def. de R]

(b) $f^* \circ q_R = f$:

$$\begin{aligned}
(f^* \circ q_R)(x) &= f^*(q_R(x)) \\
&= f^*(\overline{x}) \\
&= f(x).
\end{aligned}$$

(c) f^* es la única función tal que $f^* \circ q = f$:

En efecto, sea

$g : A/R \longrightarrow$ B tal que $g \circ q = f$,

entonces dado $a_R \in A/R$ se verifica

$g(a_R) = g(q(a))$

$= f(a)$ $[g \circ q = f]$

$= f^*(q(a))$ $[f^* \circ q = f]$

$= f^*(a_R).$

Luego, $g = f^*$.

Además,

(i) f es inyectiva:

Sean

(1) $(C, f(x)), (D, f(x)) \in f^*$,

entonces,

(2) $x \in C$ y $x \in D$, [de (1)]

(3) $C \cap D \neq \emptyset$, [de (2)]

(1) $C = D$. [de (3)]

(ii) f^* es sobreyectiva si, y sólo si, f lo es: la demostración queda como ejercicio. ■

5.11 Relaciones de orden

D 5.11.1 *Sea $R \in Rel(X)$, $R \neq \emptyset$. Diremos que R es una relación de:*

(i) *pre – orden: si es reflexiva y transitiva,*

(ii) *orden: si es reflexiva, antisimétrica y transitiva.*

Nota. Las relaciones de orden (de equivalencia) son las relaciones de pre – orden que verifican la propiedad antisimétrica (simétrica).

Conjuntos ordenados

D 5.11.2 *Llamaremos conjunto ordenado (c.o.) a todo par (A, R) formado por un conjunto no vacío A y una relación R de orden definida sobre A. También diremos que A es el soporte del c.o. (A, R).*

Ejemplo

El par (A, R), donde $A = \{a, b, c\}$ y $R = \{(a, a), (b, b), (c, c), (a, c), (b, c)\}$ es un c.o..

Notaciones

(i) A veces para simplificar, representaremos al c.o. por medio de su conjunto soporte y diremos, *sea A un c.o.*.

(ii) Habitualmente designaremos a las relaciones de orden con el símbolo $\leq$ ó $\prec$.

(iii) Sea $\mathcal{A} = (A, \leq)$ un c.o.. De acuerdo a una convención ya fijada escribiremos $a \leq b$ para indicar que se verifica $(a, b) \in \leq$.

Si $a \leq b$ diremos que, *a precede a b*, o que *a es menor o igual que b.*

(iv) Si $\mathcal{A} = (A, \leq)$ es un c.o., representaremos con $\geq$ a la relación opuesta de $\leq$, y diremos que $\mathcal{A}^* = (A, \geq)$ es el c.o. dual de $\mathcal{A}$.

Es claro que $a \geq b$ si, y sólo si, $b \leq a$.

Si $x \geq y$, diremos que *x sucede a y* o que x es *mayor o igual que y.*

(v) Escribiremos $a_1 \leq a_2 \leq \ldots \leq a_{n-1} \leq a_n$ para indicar que se verifican

$a_1 \leq a_2$, $a_2 \leq a_3$, $\ldots$, $a_{n-1} \leq a_n$.

Ejemplo

Consideremos el c.o. $(A, \leq)$, donde

$A = \{1, 2, 3, 4\}$,

$\leq = \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$.

Entonces podemos escribir

$1 \leq 1$, $1 \leq 2$, $1 \leq 3$, $1 \leq 4$,

$2 \leq 2$, $2 \leq 3$, $2 \leq 4$,

$3 \leq 3$, $3 \leq 4$,

$4 \leq 4$.

La relación de orden estricto determinada por una relación de orden

D 5.11.3 *Sean* $(A, \leq)$ *un c.o. y* $a, b \in A$. *Escribiremos* $a < b$ *si* $a \leq b$ *y* $a \neq b$.

La fórmula $a < b$ se lee, a precede estrictamente a b ó b sigue estrictamente a a.

Escribiremos $a_1 < a_2 < \ldots < a_{n-1} < a_n$ para indicar que $a_1 < a_2$, $a_2 < a_3$,..., $a_{n-1} < a_n$.

Nota. La relación $<$ asociada a una relación de orden $\leq$ es transitiva y además verifica la propiedad $a \not< a$, para todo $a \in A$.

Entonces $<$ nunca es una relación de orden. Sin embargo, algunos autores dicen que es una relación de orden estricto, lo cual nos parece inapropiado por la razón expuesta.

5.12 Diagrama de Hasse de un conjunto ordenado finito

D 5.12.1 *Sea* $(A, \leq)$ *un conjunto ordenado y* $m, n \in A$. *Diremos que* n *cubre a* m*, o que* n *es un sucesor inmediato de* m*, si* $m < n$ *y no existe otro elemento* p *tal que* $m < p < n$.

Diagrama de Hasse de un c.o. finito

El diagrama de Hasse de un conjunto ordenado $(A, \leq)$, donde A es un conjunto finito, se construirá mediante el siguiente procedimiento:

Paso 1

Los elementos de A serán representados en el plano (una hoja de papel, el pizarrón, etc.) por medio de una señal (un punto, una pequeña circunferencia, etc.), dicha señal se denominará *el afijo* del elemento.

Paso 2

Si $a < b$ el afijo de b se dibuja por encima del afijo de a (en algunos casos especiales a esta regla no se la tendrá en cuenta).

Paso 3

Si b cubre a a, uniremos el afijo de a y el de b con un segmento.

Ejemplos

Sea $(A, \leq)$ el siguiente c.o.:

(i) $A = \{a, b, c, d\}$, y

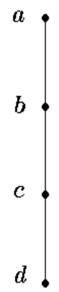
$a \leq a$, $a \leq b$, $a \leq c$, $a \leq d$,

$b \leq b$, $b \leq c$, $b \leq d$,

$c \leq c$, $c \leq d$,

$d \leq d$.

Entonces su diagrama de Hasse es



(ii) $A = \{a, b, c, d, e\}$ y

$$\leq = \{(a,a), (a,b), (b,b), (c,d), (d,d), (a,c), (c,c), (a,d), (a,e), (b,d), (d,e), (b,e), (e,e), (c,e)\}.$$

En general es conveniente escribir la relación $<$, y partir de ella detectar cuáles son los sucesores inmediatos de cada elemento. Entonces escribimos $<$ del siguiente modo:

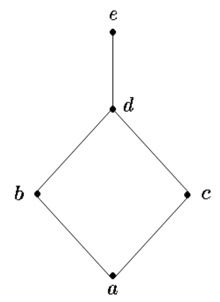
(a, b), (a, c), (a, d), (a, e), [b, c, d, e siguen a a]

(b, d), (b, e), [d, e siguen a b]

(c, d), (c, e), [d, e siguen a c]

(d, e). [e sigue a d]

Entonces su diagrama de Hasse es



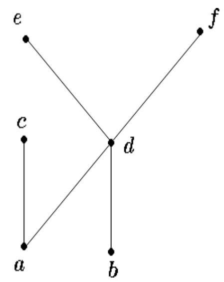
Uso del diagrama de Hasse

(i) En primer lugar observemos que si la relación R no es un orden, entonces no admite diagrama de Hasse.

(ii) A partir del diagrama de Hasse podemos recuperar el orden.

Ejemplo

Sea $(C, \leq)$ cuyo diagrama de Hasse es el indicado en la figura



entonces:

$a \leq a$, $a \leq c$, $a \leq d$, $a \leq e$, $a \leq f$,

$b \leq b$, $b \leq d$, $b \leq e$, $b \leq f$,

$c \leq c$,

$d \leq d$, $d \leq e$, $d \leq f$,

$e \leq e,$

$f \leq f.$

Conjuntos totalmente ordenados

D 5.12.2 *Sea $(A, \leq)$ un c.o.. Diremos que $\leq$ es un orden total y que $(A, \leq)$ es un conjunto totalmente ordenado, o cadena, si se verifica*

$$a, b \in A \text{ y } a \neq b \Rightarrow a \leq b \text{ ó } b \leq a.$$

Ejemplo

Sea $(A, \leq)$ el siguiente c.o.:

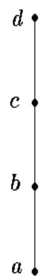
$A = \{a, b, c, d\},$

$\leq = I_A \cup \{(a, b), (a, c)(a, d), (b, c), (b, d)(c, d)\}.$

Entonces

$a < b < c < d,$

y $(A, \leq)$ es una cadena. Su diagrama de Hasse es:



Nota. Algunos autores llaman orden parcial a las relaciones que nosotros hemos llamado orden y orden a las que hemos llamado orden total.

5.13 Subconjuntos ordenados

D 5.13.1 *Sean* $(A, \leq)$ *un c.o. y* $B \subseteq A$. *Llamaremos orden sobre* B *inducido por* $\leq$ *a* $\leq_1 = (B \times B) \cap \leq$, *y diremos que* $(B, \leq_1)$ *es un subconjunto ordenado de* $(A, \leq)$.

Cuando no haya lugar a confusión, para simplificar la notación, escribiremos $(B, \leq)$ en lugar de $(B, \leq_1)$, aún cuando tengamos que $\leq \neq \leq_1$.

A veces simplificaremos más y diremos, *sea* B *el subconjunto ordenado del c.o.* A.

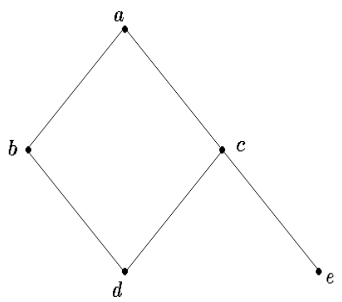
Ejemplo

Sean

$$A = \{a, b, c, d, e\},$$

$$\leq = I_A \cup \{(e,c), (d,c), (d,b), (d,a), (e,a), (b,a), (c,a)\}.$$

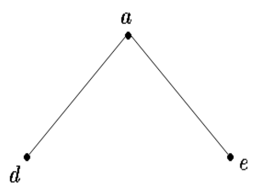
Entonces



Sea $B = \{d, a, e\} \subseteq A$. Luego,

$$B \times B = I_B \cup \{(d,a), (d,e), (a,d), (a,e), (e,d), (e,a)\},$$

$$\leq_1 = (B \times B) \cap \leq = I_B \cup \{(d,a), (e,a)\}.$$



5.14 Elementos especiales de un conjunto ordenado

Sea $(A, \leq)$ un conjunto ordenado. A continuación definiremos ciertos elementos especiales, los cuales pueden existir o no.

D 5.14.1 *Sea $m \in A$. Entonces m es:*

(i) *minimal si $x \leq m \Rightarrow x = m$,*

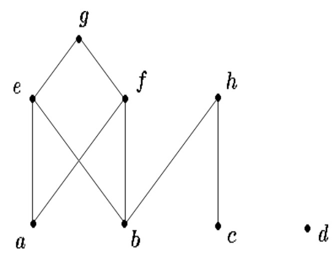
(ii) *maximal si $m \leq x \Rightarrow x = m$,*

(iii) *primer elemento si $m \leq x$ para todo $x \in A$,*

(iv) *último elemento si $x \leq m$ para todo $x \in A$.*

Ejemplo

Sea $(A, \leq)$ el c.o. cuyo diagrama de Hasse es el de la figura



Los conjuntos de los elementos minimales y elementos maximales de A son $A_{min} = \{a, b, c, d\}$ y $A_{max} = \{h, g, d\}$, respectivamente. A no tiene ni primer ni último elemento.

Notas.

(i) El ejemplo anterior muestra que existen c.o. que no tienen ni primer ni último elemento.

(ii) Si $x \in A$ es simultáneamente maximal y minimal, entonces en el diagrama de Hasse de A, x es un punto aislado.

Existencia de elementos minimales en un c.o. finito

T 5.14.1 *Si* $(A, \leq)$ *es un c.o. finito, entonces tiene elementos minimales.*

Dem.

(1) Sea $a_1 \in A$. Si a_1 es minimal, entonces $(A, \leq)$ tiene elementos minimales. En caso contrario vale (2).

(2) Existe $a_2 \in A$ tal que $a_2 < a_1$. Si a_2 es minimal, entonces $(A, \leq)$ tiene elementos minimales. En caso contrario vale (3).

(3) Existe $a_3 \in A$ tal que $a_3 < a_2$. Si a_3 es minimal, entonces ...

Como el conjunto ordenado A es finito, el proceso anterior debe parar en algún elemento a_n, el cual es minimal. ■

Notas.

(i) De manera totalmente análoga se demuestra que todo c.o. finito tiene elementos maximales.

(ii) Si un c.o. finito A tiene un único elemento minimal (maximal), entonces dicho elemento es el primer (último) elemento.

Existencia del diagrama de Hasse de un c.o. finito

T 5.14.2 *Todo c.o. finito admite diagrama de Hasse.*

Dem. La demostración la haremos por inducción sobre el número de elementos del c.o..

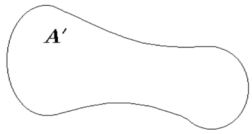
(i) Si A es un c.o. con un solo elemento, entonces A tiene diagrama de Hasse, el cual se reduce a un punto.

(ii) Supongamos que el enunciado vale para todo conjunto ordenado B tal que $|B| \leq n$. (hipótesis de inducción)

(iii) Sea A un conjunto ordenado tal que $|A| = n + 1$.

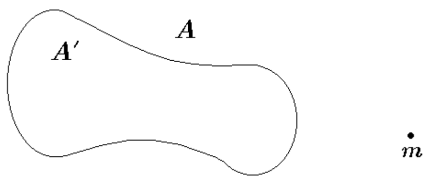
Como A es un c.o. finito, A tiene por lo menos un elemento minimal m.

Considerando el subconjunto ordenado $A' = A \setminus \{m\}$, tenemos que $|A'| = n$, luego de (ii) (la hipótesis de inducción) resulta que A' tiene diagrama de Hasse.

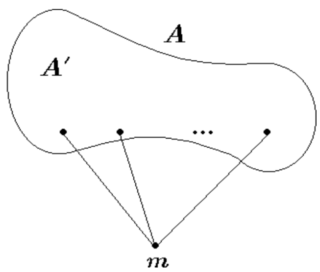


Sea C el conjunto de elementos de A' que cubren a m, entonces

(a) si $C = \emptyset$, el diagrama de Hasse de A es el de A' al que se le ha agregado el afijo de m, el cual es un punto aislado.



(b) si $C \neq \emptyset$, entonces el diagrama de Hasse de A es el de A' al que se le ha agregado el afijo de m y se ha unido el afijo de m con cada uno de los afijos de los elementos de C.



5.15 Cotas y conjuntos acotados

D 5.15.1 *Sean* $(A, \leq)$ *un c.o.,* $X \subseteq A$ *y* $c \in A$*. Diremos que:*

(i) c *es cota inferior de* X*, si* $c \leq x$ *para todo* $x \in X$*.*

(ii) X *es acotado inferiormente, si tiene cotas inferiores.*

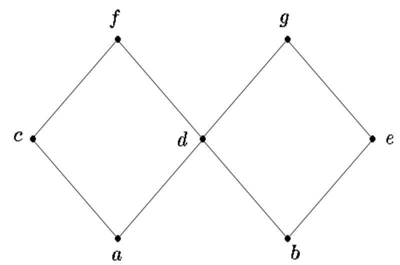
(iii) c *es cota superior de* X*, si* $x \leq c$ *para todo* $x \in X$*.*

(iv) X *es acotado superiormente si tiene cotas superiores.*

(v) X *es acotado, si tiene cotas inferiores y cotas superiores.*

Ejemplo

Sea $(A, \leq)$ el conjunto ordenado cuyo diagrama de Hasse es



entonces,

X	cotas inferiores de X	cotas superiores de X
$\{a, b\}$	—	d, f, g
$\{f\}$	a, b, c, d, f	f
$\{d, e\}$	b	g
$\{c, g\}$	a	—

El ejemplo anterior, muestra que:

(i) pueden existir o no cotas inferiores (superiores),

(ii) la cota inferior (superior), si existe, puede no ser única,

(iii) si existen cotas inferiores (superiores) de un conjunto X, éstas pueden pertenecer o no a X.

Infimo y supremo de un subconjunto ordenado

D 5.15.2 *Sean $(A, \leq)$ un c.o., $X \subseteq A$ y $a \in A$. Diremos que:*

(i) *a es el ínfimo de X si:*

(I1) *$a \leq x$ para todo $x \in X$,*

(I2) *la hipótesis, $z \in A$ es tal que $z \leq x$ para todo $x \in X$, implica que $z \leq a$.*

(ii) *a es el supremo de X si:*

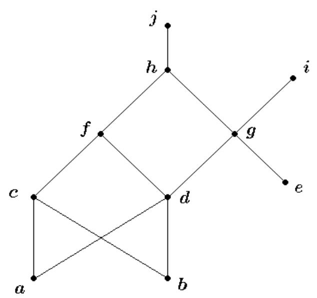
(S1) *$x \leq a$ para todo $x \in X$,*

(S2) *la hipótesis, $z \in A$ es tal que $x \leq z$ para todo $x \in X$, implica que $a \leq z$.*

Nota. La definición anterior indica que el ínfimo (supremo) de un conjunto X es la mayor (menor) de las cotas inferiores (superiores) de X.

Ejemplo

Sea $(A, \leq)$ el conjunto ordenado cuyo diagrama de Hasse es



entonces

X	$infX$	$supX$
$\{c, d\}$	—	f
$\{d, f, g, h, i\}$	d	—

El ejemplo anterior, muestra que el ínfimo (supremo) de un conjunto X puede existir o no y que, en caso de existir, puede pertenecer o no a X.
Nota. Observemos que el ínfimo (supremo) de un conjunto, si existe, es único.

5.16 Retículos

D 5.16.1 *Sea A un c.o.. Diremos que A es un:*

(i) *retículo inferior, si cualquier subconjunto de A con dos elementos tiene ínfimo,*

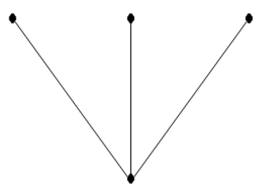
(ii) *retículo superior, si cualquier subconjunto de A con dos elementos tiene supremo,*

(iii) *retículo, si es simultáneamente retículo inferior y retículo superior.*

Nota. Observemos que si $(A, \leq)$ es un retículo inferior (superior), entonces $(A, \geq)$ es un retículo superior (inferior). Luego, si $(A, \leq)$ es un retículo, entonces $(A, \geq)$ también es un retículo.

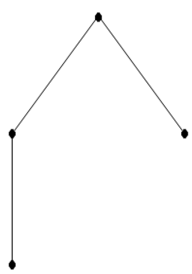
Ejemplos

(i)



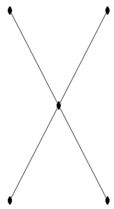
es retículo inferior,
no es retículo superior,
no es retículo,

(ii)



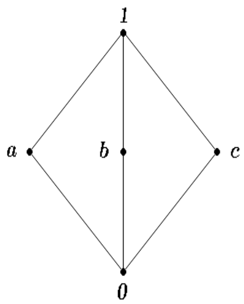
no es retículo inferior,
es retículo superior,
no es retículo,

(iii)



no es retículo inferior,
no es retículo superior,
no es retículo,

(iv)



es retículo inferior,
es retículo superior,
es retículo,

Retículos con primer elemento y retículos con último elemento

Observemos que existen retículos que no tienen primer elemento o último elemento.

Ejemplos

(i) $(\mathbb{N}, \leq)$ es un retículo con primer elemento y sin último elemento.

(ii) $(\mathbb{Z}, \leq)$ es un retículo sin primer y sin último elemento.

retículos inferiores finitos

T 5.16.1 *Todo retículo inferior finito tiene primer elemento.*

Dem. Sea $(A, \leq)$ un retículo inferior finito, entonces

(1) $(A, \leq)$ es un conjunto ordenado finito, [hipótesis]

(2) A tiene elementos minimales. [(1)]

Probemos ahora que A tiene un único minimal y que dicho minimal es primer elemento de A. Sean

(3) m_1 minimal de A, [hipótesis]

(4) m_2 minimal de A, [hipótesis]

entonces,

(5) existe $i = inf\ \{m_1, m_2\}$, [hipótesis inicial]

(6) $i \leq m_1$, [(5)]

(7) $i \leq m_2$, [(5)]

(8) $i = m_1$, [(6),(3)]

(9) $i = m_2$, [(7),(4)]

(10) $m_1 = m_2$. [(8),(9)]

Veamos que m_1 es primer elemento de A.
Sea $x \in A$, entonces:

(11) existe $a = inf\ \{m_1, x\}$,

(12) $a \leq m_1$, [(11)]

(13) $a \leq x$, [(11)]

(14) $a = m_1$, [(12),(3)]

(15) $m_1 \leq x$, [(13),(14)]

(16) m_1 es primer elemento. [(15)] ■

Nota. En forma análoga se demuestra que todo retículo superior finito tiene último elemento.

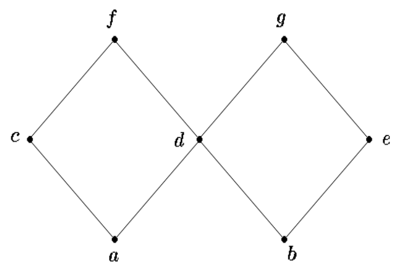
Retículos complementados

D 5.16.2 *Sea* $(A, \leq)$ *un retículo con primer elemento* 0 *y último elemento* 1. *Dado* $a \in A$, *diremos que* $b \in A$ *es un complemento de* a *si*

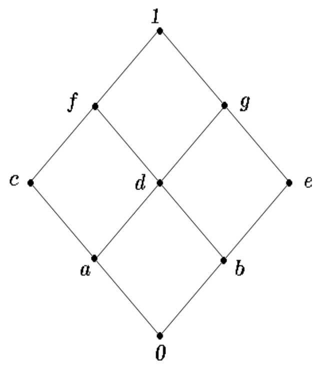
(i) $inf\ \{a, b\} = 0$,

(ii) $sup\ \{a, b\} = 1$.

Ejemplos



x	complementos de x
0	1
a	b, c
b	a, c
c	a, b
1	0



x	complementos de x
0	1
a	$-$
b	$-$
c	e
d	$-$
e	c
f	$-$
g	$-$
1	0

Los ejemplos anteriores muestran que:

(i) un elemento puede tener o no complementos,

(ii) el complemento de un elemento, si existe, puede no ser único.

D 5.16.3 *Sea* $(A, \leq)$ *un retículo con primer elemento* 0 *y último elemento* 1*. Diremos que* A *es complementado si todo elemento tiene complemento.*

5.17 Ejercicios

E 5.17.1

Indicar, en cada caso, si $R \in Rel(A)$ es reflexiva, simétrica, antisimétrica y/o transitiva

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

(i) $R = \{(1,1), (2,2), (3,3)\}$,

(ii) $R = \{(1,2), (2,1), (1,3), (2,2)\}$,

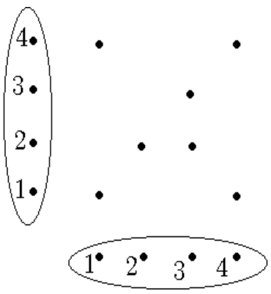
(iii) $R = A \times A$,

(iv) $R = \{(1,1), (2,2), (1,3), (1,2), (2,3), (3,3)\}$,

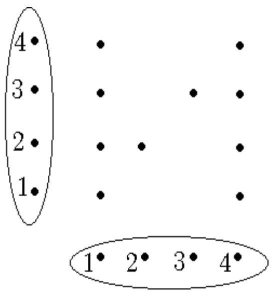
(v) $R = \emptyset$.

(b) $A = \{1, 2, 3, 4\}$

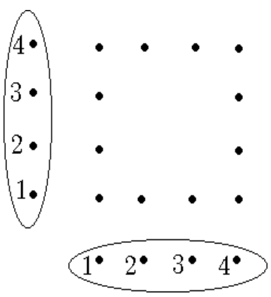
(i)



(ii)

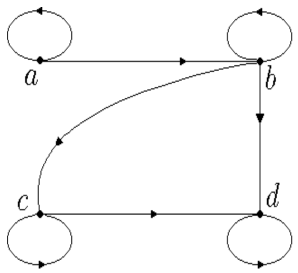


(iii)

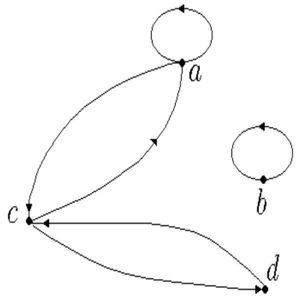


(c) $A = \{a, b, c, d\}$

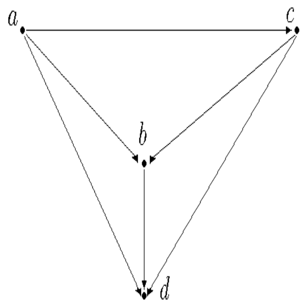
(i)



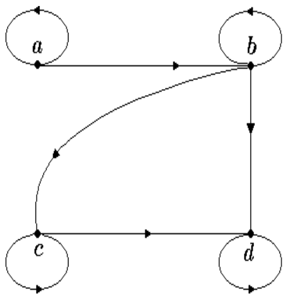
(ii)



(iii)



(iv)



(d) $A = \{a, b, c\}$

(i)

$$R = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

(ii)

$$R = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

(iii)

$$R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

(e) A es el conjunto de todas la rectas del plano,

$l_1 \, R \, l_2$ si, y sólo si, l_1 es perpendicular a l_2,

(f) $A = \mathbb{Z}$,

xRy si, y sólo si, $x - y$ es par,

(g) $A = \mathbb{Z}^2$,

$(a, b)R(c, d)$ si, y sólo si, $a \leq c$.

E 5.17.2

$R \in Rel(A)$ se dice circular si para todo $x, y, z \in A$, las hipótesis xRy e yRz implican zRx.
Probar que

(a) si $R \in Rel(A)$ es una relación simétrica, entonces las siguientes condiciones son equivalentes:

(i) R es transitiva,

(ii) R es circular.

(b) si $R \in Rel(A)$ es una relación circular y reflexiva, entonces es simétrica.

E 5.17.3

Sean $R_1, R_2 \in Rel(A)$. Averiguar si las siguientes afirmaciones son verdaderas o falsas, justificando las respuestas:

(a) si R_1 y R_2 son reflexivas, entonces $R_1 \cap R_2$ es reflexiva,

(b) si R_1 y R_2 son simétricas, entonces $R_1 \cap R_2$ es simétrica,

(c) si R_1 y R_2 son antisimétricas, entonces $R_1 \cup R_2$ es antisimétrica,

(d) si R_1 y R_2 son transitivas, entonces $R_1 \cup R_2$ es transitiva.

E 5.17.4

(a) Sean $R_1, R_2 \in Sim(X)$. Probar que

(i) $R_2 \circ R_1 \in Sim(X)$ si, y sólo si, $R_1 \circ R_2 = R_2 \circ R_1$,

(ii) si $R_2 \circ R_1 \subseteq R_1 \cup R_2$, entonces $R_1 \circ R_2 \subseteq R_1 \cup R_2$.

(b) Sean $R_1, R_2 \in Ref(X)$. Probar que $R_1 \cup R_2 \subseteq R_2 \circ R_1$.

(c) Sea $R_2 \in Ref(X)$. Probar que si $R_2 \circ R_1 \subseteq R_2$, entonces $R_1 \subseteq R_2$. ¿Es válida la recíproca?

E 5.17.5

Dada $R \in Rel(X)$, sean R^{RF} y R^{SIM} las clausuras reflexiva y simétrica de R, respectivamente. Probar que

(a) $R^{RF} = R \cup I_X$,

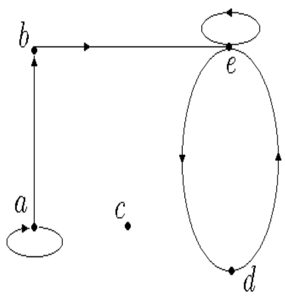
(b) $R^{SIM} = R \cup R^{op}$.

E 5.17.6

Sea $A = \{a, b, c, d, e\}$ y $R \in Rel(A)$. Hallar las clausuras reflexiva, simétrica y transitiva de R, siendo

(a) $R = \{(a, a), (c, b), (b, b), (a, c), (c, e), (c, c), (d, d), (e, e), (e, b), (c, a), (a, e)\}$,

(b)



E 5.17.7

Determinar si $R \in EQ(A)$, siendo

(a) $A = \mathbb{Z}$, xRy si, y sólo si, $x + y$ es un número impar,

(b) $A = \{1, 2, 3, 4\}$, $R = \{(1, 1), (2, 2), (1, 3), (3, 3), (2, 4), (4, 4), (4, 2), (3, 1)\}$,

(c) U un conjunto referencial dado y $C \subseteq U$ fijo.

$A = \mathcal{P}(U)$, DRB si, y sólo si, $D \cap C = B \cap C$,

(d) $A = \mathbb{Z}$, xRy si, y sólo si, $7/(x-y)$,

(e) $A = \{a, b, c, d\}$, y R la relación definida por la siguiente matriz

$$M(R) = \begin{array}{c c} & \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \end{array} & \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}.$$

(f) $A = \{x : x$ es estudiante del curso de Matemática Discreta$\}$,

xRy si, y sólo si, x se sienta en la misma fila que y,

(g) $A = \mathbb{R}^2$, $(a, b)R(c, d)$ si, y sólo si, $a^2 + b^2 = c^2 + d^2$,

(h) $A = \mathbb{R}^2$, $(x, y)R(z, t)$ si, y sólo si, $y^2 = t^2$.

E 5.17.8

Sean $A = \{1, 2, 3, 4\}$ y $S = \{(1, 1), (2, 1), (3, 2), (2, 3)\} \subseteq A \times A$:

(a) probar que $S \notin EQ(A)$,

(b) hallar S^{EQ}.

E 5.17.9

Sean $R_1, R_2 \in EQ(A)$. Probar que $(R_2 \cup R_1)^{EQ} = R_2 \circ R_1$ si, y sólo si, $R_1 \circ R_2 = R_2 \circ R_1$.

E 5.17.10

Sean $A = \{1, 2, 3, 4\}$ y $R \in EQ(A)$. Hallar 1_R y 2_R, siendo

(a) $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (3, 1)\}$,

(b) $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (1, 4), (4, 1), (2, 4), (4, 2)\}$.

E 5.17.11

Para cada par de conjuntos A, B y funciones $f : A \longrightarrow B$:

(a) determinar la relación de equivalencia R_f asociada a f,

(b) hallar las clases de equivalencia.

  (i) $A = \{-3, -1, 0, 1, 3, 5, \sqrt{2}\}$, $B = \mathbb{Z}$, $f(x) = x^2 + 1$,

  (ii) $A = B = \mathbb{Z}$, $f(x) = 7x + 4$,

  (iii) $A = B = \mathbb{Z}$, $f(x) = -x^2 + 2$,

  (iv) $A = \mathbb{R}^2$, $B = \mathbb{R}$, $f((x, y)) = 2x + 3$.

E 5.17.12

Calcular todas las posibles particiones de un conjunto con

(a) tres elementos,

(b) cuatro elementos.

E 5.17.13

(a) Sea $P = \{\{1, 2, 3\}, \{4\}, \{5, 6\}\}$ una partición de $A = \{1, 2, 3, 4, 5, 6\}$.

Indicar la relación $R(P)$ asociada a dicha partición.

(b) Dado $A = \{1, 2, 3, 4, 5\} \times \{1, 2, 3, 4, 5\}$ y $R \in EQ(A)$ definida por

$(x, y)R(z, t)$ si, y sólo si, $x + y = z + t$.

Hallar:

  (i) $\overline{(1, 3)}$, $\overline{(2, 4)}$ y $\overline{(1, 1)}$,

  (ii) la partición de A asociada a R.

(c) Dados $U = \{1, 2, 3\}$, $C = \{1, 2\}$ y R la relación de equivalencia del ejercicio 5.17.7 inciso (c). Determinar la partición asociada a R.

E 5.17.14

(a) Hallar las clases de equivalencia y el conjunto cociente para cada una de las relaciones dadas en:

(i) ejercicio 5.17.10,

(ii) ejercicio 5.17.7, incisos (b), (e), (g), (h).

(b) Hallar el conjunto cociente para cada una de las relaciones dadas en el ejercicio 5.17.11.

E 5.17.15

Hallar las funciones q_R y f^* (del teorema del triángulo), siendo:

(a) $A = \{1, 2, 3, 4, 5, 6, 7\}$, $B = \{a, b, c, d\}$

x	1	2	3	4	5	6	7
$f(x)$	a	b	b	c	b	a	d

(b) $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$, $B = \mathbb{N}$, $f : A \longrightarrow B$ definida por $f(x) = 2x^2 + 3$,

(c) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $f(x) = -3x^2$.

Determinar, en cada inciso, si f^* es biyectiva.

E 5.17.16

Dibujar el diagrama de Hasse correspondiente a cada uno de los siguientes conjuntos ordenados:

(a) $A = \{2, 3, 4, 8, 9, 27, 45, 1215\}$,

aRb si, y sólo si, a divide a b.

¿Cuál es el sucesor inmediato de 4?

(b) $A = \{1, 2, 3, 5, 7, 11\}$,

aRb si, y sólo si, a es múltiplo de b,

(c) $A = \{\{1\}, \{5\}, \{2, 3\}, \{1, 3\}, \{1, 3, 5\}, \emptyset\}$,

XRY si, y sólo si, $X \supseteq Y$,

(d) $(\mathcal{P}(A), \subseteq)$, siendo

(i) $|A| = 0$, (ii) $|A| = 1$,

(iii) $|A| = 2$, (iv) $|A| = 3$.

E 5.17.17

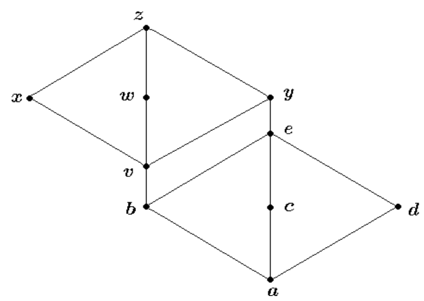
Para cada uno de los conjuntos ordenados del Ejercicio 5.17.16, hallar

(a) si existen, el primer elemento y el último elemento,

(b) elementos maximales y elementos minimales.

E 5.17.18

Sea $A = \{a, b, c, d, e, v, w, x, y, z\}$ y consideremos el orden sobre A definido por el siguiente diagrama



(a) hallar

(i) $sup\{b, c\}$, (ii) $sup\{b, w\}$, (iii) $sup\{e, x\}$,

(iv) $inf\{c, b\}$, (v) $inf\{d, x\}$, (vi) $inf\{c, e\}$,

(vii) $inf\ \{a, v\}$.

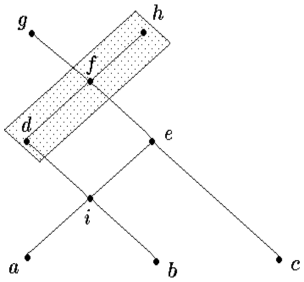
(b) Hallar el subconjunto ordenado $(B, \leq)$, siendo

(i) $B = \{a, e, d\}$, (ii) $B = \{a, w, y, z\}$, (iii) $B = \{e, x, y, z\}$.

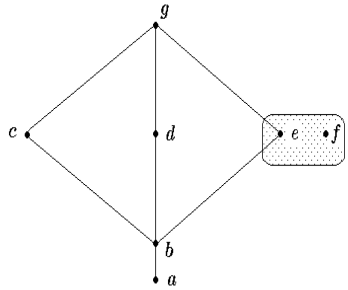
E 5.17.19

Dados los conjuntos ordenados,

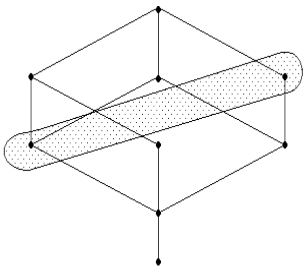
(i)



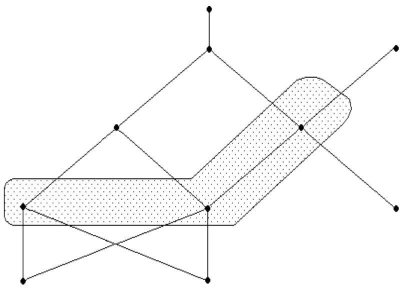
(ii)



(iii)



(iv)



(a) indicar elementos maximales y elementos minimales,

(b) en los subconjuntos que se indican en cada diagrama hallar, si existen, cotas superiores, cotas inferiores, supremo e ínfimo.

E 5.17.20

Sea $(A, \leq)$ un c.o., y sean $B \subseteq C \subseteq A$, B y C subconjuntos no vacíos. Probar que si $sup\, B$ y $sup\, C$ existen y $sup\, C \in B$, entonces $sup\, B = sup\, C$.

E 5.17.21

Sea A un c.o. y $X \subseteq A$. Probar que si existe:

(a) el ínfimo de X, éste es único,

(b) el supremo de X, éste es único.

E 5.17.22

Sea A un c.o.. Probar que:

(a) si A tiene primer elemento, éste es único,

(b) si A tiene más de un elemento minimal, entonces A no tiene primer elemento,

(c) si A es retículo superior finito, entonces tiene último elemento.

E 5.17.23

Sea (A, R) un c.o. finito y $M(R)$ una matriz asociada a R. Observando dicha matriz, determinar cómo se puede reconocer:

(a) un elemento minimal y un elemento maximal de A,

(b) la existencia del primer elemento y del último elemento de A.

6 Sistemas algebraicos

En este capítulo presentaremos las definiciones y los teoremas en forma general para operaciones n–arias donde n es un entero no negativo, pero en este curso trabajaremos sólo con $n = 0$, $n = 1$ y $n = 2$, y las demostraciones las haremos solamente para los dos últimos valores de n. Todos los temas generales que veremos, pertenecen a la disciplina matemática conocida con el nombre de *álgebra universal*.

6.1 Operaciones $n-$arias

D 6.1.1 *Sea A un conjunto no vacío, llamaremos operación $n-$aria definida sobre A, $n \in \mathbb{N}$, a toda función $f : A^n \longrightarrow A$. Diremos que n es la aridad de f y notaremos $ar(f) = n$.*

Ejemplos

(i) $+ : \mathbb{R}^2 \longrightarrow \mathbb{R}$,

$(x, y) \longrightarrow +(x, y) = x + y$ es una operación $2-$aria sobre $\mathbb{R}$.

(ii) $p : \mathbb{R} \longrightarrow \mathbb{R}$,

$x \longrightarrow p(x) = x^2$ es una operación $1-$aria sobre $\mathbb{R}$.

Queremos extender la definición anterior para $n = 0$; para ello debemos definir A^0. Es natural considerar A^0 como un conjunto con un solo elemento, esto es $A^0 = \{\emptyset\}$. Llamaremos operación $0-$aria a cualquier $f : A^0 \longrightarrow A$.

Luego, tenemos $f = \{(\emptyset, f(\emptyset))\} = \{(\emptyset, a) : a \in A,\ \text{a fijo}\ \}$, esto es, podemos interpretar a una operación $0-$aria como un elemento fijo de A y esta última interpretación es en realidad la definición de operación $0-$aria.

D 6.1.2 *Sea A un conjunto no vacío, una operación $0-$aria definida sobre A es cualquier elemento fijo de A.*

6.2 Algebras

D 6.2.1 *Un sistema algebraico, conjunto algebrizado o simplemente álgebra es un par $\mathcal{A} = \langle A, F\rangle$, donde $A \neq \emptyset$ y F es un conjunto de operaciones finitarias sobre A.*

Ejemplos

$\langle \mathbb{R}, \{+\}\rangle$, $\langle \mathbb{R}, \{\cdot\}\rangle$, $\langle \mathbb{R}, \{+, \cdot, 1\}\rangle$ son álgebras.

D 6.2.2 *Sea $\mathcal{A} = \langle A, F\rangle$ un álgebra. Llamaremos*

(i) *soporte del álgebra al conjunto A. Cuando no haya lugar a confusión sobre F representaremos al álgebra por su conjunto soporte y diremos sea A un álgebra.*

(ii) *reducto de $\langle A, F\rangle$ a toda álgebra $\mathcal{B} = \langle A, F'\rangle$ con $F' \subseteq F$.*

Ejemplos

(i) $\mathbb{R}$ es el soporte de $\langle \mathbb{R}, \{+, \cdot, 1\}\rangle$.

(ii) $\langle \mathbb{R}, \{+\}\rangle$ y $\langle \mathbb{R}, \{\cdot\}\rangle$ son reductos de $\langle \mathbb{R}, \{+, \cdot, 1\}\rangle$.

Nota. En lo que sigue escribiremos $\langle A, f_1, f_2, \ldots, f_k\rangle$ en lugar de $\langle A, \{f_1, f_2, \ldots, f_k\}\rangle$.

Tipo de similaridad de un álgebra

D 6.2.3 *Sea $\langle A, F\rangle$ un álgebra y $F = \{f_1, \ldots, f_k\}$ con $ar(f_1) = n_1, \ldots, ar(f_k) = n_k$, entonces diremos que $\langle A, F\rangle$ es un álgebra de tipo de similaridad $(n_1, \ldots, n_k)$.*

En general $n_1 \leq n_2 \leq \ldots \leq n_k$.

Ejemplos

(i) $\langle \mathbb{R}, +, \cdot\rangle$ es un álgebra de tipo $(2, 2)$.

(ii) $\langle \mathbb{R}, +, \cdot, 0, 1\rangle$ es un álgebra de tipo $(2, 2, 0, 0)$.

D 6.2.4 *Dos álgebras $\langle A, F\rangle$ y $\langle A', F'\rangle$ son similares si existe una biyección $\alpha : F \longrightarrow F'$ tal que si $ar(f) = n$, entonces $ar(\alpha(f)) = n$, para toda $f \in F$.*

Ejemplos

(i) $\langle \mathbb{R}, +\rangle$ y $\langle \mathbb{R}, \cdot\rangle$ son similares.

(ii) $\langle M_n(\mathbb{R}), +, \cdot, \mathbb{O}, \mathbb{I}\rangle$ y $\langle \mathbb{R}, +, \cdot, 0, 1\rangle$ son similares.

Clases de álgebras

D 6.2.5 *Una clase de álgebras es una familia $\mathcal{K}$ de álgebras similares.*

Observaciones

(i) Cuando no haya lugar a confusión usaremos el mismo conjunto F para todas las álgebras de la clase.

(ii) Cuando trabajemos en forma teórica diremos sea $\mathcal{K}$ una clase de álgebras y $A \in \mathcal{K}$ o también, sea A una $\mathcal{K}-$álgebra.

Diversos ejemplos de clases de álgebras

Los semigrupos ($\mathcal{S}$)

D 6.2.6 *Un álgebra $\langle A, * \rangle$ de tipo 2 es un semigrupo si se verifica $x * (y * z) = (x * y) * z$, para todo $x, y, z \in A$.*

Representaremos con $\mathcal{S}$ a la clase de los semigrupos.

Ejemplos

(i) $\langle I\!N, + \rangle$ y $\langle I\!N, \cdot \rangle$ son semigrupos.

(ii) $\langle A, + \rangle \in \mathcal{S}$, donde $A = \{0, 1\}$ y $+$ está definida por medio de la siguiente tabla:

$+$	0	1
0	0	1
1	1	1

Los semigrupos conmutativos ($\mathcal{S}_C$)

D 6.2.7 $\langle A, * \rangle \in \mathcal{S}$ *es un semigrupo conmutativo si verifica $x * y = y * x$, para todo $x, y \in A$.*

Representaremos con $\mathcal{S}_C$ a la clase de los semigrupos conmutativos.

Los semigrupos con unidad ($\mathcal{S}_U$)

D 6.2.8 *Un álgebra* $\langle A, *, e\rangle$ *de tipo* $(2, 0)$ *es un semigrupo con unidad o monoide si se verifica:*

(i) $\langle A, *\rangle \in \mathcal{S}$,

(ii) $e * x = x * e = x$, *para todo* $x \in A$.

Representaremos con $\mathcal{S}_{\boldsymbol{U}}$ a la clase de los semigrupos con unidad.

Las bandas o semiretículos $(\mathcal{S}_{\boldsymbol{L}})$

D 6.2.9 $\langle A, *\rangle \in \mathcal{S}_{\boldsymbol{C}}$ *es una banda si se verifica* $x * x = x$, *para todo* $x \in A$.

Los grupos $(\mathcal{G})$

D 6.2.10 *Un álgebra* $\langle A, *, ', e\rangle$ *de tipo* $(2, 1, 0)$ *es un grupo si:*

(i) *el reducto* $\langle A, *, e\rangle \in \mathcal{S}_{\boldsymbol{U}}$,

(ii) *se verifica* $x * x' = x' * x = e$, *para todo* $x \in A$.

Representaremos con $\mathcal{G}$ a la clase de los grupos.

Ejemplos

(i) $\langle \mathbb{Z}, +, -, 0\rangle$, $\langle \mathbb{Q}, +, -, 0\rangle$ y $\langle \mathbb{R}, +, -, 0\rangle$ son grupos.

(ii) $\langle M_n(\mathbb{R}), +, -, \mathbb{O}\rangle \in \mathcal{G}$.

(ii) Sea X un conjunto. Representaremos con $B(X)$ al conjunto de todas las biyecciones de X sobre X. Entonces $\mathcal{B}_X = \langle B(X), \circ, ^{-1}, I_X\rangle$ es un grupo llamado *el grupo simétrico* sobre X.

Si $X = \{1, 2, \ldots, n\}$ escribiremos $\mathcal{B}_n$ en lugar de $\mathcal{B}_X$ y diremos que $\mathcal{B}_n$ es el grupo simétrico de orden n.

Los grupos abelianos $(\mathcal{G}_{\boldsymbol{a}})$

D 6.2.11 $\langle A, *, ', e\rangle \in \mathcal{G}$ *es un grupo abeliano o conmutativo si se verifica* $x * y = y * x$, *para todo* $x, y \in A$.

Ejemplos

(i) $\langle \mathbb{Z}, +, -, 0\rangle$, $\langle \mathbb{R}^*, \cdot, ^{-1}, 1\rangle$, con $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, son grupos abelianos.

(ii) $\mathcal{B}_n \notin \boldsymbol{\mathcal{G}_a}$ pues, en general, $f \circ g \neq g \circ f$.

Los anillos ($\boldsymbol{\mathcal{A}}$)

D 6.2.12 *Un álgebra* $\langle A, +, \cdot, -, 0\rangle$ *de tipo* $(2, 2, 1, 0)$ *es un anillo si:*

(i) $\langle A, +, -, 0\rangle \in \boldsymbol{\mathcal{G}_a}$,

(ii) $\langle A, \cdot\rangle \in \boldsymbol{\mathcal{S}}$,

(iii) *se verifican* $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$, *para todo* $x, y, z \in A$.

Ejemplos

$\langle \mathbb{Z}, +, \cdot, -, 0\rangle$, $\langle M_n(\mathbb{R}), +, \cdot, -, \mathbb{O}\rangle$, $\langle \mathbb{Q}, +, \cdot, -, 0\rangle$ y $\langle \mathbb{R}, +, \cdot, -, 0\rangle$ son anillos.

Los anillos conmutativos ($\boldsymbol{\mathcal{A}_C}$)

D 6.2.13 *Un álgebra* $\langle A, +, \cdot, -, 0\rangle$ *de tipo* $(2, 2, 1, 0)$ *es un anillo conmutativo si:*

(i) $\langle A, +, \cdot, -, 0\rangle \in \boldsymbol{\mathcal{A}}$,

(ii) *se verifica* $x \cdot y = y \cdot x$, *para todo* $x, y \in A$.

Los anillos unitarios ($\boldsymbol{\mathcal{A}_U}$)

D 6.2.14 *Un álgebra* $\langle A, +, \cdot, -, 0, 1\rangle$ *de tipo* $(2, 2, 1, 0, 0)$ *es un anillo unitario si se verifican:*

(i) $\langle A, +, \cdot, -, 0\rangle \in \boldsymbol{\mathcal{A}}$,

(ii) $\langle A, \cdot, 1\rangle \in \boldsymbol{\mathcal{S}_U}$.

Los anillos sin divisores de cero ($\boldsymbol{\mathcal{A}_0}$)

D 6.2.15 *Un álgebra* $\langle A, +, \cdot, -, 0\rangle \in \boldsymbol{\mathcal{A}}$ *de tipo* $(2, 2, 1, 0)$ *es un anillo sin divisores de cero si verifica:*

(P) *la hipótesis* $x \cdot y = 0$ *implica* $x = 0$ *o* $y = 0$.

Los anillos con división $(\mathcal{A}_{\boldsymbol{D}})$

D 6.2.16 *Un álgebra* $\langle A, +, \cdot, -, 0, 1\rangle \in \mathcal{A}_{\boldsymbol{U}}$ *de tipo* $(2, 2, 1, 0, 0)$ *es un anillo con división si verifica:*

(D) *para cada* $x \in A, x \neq 0$, *existe* $y \in A$ *tal que* $x \cdot y = y \cdot x = 1$.

Ejemplos

(i) $\langle \mathbb{Z}, +, \cdot, -, 0, 1\rangle$, $\langle \mathbb{Q}, +, \cdot, -, 0, 1\rangle$, $\langle \mathbb{R}, +, \cdot, -, 0, 1\rangle$ son anillos unitarios,

(ii) $\langle M_n(\mathbb{R}), +, \cdot, -, \mathbb{O}, \mathbb{I}\rangle \notin \mathcal{A}_{\boldsymbol{U}}$,

(iii) $\langle \mathbb{Z}, +, \cdot, -, 0, 1\rangle \notin \mathcal{A}_{\boldsymbol{D}}$, $\langle \mathbb{R}, +, \cdot, -, 0, 1\rangle \in \mathcal{A}_{\mathbf{0}}$.

Los cuerpos $(\mathfrak{C})$

D 6.2.17 $A \in \mathcal{A}_{\boldsymbol{D}}$ *es un cuerpo si* $x \cdot y = y \cdot x$, *para todo* $x, y \in A$.

Ejemplos

$\langle \mathbb{Q}, +, \cdot, -, 0, 1\rangle$, $\langle \mathbb{R}, +, \cdot, -, 0, 1\rangle$ y $\langle \mathbb{C}, +, \cdot, -, 0, 1\rangle$ son cuerpos.

A continuación consideraremos una clase de álgebras $\boldsymbol{\mathcal{K}}$ fija.

6.3 Subálgebras

D 6.3.1 *Sean* $A \in \boldsymbol{\mathcal{K}}$ *y* $S \subseteq A$. *Diremos que* S *es una subálgebra de* A, *y lo notaremos* $S \lhd A$, *si se verifican:*

(S0) $S \neq \emptyset$,

(S1) *si* $a \in A$ *es una operación* $0-$*aria, entonces* $a \in S$,

(S2) *si* $x_1, \ldots, x_k \in S$ *y* f *es una operación* $k-$*aria, entonces* $f(x_1, \ldots, x_k) \in S$.

Notas.

(i) Es usual decir que S es una subálgebra de A si, y sólo si, S es un subconjunto no vacío de A cerrado con respecto a todas las operaciones de A.

(ii) De la definición resulta que $A \lhd A$.

Ejemplo

Sea $\langle A, +, 0\rangle$ de tipo $(2, 0)$ donde $A = \{0, a, b, c\}$ y $+$ está definida por medio de la siguiente tabla:

$+$	0	a	b	c
0	0	a	b	c
a	a	a	c	c
b	b	c	b	c
c	c	c	b	c

Entonces se verifican:

(a) $S = \{b, c\}$ no es subálgebra de A, pues $0 \notin S$,

(b) $\{0, a\} \lhd A$.

Ejercicio

Sean $A \in \mathcal{K}$ y $\{S_i\}_{i\in I}$ una familia de subálgebras de A. Demostrar que si $S = \bigcap_{i\in I} S_i \neq \emptyset$, entonces S es una subálgebra de A.

6.4 Subálgebra generada por una parte

D 6.4.1 *Sean $A \in \mathcal{K}$ y $X \subseteq A$, $X \neq \emptyset$. Llamaremos subálgebra generada por X en $\mathcal{K}$, y la representaremos con $[X]_{\mathcal{K}}$ o $[X]$, a la intersección de todas las subálgebras de A que contienen a X.*

Observemos que:

(i) la definición de subálgebra generada tiene sentido por que siempre existe una subálgebra de A que contiene a X y la intersección no vacía de subálgebras es una subálgebra.

(ii) $[X]$ es la menor (en el sentido de la inclusión) de todas las subálgebras de A que contienen a X.

Ejercicio

Sea $A \in \mathcal{K}$ y $X \subseteq A$, $X \neq \emptyset$. Probar que las siguientes condiciones son equivalentes:

(i) $B = [X]$,

(ii) $B \subseteq A$ verifica las siguientes condiciones:

(a) $X \subseteq B$,

(b) $B \lhd A$,

(c) las hipótesis $X \subseteq S$ y $S \lhd A$ implican que $B \subseteq S$.

Ejemplo

Sean $\langle A, * \rangle \in \mathbf{S}$ y $X \subseteq A$, $X \neq \emptyset$. Vamos a probar que

$[X]_{\mathbf{S}} = \{u \in A : \text{ existen } x_1, \ldots, x_n \in X \text{ tal que } u = x_1 * \ldots * x_k\}$.

En efecto, sea
$B = \{u \in A : \text{ existen } x_1, \ldots, x_k \in X \text{ tal que } u = x_1 * \ldots * x_n\}$,
entonces

(a) $X \subseteq B$: pues tenemos $x = x$ con $x \in X$.

(b) $B \lhd A$: sean

$u = x_1 * \ldots * x_n$,

$v = y_1 * \ldots * y_n$,

entonces

$u * v = x_1 * \ldots * x_k * y_1 * \ldots * y_n \in B$.

(c) $S \lhd A$ y $X \subseteq S$ implican $B \subseteq S$:

(1) $u \in B$, [hipótesis]

(2) $u = x_1 * \ldots * x_n$, $x_1, \ldots, x_n \in X$, [(1) y def. de B]

(3) $X \subseteq S$, [hipótesis]

(4) $x_1, \ldots, x_n \in S$, [(2) y (3)]

(5) $S \lhd A$, [hipótesis]

(6) $u \in S$. [(2),(4) y (5)]

Sistemas de generadores

D 6.4.2 *Sean $A \in \mathcal{K}$ y $G \subseteq A$, diremos que G es un sistema de generadores de A si $[G] = A$.*

Algebras finitamente generadas

D 6.4.3 *Diremos que $A \in \mathcal{K}$ es finitamente generada (f.g.) si tiene un conjunto finito de generadores.*

D 6.4.4 *Diremos que la clase $\mathcal{K}$ es localmente finita si toda álgebra de $\mathcal{K}$ f.g. es finita.*

6.5 Homomorfismos

D 6.5.1 *Sean $A, B \in \mathcal{K}$. Una aplicación $h : A \longrightarrow B$ es un $\mathcal{K}-$homomorfismo, o simplemente un homomorfismo, si se verifican:*

(H1) *si $a \in A$ es una operación $0-$aria, entonces $h(a) = a$,*

(H2) *si $x_1, \ldots, x_k \in A$ y f es una operación $k-$aria, entonces*

$$h(f(x_1, \ldots, x_k)) = f(h(x_1), \ldots, h(x_k)).$$

Indicaremos $Hom_{\mathcal{K}}(A, B)$ u $Hom(A, B)$ al conjunto de todos los homomorfismos de A en B.

Monomorfismos, epimorfismos, isomorfismos

D 6.5.2 *Sean $A, B \in \mathcal{K}$ y $h \in Hom(A, B)$. Entonces h es:*

(i) *monomorfismo si h es inyectiva,*

(ii) *epimorfismo si h es epiyectiva,*

(iii) *isomorfismo si h es biyectiva.*

Además si:

(iv) *h es un isomorfismo, diremos que las álgebras A y B son isomorfas y escribiremos $A \simeq B$. Dos álgebras isomorfas tienen exactamente las mismas propiedades algebraicas y en los casos necesarios podemos reemplazar una por otra.*

(v) $A = B$, *diremos que h es endomorfismo y en lugar de* $Hom(A, A)$ *escribiremos* $End(A)$.

(vi) h *es un endomorfismo biyectivo, diremos que h es un automorfismo y representaremos con* $Aut(A)$ *al conjunto de todos los automorfismos de* A.

Ejemplo

Sea $\langle \mathbb{R}^*, \cdot \rangle$, con $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, el semigrupo multiplicativo y $\langle A, \circ \rangle \in \boldsymbol{\mathcal{S}}$, donde $A = \{a, b\}$ y $\circ$ está definido por la tabla

$\circ$	a	b
a	b	a
b	a	b

La aplicación $h : \mathbb{R}^* \longrightarrow A$ definida por

$$h(x) = \begin{cases} a, & \text{si } x < 0 \\ b, & \text{si } x > 0 \end{cases},$$

es un $\boldsymbol{\mathcal{S}}-$epimorfismo.

Propiedades de los homomorfismos

T 6.5.1 *Sean* $A, B \in \boldsymbol{\mathcal{K}}$ *y* $h \in Hom(A, B)$. *Si*

(i) $S \triangleleft A$, *entonces* $h(S) \triangleleft B$.

(ii) $S' \triangleleft B$ *y* $h^{-1}(S') \neq \emptyset$, *entonces* $h^{-1}(S') \triangleleft A$.

Dem. Esbozaremos la demostración para el caso de las operaciones binarias ya que para las restantes el razonamiento es análogo.

(i) Sean $x', y' \in h(S)$ y $*$ una operación binaria,

(1) $x' = h(s)$, $s \in S$, [hipótesis]

(2) $y' = h(t)$, $t \in S$, [hipótesis]

(3) $x' * y' = h(s) * h(t)$ [(1) y (2)]

$= h(s * t)$ [h es homomorfismo]

(4) $s * t \in S$, [(1),(2) y $S \lhd A$]

$x' * y' \in h(S)$.

(ii) Se demuestra de manera análoga a (i). ■

Ejemplo

Sean $A, B \in \mathbf{S}$, donde $A = \{a, b, c\}$, $B = \{m, n, p\}$ y las operaciones están dadas por las siguientes tablas:

$*$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c

$*$	m	n	p
m	m	m	m
n	m	n	m
p	m	m	p

Si $h : A \longrightarrow B$ es la aplicación que transforma $S_1 = \{b, c\}$ en $S_2 = \{n, p\}$, entonces por (i) h no es un $\mathbf{S}-$homomorfismo pues $S_1 \lhd A$ y $S_2 \not\lhd B$.

T 6.5.2 *Si* $A, B \in \mathcal{K}$, $h \in Hom(A, B)$ *y* $X \subseteq A$, *entonces* $h([X]) = [h(X)]$.

Dem. Sea $C = h([X])$, entonces:

(i) $h(X) \subseteq C$:

(1) $X \subseteq [X]$, [def. de subálgebra generada]

(2) $h(X) \subseteq h([X])$, [(1)]

(3) $h(X) \subseteq C$. [(2)]

(ii) $C \lhd B$:

(1) $X \subseteq A$, [hipótesis]

(2) $[X] \lhd A$, [(1)]

(3) $h \in Hom(A, B)$, [hipótesis]

(4) $h([X]) \lhd B$. [(2),(3) y T 6.5.1]

(iii) Si $S \lhd B$ y $h(X) \subseteq S$, entonces $C \subseteq S$:

(1) $h(X) \subseteq S$, [hipótesis]

(2) $X \subseteq h^{-1}(S)$, [(1) y def. imagen completa inversa]

(3) $S \lhd B$, [hipótesis]

(4) $h^{-1}(S) \lhd A$, [(3) y T 6.5.1]

(5) $[X] \subseteq h^{-1}(S)$, [(2),(4) y def. subálgebra generada]

(6) $h([X]) \subseteq S$. [(5) y def. de imagen
completa inversa]

De (i), (ii) y (iii) resulta $h([X]) = C = [h(X)]$. ■

T 6.5.3 *Sean $A, B \in \mathcal{K}$, G un sistema de generadores de A y $f : G \longrightarrow B$ una función arbitraria. Entonces existe a lo sumo un homomorfismo $h : A \longrightarrow B$ tal que $h(g) = f(g)$, para todo $g \in G$.*

Dem. Supongamos que $h, h_1 : A \longrightarrow B$ son homomorfismos tales que

(1) $h(g) = f(g) = h_1(g)$, para todo $g \in G$,

y probemos que $h = h_1$.
Sea $S = \{x \in A : h(x) = h_1(x)\}$, entonces

(i) $G \subseteq S$, [(1)]

(ii) $S \lhd A$:

sean $x, y \in S$ y $*$ una operación binaria

(2) $h(x) = h_1(x)$, [hipótesis]

(3) $h(y) = h_1(y)$, [hipótesis]

(4) $h(x) * h(y) = h_1(x) * h_1(y)$, [(2) y (3)]

(5) $h(x * y) = h_1(x * y)$ [(4) y h, h_1 homomorfismos]

(6) $x * y \in S$.

De (i) y (ii) tenemos que $[G] \subseteq S$ y como $A = [G]$, resulta $A = S$. ■

Por el teorema anterior tenemos que si f puede extenderse a un homomorfismo h, él es único, pero puede suceder que tal extensión no exista.

Ejemplo

Sean $\langle A, +\rangle, \langle B, +\rangle \in \mathbf{S}_C$ donde $A = \{a, b, c\}$, $B = \{0, 1\}$ y las operaciones están definidas por medio de las siguientes tablas:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$+$	0	1
0	0	1
1	1	0

Sea $G = \{b, c\}$ un sistema de generadores de A y $f : G \longrightarrow B$ definida por $f(b) = f(c) = 1$.

Verifiquemos que no existe ningún homomorfismo $h : A \longrightarrow B$ que prolonga a f. En efecto, si existiera tal homomorfismo tendríamos

$$h(c + c) = h(c) + h(c),$$

pero

$$h(c + c) = h(b) = 1,$$

$$h(c) + h(c) = 1 + 1 = 0,$$

luego,

$$h(c + c) \neq h(c) + h(c).$$

6.6 Congruencias y álgebras cociente

D 6.6.1 *Sea $A \in \boldsymbol{\mathcal{K}}$. $R \in EQ(A)$ es una $\boldsymbol{\mathcal{K}}$–congruencia, o simplemente una congruencia sobre A, si R es compatible con todas las operaciones n–arias, $n > 0$ definidas sobre A. Esto es, si se verifica:*

(Ck) *las hipótesis f operación k–aria sobre A y $x_1Ry_1, \ldots, x_kRy_k$ implican*

$$f((x_1, \ldots, x_k))Rf((y_1, \ldots, y_k)).$$

Indicaremos con $Con_{\boldsymbol{\mathcal{K}}}(A)$ o $Con(A)$, al conjunto de todas las congruencias de A.

Relación núcleo

T 6.6.1 *Sean $A, B \in \boldsymbol{\mathcal{K}}$, $h \in Hom(A, B)$ y R_h la relación de equivalencia asociada a h, entonces $R_h \in Con(A)$.*

Dem. Verificaremos la condición (Ck) de D6.6.1 para $k = 1, 2$.

(C1) Sea $*$ una operación unaria, entonces

(1) xR_hy, [hipótesis]

(2) $h(x) = h(y)$, [(1) y def. R_h]

(3) $*h(x) = *h(y)$, [(2)]

(4) $h(*x) = h(*y)$, [(3) y h homomorfismo]

(5) $*xR_h * y$. [(4) y def. R_h]

(C2) Sea $\circ$ una operación binaria, entonces

(1) xR_hy, [hipótesis]

(2) $x'R_hy'$, [hipótesis]

(3) $h(x) = h(y)$, [(1) y def. R_h]

(4) $h(x') = h(y')$, [(2) y def. R_h]

(5) $h(x) \circ h(x') = h(y) \circ h(y')$, [(3) y (4)]

(6) $h(x \circ x') = h(y \circ y')$, [(5) y h homomorfismo]

(7) $(x \circ x')R_h(y \circ y')$. [(6) y def. R_h] ■

D 6.6.2 *Sean $\langle A, F\rangle, \langle B, F\rangle \in \boldsymbol{\mathcal{K}}$ y $h \in Hom(A, B)$. Llamaremos relación núcleo de h a la relación de equivalencia R_h asociada a h.*

En lo que sigue si $h \in Hom(A, B)$, denotaremos con $N(h)$ a R_h.

Algebras cociente

T 6.6.2 *Sean $\langle A, F\rangle \in \boldsymbol{\mathcal{K}}$ y $R \in Con(A)$. Para cada operación k–aria $f \in F$ y cada $(C_1, \dots, C_k) \in (A/R)^k$, definimos:*

$$f^*((C_1, \dots, C_k)) = C, \text{ donde } C = (f((x_1, \dots, x_k)))_R, \text{ con } x_1 \in C_1, \dots, x_k \in C_k.$$

Si $F^* = \{f^* : f \in F\}$, entonces se verifica que $\langle A/R, F^*\rangle$ es un álgebra del mismo tipo de similaridad que A.

Dem. Es claro que de acuerdo a la forma en que han sido definidas las operaciones en A/R, solamente debemos verificar que las mismas son independientes de los representantes elegidos en cada clase.

Haremos la demostración para el caso de las operaciones binarias.

Sean $C_1, C_2 \in A/R$, $x_1, x_2 \in C_1$, $y_1, y_2 \in C_2$ y supongamos que $C = (x_1 \circ y_1)_R$ y $C' = (x_2 \circ y_2)_R$, entonces probemos que $C = C'$.

En efecto,

(1) $x_1 R x_2$, [hipótesis]

(2) $y_1 R y_2$, [hipótesis]

(3) $(x_1 \circ y_1)R(x_2 \circ y_2)$, [(1),(2) y R congruencia]

(4) $(x_1 \circ y_1)_R = (x_2 \circ y_2)_R$, [(3)]

(5) $C = C'$. ■

Nota. En lo que sigue también representaremos con F al conjunto F^*, es decir usaremos en A y A/R los mismos símbolos de operaciones.

Después del resultado anterior podemos introducir la siguiente definición:

D 6.6.3 *Diremos que $\langle A/R, F\rangle$ es el álgebra cociente de A por la relación R.*

Nota. Es fácil ver que la aplicación canónica $q : A \longrightarrow A/R$ es un homomorfismo llamado el epimorfismo canónico o natural.

T 6.6.3 (Teorema del triángulo para álgebras) *Si $\langle A, F\rangle$, $\langle B, F\rangle \in \boldsymbol{\mathcal{K}}$ y $h \in Hom(A, B)$, entonces existe un único homomorfismo $\overline{h} : \langle A/N(h), F\rangle \longrightarrow \langle B, F\rangle$ tal que $\overline{h} \circ q = h$. Además*

(i) *$\overline{h}$ es inyectiva,*

(ii) *$\overline{h}$ es sobre si, y sólo si, h lo es.*

Dem. Sabemos que existe una única función $\overline{h} : A/N(h) \longrightarrow B$ tal que $\overline{h} \circ q = h$, que verifica las condiciones (i) y (ii).

Probemos que $\overline{h} \in Hom(A/N(h), B)$.

Sean x_R, $y_R \in A/N(h)$ y $* \in F$ una operación binaria, entonces:

$$\begin{aligned}
\overline{h}(x_R * y_R) &= \overline{h}((x * y)_R) \\
&= \overline{h}(q(x * y)) \\
&= (\overline{h} \circ q)(x * y) \\
&= h(x * y) \\
&= h(x) * h(y) && [h \in Hom(A, B)] \\
&= \overline{h}(q(x)) * \overline{h}(q(y)) \\
&= \overline{h}(x_R) * \overline{h}(y_R).
\end{aligned}$$

■

6.7 Algebras libres

Algebras absolutamente libres

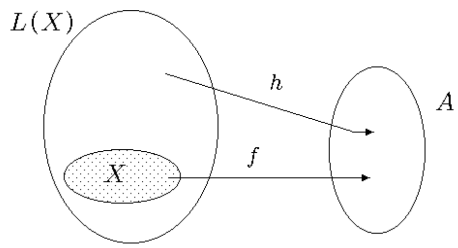
D 6.7.1 *Sea $\langle L, F\rangle$ un álgebra y sea $X \subseteq L$. Diremos que L es absolutamente libre si se verifican las siguientes condiciones:*

(A1) $[X] = L$,

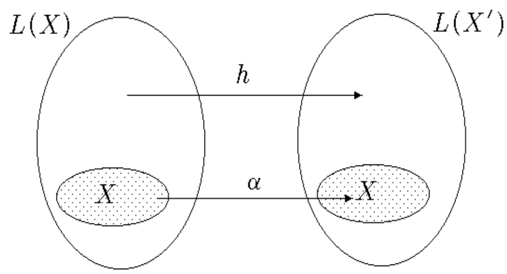
(A2) *si $\langle A, F\rangle$ es un álgebra similar y $f : X \longrightarrow A$ es una función arbitraria, entonces existe un homomorfismo $h : L \longrightarrow A$ que extiende a f.*

En este caso diremos que X es un conjunto de generadores libres para L y notaremos $L = L(X)$.

Observemos que de T 6.5.3 resulta que el homomorfismo h de la condición (A2) de D 6.7.1 es único.



T 6.7.1 *Sean $\langle L(X), F\rangle$ y $\langle L(X'), F\rangle$ dos álgebras libres similares que tienen a X y X' como conjunto de generadores libres, respectivamente. Si $|X| = |X'|$, entonces existe un isomorfismo $h : L(X) \longrightarrow L(X')$.*



Dem. Sea

(1) $\alpha : X \longrightarrow X'$ biyectiva, [hipótesis]

entonces existen

(2) $\beta = \alpha^{-1} : X' \longrightarrow X$, [(1)]

(3) $h : L(X) \longrightarrow L(X')$ homomorfismo que prolonga a α, [(1), D 6.7.1 (A2)]

(4) $h' : L(X') \longrightarrow L(X)$ homomorfismo que prolonga a β, [(1), D 6.7.1 (A2)]

(5) $f = h' \circ h : L(X) \longrightarrow L(X)$ es un homomorfismo. [(3), (4)]

Ahora probaremos que:

(i) $h' \circ h = I_{L(X)}$:

Sea $B = \{z \in L(X) : f(z) = z\}$, entonces

(6) $X \subseteq B$: Si $x \in X$,

$$
\begin{aligned}
f(x) &= h'(h(x)) && [(5)]\\
&= h'(\alpha(x)) && [(3)]\\
&= \beta(\alpha(x)) && [(4)]\\
&= x. && [(2)]
\end{aligned}
$$

(7) $B \lhd L(X)$: Si $*$ es una operación binaria y $z_1, z_2 \in B$,

$$
\begin{aligned}
z_1 * z_2 &= f(z_1) * f(z_2)\\
&= f(z_1 * z_2). && [(5)]
\end{aligned}
$$

(8) $B = L(X)$. [(6),(7)]

(ii) $h \circ h' = I_{L(X')}$: se prueba de manera análoga a (i).

(iii) h es un isomorfismo: es consecuencia directa de (i) y (ii). ■

T 6.7.2 *Sea $\langle L, F\rangle$ un álgebra absolutamente libre tal que X y X' son conjunto de generadores libres. Entonces se verifica $|X| = |X'|$.*

Dem. Supongamos que

(1) $|X| \prec |X'|$, [hipótesis]

entonces

(2) existe $f : X \longrightarrow X'$ inyectiva, [(1)]

(3) $f(X) \subseteq X'$, [(2)]

(4) $[f(X)]$ es libre con $f(X)$ como conjunto de generadores libres, [(2), Ejercicio 6.9.17]

(5) $[f(X)] = L$, [(2), Ejercicio 6.9.17]

(6) existe $x' \in X' \setminus f(X)$, [(1),(2)]

(7) $f(X) \subseteq X' \setminus \{x'\}$, [(2),(6)]

(8) $[f(X)] \subseteq [X' \setminus \{x'\}]$, [(7)]

(9) $L \subseteq [X' \setminus \{x'\}]$, [(5),(8)]

(10) $[X' \setminus \{x'\}] \subset L$, [hip., Ejercicio 6.9.15]

(9) y (10) se contradicen.

En forma análoga se prueba que la hipótesis $|X'| \prec |X|$ conduce a una contradicción. Entonces vale $|X'| = |X|$. ■

Notas.

(i) De T 6.7.1 resulta la unicidad del álgebra libre L que tiene a X como conjunto de generadores libres, en el sentido de que cualquier otra álgebra que tenga un conjunto de generadores libres con el cardinal de X, es isomorfa a L.

(ii) De T 6.7.2 resulta que álgebra libre L puede tener más de un conjunto de generadores libres, pero todos ellos tienen el mismo cardinal. En particular si $L = L(X)$ y $|X| = n$, entonces cualquier otro conjunto de generadores libres tiene n elementos.

Una construcción del álgebra absolutamente libre

Ahora consideraremos ciertas álgebras cuyos conjuntos soportes se construyen por medio de las reglas indicadas para construir al conjunto $For[X]$ de las formas polinomiales estudiados en la sección 1.2 del capítulo 1.

Entonces, sea X un conjunto no vacío y F un conjunto de símbolos de operaciones finitarias. Con $For[X]$ designaremos al conjunto cuyos elementos llamaremos *formas polinomiales* (f.p.), que se construyen por medio de las siguientes reglas:

(R1) $X \subseteq For[X]$,

(R2) si $a \in F$ es un símbolo de operación 0–aria, entonces $a \in For[X]$,

(R3) si $p_1, \ldots, p_k \in For[X]$ y $f \in F$ es un símbolo de operación k–aria con $k \geq 1$, entonces $f((p_1, \ldots, p_k)) \in For[X]$,

(R4) (de cierre) Las únicas f.p. son las determinadas por R1, R2 y R3.

Ahora algebrizaremos a $For[X]$ tomando como operaciones sobre este conjunto al propio F, es decir:

(i) Elegimos como operaciones 0–arias de $For[X]$ a los símbolos de operaciones 0–arias de F. Esto es posible, pues por R1, estos objetos están en $For[X]$.

(ii) Si $f \in F$ es un símbolo de operación k–aria, entonces podemos considerar la correspondencia $(p_1, \ldots, p_k) \longrightarrow f((p_1, \ldots, p_k))$, y por R3 tenemos que

$f : For[X]^n \longrightarrow For[X]$ es una operación k–aria sobre $For[X]$.

Entonces se puede probar que la F–álgebra $\langle For[X], F\rangle$ es absolutamente libre y tiene a X como conjunto de generadores libres.

Algebras relativamente libres

Existe una noción más restringida que la de álgebra absolutamente libre.

D 6.7.2 *Sea $\mathcal{K}$ una clase de álgebras, $\langle L, F\rangle \in \mathcal{K}$ y $X \subseteq L$. Diremos que L es relativamente libre (relativa a $\mathcal{K}$) si se verifican:*

(L1) $[X]_{\mathcal{K}} = L$,

(L2) *si $A \in \mathcal{K}$ y $f : X \longrightarrow A$ es una función arbitraria, entonces existe un $\mathcal{K}$–homomorfismo $h : L \longrightarrow A$ que prolonga a f.*

6.8 El semigrupo libre

Ahora veremos un ejemplo muy importante de álgebra relativamente libre.

Sea $X \neq \emptyset$, llamaremos *palabra* a toda sucesión finita y no vacía de elementos de X. Esto es si $x, y, z \in X$, entonces $p_1 = x$, $p_2 = xx$, $p_3 = xxyz$, $p_4 = zzyy$ son palabras.

Sea $S(X)$ el conjunto de todas las palabras construíbles sobre X. En $S(X)$ vamos a definir una operación binaria llamada operación de concatenación del siguiente modo:

dadas

$p = x_1x_2 \ldots x_m,\ x_1, x_2, \ldots , x_m \in X,$

$q = y_1y_2 \ldots y_k,\ y_1, y_2, \ldots , y_k \in X,$

entonces

$p \cdot q = x_1x_2 \ldots x_my_1y_2 \ldots y_k.$

Luego

(i) $\langle S(X), \cdot\rangle$ es un semigrupo.

En efecto, sean

$p = x_1 \ldots x_m,\ q = y_1 \ldots y_k,\ r = z_1 \ldots z_s \in S(X),$

entonces

$$\begin{aligned}(p \cdot q) \cdot r &= (x_1 \ldots x_my_1 \ldots y_k) \cdot r\\ &= x_1 \ldots x_my_1 \ldots y_kz_1 \ldots z_s\\ &= x_1 \ldots x_m(y_1 \ldots y_kz_1 \ldots z_s)\end{aligned}$$

$$= p \cdot (q \cdot r).$$

(ii) X es un conjunto de generadores libres de $S(X)$.

(a) $X \subseteq S(X)$:

Si $x \in X$, $p = x$ es una palabra, entonces $X \subseteq S(X)$.

(b) $[X]_{\mathfrak{S}} \subseteq S(X)$:

(1) $X \subseteq S(X)$, [(a)]

(2) $[X]_{\mathfrak{S}} \subseteq S(X)$. [(1)]

(c) $S(X) \subseteq [X]_{\mathfrak{S}}$:

Sea $p = x_1 \ldots x_n \in S(X),\ x_1, \ldots , x_n \in X$,

entonces

$x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_n = x_1 x_2 \ldots x_n$, [verificarlo]

$x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_n \in [X]_{\mathfrak{S}}$, [verificarlo]

luego

$$p = x_1 x_2 x_3 \ldots x_n \in [X]_{\mathfrak{S}}.$$

(d) $[X]_{\mathfrak{S}} = S(X)$:

Es consecuencia de (b) y (c).

(e) Sea $\langle A, * \rangle \in \mathfrak{S}$ y $f : X \longrightarrow A$ una función arbitraria. Para cada $p \in S(X)$, $p = x_1 x_2 \ldots x_n$, con $x_1, x_2, \ldots , x_n \in X$ sea

$$h(p) = f(x_1) * f(x_2) * \ldots * f(x_n).$$

La aplicación $h : S(X) \longrightarrow A$, así definida es un homomorfismo. En efecto, si $p, q \in S(X)$,

$$p = x_1 x_2 \ldots x_n,\ \ x_1, x_2, \ldots , x_n \in X,$$

$$q = y_1 y_2 \ldots y_m,\ \ y_1, y_2, \ldots , y_m \in X,$$

entonces

$$\begin{aligned} h(p \cdot q) &= h(x_1 x_2 \ldots x_n y_1 y_2 \ldots y_m) \\ &= f(x_1) * \ldots * f(x_n) * f(y_1) * \ldots * f(y_m) \end{aligned}$$

$$= h(p) * h(q).$$

Además, si

$$p = x, \text{ con } x \in X,$$

vale

$$h(x) = f(x), \qquad \text{[def. de } h\text{]}$$

y por lo tanto h prolonga a f. ■

6.9 Ejercicios

E 6.9.1

Determinar si las siguientes aplicaciones definen una operación n-aria sobre A. En caso afirmativo, indicar su aridad.

(i) $A = I\!N,\ \ f((x, y)) = (x + y)^2$,

(ii) $A = Q^+,\ \ f((x, y)) = \sqrt{x + y}$. ¿Y si $A = I\!R^+$?,

(iii) $A = \{1, 2, 3\},\ \ f(x) = 3$. ¿Y si $A = \{1, 2\}$?,

(iv) $A = Antisim(X),\ \ f((R_1, R_2)) = R_1 \cup R_2$,

(v) $A = M_{2\times 3}(I\!R),\ \ f(X, Y, Z) = (2X + Y) \cdot Z$.¿Y si $A = M_2(I\!R)$?,

(vi) $A = I\!R^2,\ \ f((x, y), (z, t)) = \begin{cases} (e^x + t, z) & \text{si } x \leq 0 \\ (y, logx) & \text{si } x > 0 \end{cases}.$

E 6.9.2

Determinar si las siguientes álgebras de tipo 2 son semigrupos o semigrupos conmutativos. ¿Pueden ser transformados en semigrupos con unidad?. ¿Y en grupos?

(i) $\langle A, \circ\rangle$, donde $A = \{a, b\}$ y $\circ$ está dada por la tabla

$\circ$	a	b
a	a	a
b	b	b

(ii) $\langle \mathbb{R}_{>0}, * \rangle$, donde $x * y = \dfrac{x}{y}$,

(iii) $\langle \mathcal{P}(S), * \rangle$, donde $S \neq \emptyset$ y $*$ es la intersección de conjuntos,

(iv) $\langle \mathbb{N} \cup \{0\}, * \rangle$, donde $x * y = \max\{x, y\}$,

(v) $\langle \mathbb{Z}^* \times \mathbb{Z}, \circ \rangle$, donde $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, $(x, y) \circ (z, t) = (x \cdot z, y + t)$,

(vi) $\langle \mathbb{N} \cup \{0\}, \circ \rangle$, donde $x \circ y = \min\{x, y\}$,

(vii) $\langle \mathbb{R}^* \times \mathbb{R}, \circ \rangle$, donde $\mathbb{R}^* = \mathbb{R} - \{0\}$, $(a, b) \circ (c, d) = (a \cdot c, a \cdot d + b)$,

(viii) $\langle A, \cdot \rangle$, donde $A = \{x : \ x = 2^n, \, n \in \mathbb{Z}\}$ y $\cdot$ es el producto habitual.

E 6.9.3

Sean $\langle M, *, e \rangle \in \mathcal{S}_{\mathcal{U}}$, $\langle G, *, ', e \rangle \in \mathcal{G}$ y $\langle A, +, \cdot, -, 0 \rangle \in \mathcal{A}$. Probar que

(i) si $e_1 \in M$ verifica $x * e_1 = e_1 * x = x$, para todo $x \in M$, entonces $e = e_1$,

(ii) para todo x, y, $z \in G$,

- (a) si existe $w \in G$ que verifica $w * x = x * w = e$, entonces $w = x'$,
- (b) si $x * z = y * z$, entonces $x = y$ (ley de cancelación a derecha),
- (c) si $z * x = z * y$, entonces $x = y$ (ley de cancelación a izquierda),
- (d) $x'' = x$,
- (e) $(x * y)' = y' * x'$,

(iii) si a, $b \in A$, entonces

- (a) $a \cdot 0 = 0 \cdot a = 0$,
- (b) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$,
- (c) $(-a) \cdot (-b) = a \cdot b$.

E 6.9.4

(i) Sea $\langle \mathbb{Z}^3, +, (0, 0, 0) \rangle \in \mathcal{S}_{\mathcal{U}}$. Determinar si $T \lhd_{\mathcal{S}_{\mathcal{U}}} \mathbb{Z}^3$, donde

- (a) $T = \{(x, y, z) \in \mathbb{Z}^3 : x + y = 0\}$,

(b) $T = \{(x,y,z) \in \mathbb{Z}^3 : x = 0,\ z = 1\}$.

(ii) Dado el grupo simétrico $\mathcal{B}_3$, averiguar si $T \lhd_{\mathcal{G}} \mathcal{B}_3$, donde

(a) $T = \{f \in \mathcal{B}_3 : f(1) = 2\}$,

(b) $T = \{f \in \mathcal{B}_3 : f(1) = 1\}$.

(iii) Dado el anillo $\mathbb{R}$ de los números reales, determinar si $T \lhd_{\mathcal{A}} \mathbb{R}$, donde

(a) $T = \{x \in \mathbb{R} : x = q_1 + q_2\sqrt{2},\ q_1,\ q_2 \in \mathbb{Q}\}$,

(b) $T = \{x \in \mathbb{R} : x = \dfrac{m}{2},\ m \in \mathbb{Z}\}$.

E 6.9.5

Sea $\mathbb{Z}$ el grupo conmutativo de los enteros. Probar que

(i) si $n \in \mathbb{N}$ y $n \cdot \mathbb{Z} = \{x \in \mathbb{Z} : x = nz \ \textit{para algún}\ z \in \mathbb{Z}\}$, entonces $n \cdot \mathbb{Z} \lhd \mathbb{Z}$,

(ii) si $S \lhd \mathbb{Z}$ y $S \neq \{0\}$, entonces existe $n_0 \in \mathbb{N}$ tal que $S = n_0 \cdot \mathbb{Z}$.

E 6.9.6

(i) Dado el semigrupo $\langle \mathbb{Z}, \cdot \rangle$ y $X \subseteq \mathbb{Z}$, hallar $[X]_{\mathcal{S}}$, donde

(a) $X = \{1\}$,

(b) $X = \{-1, 2\}$.

(ii) Dado el grupo simétrico $\mathcal{B}_3$ y $X \subseteq \mathcal{B}_3$, hallar $[X]_{\mathcal{G}}$, donde

(a) $X = \{f \in \mathcal{B}_3 : f(3) = 3\}$,

(b) $X = \{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\}$.

(c) $X = \{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$.

Determinar, en cada caso, si X es un sistema de generadores.

E 6.9.7

Sean $\langle A, *, p\rangle \in \mathcal{S}_{\mathcal{U}}$ y $\langle B, \circ, d\rangle \in \mathcal{S}_{\mathcal{U}}$, donde $A = \{m, n, p\}, B = \{a, b, c, d\}$ y $*$, $\circ$ están dadas por las tablas

$*$	m	n	p
m	m	m	m
n	m	n	n
p	m	n	p

$\circ$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

Determinar en cada caso, si $h \in Hom_{\mathcal{S}_{\mathcal{U}}}(A, B)$, siendo

(i) $h(m) = a$, $h(n) = b$, $h(p) = d$. ¿Es h un isomorfismo?,

(ii) $h(m) = c$, $h(n) = b$, $h(p) = d$.

E 6.9.8

Determinar en cada caso, si

(i) $h \in Hom_{\mathcal{S}}(A, B)$, siendo

(a) $A = B = \langle M_2(\mathbb{R}), \cdot\rangle$ y $h(X) = X^{tr}$ ¿ Y si $A = B = \langle M_2(\mathbb{R}), +\rangle$?,

(b) $A = \langle \mathbb{Z}, +\rangle$, $B = \langle \mathbb{Z}, \cdot\rangle$ y

$$h(x) = \begin{cases} 1 & \text{si } x \text{ es par} \\ -1 & \text{si } x \text{ es impar} \end{cases},$$

(ii) $h \in Hom_{\mathcal{S}_{\mathcal{U}}}(A, B)$, siendo $A = \langle \mathbb{Z}, +, 0\rangle$, $B = \langle \mathbb{Z}, \cdot, 1\rangle$ y h definida como en el ejercicio 5.9.8 (i) (b).

(iii) $h \in Hom_{\mathcal{G}}(A, B)$, siendo

(a) $A = \langle \mathbb{R}_{>0}, \cdot, ^{-1}, 1\rangle$, $B = \langle \mathbb{R}, +, -, 0\rangle$ y $h(x) = log_2(x)$,

(b) $A = B = \langle \mathbb{R}, +, -, 0\rangle$ y $h(x) = x^3$.

Clasificar los homomorfismos hallados en monomorfismos, epimorfismos, isomorfismos, endomorfismos y automorfismos.

E 6.9.9

Sean $G_1, G_2 \in \mathcal{G}$. Probar que si $f : G_1 \longrightarrow G_2$ verifica $f(x \cdot y) = f(x) \cdot f(y)$, entonces $f \in Hom_{\mathcal{G}}(G_1, G_2)$.

E 6.9.10

Sean $\langle A, *, s\rangle$, $\langle B, \circ, r\rangle \in \mathcal{S}_{\mathcal{U}}$ y $h \in Hom_{\mathcal{S}_{\mathcal{U}}}(A, B)$.

(i) Determinar si $X = \{x \in A : h(x) = r\} \lhd_{\mathcal{S}_{\mathcal{U}}} A$.

(iii) Sea $c \in A$ tal que $c * c = s$. Determinar si $h(\{c, s\}) \lhd_{\mathcal{S}_{\mathcal{U}}} B$.

E 6.9.11

(i) Sean $\langle G, *, ', e\rangle \in \mathcal{G}$ y $R \in EQ(G)$. Probar que las siguientes condiciones son equivalentes:

  (a) $R \in Con_{\mathcal{G}}(G)$,

  (b) R es compatible con $*$.

(ii) Sea $\langle A, +, \cdot, -, 0\rangle \in \mathcal{A}$ y $R \in EQ(A)$. Probar que las siguientes condiciones son equivalentes:

  (a) $R \in Con_{\mathcal{A}}(A)$,

  (b) R es compatible con $+$ y $\cdot$.

E 6.9.12

Sea $\langle \mathbb{Z}, +, -, 0\rangle \in \mathcal{G}_a$. Dado $n \in \mathbb{N}$ fijo, sea $\equiv_n$ la relación definida sobre $\mathbb{Z}$ del siguiente modo:

$x \equiv_n y$ si, y sólo si, existe $k \in \mathbb{Z}$ tal que $x + (-y) = nk$.

Nota: La relación definida anteriormente se denomina congruencia módulo n.

(i) Probar que $\equiv_n \in Con_{\mathcal{G}_a}(\mathbb{Z})$.

(ii) Calcular los grupos $\langle \mathbb{Z}_2, +, -, 0\rangle$ y $\langle \mathbb{Z}_3, +, -, 0\rangle$.

E 6.9.13

(i) Sea $\langle \mathbb{Z}, +, \cdot, -, 0\rangle \in \mathcal{A}_{\mathcal{C}}$ y $n \in \mathbb{N}$ fijo. Probar que $\equiv_n \in Con_{\mathcal{A}_C}(\mathbb{Z})$.

(ii) Calcular los anillos $\langle \mathbb{Z}_3, +, \cdot, -, 0\rangle$ y $\langle \mathbb{Z}_4, +, \cdot, -, 0\rangle$.

E 6.9.14

Sea L un álgebra absolutamente libre (relativamente libre) que tiene a X como conjunto de generadores libres. Probar que si $Y \subseteq X$, entonces $L_0 = [Y]$ es un álgebra absolutamente libre (relativamente libre) que tiene a Y como conjunto de generadores libres.

E 6.9.15

Sea L un álgebra absolutamente libre (relativamente libre) que tiene a X como conjunto de generadores libres. Probar que $[X \setminus \{x\}] \neq L$ para todo $x \in X$.

E 6.9.16

Verificar que existe un álgebra A tal que:

(i) $A = [X]$,

(ii) $A \neq [X \setminus \{x\}]$ para todo $x \in X$,

y A no es libre.

E 6.9.17

Sea L un álgebra absolutamente libre (relativamente libre) que tiene a X y a Y como conjuntos de generadores libres. Probar que para toda $f : X \longrightarrow Y$ se verifica que $[f(X)]$ es el álgebra absolutamente libre (relativamente libre) que tiene a $f(X)$ como conjunto de generadores libres. Además si f es inyectiva, entonces $[f(X)] = L$.

E 6.9.18

Indicar un ejemplo de un álgebra L relativamente libre que tiene a X como conjunto de generadores libres y tal que existen $Y \subseteq L$, $f : X \longrightarrow Y$ inyectiva y sin embargo $[f(X)]$ no es relativamente libre.

Este ejemplo muestra que la hipótesis de que Y es un conjunto de generadores libres del ejercicio 6.9.17 no se puede eliminar.

7 Retículos distributivos y álgebras de Boole

7.1 La clase $\mathfrak{R}$ de los retículos

D 7.1.1 *Un álgebra* $\langle A, +, \cdot \rangle$ *de tipo* $(2, 2)$ *es un retículo si para todo* $x, y, z \in A$ *se verifican:*

(R1) $x + (y + z) = (x + y) + z$,

(R2) $x + y = y + x$,

(R3) $x + x = x$,

(R4) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,

(R5) $x \cdot y = y \cdot x$,

(R6) $x \cdot x = x$,

(R7) $x + (x \cdot y) = x$,

(R8) $x \cdot (x + y) = x$.

Representaremos con $\mathfrak{R}$ a la clase de los retículos.

T 7.1.1 *Sea* $\langle A, * \rangle$ *una banda. La relación* $\leq_*$ *definida por* $x \leq_* y$ *si, y sólo si,* $x * y = x$*, es una relación de orden sobre* A*.*

Dem.

(O1) $x \leq_* x$, para todo $x \in A$:

$x * x = x$, para todo $x \in A$. [A es banda]

(O2) $x \leq_* y$, $y \leq_* x$ implican $x = y$:

(1) $x = x * y$, [por la hipótesis]

(2) $y = y * x$, [por la hipótesis]

(3) $x * y = y * x$, [prop. conmutativa]

(4) $x = y$. [(1),(2),(3)]

(O3) $x \leq_* y$ e $y \leq_* z$, implican $x \leq_* z$:

(1) $x = x * y$, [por la hipótesis]

(2) $y = y * z$, [por la hipótesis]

(3) $x = x * (y * z)$, [(1),(2)]

$= (x * y) * z$

$= x * z$. [(1),(2)] ■

Nota. Si $\langle A, +, \cdot \rangle \in \mathfrak{R}$, entonces sobre A podemos definir dos órdenes inducidos por las operaciones $+$ y $\cdot$ respectivamente. Obtenemos así dos estructuras ordenadas:

(i) $\langle A, \leq_+ \rangle$, donde $x \leq_+ y \Leftrightarrow x = x + y$,

(ii) $\langle A, \leq_\cdot \rangle$, donde $x \leq_\cdot y \Leftrightarrow x = x \cdot y$.

T 7.1.2 *Sea* $\langle A, +, \cdot \rangle \in \mathfrak{R}$ *entonces* $\leq_\cdot^{op} = \leq_+$.

Dem.

(i) $\leq_\cdot^{op} \subseteq \leq_+$:

(1) $(x, y) \in \leq_\cdot^{op}$, [hipótesis]

(2) $(y, x) \in \leq_\cdot$, [(1) y def. de opuesta]

(3) $y = x \cdot y$, [(2) y def. de $\leq_\cdot$]

(4) $x + y = x + (x \cdot y)$ [(3) sumando x a ambos miembros]

$= x$, [R7]

(5) $(x, y) \in \leq_+$. [(4) y def. de $\leq_+$].

(ii) $\leq_+ \subseteq \leq_\cdot^{op}$:

La demostración es análoga a (i) y queda propuesta como ejercicio.

De (i) y (ii) resulta $\leq_\cdot^{op} = \leq_+$. ■

De lo expuesto todo retículo es un conjunto ordenado, por lo tanto la teoría de los retículos puede ubicarse dentro de la teoría de las estructuras ordenadas.

De ahora en adelante dado un retículo consideraremos únicamente el orden $\leq_\cdot = \leq_+^{op}$ y para abreviar escribiremos $\leq$ en lugar de $\leq_\cdot$, es decir

$x \leq y \Leftrightarrow x = x \cdot y \Leftrightarrow x + y = y.$

T 7.1.3 *Sea* $\langle A, +, \cdot \rangle \in \mathfrak{R}$. *Entonces* $(A, \leq)$ *es un conjunto ordenado retículo donde para todo* $a, b \in A$ *se verifican:*

(i) $inf\ \{a, b\} = a \cdot b$,

(ii) $sup\ \{a, b\} = a + b$.

Dem.

(i) Debemos probar que

(a) $a \cdot b \leq a$:

(1) $(a \cdot b) \cdot a = a \cdot (a \cdot b)$ [R5]

$= (a \cdot a) \cdot b$ [R4]

$= a \cdot b.$ [R6]

(b) $a \cdot b \leq b$:
Es análoga a la de (a).

(c) Si $z \in A$ es tal que $z \leq a$ y $z \leq b$ entonces $z \leq a \cdot b$:

(1) $z = z \cdot a,$ [por la hipótesis]

(2) $z = z \cdot b,$ [por la hipótesis]

(3) $z \cdot (a \cdot b) = (z \cdot a) \cdot b$ [R4]

$= z \cdot b$ [(1)]

$= z.$ [(2)]

De (a) y (b) resulta que $a \cdot b$ es cota inferior de $\{a, b\}$ y de (c) resulta que es la mayor de las cotas inferiores, luego (i) queda demostrado.

(ii) La demostración queda propuesta como ejercicio. ■

También se verifica el teorema recíproco.

T 7.1.4 *Sea $(A, \leq)$ un conjunto ordenado retículo. Si para todo $x, y \in A$ definimos:*

(i) $x + y = sup\ \{x, y\}$,

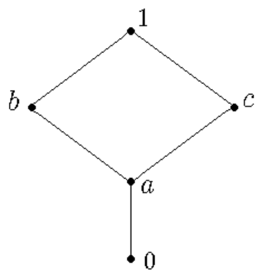
(ii) $x \cdot y = inf\ \{x, y\}$,

entonces $\langle A, +, \cdot \rangle \in \mathfrak{R}$.

Dem. Ejercicio. ■

Ejemplos

(i) Consideremos el conjunto ordenado cuyo diagrama de Hasse es el siguiente



$(A, \leq)$ es un conjunto ordenado retículo, luego por T 7.1.4 resulta que $\langle A, +, \cdot \rangle \in \mathfrak{R}$ donde $+$ y $\cdot$ están dadas por las tablas

$+$	0	a	b	c	1
0	0	a	b	c	1
a	a	a	b	c	1
b	0	b	b	1	1
c	c	c	1	c	1
1	1	1	1	1	1

$\cdot$	0	a	b	c	1
0	0	0	0	0	0
a	0	a	a	a	a
b	0	a	b	a	b
c	0	a	a	c	c
1	0	a	b	c	1

(ii) Sea $\langle A, +, \cdot \rangle \in \mathfrak{R}$, donde $A = \{a, b\}$ y las operaciones están dadas por las tablas

$+$	a	b
a	a	b
b	b	b

$\cdot$	a	b
a	a	a
b	a	b

Entonces por T 7.1.1,

$$\leq = \{(a,a),(a,b),(b,b)\}$$

y $(A,\leq)$ tiene el siguiente diagrama:

La clase $\mathfrak{R}_{\mathbf{0,1}}$ de los retículos con primer y último elemento

D 7.1.2 *Un álgebra* $\langle A,+,\cdot,0,1\rangle$ *de tipo* $(2,2,0,0)$ *es un* $(0,1)$*–retículo si verifica:*

(i) $\langle A,+,\cdot\rangle \in \mathfrak{R}$,

(ii) *para todo* $x \in A$*, valen:*

(R9) $x \cdot 0 = 0$,

(R10) $x + 1 = 1$.

Representaremos con $\mathfrak{R}_{\mathbf{0,1}}$ a la clase de los $(0,1)$–retículos.

Ya hemos visto que las nociones de conjunto ordenado retículo y retículo son equivalentes. Luego si A es un retículo finito, entonces $A \in \mathfrak{R}_{\mathbf{0,1}}$.

7.2 La clase $\mathfrak{D}$ de los retículos distributivos

D 7.2.1 $\langle A,+,\cdot\rangle \in \mathfrak{R}$ *es distributivo si para todo* $x,y,z \in A$ *se verifica:*

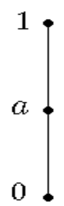
(D) $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$.

Representaremos con $\mathfrak{D}$ a la clase de los retículos distributivos.

Ejemplos

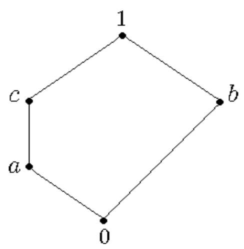
(i) Sea $X \neq \emptyset$ un conjunto arbitrario y $\mathcal{P}(X)$ el conjunto de las partes de X, entonces $\langle P(X), \cup, \cap \rangle \in \mathfrak{D}$.

(ii) Sea $A = \{0, a, 1\}$ el conjunto ordenado cuyo diagrama de Hasse es el siguiente:



Entonces, se puede verificar que $\langle A, +, \cdot \rangle$ es un retículo distributivo.

(iii) Sea $A = \{0, a, b, c, 1\}$ el conjunto ordenado cuyo diagrama es el siguiente:



Entonces $\langle A, +, \cdot \rangle$ es un retículo pero no es distributivo. En efecto:

$$c \cdot (a + b) = c \cdot 1 = c,$$

$$(c \cdot a) + (c \cdot b) = a + 0 = a.$$

Luego $c \cdot (a + b) \neq (c \cdot a) + (c \cdot b)$.

Dado un retículo verificar, por medio de tablas, si es o no distributivo es un proceso computacionalmente largo.

Nosotros vamos a indicar para los retículos finitos un método simple para determinar si se cumple o no la ley distributiva.

7.3 Elementos irreducibles, primos y átomos

D 7.3.1 *Sea* $\langle A, +, \cdot, 0, 1\rangle \in \mathfrak{R}_{\mathbf{0,1}}$ *y* $a \in A$. *Diremos que*

(i) *a es irreducible si:*

(I1) $a \neq 0$,

(I2) *la hipótesis* $a = x + y$, *implica* $a = x$ *ó* $a = y$.

(ii) *a es primo si:*

(P1) $a \neq 0$,

(P2) *la hipótesis* $a \leq x + y$, *implica* $a \leq x$ *ó* $a \leq y$.

(iii) *a es átomo si:*

(A1) $a \neq 0$,

(A2) *las hipótesis* $b \in A$ *y* $0 \leq b \leq a$ *implican* $b = 0$ *o* $b = a$.

Con $Ir(A)$, $Pr(A)$ y $\Pi(A)$ indicaremos al conjunto de los elementos irreducibles, primos y átomos de A respectivamente.

A continuación vamos a indicar métodos para determinar elementos irreducibles y primos de $\langle A, +, \cdot, 0, 1\rangle \in \mathfrak{R}_{\mathbf{0,1}}$

Método para determinar los elementos irreducibles

Dado $a \in A$, $a \neq 0$:

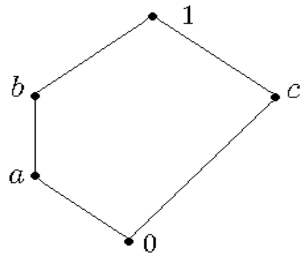
(1) considerar el conjunto $L_i(a) = \{x \in A : x < a\}$,

(2) determinar si $L_i(a)$ tiene último elemento,

(3) si el paso (2) es afirmativo, a es irreducible.

Ejemplo

Sea $\langle A, +, \cdot, 0, 1\rangle \in \mathfrak{R}_{\mathbf{0,1}}$, cuyo diagrama se indica a continuación



$L_i(a) = \{0\}$, su diagrama de Hasse es

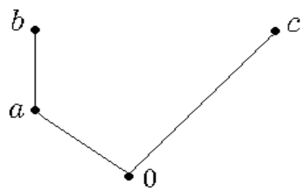
Luego, a es irreducible.

$L_i(b) = \{0\}$, es análogo al caso anterior. Luego, b es irreducible.

$L_i(c) = \{0, a\}$, su diagrama es

Luego, c es irreducible.

$L_i(1) = \{0, a, b, c\}$, su diagrama es



Entonces 1 no es irreducible.

Por lo tanto $Ir(A) = \{a, b, c\}$.

Método para determinar los elementos primos

Dado $a \in A,\ a \neq 0$:

(1) considerar el conjunto $T_s(a) = \{x \in A : a \leq x\}$,

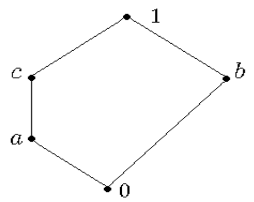
(2) calcular $A \setminus T_s(a)$,

(3) determinar si $A \setminus T_s(a)$ tiene último elemento,

(4) si el paso (3) es afirmativo, a es primo.

Ejemplo

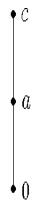
Sea $\langle A, +, \cdot, 0, 1\rangle \in \mathfrak{R}_{\mathbf{0,1}}$, cuyo diagrama se indica a continuación



$T_s(a) = \{a, c, 1\}$, $A \setminus T_s(a) = \{0, b\}$ y su diagrama es

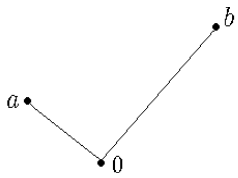
Por lo tanto a es primo.

$T_s(b) = \{b, 1\}$, $A \setminus T_s(b) = \{0, a, c\}$ y su diagrama es



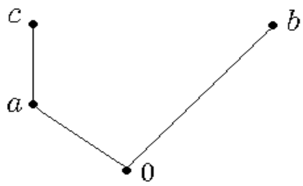
Luego, b es primo.

$T_s(c) = \{c, 1\}$, $A \setminus T_s(c) = \{0, a, b\}$ y su diagrama es



Entonces, c no es primo.

$T_s(1) = \{1\}$, $A \setminus T_s(1) = \{0, a, b, c\}$ y su diagrama es



Luego, 1 no es primo.

Entonces $Pr(A) = \{a, b\}$.

T 7.3.1 *Si* $\langle A, +, \cdot, 0, 1\rangle \in \mathfrak{R}_{\mathbf{0,1}}$ *es, entonces* $Pr(A) \subseteq Ir(A)$.

Dem. Sea

(1) $a \in Pr(A)$, [hipótesis]

entonces

(I1) $a \neq 0$. [(1)]

(I2) Supongamos que

(2) $a = x + y$,

(3) $x \leq a$, [(2), $a = sup\{x, y\}$]

(4) $y \leq a$, [(2), $a = sup\{x, y\}$]

(5) $a \leq x + y$, [(2)]

(6) $a \leq x$ o $a \leq y$, [(5),(1)]

(7) $a = x$ o $a = y$. [(3),(4),(6)] ■

La otra inclusión sólo vale para retículos distributivos, más precisamente se verifica:

T 7.3.2 *Sea* $\langle A, +, \cdot, 0, 1\rangle \in \mathfrak{R}_{\mathbf{0,1}}$ *finito. Entonces las siguientes condiciones son equivalentes:*

(i) $A \in \mathfrak{D}_{\mathbf{0,1}}$,

(ii) $Pr(A) = Ir(A)$.

El resultado anterior, aunque no lo vamos a demostrar, muestra la importancia de los elementos irreducibles y primos en los retículos finitos y proporciona un método más rápido para saber si un retículo finito es distributivo o no.

7.4 La clase $\mathfrak{B}$ de las álgebras de Boole

Elementos booleanos

D 7.4.1 *Sea* $A \in \mathfrak{R}_{\mathbf{0,1}}$ *y* $a \in A$. *Diremos que:*

(i) $b \in A$ *es un complemento de* a *si se verifican:*

$$a + b = 1,$$

$$a \cdot b = 0.$$

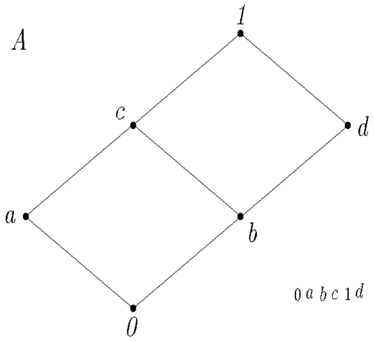
(ii) a *es booleano si tiene complemento.*

Representaremos con $B(A)$ al conjunto de los elementos booleanos de A.

Ejemplos

(i)

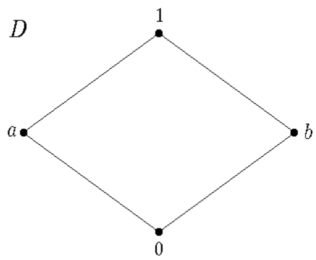
x	complemento de x
0	1
a	d
b	–
c	–
d	a
1	0



$B(A) = \{0, a, d, 1\}$.

(ii)

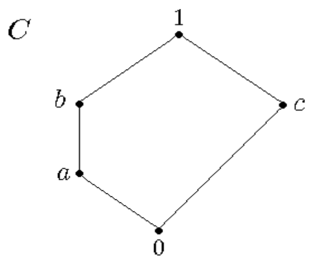
x	complemento de x
0	1
a	b
b	a
1	0



$B(D) = D$.

(iii)

x	complemento de x
0	1
a	c
b	c
c	a, b
1	0



$B(C) = C$.

T 7.4.1 *Si* $A \in \mathfrak{D}_{\mathbf{0,1}}$ *y* $a \in A$ *es booleano, entonces* a *tiene un único complemento.*

Dem. Sean $b_1, b_2 \in A$ tales que

(1) b_1, b_2 son complementos de a, [hipótesis]

entonces

(2) $b_1 + a = 1 = b_2 + a$,

$b_1 \cdot a = 0 = b_2 \cdot a$, [(1)]

(3) $b_1 = b_2$. [(2) y ley del corte]■

En lo que sigue si $A \in \mathfrak{D}_{\mathbf{0,1}}$ y $a \in A$ es booleano, denotaremos con a' o $-a$ al complemento de a.

D 7.4.2 *Sea $A \in \mathfrak{D}_{\mathbf{0,1}}$. Si $B(A) = A$, diremos que A es un retículo booleano.*

Es claro que la familia de los retículos booleanos constituyen una subclase de $\mathfrak{D}_{\mathbf{0,1}}$, donde las álgebras de esta subclase no están definidas por axiomas que son *igualdades*. Sin embargo, existen ciertas álgebras, llamadas álgebras de Boole, que son definibles por *igualdades* y que son *equivalentes* a los retículos booleanos.

D 7.4.3 *Un álgebra $\langle A, +, \cdot, ', 0, 1\rangle$ de tipo $(2, 2, 1, 0, 0)$ es un álgebra de Boole si:*

(i) *el reducto $\langle A, +, \cdot, 0, 1\rangle \in \mathfrak{D}_{\mathbf{0,1}}$,*

(ii) *para todo $x \in A$, se verifican*

(B1) $x \cdot x' = 0$,

(B2) $x + x' = 1$.

Representaremos con $\mathfrak{B}$ a la clase de las álgebras de Boole.

Ejemplos

(i) Sea X un conjunto no vacío. Sabemos que $\langle \mathcal{P}(X), \cup, \cap, \emptyset, X\rangle \in \mathfrak{D}_{\mathbf{0,1}}$. Para cada $A \in \mathcal{P}(X)$, sea $\mathcal{C}(A)$ el complemento de A en X. Entonces se verifican:

(1) $A \cap \mathcal{C}(A) = \emptyset$,

(2) $A \cup \mathcal{C}(A) = X$.

Luego $\langle \mathcal{P}(X), \cup, \cap, \mathcal{C}, \emptyset, X\rangle \in \mathfrak{B}$. Esta álgebra se denomina *álgebra de Boole de conjuntos.*

Este ejemplo es muy importante pues se puede demostrar que toda álgebra de Boole finita es isomorfa a un álgebra de Boole de conjuntos.

(ii) Sea B el retículo distributivo indicado en la figura

entonces $0' = 1$ y $1' = 0$. Luego $B \in \mathfrak{B}$ y la denotaremos $\mathbb{B}_1$.

Ahora probaremos que en el álgebra $\langle \mathcal{P}(X), \cup, \cap, \mathcal{C}, \emptyset, X\rangle$ lo único relevante es la cardinalidad de X y no *la naturaleza* de sus elementos. Más precisamente,

T 7.4.2 *Sean X e Y dos conjuntos no vacíos y $f : X \longrightarrow Y$ una biyección. Entonces $\langle \mathcal{P}(X), \cup, \cap, \mathcal{C}, \emptyset, X\rangle$ y $\langle \mathcal{P}(Y), \cup, \cap, \mathcal{C}, \emptyset, Y\rangle$ son álgebras isomorfas.*

Dem. Consideremos $F^* : \mathcal{P}(Y) \longrightarrow \mathcal{P}(X)$ definida por $F^*(A) = f^{-1}(A)$, para cada $A \in \mathcal{P}(Y)$ y veamos que

(i) F^* es inyectiva: Sean $A, B \in \mathcal{P}(Y)$ y supongamos que

(1) $F^*(A) = F^*(B)$, [hip.]

(2) $f^{-1}(A) = f^{-1}(B)$, [(1)]

(3) $f(f^{-1}(A)) = f(f^{-1}(B))$, [(2)]

(4) $A = B$. [(3), f sobreyectiva]

(ii) F^* es sobreyectiva: Sea

(1) $C \in \mathcal{P}(X)$, [hip.]

(2) $f(C) \in \mathcal{P}(Y)$, [(1)]

(3) $C = f^{-1}(f(C))$, [f inyectiva]

(4) $C = F^*(D)$ con $D = f(C) \in \mathcal{P}(Y)$. [(3), (2)]

(iii) F^* es homomorfismo: Es consecuencia inmediata de las propiedades de F^* vistas en el Capítulo 2. ■

Congruencias booleanas

En esta sección describiremos el conjunto de las congruencias booleanas de un álgebra A por medio de la familia de los filtros de A.

D 7.4.4 *Sea $A \in \mathbf{\mathfrak{B}}$. Diremos que $F \subseteq A$ es un filtro de A si verifica las siguientes condiciones:*

(F1) $1 \in F$,

(F2) *si* $x, y \in F$, *entonces* $x \cdot y \in F$,

(F3) *si* $x \in F$ *y* $x \leq y$, *entonces* $y \in F$.

Representaremos con $\mathcal{F}(A)$ a la familia de todos los filtros de A. Observemos que para toda $A \in \mathbf{\mathfrak{B}}$ se verifica que $\mathcal{F}(A) \neq \emptyset$, ya que $\{1\}$, $A \in \mathcal{F}(A)$.

T 7.4.3 *Si $A \in \mathbf{\mathfrak{B}}$ y $F \in \mathcal{F}(A)$, entonces*

$$R(F) = \{(x, y) \in A \times A : \textit{ existe } f \in F \textit{ tal que } x \cdot f = y \cdot f\}$$

es una congruencia de A.

Dem. En primer lugar veamos que

(i) $R(F) \in EQ(A)$.

(a) $R(F)$ es reflexiva: Como $F \neq \emptyset$, entonces para todo $x \in A$, $\ x \cdot f = x \cdot f$ cualquiera sea $f \in F$.

(b) $R(F)$ es simétrica: Inmediata.

(c) $R(F)$ es transitiva: Si

(1) $(x, y) \in R(F)$, [hip.]

(2) $(y, z) \in R(F)$, [hip.]

entonces

(3) existe $f_1 \in F$ tal que $x \cdot f_1 = y \cdot f_1$, [(1)]

(4) existe $f_2 \in F$ tal que $y \cdot f_2 = z \cdot f_2$, [(2)]

(5) $x \cdot (f_1 \cdot f_2) = y \cdot (f_1 \cdot f_2)$, [(3), R4]

(6) $y \cdot (f_1 \cdot f_2) = z \cdot (f_1 \cdot f_2)$ [(4), R4, R5]

(7) $f_1 \cdot f_2 = f \in F$ [F filtro, $f_1, f_2 \in F$]

(8) existe $f \in F$ tal que $\ x \cdot f = z \cdot f$, [(7), (5), (6)]

(9) $(x, z) \in R(F)$. [(8)]

Además,

(ii) $R(F)$ es compatible con $\cdot$: Sean

(1) $(x, y) \in R(F)$, [hip.]

(2) $(z, w) \in R(F)$, [hip.]

entonces

(3) existe $f_1 \in F$ tal que $x \cdot f_1 = y \cdot f_1$, [(1)]

(4) existe $f_2 \in F$ tal que $z \cdot f_2 = w \cdot f_2$, [(2)]

(5) $f = f_1 \cdot f_2 \in F$, [F filtro, $f_1, f_2 \in F$]

(6) existe $f \in F$ tal que $(x \cdot z) \cdot f = (y \cdot w) \cdot f$, [(3), (4), (5), R4, R5]

(7) $(x \cdot z, y \cdot w) \in R(F)$. [(6)]

(iii) $R(F)$ es compatible con $'$: Sea

(1) $(x, y) \in R(F)$, [hip.]

entonces

(2) existe $f \in F$ tal que $x \cdot f = y \cdot f$, [(1)]

(3) $x' + f' = y' + f'$, [(2)]

(4) existe $f \in F$ tal que

$$
\begin{aligned}
x' \cdot f &= (x' \cdot f) + (f' \cdot f) \\
&= (x' + f') \cdot f && [\mathrm{D},\ f' \cdot f = 0] \\
&= (y' + f') \cdot f, && [(3)] \\
&= (y' \cdot f) + (f' \cdot f), && [\mathrm{D}] \\
&= y' \cdot f,
\end{aligned}
$$

(5) existe $f \in F$ tal que $x' \cdot f = y' \cdot f$, [(4)]

(6) $(x', y') \in R(F)$. [(4), (5)]□

T 7.4.4 *Sea* $A \in \mathfrak{B}$ *y* $R \in Con(A)$*. Entonces* $1_R = \{x \in A : (x, 1) \in R\} \in \mathcal{F}(A)$.

Dem. Debemos probar que:

(F1) $1 \in 1_R$: Inmediato pues $(1, 1) \in R$, [R ref.]

(F2) Sean

(1) $x \in 1_R$, [hip.]

(2) $y \in 1_R$, [hip.]

entonces

(3) $(x, 1) \in R$, [(1)]

(4) $(y, 1) \in R$, [(2)]

(5) $(x \cdot y, 1) \in R$, [(3), (4), $R \in Con(A)$]

(6) $x \cdot y \in 1_R$, [(5)]

(F3) Si

(1) $x \in 1_R$, [hip.]

(2) $x \leq y$, [hip.]

entonces

(3) $(x, 1) \in R$, [(1)]

(4) $(x + y, 1 + y) \in R$, [(3), $R \in Con(A)$]

(5) $(x + y, 1 + y) = (y, 1)$, [(2)]

(6) $y \in 1_R$, [(5)]□

T 7.4.5 *Sea $A \in \mathfrak{B}$. Entonces $Con(A) = \{R(F) : F \in \mathcal{F}(A)\}$.*

Dem.

(i) $\{R(F) : F \in \mathcal{F}(A)\} \subseteq Con(A)$: es consecuencia directa de T 7.4.3.

(ii) $Con(A) \subseteq \{R(F) : F \in \mathcal{F}(A)\}$: Sea

(1) $T \in Con(A)$ [hip.]

entonces

(2) $1_T \in \mathcal{F}(A)$. [(1), T7.4.4]

(3) $R(1_T) = T$.

En efecto,

(a) $R(1_T) \subseteq T$:

(4) $(x, y) \in R(1_T)$, [hip.]

(5) existe $f \in 1_T$ tal que $x \cdot f = y \cdot f$, [(4), (2), T7.4.3]

(6) $(f, 1) \in T$, [(5)]

(7) $(x \cdot f, x) \in T$, [(6), (1)]

(8) $(y \cdot f, y) \in T$, [(6), (1)]

(9) $(x, y) \in T$, [(7), (8), (1)]

(b) $T \subseteq R(1_T)$:

(10) $(x, y) \in T$, [hip.]

(11) $(x + y', 1) \in T$, [(10), (1)]

$$
\begin{array}{lll}
(12) & (y+x',1) \in T, & [(10),\ (1)] \\
(13) & ((x+y')\cdot(y+x'),1) \in T, & [(11),\ (12),\ (1)] \\
(14) & f = (x+y')\cdot(y+x') \in 1_T, & [(13)] \\
(15) & x\cdot f = x\cdot(x+y')\cdot(y+x') & \\
 & \qquad = x\cdot(y+x') & [\mathrm{R8}] \\
 & \qquad = x\cdot y & [\mathrm{D}] \\
(16) & y\cdot f = y\cdot(x+y')\cdot(y+x') & [(14)] \\
 & \qquad = y\cdot x, & [\mathrm{R8,\ D}] \\
(17) & (x,y) \in R(1_T). & [(14),\ (15),\ (16),\ \mathrm{T7.4.3}]\square
\end{array}
$$

Notas.

(i) De lo expuesto resulta que para hallar todas la congruencias de un álgebra de Boole A podemos proceder de la siguiente manera:

(1) determinamos todos los subconjuntos de A que son filtros,

(2) para cada filtro F de A hallamos $R(F) = \{(x,y) \in A \times A :$ existe $f \in F$ tal que $x \cdot f = y \cdot f\}$.

(ii) En la sección siguiente referida a las álgebras de Boole finitas, aplicaremos el método anterior a un ejemplo concreto.

(iii) Si $A \in \mathcal{B}$ y $F \in \mathcal{F}(A)$, entonces por T 7.4.5 el álgebra cociente $A/R(F)$ es un álgebra de Boole que notaremos A/F.

7.5 Algebras de Boole finitas

Congruencias

T 7.5.1 *Sean A un álgebra de Boole finita y $F \subseteq A$. Entonces las siguientes condiciones son equivalentes:*

(i) $F \in \mathcal{F}(A)$,

(ii) *existe $a \in A$ tal que $F = [a)$, donde $[a) = \{x \in A : a \leq x\}$.*

Dem. (i) $\Longrightarrow$ (ii): Sea

(1) $F = \{f_1, f_2, ..., f_k\}$, [$A$ finita]

(2) $a = f_1 \cdot f_2 \cdot ... \cdot f_k \in F$. [(1), (i)]

Veamos que $F = [a)$. En efecto,

(a) $F \subseteq [a)$: sea

(3) $f \in F$, [hip.]

(4) $a \leq f$, [(2), (3)]

(5) $f \in [a)$. [(4)]

(b) $[a) \subseteq F$: sea

(6) $x \in [a)$, [hip.]

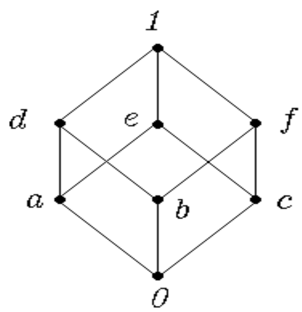
(7) $a \leq x$, [(6)]

(8) $x \in F$. [(2), (7), (i)]

(ii) $\Longrightarrow$ (i): Ejercicio. $\square$

Ejemplo

Sea A el álgebra de Boole indicada en la figura



Entonces $\mathcal{F}(A) = \{[0), [a), [b), [c), [d), [e), [f), [1)\}$, donde

$$
\begin{aligned}
&[0) = A, && A/[0) = A,\\
&[a) = \{a, d, e, 1\}, && A/[a) = \{\{0, b, c, f\}, \{a, d, e, 1\}\},\\
&[b) = \{b, d, f, 1\}, && A/[b) = \{\{0, a, c, e\}, \{b, d, f, 1\}\},\\
&[c) = \{c, e, f, 1\}, && A/[c) = \{\{0, a, b, d\}, \{c, e, f, 1\}\},\\
&[d) = \{d, , 1\}, && A/[d) = \{\{0, c\}, \{a, e\}, \{b, f\}, \{d, 1\}\},\\
&[e) = \{e, 1\}, && A/[e) = \{\{0, b\}, \{a, d\}, \{c, f\}, \{e, 1\}\},\\
&[f) = \{f, 1\}, && A/[f) = \{\{0, a\}, \{b, d\}, \{c, e\}, \{f, 1\}\},\\
&[1) = \{1\}, && A/[1) = \{\{0\}, \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{f\}, \{1\}\} \simeq A.
\end{aligned}
$$

A continuación veremos que en las álgebras de Boole finitas los *átomos* desempeñan un papel análogo al de las bases en los espacios vectoriales.

T 7.5.2 *Sean* $A \in \mathfrak{R}_\mathbf{0}$ *y* $a \in A$. *Entonces las siguientes condiciones son equivalentes:*

(i) a *es un átomo de* A,

(ii) a *verifica:*

> (a) $a \neq 0$,
>
> (b) *para cada* $x \in A$, $a \cdot x = 0$ *ó* $a \cdot x = a$.

Dem. (i) $\Longrightarrow$ (ii):

(a) Es consecuencia directa de la hipotésis.

(b) (1) $0 \leq a \cdot x \leq a$, [0 primer elemento de A y $a \cdot x = inf\ \{x, a\}$]

(2) $a \cdot x = 0$ ó $a \cdot x = a$. [(1),(i)]

(ii) $\Longrightarrow$ (i):

(A1) Es consecuencia directa de (a).

(A2) Sea $b \in A$ tal que

(1) $0 \leq b \leq a$, [hipótesis]

entonces

(2) $b = a \cdot b,$ [(1)]

(3) $a \cdot b = 0$ ó $a \cdot b = a,$ [(b)]

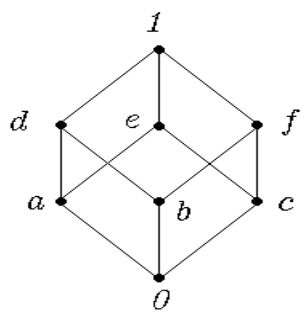
(4) $b = 0$ ó $b = a.$ [(2),(3)] ■

Sea A un álgebra de Boole finita y $x \in A$, entonces indicaremos con Π_x al conjunto

$$\Pi_x = \begin{cases} \emptyset, & \text{si } x = 0 \\ \{a \in \Pi(A) : a \leq x\}, & \text{en otro caso} \end{cases}.$$

Ejemplo

x	Π_x
0	$\emptyset$
a	$\{a\}$
b	$\{b\}$
c	$\{c\}$
d	$\{a,b\}$
e	$\{a,c\}$
f	$\{b,c\}$
1	$\Pi(A)$



T 7.5.3 *Sea A un álgebra de Boole finita y $x \in A$, $x \neq 0$, entonces $\Pi_x \neq \emptyset$.*

Dem.

(i) Si $x \in \Pi(A)$, entonces $x \in \Pi_x$. [$x \leq x$]

Luego $\Pi_x \neq \emptyset$.

(ii) Si $x \notin \Pi(A)$, existe $x_1 \in A$ tal que

(1) $x_1 \cdot x \neq 0$ y $x_1 \cdot x \neq x,$ [T 7.5.2]

(2) $0 < x_1 \cdot x < x.$ [(1) y $x_1 \cdot x = inf\ \{x_1, x\}$]

Si

(3) $x_1 \cdot x \in \Pi(A)$,

entonces

(4) $x_1 \cdot x \in \Pi_x$, [(2),(3)]

(5) $\Pi_x \neq \emptyset$. [(4)]

Si

(6) $x_1 \cdot x \notin \Pi(A)$, se repite el razonamiento a partir de (ii).

Como A es finita el proceso concluye en un número finito de pasos y el elemento obtenido pertenece a Π_x.

Luego $\Pi_x \neq \emptyset$. ■

T 7.5.4 *Si A es un álgebra de Boole finita, entonces para todo $x \in A$, $x \neq 0$ se verifica que $x = \sum\limits_{a \in \Pi_x} a$.*

Dem. Como $x \neq 0$, por T 7.5.3 tenemos que $\Pi_x \neq \emptyset$. Además, por la hipótesis, Π_x es finito. Sean

(1) $\Pi_x = \{a_1, \ldots, a_k\}$,

(2) $y = a_1 + a_2 + \ldots + a_k$,

y probemos que $y = x$. En efecto,

(a) $y \leq x$:

(3) $a_j \leq x$, para todo j, $1 \leq j \leq k$, [(1)]

(4) $sup\{a_1, \ldots, a_k\} \leq x$, [(3)]

(5) $a_1 + \ldots + a_k \leq x$. [(4)]

De (2) y (5) resulta (a).

(b) $x \leq y$:

(6) $x = x \cdot 1$ [$x \leq 1$, para todo $x \in A$]

$= x \cdot (y + y')$ [def. de complemento]

$= (x \cdot y) + (x \cdot y')$. [prop. distributiva]

Si suponemos $x \cdot y' \neq 0$, entonces

(7) existe $a \in \Pi(A)$, $a \leq x \cdot y'$, [por T 7.5.3]

(8) $x \cdot y' \leq y'$,

(9) $x \cdot y' \leq x$,

(10) $a \leq y'$, [(7), (8)]

(11) $a \leq x$, [(7),(9)]

(12) $a \in \Pi_x$, [(7),(11)]

(13) $a \leq y$, [(12),(1),(2)]

(14) $a \leq y \cdot y'$, [(10),(13)]

(15) $a = 0$, absurdo. [(14)]

Por lo tanto

(16) $x \cdot y' = 0$.

Entonces

(17) $x = x \cdot y$, [(6),(16)]

de donde resulta $x \leq y$.

De (a) y (b) resulta $x = \sum_{a \in \Pi_x} a$. ■

Nota. El T 7.5.4 expresa que, en las álgebras de Boole finitas todo elemento distinto de cero es la suma de los átomos que lo preceden, lo que significa que conociendo los átomos se pueden determinar todos sus elementos. Es decir, $\Pi(A)$ es la *información mínima* que se debe tener para conocer todos los elementos de un álgebra de Boole finita.

T 7.5.5 *Si A es un álgebra de Boole finita y no trivial, entonces:*

(i) $\Pi(A) \neq \emptyset$,

(ii) $\sum\limits_{a \in \Pi(A)} a = 1$.

Dem.

(i) Como $|A| > 1$, existe $x \in A$, $x \neq 0$ y por T 7.5.3, $\Pi_x \neq \emptyset$. Luego, $\Pi(A) \neq \emptyset$.

(ii) Como $1 \neq 0$,

(1) $1 = \sum\limits_{a \in \Pi_1} a$. [por T 7.5.4]

Además,

(2) $\Pi(A) = \Pi_1$.

En efecto,

(a) $\Pi_1 \subseteq \Pi(A)$, [def. de Π_1]

(b) $\Pi(A) \subseteq \Pi_1$. [$a \leq 1$]

Entonces, $\sum\limits_{a \in \Pi(A)} a = 1$. [(1),(2)] ■

Teoremas de representación

Ahora demostraremos el resultado más importante de esta sección.

T 7.5.6 *Si A un álgebra de Boole finita, entonces A y $\mathcal{P}(\Pi(A))$ son álgebras isomorfas.*

Dem. Sea $f : A \longrightarrow \mathcal{P}(\Pi(A))$ definida por $f(x) = \Pi_x$, para cada $x \in A$. Veamos que:

(i) f es inyectiva.

Si $x_1, x_2 \in A$ y

(a) (1) $f(x_1) = f(x_2) = \emptyset$,

entonces

(2) $x_1 = x_2 = 0$. [(1) y def. de f]

(b) (3) $f(x_1) = f(x_2) \neq \emptyset$,

entonces

(4) $\Pi_{x_1} = \Pi_{x_2}$, [(3) y def. de f]

(5) $\sum_{a \in \Pi_{x_1}} a = \sum_{a \in \Pi_{x_1}} a$, [(4)]

(6) $x_1 = x_2$. [(5) y T 7.5.4]

De (a) y (b) resulta (i).

(ii) f es sobre.

Sea $X \in \mathcal{P}(\Pi(A))$,

(a) si $X = \emptyset$, entonces $f(0) = \emptyset$.

(b) si $X \neq \emptyset$, entonces como A es finita, X es finito,

(1) $X = \{a_1, \dots, a_k\}$,

(2) $y = a_1 + \cdots + a_k$.

Probaremos ahora que $\Pi_y = X$. En efecto, sea

(3) $b \in \Pi_y$,

entonces

(4) $b \leq y$, [por def. de Π_y]

(5) $b \cdot y = b$, [(4)]

(6) $b \cdot y = b \cdot (a_1 + \ldots + a_k)$ [(2)]

$= (b \cdot a_1) + \ldots + (b \cdot a_k).$

Si

(7) $b \neq a_i, \quad 1 \leq i \leq k,$

entonces

(8) $b \cdot a_i = 0, \quad 1 \leq i \leq k,$ [(7) y Ej.7.6.9(i)]

(9) $b \cdot y = 0,$ [(6),(8)]

(10) $b = 0.$

Luego, para algún $i, \quad 1 \leq i \leq k$, se verifica [de (5) y (9)]

(11) $b = a_i,$

(12) $b \in X,$ [(11),(1)]

(13) $\Pi_y \subseteq X,$ [(3),(12)]

(14) $X \subseteq \Pi_y.$ [(1),(2)]

Es claro que $f(y) = X$, y por lo tanto f es sobre.

(iii) $f(0) = \emptyset$.

Inmediata por la definición de f.

(iv) $f(x \cdot y) = f(x) \cap f(y)$.

Teniendo en cuenta la definición de f debemos verificar que $\Pi_{x \cdot y} = \Pi_x \cap \Pi_y$. En efecto,

$$
\begin{aligned}
a \in \Pi_{x \cdot y} &\Leftrightarrow a \leq x \cdot y \\
&\Leftrightarrow a \leq x,\ a \leq y \\
&\Leftrightarrow a \in \Pi_x \cap \Pi_y.
\end{aligned}
$$

(v) $f(x') = \mathcal{C}f(x)$.

Debemos probar que $\Pi_{x'} = \mathcal{C}\Pi_x$.

(a) $\Pi_{x'} \subseteq \mathcal{C}\Pi_x$:

Sea

(1) $a \in \Pi_{x'}$, [hip.]

(2) $a \leq x'$. [(1)]

Si suponemos que

(3) $a \leq x$,

entonces

(4) $a \leq x \cdot x'$, [(2),(3)]

(5) $a = 0$, absurdo. [(4)]

Luego

(6) $a \nleq x$,

(7) $a \notin \Pi_x$, [(6)]

(8) $a \in \mathcal{C}\Pi_x$, [(7)]

(b) $\mathcal{C}\Pi_x \subseteq \Pi'_x$:

Sea $a \in \Pi(A)$ tal que

(1) $a \in \mathcal{C}\Pi_x$, [hip.]

(2) $a \nleq x$. [(1)]

(3) $a \leq 1 = x + x'$.

(4) $a \leq x'$, [(2),(3), Ej. 7.6.9(ii)]

(5) $a \in \Pi_{x'}$. [(4)]

De (i) a (v) y el ejercicio 7.6.18 resulta que f es un isomorfismo. ■

Los dos teoremas siguientes, son consecuencia inmediata del T 7.5.6

T 7.5.7 *Si A es un álgebra de Boole finita tal que $|\Pi(A)| = n$, entonces $|A| = 2^n$.*

Dem. Es consecuencia directa de T 7.5.6, teniendo en cuenta que $|\mathcal{P}(\Pi(A))| = 2^n$. ■

D 7.5.1 *Sea $\{A_i\}_{1\leq i\leq n}$ una familia de álgebras de Boole y $A = \prod_{i=1}^{n} A_i$. Dados $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in A$ definimos*

$$x + y = (x_1 + y_1, \ldots, x_n + y_n),$$

$$x \cdot y = (x_1 \cdot y_1, \dots, x_n \cdot y_n),$$

$$x' = ({x_1}', {x_2}', \dots, {x_n}'),$$

$$\mathbb{O} = (0, 0, \dots, 0),$$

$$\mathbb{I} = (1, 1, \dots, 1).$$

Entonces $\langle \prod_{i=1}^{n} A_i, +, \cdot, ', \mathbb{O}, \mathbb{I} \rangle$ *es un álgebra de Boole que se denomina álgebra producto de las álgebras* A_i, $1 \leq i \leq n$.

Si $A_1 = A_2 = \dots = A_n = A$, *entonces* $\prod_{i=1}^{n} A_i$ *se nota* A^n.

T 7.5.8 *Sea* A *un álgebra de Boole finita tal que* $|\Pi(A)| = n$. *Entonces* A *y* $\mathbb{B}_1^n$ *son álgebras isomorfas.*

Dem. Como $A \simeq \mathcal{P}(\Pi(A))$ y $\mathbb{B}_1^n \simeq \mathcal{P}(\Pi(\mathbb{B}_1^n))$, para completar la demostración es suficiente probar que $\Pi(\mathbb{B}_1^n)$ tiene n elementos y aplicar T 7.4.2 y T 7.5.6.

Ahora probaremos que $\Pi(\mathbb{B}_1^n) = \{e_1, e_2, \dots, e_n\}$ donde $e_i = (x_{ij})$ con $x_{ij} = 1$ si $i = j$ y $x_{ij} = 0$ en caso contrario. En efecto, es claro que $e_i \neq \mathbb{O}$ para todo i, $1 \leq i \leq n$. Además, si $b = (b_j)_{1 \leq j \leq n} \in \mathbb{B}_1^n$ y $\mathbb{O} \leq b \leq e_i$, entonces $0 \leq b_j \leq x_{ij}$, para todo j, $1 \leq j \leq n$. Luego, $b_j = 0$ para todo $j \neq i$, $1 \leq j \leq n$ y $b_i = 0$ ó $b_i = 1$. Si $b_i = 0$, entonces $b = \mathbb{O}$, en caso contrario $b = e_i$.

Por lo tanto, $e_i \in \Pi(\mathbb{B}_1^n)$ para todo i, $1 \leq i \leq n$. Además, es claro que éstos son los únicos átomos. Luego, $|\Pi(\mathbb{B}_1^n)| = n$. ■

7.6 Ejercicios

E 7.6.1

Indicar si las siguientes álgebras son bandas, retículos o retículos distributivos. En caso que sean retículos determinar si tienen primer y último elemento.

(i) $\langle A, + \rangle$, donde $A = \{a, b, c\}$ y

$+$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c

(ii) $\langle I\!N, \circ, * \rangle$, donde $x \circ y = max\ \{x, y\}$ y $x * y = min\ \{x, y\}$.

E 7.6.2

Sea $A \in \mathcal{R}_{0,1}$, donde $A = \{0, a, b, c, 1\}$ y $+, \cdot$ están dadas por las siguientes tablas:

$+$	0	a	b	c	1
0	0	a	b	c	1
a	a	a	c	c	1
b	b	c	b	c	1
c	c	c	c	c	1
1	1	1	1	1	1

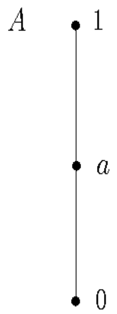
$\cdot$	0	a	b	c	1
0	0	0	0	0	0
a	0	a	0	a	a
b	0	0	b	b	b
c	0	a	b	c	c
1	0	a	b	c	1

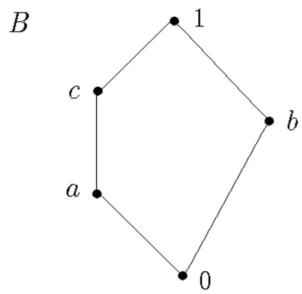
Determinar si $B \lhd A$, siendo

(a) $B = \{0, a, b, 1\}$, (b) $B = \{0, b, 1\}$.

E 7.6.3

(i) Dados $A, B \in \mathcal{R}$ determinar todos sus subretículos.





(ii) Idem inciso anterior suponiendo $A, B \in \mathcal{R}_{0,1}$.

E 7.6.4

Sean $\langle A, +, \cdot \rangle \in \mathcal{R}$ y $[a) = \{x \in A : a \leq x\}$. Probar que

(i) $[a) \lhd_{\mathcal{R}} A$,

(ii) $[a) \cap [b) = [a + b)$,

(iii) si $a \leq b$, entonces $[b) \subseteq [a)$.

E 7.6.5

Sea $A \in \mathcal{R}$, donde $A = \{0, a, b, c, 1\}$ y $+, \ \cdot$ son las indicadas en el ejercicio 8.8.2. Sean $X_1 = \{c\}$ y $X_2 = \{a, b\}$. Hallar $[X_1]_{\mathcal{R}}$ y $[X_2]_{\mathcal{R}}$.

E 7.6.6

Sea $A \in \mathcal{R}$. Probar que para todo $x, y \in A$, si $x \leq y$, entonces

(i) $x \cdot z \leq y \cdot z$, para todo $z \in A$,

(ii) $x + z \leq y + z$, para todo $z \in A$.

E 7.6.7

Sea $A \in \mathcal{R}$. Probar que para todo $x, y, z, w \in A$

(i) si $x \leq y$ y $z \leq w$, entonces $x \cdot z \leq y \cdot w$ y $x + z \leq y + w$,

(ii) $x \cdot y = x + y$ si, y sólo si, $x = y$,

(iii) $(x \cdot y) + (z \cdot y) \leq (x + z) \cdot y$,

(iv) $x + (y \cdot z) \leq (x + y) \cdot (x + z)$,

(v) si $y \cdot z \leq x \leq z \leq x + y$, entonces $y \cdot z = x \cdot y$, $y + z = x + y$. De un ejemplo donde no valga la recíproca,

(vi) si $(x + y) \cdot (y + z) = y$, entonces $x \cdot z \leq y$. De un ejemplo donde no valga la recíproca.

E 7.6.8

Sea $X \neq \emptyset$ y consideremos $\langle \mathcal{P}(X), \cup, \cap, \emptyset, X \rangle \in \mathcal{R}_{0,1}$. Probar que
$\Pi(\mathcal{P}(X)) = \{\{x\} : x \in X\}$.

E 7.6.9

(i) Sea $A \in \mathcal{R}_{0,1}$. Probar que si $a, b \in \Pi(A)$ y $a \neq b$, entonces $a \cdot b = 0$.

(ii) Sea $A \in \mathcal{D}_{0,1}$. Si $a \in \Pi(A)$ y $x_1, ..., x_n \in A$ son tales que $a \leq x_1 + ... + x_n$, probar que $a \leq x_i$, para algún i, $1 \leq i \leq n$.

E 7.6.10

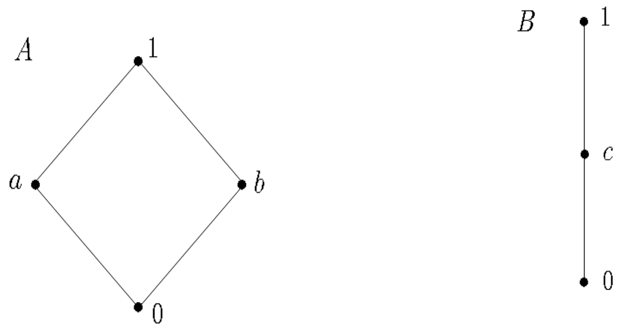
Sea A un retículo distributivo. Probar que

(i) $x + (y \cdot z) = (x + y) \cdot (x + z)$,

(ii) si $x \cdot z = y \cdot z$ y $x + z = y + z$, entonces $x = y$. (Ley del corte)

E 7.6.11

Sean $A, B \in \mathcal{R}_{0,1}$, cuyos diagramas de Hasse asociados son



y sean $f : A \to B$ y $g : B \to A$ las funciones definidas por medio de las siguientes tablas:

x	0	a	b	1
$f(x)$	0	0	c	1

x	0	c	1
$g(x)$	0	a	1

Determinar si f y g son $\mathcal{R}_{0,1}$-homomorfismos.

E 7.6.12

Sea $\langle A, +, \cdot, ', a, b \rangle$ un álgebra de tipo $(2, 2, 1, 0, 0)$, donde $A = \{a, b\}$. Indicar, en cada caso, si A es un álgebra de Boole.

(i)

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

x	x'
a	a
b	b

(ii)

$+$	a	b
a	a	b
b	b	b

$\cdot$	a	b
a	a	a
b	a	b

x	x'
a	b
b	a

E 7.6.13

Sea $A \in \mathfrak{B}$ y $X \neq \emptyset$ un conjunto arbitrario. Consideremos el conjunto $A^X = \{f : X \longrightarrow A\}$ en el cual, para todo $x \in X$ y para todo par de funciones $f, g \in A^X$ se definen las siguientes operaciones:

(i) $f + g : X \longrightarrow A$, $(f + g)(x) = f(x) + g(x)$,

(ii) $f \cdot g : X \longrightarrow A$, $(f \cdot g)(x) = f(x) \cdot g(x)$,

(iii) $f' : X \longrightarrow A$, $(f')(x) = (f(x))'$,

(iv) $\mathbb{I} : X \longrightarrow A$, $\mathbb{I}(x) = 1$,

(v) $\mathbb{O} : X \longrightarrow A$, $\mathbb{O}(x) = 0$.

Probar que $\langle A^X, +, \cdot, ', \mathbb{O}, \mathbb{I}\rangle \in \mathfrak{B}$.

E 7.6.14

Probar que en toda álgebra de Boole valen las siguientes propiedades:

(i) $(x')' = x$,

(ii) si $x + y = 1$ y $x \cdot y = 0$, entonces $y = x'$,

(iii) $0' = 1, \quad 1' = 0$,

(iv) $(x + y)' = x' \cdot y'$,

(v) $(x \cdot y)' = x' + y'$,

(vi) $x + (x' \cdot y) = x + y$,

(vii) $x \cdot (x' + y) = x \cdot y$,

(viii) $(x + y') \cdot z = ((x' + z') \cdot (y + z'))'$,

(ix) $x = y$ si, y só lo si, $(x + y') \cdot (y + x') = 1$.

Nota. (iv) y (v) son la leyes de De Morgan.

E 7.6.15

Sea $A \in \mathfrak{B}$. Definimos en A una nueva operación binaria por medio de la siguiente fórmula:

$$x \oplus y = (x \cdot y') + (y \cdot x').$$

Probar que se verifican:

(i) $x \oplus y = y \oplus x$,

(ii) $x \oplus x = 0$,

(iii) $0 \oplus x = x$,

(iv) $1 \oplus x = x'$.

E 7.6.16

Sea $A \in \mathfrak{B}$. Probar que

(i) las siguientes condiciones son equivalentes:

  (a) $a + b = b$,

  (b) $a \cdot b = a$,

  (c) $a' + b = 1$,

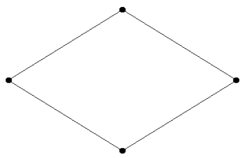
  (d) $a \cdot b' = 0$.

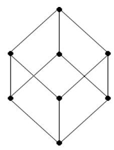
(ii) si $x \cdot y = x \cdot z$ y $x' \cdot y = x' \cdot z$, entonces $y = z$.

E 7.6.17

(i) Definir la noción de subálgebra de Boole.

(ii) Indicar todas las subálgebras de las álgebras de Boole cuyos diagramas son:





E 7.6.18

(i) Sean $A, B \in \mathfrak{B}$. Definir la noción de homomorfismo booleano de A en B.

(ii) Sean $A, B \in \mathfrak{B}$ y sea $h : A \longrightarrow B$. Probar que las siguientes condiciones son equivalentes:

(a) $h \in Hom(A, B)$,

(b) h verifica

(1) $h(x + y) = h(x) + h(y)$,

(2) $h(x') = (h(x))'$,

(c) h verifica

(3) $h(x \cdot y) = h(x) \cdot h(y)$,

(4) $h(x') = (h(x))'$.

8 Sistemas proposicionales

8.1 Lenguajes de orden cero

D 8.1.1 *Llamaremos lenguaje de orden cero a toda F–álgebra absolutamente libre $\mathfrak{For}[X] = \langle For[X], F\rangle$.*

Ejemplos

(i) Si $F_0 = \emptyset$, $F_1 = \{\sim\}$ y $F_2 = \{\wedge, \vee, \rightarrow\}$ entonces $\mathfrak{For}[X]$ es el álgebra de las formas proposicionales que vimos en la sección 1.2, que en adelante designaremos con $\mathfrak{For}_{\mathrm{Cl}}[X]$. Los elementos del conjunto X son los símbolos con los que representabamos a las proposiciones simples del lenguaje coloquial y los elementos de $For[X]$ que no están en X son los símbolos con los que representábamos a las proposiciones compuestas del lenguaje coloquial.

(ii) Llamaremos álgebra de las formas booleanas al álgebra absolutamente libre $\mathfrak{For}_{Bol}[X] = \langle For[X], F\rangle$ cuando elegimos como conjunto de operaciones a $F_0 = \emptyset$, $F_1 = \{\sim\}$ y $F_2 = \{\wedge, \vee\}$.

Sustituciones

D 8.1.2 *Llamaremos sustitución a toda función de X en $For[X]$.*

Como $\mathfrak{For}[X]$ es absolutamente libre, para cada $\rho : X \longrightarrow For[X]$ existe un único $\overline{\rho} \in End(\mathfrak{For}[X])$ que prolonga a ρ , esto es, se verifica $\rho(x) = \overline{\rho}(x)$, para todo $x \in X$.

Por este motivo también llamaremos sustituciones a los elementos de $End(\mathfrak{For}[X])$.

Ejemplo

En $\mathfrak{For}_{\mathrm{Cl}}[X]$, sea $\rho : X \longrightarrow For[X]$ una función tal que

$\rho(x_1) = x_3 \rightarrow x_2$,

$\rho(x_2) = \sim x_1$,

$\rho(x_3) = x_4 \vee x_2$,

y sea

$$p = ((x_1 \to x_2) \to (x_3 \to (x_1 \wedge x_2))) \in ForX,$$

entonces

$$\begin{aligned}
\overline{\rho}(p) &= \overline{\rho}((x_1 \to x_2) \to (x_3 \to (x_1 \wedge x_2))) \\
&= (\overline{\rho}(x_1) \to \overline{\rho}(x_2)) \to (\overline{\rho}(x_3) \to (\overline{\rho}(x_1) \wedge \overline{\rho}(x_2))) \\
&= (\rho(x_1) \to \rho(x_2)) \to (\rho(x_3) \to (\rho(x_1) \wedge \rho(x_2))) \\
&= ((x_3 \to x_2) \to \sim x_1) \to ((x_4 \vee x_2) \to ((x_3 \to x_2) \wedge \sim x_1)).
\end{aligned}$$

Valuaciones

D 8.1.3 *Dadas las F–álgebras $\mathcal{F}or[X] = \langle For[X], F\rangle$ y $\mathcal{A} = \langle A, F\rangle$, llamaremos $\mathcal{A}$–valuación a toda función de X en A.*

Como para cada $v : X \longrightarrow A$ existe un único homomorfismo $\overline{v} : For[X] \longrightarrow A$ que prolonga a v, esto es, se verifica $v(x) = \overline{v}(x)$, para todo $x \in X$, también llamaremos $\mathcal{A}$–valuaciones a los elementos de $Hom(For[X], A)$.

8.2 Sistemas proposicionales

Operadores de clausura y sistemas proposicionales

D 8.2.1 *Diremos que una función $C : \mathcal{P}(For[X]) \longrightarrow \mathcal{P}(For[X])$ es un operador de clausura sobre $For[X]$ si para todo $H, K \in \mathcal{P}(For[X])$ se verifican:*

(C1) $H \subseteq C(H)$, [creciente]

(C2) *si* $H \subseteq K$, *entonces* $C(H) \subseteq C(K)$, [monótona]

(C3) $C(C(H)) = C(H)$. [idempotente]

D 8.2.2 *Llamaremos sistema proposicional (s.p.) o lógica de orden cero a toda terna $\mathcal{C} = \langle For[X], F, C\rangle$, donde C es un operador de clausura sobre $For[X]$ y diremos que los elementos de $C(\emptyset)$ son los C–teoremas de $\mathcal{C}$.*

Fragmentos y extensiones de un sistema proposicional

D 8.2.3 *Sean* $\mathcal{C} = \langle For[X], F, C\rangle$ *y* $\mathcal{C}' = \langle For'[X], F', C'\rangle$ *dos s.p.. Diremos que* $\mathcal{C}'$ *es una extensión de* $\mathcal{C}$ *o que* $\mathcal{C}$ *es un fragmento de* $\mathcal{C}'$*, si se verifican:*

(i) $F \subset F'$,

(ii) $C(H) \subseteq C'(H)$, *para todo* $H \subseteq For[X]$.

Si $C(\emptyset) \subset C'(\emptyset)$, *entonces diremos que* $\mathcal{C}'$ *es una extensión propia de* $\mathcal{C}$.

8.3 Sistemas proposicionales semánticos

Matrices

D 8.3.1 *Llamaremos matriz asociada a* $\mathcal{F}or[X] = \langle For[X], F\rangle$ *a toda terna* $\mathcal{M}(\mathcal{A}) = \langle A, F, U\rangle$ *tal que* $\mathcal{A} = \langle A, F\rangle$ *es una* F*–álgebra y* U *es un subconjunto de* A. *A los elementos de* U *los llamaremos elementos designados.*

Consecuencias semánticas

D 8.3.2 *Sea* $\mathcal{M}(\mathcal{A}) = \langle A, F, U\rangle$ *una matriz dada. Para cada* $H \subseteq For[X]$ *y cada* $p \in For[X]$ *diremos que* p *es consecuencia semántica de* H *según la matriz* $\mathcal{M}(\mathcal{A})$ *y escribiremos* $H \models_{\mathcal{A}} p$, *si existen* $p_1, p_2, \ldots, p_n \in H$ *tales que para toda valuación* $v \in Hom(For[X], A)$, *las hipótesis* $v(p_1) \in U, v(p_2) \in U, \ldots, v(p_n) \in U$ *implican* $v(p) \in U$.

D 8.3.3 *Diremos que el conjunto* $C_{\mathcal{A}}(H) = \{p \in For[X] : H \models_{\mathcal{A}} p,\}$ *es el conjunto de todas las consecuencias semánticas de* H *según la matriz* $\mathcal{M}(\mathcal{A})$.

Si $\mathcal{A} = \langle A, F\rangle$ es un álgebra fija escribiremos simplemente $H \models p$ en lugar de $H \models_{\mathcal{A}} p$.

Operadores de clausura semánticos y s.p. semánticos

Se verifica sin dificultad que la aplicación $C_A : \mathcal{P}(For[X]) \longrightarrow \mathcal{P}(For[X])$ tal que a cada $H \subseteq For[X]$ le asigna el conjunto $C_A(H)$ es un operador de clausura sobre $For[X]$. Los operadores de clausura obtenidos por matrices se llaman operadores semánticos.

D 8.3.4 *Diremos que un operador de clausura C sobre $\langle For[X], F\rangle$ es semántico si existe una matriz $\mathcal{M}(\mathcal{A}) = \langle A, F, U\rangle$ tal que $C = C_A$.*

D 8.3.5 *Diremos que el s.p. $\mathcal{C} = \langle For[X], F, C\rangle$ es semántico si C es un operador de clausura semántico.*

Es decir un s.p. es semántico si existe una matriz $\mathcal{M}(\mathcal{A})$ tal que para todo $H \subseteq For[X]$ se verifique que
$C(H) = C_{\mathcal{A}}(H) = \{p \in For[X] : H \models_A p\}$.

Ejemplos

(i) Dada la matriz $\mathcal{M}(\mathcal{B}_2) = \langle B_2, \{+, \cdot, \Rightarrow, -\}, U\rangle$ donde:

(a) $B_2 = \{0, 1\}$,

(b) $\mathcal{B}_2 = \langle B_2, +, \cdot, \Rightarrow, -\rangle$ es el álgebra de prueba del lenguaje coloquial,

(c) $U = \{1\}$ es el conjunto de los elementos designados,

al s.p. $\mathcal{C}_{\mathcal{B}_2} = \langle For[X], F, C_{\mathcal{B}_2}\rangle$ lo llamaremos la versión semántica del sistema proposicional clásico.

(ii) Dada la matriz $\mathcal{M}(\mathcal{I}_2) = \langle I_2, \{\rightarrow\}, U\rangle$ donde:

(a) $I_2 = B_2$,

(b) $\mathcal{I}_2 = \langle I_2, \rightarrow\rangle$ es el reducto implicativo del álgebra $\mathcal{B}_2$,

(c) $U = \{1\}$ es el conjunto de los elementos designados,

al s.p. $\mathcal{C}_{\mathcal{I}_2} = \langle For[X], F, C_{\mathcal{I}_2}\rangle$ lo llamaremos la versión semántica del sistema proposicional implicativo clásico.

(iii) Dada la matriz $\mathcal{M}(\mathcal{H}) = \langle [0, 1], \{\wedge, \vee, \rightarrow, \neg\}, U\rangle$ donde:

(a) $[0, 1]$ es el intervalo real,

(b) las operaciones $\wedge, \vee, \rightarrow, \neg$ estan definidas por

$x \wedge y = min\{x, y\}$,

$x \vee y = max\{x, y\}$,

$$\neg x = \begin{cases} 1, & \text{si } x = 0 \\ 0, & \text{en otro caso} \end{cases},$$

$$x \to y = \begin{cases} 1, & \text{si } x \leq y \\ y, & \text{en otro caso} \end{cases},$$

(c) $U = \{1\}$,

al s.p. $\mathcal{C}_{\mathcal{H}} = \langle For[X], F, C_{\mathcal{H}} \rangle$ lo llamaremos la versión semántica del sistema proposicional intuicionista.

(iv) Dada la matriz $\mathcal{M}(\mathcal{I}) = \langle [0,1], \{\to\}, U \rangle$ donde:

(a) $[0, 1]$ es el intervalo real,

(b) $\to$ es la indicada en iii2) del ejemplo anterior,

(c) $U = \{1\}$,

al s.p. $\mathcal{C}_{\mathcal{I}} = \langle For[X], F, C_{\mathcal{I}} \rangle$ lo llamaremos la versión semántica del sistema proposicional implicativo positivo (intuicionista).

(v) Dada la matriz $\mathcal{M}(\mathcal{L}) = \langle [0,1], \{\to, \sim\}, U \rangle$ donde:

(a) $[0, 1]$ es el intervalo real,

(b) $\to$ y $\sim$ están definidas por

$x \to y = min\{1, 1 - x + y\}$,

$\sim x = 1 - x$,

(c) $U = \{1\}$,

al s.p. $\mathcal{C}_{\mathcal{L}} = \langle For[X], F, C_{\mathcal{L}} \rangle$ lo llamaremos la versión semántica del sistema proposicional de Łukasiewicz infinito-valuado.

(vi) Dada la matriz $\mathcal{M}(\mathcal{L}_{n+1}) = \langle L_{n+1}, \{\to, \sim\}, U\rangle$ donde:

(a) $L_{n+1} = \{0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, 1\} \subset [0,1]$,

(b) $\to$ y $\sim$ son las indicadas en (v2) del ejemplo anterior,

(c) $U = \{1\}$,

al s.p. $\mathcal{C}_{\mathcal{L}_{n+1}} = \langle For[X], F, C_{\mathcal{L}_{n+1}}\rangle$ lo llamaremos la versión semántica del sistema proposicional de Łukasiewicz $(n+1)$–valuado.

$\mathcal{M}(\mathcal{A})$–tautologías

D 8.3.6 *Sea $\mathcal{M}(\mathcal{A}) = \langle A, F, U\rangle$ una matriz asociada a $\mathcal{F}or[X]$. Diremos que $p \in For[X]$ es una $\mathcal{M}(\mathcal{A})$–tautología si $v(p) \in U$, para toda $\mathcal{A}$–valuación v.*

Designaremos con $\mathcal{T}_A$ al conjunto de todas las $\mathcal{M}(\mathcal{A})$–tautologías.

8.4 Sistemas Proposicionales sintácticos

Axiomas

D 8.4.1 *Llamaremos axiomas a los elementos de un subconjunto fijo $\mathfrak{A}$ de $For[X]$.*

Reglas de inferencia

D 8.4.2 *Dado $P \subseteq (For[X])^n$, llamaremos regla de inferencia (r.i.), o regla de deducción, a toda función $r : P \longrightarrow For[X]$. Si $(p_1, p_2, \cdots, p_n) \in P$ y $p = r(p_1, p_2, \cdots, p_n)$, diremos que $p_1, p_2, \cdots, p_n$ son las premisas y p es la conclusión de esas premisas por medio de la regla r.*

Usualmente escribiremos

$$r : \frac{p_1, p_2, \cdots, p_n}{p}$$

en lugar de $p = r(p_1, p_2, \cdots, p_n)$.

Demostraciones formales

Consideremos un conjunto $\mathfrak{A}$ de axiomas y un conjunto $\{r_1, \dots, r_k\}$ de reglas de inferencia.

D 8.4.3 *Sean $H \subseteq For[X]$ y $p \in For[X]$. Diremos que la n–upla $(p_1, \dots, p_n) \in (For[X])^n$ es una demostración formal de p, a partir del conjunto de hipótesis H si se verifican las siguientes condiciones:*

(1) $p_1 \in H \cup \mathfrak{A}$,

(2) $p_2 \in H \cup \mathfrak{A}$,

$\vdots$

(j) $p_j \in H \cup \mathfrak{A}$, *o* $r_t : \dfrac{p_{i_1}, p_{i_2}, \dots, p_{i_m}}{p_j}$, $i_s \in \{1, 2, \dots, j-1\}$, $t \in \{1, 2, \dots, k\}$,

$\vdots$

(n) p_n *es* p.

Consecuencias sintácticas

D 8.4.4 *Diremos que p es consecuencia sintáctica de H y escribiremos $H \vdash p$, si existe una demostración formal de p a partir de las hipótesis H, los axiomas $\mathfrak{A}$ y las reglas $\{r_1, \dots, r_k\}$.*

Operadores de clausura sintácticos y s.p. sintácticos

La aplicación $C_S : \mathcal{P}(For[X]) \longrightarrow \mathcal{P}(For[X])$ tal que a cada $H \subseteq For[X]$ le asigna el conjunto $C_S(H) = \{p \in For[X] : H \vdash p\}$ es un operador de clausura.

Nota. Se suele decir que C_S es la operación de derivabilidad determinada por $\mathfrak{A}$ y $\{r_1, \dots, r_k\}$.

D 8.4.5 *Diremos que un operador de clausura C sobre $\langle For[X], F\rangle$ es sintáctico si existe un conjunto de axiomas $\mathfrak{A}$ y un conjunto de reglas de inferencia $\{r_1, \dots, r_k\}$ tales que $C = C_S$.*

D 8.4.6 *Diremos que el s.p. $\mathcal{C} = \langle For[X], F, C\rangle$ es sintáctico si C es un operador de clausura sintáctico.*

Es decir un s.p. es sintáctico si existen axiomas y reglas de inferencia tales que para todo $H \subseteq For[X]$ se verifique
$C_S(H) = \{p \in For[X] : H \vdash p\}$.

Teoremas sintácticos

D 8.4.7 *Si p es un C_S–teorema, también diremos que p es un teorema sintáctico (o una tesis de $\mathcal{C}$) y escribiremos $\vdash p$.*

Con $\mathcal{T}_S$ representaremos al conjunto de todos los teoremas sintácticos de $\mathcal{C}$.

Uso de los teoremas sintácticos en las demostraciones

La definición de demostración formal se puede generalizar, de modo tal que podamos usar los teoremas sintácticos que ya han sido demostrados. En efecto, supongamos que estamos construyendo una demostración formal de la fórmula p, a partir del conjunto H y nos damos cuenta que para obtener la fórmula del paso (j) nos hace falta el teorema sintáctico q que ya habíamos obtenido. Entonces podemos agregar todas las fórmulas de la demostración de q y continuar con la obtencion de la demostración de la fórmula p.

Pero es claro, que la única fórmula de la demostración de q en la que estamos interesados es la propia q. Entonces, para simplificar, podemos modificar la definición de demostración formal del siguiente modo:

D 8.4.8 *Diremos que la n–upla $(p_1, \ldots, p_n) \in (For[X])^n$ es una demostración formal de p a partir del conjunto de hipótesis H si se verifican las siguientes condiciones:*

(1) $p_1 \in H \cup \mathcal{T}_S$,

(2) $p_2 \in H \cup \mathcal{T}_S$,

$\vdots$

(j) $p_j \in H \cup \mathcal{T}_S$, o $r_t : \dfrac{p_{i_1}, p_{i_2}, \ldots, p_{i_m}}{p_j}$, $i_s \in \{1, 2, \ldots, j-1\}$, $t \in \{1, 2, \ldots, k\}$

$\vdots$

(k) p_n es p.

Simplificación de las notaciones

En los libros y revistas especializadas, las demostraciones formales se suelen presentar de la siguiente manera abreviada:

(1) p_1, [cartel que informa sobre p_1]

(2) p_2, [cartel que informa sobre p_2]

$\vdots$

(j) p_j, [cartel que informa sobre p_j]

$\vdots$

(n) p. [cartel que informa sobre p]

Propiedades de los sistemas proposicionales sintácticos

Sea $\mathcal{C} = \langle For[X], F, C\rangle$ un s.p. sintáctico, entonces:

(i) Cualquier s.p. que se obtenga de $\mathcal{C}$, agregando operaciones a F y conservando los axiomas y reglas (pudiendo además, agregar axiomas o reglas) es un s.p. sintáctico, ampliación del primero.

(ii) Cualquier s.p. que se obtenga de $\mathcal{C}$, eliminando operaciones de F y los axiomas y reglas en que figuran las operaciones suprimidas, y conservando los restantes axiomas y reglas es un s.p. sintáctico, fragmento del primero.

Sistemas proposicionales implicacionales

D 8.4.9 *Diremos que un s.p.* $\mathcal{C} = \langle For[X], F, C\rangle$ *es implicacional si el conectivo binario* $\to$ *que llamaremos operación de implicación, pertenece a* F*.*

Todos los ejemplos de s.p. semánticos que hemos indicado son implicacionales.

Ejemplos de reglas de inferencia para s.p. implicacionales sintácticos

(i) modus ponens: Sea $P = \{(p, p \to q) : p, q \in For[X]\}$, llamaremos regla de modus ponens a $m_p : P \longrightarrow For[X]$, definida por $m_p(p, p \to q) = q$, esto es

$$m_p : \frac{p, p \to q}{q},$$

(ii) modus tollens: Sea $P = \{(p, \sim q \to \sim p) : p, q \in For[X]\}$, llamaremos regla de modus tollens a $m_t : P \longrightarrow For[X]$, definida por $m_t(p, \sim q \to \sim p) = q$, esto es

$$m_t : \frac{p, \sim q \to \sim p}{q},$$

(iii) contraposición: Sea $P = \{p \to q : p, q \in For[X]\}$, llamaremos regla de contraposición a $c : P \longrightarrow For[X]$, definida por $c(p \to q) = \sim q \to \sim p$, esto es

$$c : \frac{p \to q}{\sim q \to \sim p}.$$

8.5 El sistema proposicional clásico

En esta sección exhibiremos un ejemplo muy importante de s.p. implicacional sintáctico.

D 8.5.1 *Llamaremos s.p. clásico al s.p.* $\mathcal{C} = \langle For[X], F, C_l \rangle$ *donde* $F = \{\wedge, \vee, \to, \sim\}$ *y* C_l *es el operador de clausura determinado por la regla de modus ponens y el conjunto* $\mathfrak{A}_{\mathrm{Cl}}$ *de axiomas que indicaremos a continuación.*

Los elementos de $\mathfrak{A}_{\mathrm{C_l}}$ son las fórmulas indicadas en $A1, \ldots, A11$, y las que se pueden obtener de ellas por la regla de sustitución.

(A1) $x_1 \to (x_2 \to x_1)$,

(A2) $(x_1 \to (x_2 \to x_3)) \to ((x_1 \to x_2) \to (x_1 \to x_3))$,

(A3) $(x_1 \wedge x_2) \to x_1$,

(A4) $(x_1 \wedge x_2) \to x_2$,

(A5) $(x_3 \to x_1) \to ((x_3 \to x_2) \to (x_3 \to (x_1 \wedge x_2)))$,

(A6) $x_1 \to (x_1 \vee x_2)$,

(A7) $x_2 \to (x_1 \vee x_2)$,

(A8) $(x_1 \to x_3) \to ((x_2 \to x_3) \to ((x_1 \vee x_2) \to x_3))$,

(A9) $\sim x_1 \to (x_1 \to x_2)$,

(A10) $(x_1 \to \sim x_1) \to \sim x_1$,

(A11) $(\sim x_1 \to x_1) \to x_1$.

Regla de Sustitución: Si $p \in \mathfrak{A}_{\mathrm{Cl}}$ y $\overline{\rho} \in End(\mathfrak{For}[X])$ entonces $\overline{\rho}(p) \in \mathfrak{A}_{\mathrm{Cl}}$.

Observemos que podemos eliminar la regla de sustitución usando axiomas esquemas, del siguiente modo:

Los axiomas son esquemas de la forma:

(E1) $p \to (q \to p)$,

(E2) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$,

(E3) $(p \wedge q) \to p$,

(E4) $(p \wedge q) \to q$,

(E5) $(r \to p) \to ((r \to q) \to (r \to (p \wedge q)))$,

(E6) $p \to (p \vee q)$,

(E7) $q \to (p \vee q)$,

(E8) $(p \to r) \to ((q \to r) \to ((p \vee q) \to r))$,

(E9) $\sim p \to (p \to q)$,

(E10) $(p \to \sim p) \to \sim p$,

(E11) $(\sim p \to p) \to p$.

Entonces cualquier fórmula que tenga el esquema (la forma esquemática) de alguno de los E1,…,E11 es un axioma. Así por ejemplo,

$((\sim x_1 \to x_1) \to (x_1 \wedge x_2)) \to (((x_2 \to x_3) \to (x_1 \wedge x_2)) \to (((\sim x_1 \to x_1) \vee (x_2 \to x_3)) \to (x_1 \wedge x_2))$

es un axioma que se obtiene de E8 reemplazando

(1) p por $(\sim x_1 \to x_1)$,

(2) q por $(x_2 \to x_3)$

(3) r por $(x_1 \wedge x_2)$.

En lo que sigue trabajaremos con axiomas esquemas.

Ejemplos de demostraciones formales

(T1) $\vdash p \to p$

(1) $p \to (p \to p)$, [E1]

(2) $p \to ((p \to p) \to p)$, [E1]

(3) $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$, [E2]

(4) $(p \to (p \to p)) \to (p \to p))$, [(2),(3),$m_p$]

(5) $p \to p$. [(1),(4),m_p]

(R1) $\dfrac{p}{q \to p}$,

(1) p, [hip.]

(2) $p \to (q \to p)$, [E1]

(3) $q \to p$. [(1),(2),m_p]

(R2) $\dfrac{p \to (q \to r)}{(p \to q) \to (p \to r)}$,

(1) $p \to (q \to r)$, [hip.]

(2) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$, [E2]

(3) $(p \to q) \to (p \to r)$. [(1),(2),m_p]

(T2) $\vdash (p \to q) \to ((r \to p) \to (r \to q))$

(1) $(r \to (p \to q)) \to ((r \to p) \to (r \to q))$, [E2]

(2) $(p \to q) \to ((r \to (p \to q)) \to ((r \to p) \to (r \to q)))$, [(1),R1]

(3) $((p \to q) \to (r \to (p \to q))) \to ((p \to q) \to ((r \to p) \to (r \to q)))$, [(2),R2]

(4) $(p \to q) \to (r \to (p \to q))$, [E1]

(5) $(p \to q) \to ((r \to p) \to (r \to q))$, [(4),(3),$m_p$]

(R3) $\dfrac{p \to q}{(r \to p) \to (r \to q)}$,

(1) $p \to q$, [hip.]

(2) $(p \to q) \to ((r \to p) \to (r \to q))$, [T2]

(3) $(r \to p) \to (r \to q)$, [(1),(2),m_p]

(T3) $\vdash (p \to (p \to q)) \to (p \to q)$,

(1) $(p \to (p \to q)) \to ((p \to p) \to (p \to q))$, [E2]

(2) $((p \to (p \to q)) \to (p \to p)) \to ((p \to (p \to q)) \to (p \to q))$, [(1),R2]

(3) $p \to p$, [T1]

(4) $(p \to (p \to q)) \to (p \to p)$, [(3),R1]

(5) $(p \to (p \to q)) \to (p \to q)$, [(4),(2),$m_p$]

(R4) $\dfrac{(p \to q) \to (p \to r)}{q \to (p \to r)}$,

(1) $(p \to q) \to (p \to r)$, [hip.]

(2) $(q \to (p \to q)) \to (q \to (p \to r))$, [(1),R3]

(3) $q \to (p \to q)$, [E1]

(4) $q \to (p \to r)$, [(3),(2),m_p]

(R5) $\dfrac{p \to (q \to r)}{q \to (p \to r)}$,

(1) $p \to (q \to r)$, [hip.]

(2) $(p \to q) \to (p \to r)$, [(1),R2]

(3) $q \to (p \to r)$. [(2),R4]

8.6 El Teorema de la deducción

El siguiente resultado suministra un método para determinar si una fórmula p del s.p. implicativo es una consecuencia sintáctica de H.

T 8.6.1 *Sea* $\mathcal{C} = (For[X], \{\wedge, \vee, \to, \sim\}, C_l)$ *y* $H \subseteq For[X]$, *entonces las siguientes condiciones son equivalentes:*

(i) $H \vdash (p \to q)$,

(ii) $H \cup \{p\} \vdash q$.

Dem.

(i)$\Longrightarrow$ (ii): Supongamos que $H \vdash (p \to q)$, entonces existe una demostración formal de $p \to q$ a partir de H

(1) p_1, [$H \cup \mathcal{T}_S$]

(2) p_2, [$H \cup \mathcal{T}_S$]

$\vdots$

(n) $p \to q$.

Entonces

(1) p,

(2) p_1,

(3) p_2,

$\vdots$

$(n+1)$ $p \to q$.

$(n+2)$ q, [(1),$(n+1)$,m_p]

es una demostración de q a partir de $H \cup \{p\}$.

Luego $H \cup \{p\} \vdash q$.

(ii)$\Longrightarrow$(i): Haremos la demostración por inducción sobre la longitud de la demostración formal de la fórmula q.

Si $n = 1$, p_1 es q, luego $q \in \mathcal{T}_S \cup H \cup \{p\}$.

Caso 1. $q \in \mathcal{T}_S \cup H$:

(1) q, [hipótesis]

(2) $q \to (p \to q)$, [E1]

(3) $p \to q$. [(1),(2) y m_p]

Por lo tanto,

$$H \vdash (p \to q).$$

Caso 2. $q \in \{p\}$:

(1) $\emptyset \vdash (p \to p)$. [T1]

(2) $\emptyset \subseteq H$,

(3) $H \vdash (p \to p)$. [de (1) y (2)]

Hipótesis de inducción: Supongamos que el enunciado vale para toda fórmula r cuya demostración es de longitud menor o igual que $n-1$ y sea

(1) p_1,

(2) p_2,

$\vdots$

(n) q,

una demostración de q, a partir de $H \cup \{p\}$, de longitud n.

Caso 1. $q \in H \cup \mathcal{T}_S \cup \{p\}$.

Es análogo al caso 1 de $n = 1$.

Caso 2. $q \notin H \cup \mathcal{T}_S \cup \{p\}$.

De la hipótesis resulta que existe una demostración formal

(1) p_1,

$\vdots$

(j) p_j,

$\vdots$

$(n-1)$ $p_j \to q$,

(n) q.

Como p_j y $p_j \to q$ tienen una demostración a partir de $H \cup \{p\}$, de longitud menor o igual que $n-1$, entonces por la hipótesis de inducción tenemos que $H \vdash (p \to p_j)$ y $H \vdash (p \to (p_j \to q))$. Por lo tanto podemos escribir

(1) q_1,
$\vdots$
(t) $p \to p_j$, | [demostración de $p \to p_j$ a partir de H, ($q_i \neq p$, $1 \leq i \leq t-1$)]

$$\begin{array}{rl|r}
(1) & r_1, & \\
 & \vdots & \text{[demostración de } p \to (p_j \to q) \text{ a partir de } H, \\
(s) & p \to (p_j \to q). & (r_i \neq p,\ 1 \leq i \leq s-1)]
\end{array}$$

Entonces,

$$\begin{array}{rlr}
(1) & q_1, & \\
 & \vdots & \\
(t) & p \to p_j, & \\
(t+1) & r_1, & \\
 & \vdots & \\
(m) & p \to (p_j \to q), & \\
(m+1) & (p \to (p_j \to q)) \to ((p \to p_j) \to (p \to q)), & \text{[E2]} \\
(m+2) & (p \to p_j) \to (p \to q), & \text{[(m),(m+1),}m_p\text{]} \\
(m+3) & p \to q. & \text{[(t),(m+2),}m_p\text{]}
\end{array}$$

Por lo tanto $H \vdash (p \to q)$. ■

8.7 El Teorema de la completud

T 8.7.1 *Sea* $\mathcal{C} = (For[X], \{\wedge, \vee, \to, \sim\}, C_l)$ *y* $H \subseteq For[X]$, *entonces las siguientes condiciones son equivalentes:*

(i) $H \vdash p$,

(ii) $H \models_{\mathcal{B}_2} p$.

8.8 Ejercicios

Para el cálculo proposicional clásico $\mathcal{C} = (For[X], \to, \wedge, \vee, \sim, \mathcal{C}_l)$, tomamos como axiomas los elementos de $\mathcal{U}_{Cl} = \{E1, ..., E11\}$ dados en teoría y como regla de inferencia

$$m_p : \frac{p, p \to q}{q}$$

E 8.8.1

Sea $\mathcal{T}_S$ el conjunto de los teoremas sintácticos de $\mathcal{C}$. Verificar que

(i) $\mathcal{U}_{Cl} \subseteq \mathcal{T}_S$,

(ii) si $p, p \to q \in \mathcal{T}_S$, entonces $q \in \mathcal{T}_S$,

(iii) si $p \in \mathcal{T}_S$, entonces $q \to p \in \mathcal{T}_S$, cualquiera sea $q \in For[X]$.

E 8.8.2

Dados $p, q \in For[X]$, definimos $p \leq q$ si, y sólo si, $p \to q \in \mathcal{T}_S$. Probar que

(O1) $p \leq p$, cualquiera sea $p \in For[X]$,

(O2) si $p \leq q$ y $q \leq r$, entonces $p \leq r$.

Esto es, $\leq$ es un preorden en $For[X]$.

E 8.8.3

Dados $p, q \in For[X]$ y $\leq$ la relación definida en el E.8.8.2, definimos $p \approx q$ si, y sólo si, $p \leq q$ y $q \leq p$. Probar que $\approx \in EQ(For[X])$.

E 8.8.4

Demostrar aplicando el teorema de la deducción los siguientes teoremas:

(i) $\vdash (p \to q) \to ((q \to r) \to (p \to r))$,

(ii) $\vdash p \to ((p \to q) \to q)$,

(iii) $\vdash (p \to q) \to ((r \to p) \to (r \to q))$,

(iv) $\vdash (p \to q) \to ((p \wedge r) \to (q \wedge r))$,

(v) $\vdash (p \to q) \to ((r \wedge p) \to (r \wedge q))$.

E 8.8.5

Sean $p, q \in For[X]$ y $\leq$ la relación definida en el E.8.8.2. Probar que si $p \leq q$, entonces

(i)	$q \to r \leq p \to r$,	(ii)	$r \to p \leq r \to q$,
(iii)	$p \wedge r \leq q \wedge r$,	(iv)	$r \wedge p \leq r \wedge q$.

E 8.8.6

Consideremos $For[X]$ con la relación de equivalencia definida en el E.8.8.3. Probar que

(i) si $p \approx q$ y $r \approx t$, entonces $p \to r \approx q \to t$, [compatibilidad con $\to$]

(ii) si $p \approx q$ y $r \approx t$, entonces $p \wedge r \approx q \wedge t$. [compatibilidad con $\wedge$]

9 Bibliografía

[1] A. Barnes, J.M. Mark, *Una Introducción algebraica a la lógica matemática*, EUNIBAR, 1975.

[2] C. Berge, *The theory of graphs and its applications*, New York, John – Wiley, 1962.

[3] S. Burris, H. P. Sankappanavar, *A course in universal algebra*, New York,Springer – Verlag, 1981.

[4] I. M. Copi, *Introducción a la lógica, Bs. As.*, EUDEBA, 1994.

[5] K. Douglas, *Sistemas booleanos*, Madrid, Ed. Alhambra, 1970.

[6] J.L. Gersting, *Mathematical structures for computer science*, New York, 2nd ed.,W. H. Freeman and Co., 1987.

[7] A.G. Hamilton, *Lógica para matemáticos, Madrid*, Ed. Paraninfo, 1981.

[8] I.S. Levy, *Discrete structures of computer sciences*, New York, John Wiley, 1980.

[9] L. Oubiña, *Introducción a la teoría de conjuntos*, 7ma ed., Bs. As., Eudeba, 1974.

[10] A. Tarski, *Introducción a la lógica y a la metodología de las ciencias deductivas*, 2da ed., Madrid, Espasa-Calpe, 1968.

[11] J. Whitesitt, *Boolean algebra and its applications*, London, Addison – Wesley,1961.

Bibliografía básica

1. C. Berge, *The Theory of Graphs and its Applications*, John Wiley, New York, 1962.

2. A. V. Figallo, *Algebra y Lógica*, Apuntes de cátedra elaborados en colaboración con E. Bianco, C. Sanza y A. Ziliani, Dpto. de Matemática, U. N. del Sur, Bahía Blanca, 1994.

3. A. V. Figallo, *Matemática Discreta*, Apuntes cátedra, elaborados en colaboración con E. Bianco, C. Sanza y A. Ziliani, Dpto. de Matemática, U. N. del Sur, Bahía Blanca, 1997.

4. E. Gentile, *Estructuras Algebraicas I*, Monografías de Matemática de la O.E.A. $n^o\,3$, Washington, 1977.

5. J. Gersting, *Mathematical Structures for Computer Science*, W. H. Freeman and Co., New York, 1987.

6. C. Grimaldi, *Matemática Discreta y Combinatoria*, Addison–Wesley Iberoamericana, México, 1989.

7. B. Kolman, R. Busby, *Estructuras de Matemática Discreta para Computación*, Prentice–Hall Iberoamericana, México, 1984.

8. I. Levy, *Discrete Structures for Computer Sciences*, John Wiley, New York, 1980.

9. S. Lipschutz, *Discrete Mathemathics*, Mc Graw–Hill, New York, 1976.

10. L. Nachbin, *Algebra Elemental*, Monografías de Matemática de la O.E.A. n^o 26 , Washington, 1986.

11. J. Whitesitt, *Boolean Algebra and its Applications*, Addison–Wesley, London, 1962.

Bibliografía de consulta

1. A. Barnes, J. Mark, *Una introducción algebraica a la lógica matemática*, EUNIBAR, 1975.

2. S. Burris, H. Sankappanavar, *A Course in Universal Algebra*, Springer–Verlag, New York, 1981.

3. I. Copi, *Introducción a la Lógica*, Eudeba, Buenos Aires, 1953.

4. B. Davey, H. Priestley, *Introduction to Lattices and Order*, Cambridge University Press, New York, 1990.

5. K. Douglas, *Sistemas Booleanos*, Alhambra, Madrid, 1970.

6. G. Grätzer, Universal Algebra, Second Edition, Springer-Verlag, 1978.

7. G. Gavrilov, A. Sapozhenko, *Problemas de Matemática Discreta*, MIR, Moscú, 1980.

8. A. Hamilton, *Lógica para matemáticos*, Madrid, Ed. Paraninfo, 1981.

9. F. Hohn, *Applied Boolean Algebra*, The Macmillan Company, New York, Collier – Macmillan Limited, London.

10. E. Mendelson, *Boolean Algebra and Switching Circuits*, Mc Graw–Hill, New York, 1970.

11. L. Monteiro. *Algebras de Boole*, Informes Técnicos Internos 36 (1994), 1 - 17 Instituto de Matemática, INMABB-CONICET-UNS.

12. L. Oubiña, *Introducción a la teoría de conjuntos*, 7^{ed}, Buenos Aires, Eudeba, 1974.

13. A. Tarski, *Introducción a la lógica y a la metodología de las ciencias deductivas*, 2^{ed}, Madrid, Espasa – Calpe, 1968.