Walter Mora F.
Escuela de Matemática
Instituto Tecnológico de Costa Rica
wmora2@gmail.com

Apuntes del curso

Matemática Discreta

Versión 0.2 – Curso I Semestre, 2017

Revista digital
Matemática, Educación e Internet. (http://www.tec-digital.itcr.ac.cr/revistamatematica/).

Este libro corresponde a los apuntes para el curso Matemática Discreta, impartido el I semestre de 2017.
La mayoría de los ejemplos y los ejercicios, fueron tomados de los libros de la bibliografía y también de exámenes de años anteriores.

Esta es la versión 0.2

PROF. WALTER MORA F.
Febrero, 2017.

Índice general

1 **Lógica proposicional** — **Página 3**

1.1 Equivalencias lógicas y simplificación 8
1.2 Cuantificadores 13
1.3 Inferencias lógicas 18
1.4 Epílogo 23

2 **Teoría intuitiva de conjuntos** — **Página 25**

2.1 Introducción 25
2.2 Cardinalidad 28
2.3 Leyes de conjuntos (y sus análogas en lógica) 31
2.4 Resultados y demostraciones 32

3 **Relaciones binarias** — **Página 39**

3.1 Operaciones con relaciones 41
3.2 Matrices y grafos asociados 48
Dígrafos (gráficos dirigidos) 53
3.3 Propiedades de las relaciones 55
3.4 Relaciones de equivalencia 59
3.5 Relaciones de orden 68

4 **Funciones** — **Página 83**

4.1 Funciones inyectivas, sobreyectivas y biyectivas. 86
4.2 Función invertible. 91

5 **Inducción Matemática** — **Página 95**

5.1 Introducción 95

6 **Relaciones de recurrencia** — **Página 101**

6.1 Introducción 101

7 ESTRUCTURAS ALGEBRAICAS ____ PÁGINA 107

7.1 Ley de composición interna 107

7.2 Grupos 109

Los grupos $(\mathbb{Z}_m, +)$ y $(\mathbb{Z}_m^*, \cdot)$ 113

7.3 Subgrupos 116

(*) Grupos cíclicos 120

.... 122

Bibliografía 122

(http://tecdigital.tec.ac.cr/revistamatematica/).

Capítulo 1

Lógica proposicional

"The computer and programming languages were invented by logicians as the unexpected product of their unsuccessful effort to formalize reasoning completely. Formalism failed for reasoning, but it succeeded brilliantly for computation. In practice, programming requires more precision than proving theorems!
...But it's possible to argue that the (Gödel) incompleteness theorems completely miss the point because mathematics isn't about the consequences of rules, it's about creativity and imagination."
G. Chaitin [9].

Las leyes de la lógica son usadas para distinguir entre argumentos válidos o inválidos. La maquinaria de la lógica proposicional permite formalizar y teorizar sobre la validez de una gran cantidad de argumentos. Sin embargo, también existen argumentos que son intuitivamente válidos, pero cuya validez no se puede probar por la lógica proposicional. El propósito de este tema, en este curso, es el de enseñar al estudiante cómo entender y como contruir un argumento matemático de manera correcta.

Una proposición es una afirmación que es verdadera (V) o falsa (F), pero no ambas. Las proposiciones se denotan con las letras $P, Q, R,$ etc.

En lenguage natural nos interesan dos cosas, el valor de verdad y el significado. Pero a la lógica proposicional le interesa el "valor de verdad" de las proposiciones, no su significado.

Ejemplo 1.1

a.) $P:$ "$2 > 3$" es una proposición pues es una afirmación falsa (F)

b.) $Q:$ "$5 > 1$" es una proposición pues es una afirmación verdadera (V)

c.) $R:$ "$x + 1 = 3$" no es un proposición pues no es F ni V, su valor de verdad depende del valor de x

Principios fundamentales de la lógica formal. Tenemos tres principios

a.) **Principio de Identidad:** Si una proposición es verdadera, siempre es verdadero

b.) **Principio de No-contradición:** Ninguna proposición es falsa y verdadera

c.) **Principio del Tercero Excluído:** Una proposición o es falsa o es verdadera (no una tercera posibilidad)

La paradoja del mentiroso: Consideremos la afirmación: "Esta oración es falsa". Si fuera una proposición, por el principo del tercero excluído, debe ser verdadera o falsa, pero no es posible asignar un valor de verdad a la oración sin contradecirse.

La negación, la conjunción y la disyunción. Tablas de verdad

Muchas proposiciones son compuestas, están formadas por varias proposiciones ligados por partículas especiales del lenguage llamadas “conectivas”. Por ejemplo $R:$ ”$2>3$” y $q:$ ”$5>1$” es una proposición formada por dos proposiciones, la conectiva es la “y”.

La negación de la proposición P es $\neg P$. Por ejemplo, la negación de P : “Todos los números pares son divisibles por dos” sería $\neg P:$ “Existe al menos un número par que no es divisible por dos”.

La conectiva llamada conjunción se denota con $\wedge$. La proposición $P \wedge Q$ se lee “P y Q”

La conectiva llamada disyunción se denota con $\vee$. La proposición $P \vee Q$ se lee “P o Q”

La conectiva llamada disyunción exclusiva se denota con $\veebar$. La proposición $P \veebar Q$ se lee “P ó Q”

La conectiva llamada implicación se denota con “$\rightarrow$”. La proposición $P \rightarrow Q$ se lee “P implica Q” o también “ Si P entonces Q”.

A la lógica le inetresa solo el valor de verdad de la proposición “P implica Q”. En lenguage natural, la palabra “implica” involucra el significado de las proposiciones.

La conectiva llamada equivalencia se denota con “ $\equiv$ ”. La proposición $P \equiv Q$ se lee “P es lógicamente equivalente a Q”. También se puede denotar $P \longleftrightarrow Q$

Por ejemplo,

a.) $P \vee Q \equiv Q \vee P$
b.) $P \wedge Q \equiv Q \wedge P$

Tablas de verdad. Para determinar el valor de verdad de una proposición compuesta necesitamos conocer el valor de verdad de las proposiciones que la componen. Una tabla de verdad es una tabla que muestra el valor de verdad de una proposición compuesta, para cada combinación de verdad que se pueda asignar a cada componente individual.

Las tablas de verdad básicas son:

Negación

P	$\neg P$
V	F
F	V

Conjunción

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Disyunción

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Implicación

P	Q	$P \to Q$
V	V	V
V	F	F
F	V	V
F	F	V

Equivalencia

P	Q	$P \equiv Q$
V	V	V
V	F	F
F	V	F
F	F	V

Implicación: En la tabla de la "implicación", las dos últimas líneas dicen algo como "Falso implica cualquier cosa" y esto podría parecer "contra-intuitivo". Uno puede asumir que esto simplemente está definido así para que sea consistente con la inferencia lógica conocida como "Modus Tollens" (que veremos más adelante), o que se puede deducir de otras equivalencias.

En todo caso, para tener alguna intuición, podemos decir que $P \to Q$ es una "promesa Q en el caso que se cumpla P". La única manera de que hablemos con falsedad es que se cumpla P pero que no cumplamos Q!. Si no se cumple P, la promesa no es falsa. Por ejemplo, suponga que una Alicia le dice a Alfredo:

"Si mañana me traes un confite, entonces te doy un beso"

En circunstancias normales, la única manera de que Alicia haya hablado con falsedad es que Alfredo traiga el confite y Alicia no le da el beso. En cualquier otro caso no podemos decir que que Alicia habló con falsedad, es decir, los otros casos son no-falsos, en nuestro sistema esto equivale a decir que son verdaderos.

Hay una anéctoda del filósofo y lógico Bertand Russell.

> "The story goes that Bertrand Russell, in a lecture on logic, mentioned that in the sense of material implication, a false proposition implies any proposition.
>
> A student raised his hand and said 'In that case, given that 1 = 0, prove that you are the Pope.'
>
> Russell immediately replied, 'Add 1 to both sides of the equation: then we have 2 = 1. The set containing just me and the Pope has 2 members. But 2 = 1, so it has only 1 member; therefore, I am the Pope.'"

Pruebas de teoremas con tablas de verdad. Un teorema es una proposición cuya validez se puede obtener como consecuencia lógica de los axiomas, definiciones u otros teoremas. En lógica proposicional, una proposición compuesta por P, Q, R, etc. que es una implicación o equivalencia, es un teorema válido si su valor de verdad es V para todos los posibles valores de verdad de P, Q, R, etc. En este caso también decimos la proposición es una *tautología.*

Tautologías, contradiciones y contingencias.

Como dijimos antes, una proposición compuesta es una *tautología* si es verdadera para todos los valores de verdad de las proposiciones atómicas que la componen.

Si una proposición es falsa para todos los valores de verdad de las proposiciones atómicas que la componen, la proposición es una *contradicción*.

Si una proposición compuesta no es tautología ni contradiccón, es *una contingencia o eventualidad*

Si $P \rightarrow Q$ es una tautología, se escribe $P \implies Q$

Si $P \longleftrightarrow Q$ es una tautología, se escribe $P \iff Q$

Ejemplo 1.2

Use una tabla de verdad para probar que $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$

Solución: : Una tabla de verdad mínima requiere los valores de verdad de P, Q, $\neg (P \wedge Q)$, $\neg P \vee \neg Q$ y la equivalencia que queremos verificar: $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$

P	Q	$\neg (P \wedge Q)$	$\neg P \vee \neg Q$	$\neg (P \wedge Q) \equiv \neg P \vee \neg Q$
V	V	F	F	V
V	F	V	V	V
F	V	V	V	V
F	F	V	V	V

Ejemplo 1.3

Use una tabla de verdad para probar que $P \vee Q \not\equiv P \wedge Q$

Solución: Ejercicio. Hacemos una tabla de verdad y verificamos que $P \vee Q \equiv P \wedge Q$ no es una tautología.

P	Q	$P \vee Q$	$P \wedge Q$	$P \vee Q \equiv P \wedge Q$
V	V			
V	F			
F	V			
F	F			

Ejemplo 1.4

Use una tabla de verdad para probar que $P \rightarrow Q \equiv \neg P \vee Q$ es una tautología.

Solución: Ejercicio.

P	Q	$P \to Q$	$\neg P \vee Q$	$P \to Q \equiv \neg P \vee Q$
V	V			
V	F			
F	V			
F	F			

Ejemplo 1.5

Use una tabla de verdad para probar que $[(P \to Q) \wedge (Q \to R)] \to (P \to R)$

Solución:

P	Q	R	$P \to Q$	$Q \to R$	$(P \to Q) \wedge (Q \to R)$	$P \to R$	$[(P \to Q) \wedge (Q \to R)] \to (P \to R)$
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

Ejemplo 1.6

Use una tabla de verdad para probar que $\neg (P \vee Q) \equiv \neg P \wedge \neg Q$

Solución: Ejercicio.

P	Q	$\neg (P \vee Q)$	$\neg P \wedge \neg Q$	$\neg (P \vee Q) \equiv \neg P \wedge \neg Q$
V	V			
V	F			
F	V			
F	F			

Ejercicios

1.0.1 ▶ Use tablas de verdad para determinar si las siguientes proposiciones son tautologías, contradicciones o contingencias.

1) $P \equiv \neg\neg P$

2) $P \wedge Q \equiv P$

3) $P \equiv P \vee Q$

4) $(P \to Q) \wedge \neg Q \equiv \neg P$

5) $(P \to Q) \wedge P \equiv Q$

6) $(P \vee Q) \wedge \neg Q \equiv P$

7) $(P \to Q) \wedge (\neg P \to S) \equiv S \vee Q$

8) $(\neg P \wedge Q) \to (\neg Q \vee P)$

9) $\neg(P \to Q) \longleftrightarrow (P \wedge \neg Q)$

10) $(\neg P \wedge \neg Q) \wedge \neg(P \longleftrightarrow Q)$

11) $(P \vee Q) \to [Q \to (P \wedge Q)]$

1.1 Equivalencias lógicas y simplificación

No siempre tenemos que usar tablas de verdad para probar una equivalencia lógica. A partir de una tabla de equivalencias lógicas preestablecidas, se puede deducir y probar otras equivalencias usando *simplificación*. Aquí vamos a usar la notación $\equiv$ para equivalencia, V_0 para tautología (*proposición siempre verdadera*), F_0 para contradicción (*proposición siempre falsa*).

Primero iniciamos con una tabla de equivalencias lógicas.

Implicación-disyunción (ID)	$P \to Q \equiv \neg P \vee Q$
Contrapositiva	$P \to Q \equiv \neg Q \to \neg P$
DN	$\neg\neg P \equiv P$
De Morgan	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
Conmutatividad	$P \vee Q \equiv Q \vee P$
	$P \wedge Q \equiv Q \wedge P$
Asociatividad	$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$
	$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$
Distribuitividad	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

Idenpotencia	$P \wedge P \equiv P$
	$P \vee P \equiv P$
Inversos	$P \vee \neg P \equiv V_0$
	$P \wedge \neg P \equiv F_0$
Neutro	$P \vee F_0 \equiv P$
	$P \wedge V_0 \equiv P$
Dominación	$P \wedge F_0 \equiv F_0$
	$P \vee V_0 \equiv V_0$
Absorción	$P \vee (P \wedge Q) \equiv P$
	$P \wedge (P \vee Q) \equiv P$
Exportación	$P \to (Q \to R) \equiv (P \wedge$

Ahora, usando esta última tabla podemos hacer simplificaciones o también pruebas de equivalencias.

La equivalencias y sus sabores. Es usual encontrar las equivalencias de la tabla anterior, con sabores distintos. Por ejemplo

a.) $P \to Q \equiv \neg P \vee Q$ se puede encontrar como

$$\begin{aligned} \neg P \to Q &\equiv P \vee Q \\ (P \vee R) \to Q &\equiv \neg (P \vee R) \vee Q \\ P \to \neg Q &\equiv \neg P \vee \neg Q \end{aligned}$$

b.) $P \vee (P \wedge Q) \equiv P$ se puede encontrar como $(P \vee R) \vee ((P \vee R) \wedge Q) \equiv P \vee R$

Ejemplo 1.7

Suponga que $(P \to Q) \wedge R$ es verdadero. Determine el valor de verdad de la proposición

$$[(\neg P \vee T) \vee Q] \wedge (\neg R \to S)$$

Solución: Usando la tabla de equivalencias, podemos hacer algunas simplificaciones. Por ejemplo

$$(\neg P \vee T) \vee Q \equiv (\neg P \vee Q) \vee T \equiv (P \to Q) \vee T$$

Bien, $(P \to Q) \wedge R$ es verdadero solo si $(P \to Q)$ y R son verdaderas. Por tanto,

$[(\neg P \vee T) \vee Q] \equiv (P \to Q) \vee T$ es siempre verdadera pues $(P \to Q)$ es verdadera.

$(\neg R \to S) \equiv R \vee S$ es siempre verdadera pues R es verdadera.

$\therefore [(\neg P \vee T) \vee Q] \wedge (\neg R \to S)$ es verdadera

Ejemplo 1.8

Sean A, B, C, D y E proposiciones tales que $(A \wedge \neg B) \to C$ es falso. Determine el valor de verdad de la proposición.

$$[(A \vee D) \wedge (B \wedge D)] \to (C \vee E)$$

Solución: Una implicación $(A \wedge \neg B) \to C$ es falsa solo si $(A \wedge \neg B)$ es verdadera y C es falsa. Por tanto A es verdadera y B y C son falsas. Entonces,

$$(A \vee D) \equiv V_0 \text{ y } (B \wedge D) \equiv F_0 \text{ y por lo tanto } [(A \vee D) \wedge (B \wedge D)] \equiv F_0$$

En conclusión,

$$[(A \vee D) \wedge (B \wedge D)] \to (C \vee E) \equiv F_0 \to (C \vee E) \equiv V_0$$

Ejemplo 1.9

Determine el valor de verdad de las proposiciones A, B, C y D de manera que la siguiente proposición sea falsa.

$$\neg\,[A \to (D \wedge B)] \vee [C \to (B \vee (A \longleftrightarrow D))]$$

Solución: Una disyunción es falsa solo si las proposiciones que conecta son falsas. Por tanto,

1) $A \to (D \wedge B)$ es verdadera

2) $C \to (B \vee (A \longleftrightarrow D))$ es falsa.

Luego: $C \to (B \vee (A \longleftrightarrow D))$ es falsa si C es verdadera y si $(B \vee (A \longleftrightarrow D))$ es falsa, es decir, necesitamos que B sea falsa y A y D tengan valor de verdad diferente, así $(A \longleftrightarrow D)$ es falsa.

Como B debe ser falsa, A debe ser falsa para que $A \to (D \wedge B)$ sea verdadera.

En resumen: A y B son falsas y C y D son verdaderas.

Pruebas de equivalencias usando la tabla de equivalencias lógicas

Ejemplo 1.10

Probar que $P \wedge (Q \vee \neg Q) \equiv P$

Solución:

$$\begin{array}{rcll} P \wedge (Q \vee \neg Q) & \equiv & P \wedge \mathbf{V_0} & \text{Inversos} \\ & \equiv & P & \text{Neutro} \end{array}$$

Ejemplo 1.11

Probar que $P \to (Q \wedge R) \equiv (P \to Q) \wedge (P \to R)$

Solución:

$$\begin{array}{rcll} P \to (Q \wedge R) & \stackrel{\text{ID}}{\equiv} & \neg P \vee (Q \wedge R) & \text{ahora usamos distribuitividad,} \\ & \equiv & (\neg P \vee Q) \wedge (\neg P \vee R) & \text{ahora usamos ID,} \\ & \equiv & (P \to Q) \wedge (P \to R) & \end{array}$$

Ejemplo 1.12

Probar que $P \vee \neg(\neg R \vee P) \vee R \equiv P \vee R$

Solución: Iniciamos usando De Morgan,

$$\begin{array}{rcll}
P \vee \neg(\neg R \vee P) \vee R & \overset{\text{DM}}{\equiv} & P \vee (R \wedge \neg P) \vee R, & \text{agrupamos y usamos distribuitividad,} \\
& \equiv & [P \vee (R \wedge \neg P)] \vee R & \\
& \equiv & [(P \vee R) \wedge (P \vee \neg P)] \vee R, & \text{ahora usamos inv. y neutro,} \\
& \equiv & [(P \vee R) \wedge V_0] \vee R, & \text{ahora usamos idenpotencia y asoc.,} \\
& \equiv & P \vee R \vee R & \\
& \equiv & P \vee R &
\end{array}$$

Ejemplo 1.13

Probar que $\neg[(Q \vee P) \wedge \neg((\neg P \wedge \neg Q \wedge R) \wedge (P \vee R))] \equiv \neg P \wedge \neg Q$.

Solución:

$$\begin{array}{rcll}
\neg[(Q \vee P) \wedge \neg((\neg P \wedge \neg Q \wedge R) \wedge (P \vee R))] & \equiv & \neg[(Q \vee P) \wedge (P \vee Q \vee \neg R \vee \neg(P \vee R))] & \text{DM} \\
& \equiv & \neg[(P \vee Q) \wedge ((P \vee Q) \vee (\neg R \vee \neg(P \vee R)))] & \ldots \\
& \equiv & \neg(P \vee Q) & \ldots \\
& \equiv & \neg P \wedge \neg Q & \ldots
\end{array}$$

Ejemplo 1.14

Sean P, Q, y R proposiciones. Demuetre que se tienen las siguientes equivalencias,

a.) $P \rightarrow (Q \wedge R) \equiv (P \rightarrow Q) \wedge (P \rightarrow R)$

b.) $(P \wedge Q) \rightarrow R \equiv (P \rightarrow R) \vee (Q \rightarrow R)$

c.) $P \rightarrow (Q \vee R) \equiv (P \rightarrow Q) \vee (P \rightarrow R)$

d.) $(P \vee Q) \rightarrow R \equiv (P \rightarrow R) \wedge (Q \rightarrow R)$

Solución: a.) ya los hicimos en el ejemplo 1.7, b). Haremos solo b.) y, c.) y d.) quedan como ejercicios.

$$\text{b.)} \left\{ \begin{array}{rcll}
(P \wedge Q) \rightarrow R & \overset{\text{ID}}{\equiv} & \neg(P \wedge Q) \vee R, & \text{ahora usamos De Morgan} \\
& \equiv & \neg P \vee \neg Q \vee R, & \text{ahora usamos idenpotencia: } R \equiv R \vee R \\
& \equiv & \neg P \vee \neg Q \vee R \vee R, & \text{ahora usamos asociatividad} \\
& \equiv & (\neg P \vee R) \vee (\neg Q \vee R), & \text{usando ID:} \\
& \equiv & (P \rightarrow R) \vee (Q \rightarrow R) &
\end{array} \right.$$

Ejemplo 1.15

Probar $\neg\,[P \wedge \neg\,(T \wedge R)] \wedge (T \rightarrow \neg\,P) \equiv \neg\,P$

Solución: Primero visualizamos un plan: Distributividad. Reacomodamos todo

$$
\begin{array}{rcll}
\neg\,[P \wedge \neg\,(T \wedge R)] \wedge (T \rightarrow \neg\,P) & \equiv & (\neg\,P \vee \neg\,T) \wedge (\neg\,P \vee (T \wedge R)) & \text{ID, Morgan y conmutatividad} \\
 & \equiv & (\neg\,P \vee \neg\,T) \wedge (\neg\,P \vee (T \wedge R)) & \text{Visualizar distributividad!!!} \\
 & \equiv & \neg\,P \vee (\neg\,T \wedge (T \wedge R)) & \text{Distributividad} \\
 & \equiv & \neg\,P \vee ((\neg\,T \wedge T) \wedge R) & \text{Asociatividad, Inversos} \\
 & \equiv & \neg\,P \vee (F_0 \wedge R) & \text{Dominación} \\
 & \equiv & \neg\,P \vee F_0 & \text{Neutro} \\
 & \equiv & \neg\,P &
\end{array}
$$

Ejercicios

1.1.1 ▶ Determine el valor de verdad de las proposiciones P y Q para $[P \wedge (P \rightarrow Q)] \longleftrightarrow Q$ sea falsa

1.1.2 ▶ Determine el valor de verdad de P, Q, y R si se sabe que la proposición $[P \wedge (P \rightarrow Q)] \longleftrightarrow Q$ es falsa, y que la proposición $[(P \rightarrow Q) \wedge (\neg\,P \rightarrow R)] \longleftrightarrow (Q \vee R)$ es falsa

1.1.3 ▶ Determine el valor de verdad de las proposiciones A, B, C y D de manera que la proposición que sigue sea falsa.

$$(D \wedge B) \vee [(B \wedge (A \longleftrightarrow \neg\,D)) \rightarrow C]$$

1.1.4 ▶ Suponga que $((A \rightarrow B) \wedge C \wedge \neg\,B) \rightarrow (H \vee F)$ es falso. Determine el valor de verdad de las proposiciones involucradas.

1.1.5 ▶ Sean A, B, y C proposiciones tales que $\neg\,A \wedge \neg\,B \wedge \neg\,C$ es verdadero. Determine el valor de verdad de

$$A \rightarrow (B \vee C)$$

1.1.6 ▶ Pruebe las siguientes equivalencias haciendo uso de las leyes de la lógica. Indique la ley que utiliza en cada paso.

1) $\neg\,(\neg\,P \wedge \neg\,Q \wedge R) \equiv P \vee Q \vee \neg\,R$

2) $P \wedge (P \vee Q \vee S) \equiv P$

3) $(P \vee S) \vee (\neg\,Q \wedge S) \equiv P \vee S$

4) $P \vee (Q \wedge S) \vee (\neg\,Q \wedge S) \equiv P \vee S$

5) $[P \vee \neg(\neg Q \vee \neg S)] \vee \neg(\neg Q \rightarrow \neg S) \equiv P \vee S$

6) $\neg[P \wedge \neg(T \wedge R)] \wedge (T \rightarrow \neg P) \equiv \neg P$

7) $\neg(\neg P \wedge \neg Q \wedge R \wedge (P \vee R)) \equiv P \vee Q \vee \neg R$

8) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee \neg(P \rightarrow \neg R)$

9) $(R \wedge Q) \rightarrow T \equiv (R \rightarrow \neg Q) \vee [T \wedge (R \vee T)]$

1.1.7 ▶ Verifique que $(P \wedge Q) \not\equiv Q$ pero que $(P \wedge Q) \rightarrow Q$ sí es una taulología

1.1.8 ▶ Verifique que $((P \rightarrow Q) \wedge P) \not\equiv Q$ pero que $((P \rightarrow Q) \wedge P) \rightarrow Q$ sí es una taulología

1.2 Cuantificadores

Proposición abierta o predicado. Denotamos con $P(n)$ una proposición que depende de la variable n y $Q(x,y)$ denota una proposición que depende de as variables x e y. El *universo del discurso, o dominio,* son los objetos que se consideran en las proposiciones abiertas. Una *instanciación*[1] es un caso particular: $P(k)$ o $Q(a,b)$. Por ejemplo:

a.) Consideremos la proposición abierta "$P(n): 2^n \geq n^2$ si n es un número natural". En este caso, la *instancia* $P(3)$ es falsa pues $2^3 \not\geq 3^2$

b.) Consideremos la proposición abierta "$Q(x,y): x^2+y^2 \geq 0$ si x,y son números reales". $Q(x,y)$ es verdadera para cualquier valor de x y y pues la suma de cuadrados es cero o positiva.

Para "cuantificar" los elementos que satisfacen una proposición se usan los cuantificadores existencial y universal.

a.) Cuantificador existencial $(\exists x)[P(x)]$ se lee "existe x tal que $P(x)$". Es decir, existe al menos una *instancia* $P(x_0)$ que es verdadera.

b.) Cuantificador universal $(\forall x)[P(x)]$ se lee "para todo x, $P(x)$". Es decir, todas las *instancias* $P(x)$ son verdaderas.

c.) $\exists x \forall y\, [P(x,y)]$ es verdadera si y solo si existe un valor x_0 de x (un valor fijo) tal que para todos los posibles valores "y" se tiene que $P(x_0,y)$ es verdadera. Es decir, existe un x_0 que sirve para todos los y.

d.) $\forall x \exists y\, [P(x,y)]$ es verdadera si y solo si para cada valor x, existe un valor "y_x", (es decir, "y" posiblemente depende del valor del valor de x) tal que $P(x,y_x)$ es verdadero

Conjuntos especiales: Recordemos la notación para algunos conjuntos

a.) El conjunto de los números naturales $\mathbb{N} = \{0,1,2,3,...\}$ y los naturales positivos $\mathbb{N}^* = \mathbb{N} - \{0\}$

[1] El término en informática procede del inglés, en donde 'instance' viene del significado que podría traducirse por caso o ejemplo en castellano.

b.) El conjunto de los enteros $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\}$ y los enteros positivos $\mathbb{Z}^+ = \mathbb{N}^*$

c.) El conjunto de los números racionales $\mathbb{Q} = \left\{ \dfrac{p}{q} \text{ tal que } a, b \in \mathbb{Z} \wedge q \neq 0 \right\}$

d.) El conjunto de los números reales $\mathbb{R}$ y los reales positivos y negativos $\mathbb{R}^+ = \{x \text{ tal que } x \in \mathbb{R} \wedge x > 0\}$ y $\mathbb{R}^- = \{x \text{ tal que } x \in \mathbb{R} \wedge x < 0\}$

Ejemplo 1.16

a.) " $(\exists\, n \in \mathbb{N})\ [2^n < n^2]$ " es verdadera pues existe al menos un número natural, $n_0 = 3$, cumple con la propiedad: $2^3 < 3^2$

b.) " $(\forall\ x \in \mathbb{R})(\forall\, y \in \mathbb{R})\ [x^2 + y^2 \geq 0]$ " es verdadera pues la suma de cuadrados es siempre mayor o igual a cero.

c.) " $(\exists\, x \in \mathbb{Z})(\exists\, y \in \mathbb{Z})[x + y = 0]$ " es verdadera, por ejemplo tomamos $x = 1$ y $y = -1$.

d.) " $(\exists\, x \in \mathbb{N}^*)(\exists\, y \in \mathbb{N}^*)[x + y = 0]$ " es falsa, pues como $x > 0$ y $y > 0$, enotnces la suma $x + y > 0$.

Observe que " $\exists\, x \,\forall\, y\ P(x,y)$ " y " $\forall\, x \,\exists\, y\ P(x,y)$ " son proposiciones distintas.

Ejemplo 1.17

Considere la proposición abierta $P(x,y) : \dfrac{x}{y} \in \mathbb{N}$. Si $A = \{0, 6, 8, 9, 10, 15\}$ y $B = \{2, 3, 5, 7\}$, determine el valor de verdad de las proposiciones:

a.) $(\forall x \in A)(\exists\, y \in B)[P(x,y)]$

b.) $(\exists\, y \in B)(\forall x \in A)[P(x,y)]$

Solución:

a.) $(\forall x \in A)(\exists\, y \in B)[P(x,y)]$ es verdadera pues $\dfrac{0}{2}, \dfrac{6}{2}, \dfrac{8}{2}, \dfrac{9}{3}, \dfrac{10}{2}, \dfrac{15}{3} \in \mathbb{N}$

b.) $(\exists\, y \in B)(\forall x \in A)[P(x,y)]$ es falsa pues no existe un divisor común $y \in B$, para todos lo elementos de A. Por ejemplo, $x = 8$ y $x = 9$ necesitan un divisor $y \in B$ distinto,

Ejemplo 1.18

a.) La proposición $P(n) : (\forall\, n \in \mathbb{N}^+)(\exists\, m \in \mathbb{N}) \left[\dfrac{1}{n} \leq m \right]$ es verdadera.

En efecto: Como $\forall\, n \in \mathbb{N}^+$, $n \geq 1$, dividimos por n a ambos lados y obtenemos $\dfrac{1}{n} \leq 1$. Tomamos

$m = 1$. Tambi'en existen otros valors para m, pero lo que importa aqui es que existe al menos un valor de m.

b.) La proposición $(\exists\, y \in \mathbb{Z})(\forall\, x \in \mathbb{R}^*)\ [x \cdot y > 0]$ es falsa.

En efecto: Para cualquier x, **no existe un valor de** y **fijo** para que $xy > 0$. Si $x > 0$, sirve cualquier $y > 0$ pero si $x < 0$, se requiere un valor $y < 0$

Ejemplo 1.19

Considere las siguientes proposiciones abiertas:

- $P(x) : 3x - 1$ es un número primo
- $Q(x) : 6 \leq x < 14$
- $R(x) : x$ es un número par

Determine el valor de verdad de las proposiciones:

a.) $(\exists\, x \in \mathbb{N})[P(x) \wedge Q(x) \wedge \neg R(x)]$

b.) $(\forall\, x \in \mathbb{N})[(Q(x) \wedge R(x)) \rightarrow P(x)]$

Solución:

a.) Falsa. Los números x que cumplen $Q(x) \wedge \neg R(x)$ son los impares entre 6 y 14, es decir, $S = \{7, 9, 11, 13\}$. Pero si $x \in S$, $3x - 1$ no es primo (son pares > 2).

b.) Falsa. Los números x que cumplen $Q(x) \wedge R(x)$ son los pares $S = \{6, 8, 10, 12\}$. Pero si $x \in S$, $3x - 1$ no es necesariamente primo (por ejemplo si $x = 12 \implies 3x - 1 = 35$ que no es primo).

Ejemplo 1.20

Considere los conjuntos $A = \{x \in \mathbb{N}$ tal que $-2x + 3 = -9\}$, $B = \{1, 2, 3, 4, 5\}$ y $C = \{2, 3, 6, 7, 8\}$. Determine el valor de verdad de las siguientes proposiciones, justificando cada respuesta:

a.) $(\forall\, x \in B)(\exists\, y \in C)\ [x + 1 = y]$

b.) $\exists\, x\ [x \in B \rightarrow (x^2 + 2) \in A \cap C]$

Solución:

a.) Falsa pues para $x = 3 \in B$ pero $3 + 1 \notin C$

b.) Verdadera pues existe $x = 2 \in B$ para el que $x^2 + 2 = 6 \in A \cap C$ pues $6 \in C$ y $-2 \cdot 6 + 3 = -9$, es decir, $6 \in A$.

Teorema 1.1

a.) $\neg\,[\forall\, x\, P(x)] \;\equiv\; \exists\, x\,[\neg\, P(x)]$

b.) $\nexists\, x\, P(x) \;\equiv\; \forall\, x\,[\neg\, P(x)]$

c.) $\forall\, x\,[P(x) \wedge Q(x)] \;\equiv\; \forall\, x\, P(x) \wedge \forall\, x\, Q(x)]$

d.) $\exists\, x\,[P(x) \wedge Q(x)] \;\equiv\; \exists\, x\, P(x) \wedge \exists\, x\, Q(x)]$

e.) $\exists\, x\, P(x) \;\equiv\; \neg\, \forall\, x\,[\neg\, P(x)]$

f.) $\forall\, x\, P(x) \;\equiv\; \nexists\, x\,[\neg\, P(x)]$

Observe que

$$\neg\,[\forall\, x\,[P(x) \wedge Q(x)]] \;\equiv\; \exists\, x\,[\neg\, P(x)] \vee \exists\, x\,[\neg\, Q(x)]$$

$$\neg\,[\forall\, x\,[P(x) \vee Q(x)]] \;\equiv\; \exists\, x\,[\neg\, P(x)] \wedge \exists\, x\,[\neg\, Q(x)]$$

Ejemplo 1.21

a.) $\neg\,[\forall\, x \in \mathbb{R}\,[x > 0]] \;\equiv\; \exists\, x \in \mathbb{R}\,[x \leq 0]$

b.) $\neg\,[\forall\, x \in \mathbb{R}\,[x \neq 0]] \;\equiv\; \exists\, x \in \mathbb{R}\,[x = 0]$

c.) $\neg\,[\forall\, x \in \mathbb{R}\,[x > 0 \wedge x \neq 3]] \;\equiv\; \exists\, x \in \mathbb{R}\,[x \leq 0 \vee x = 3]$

Ejemplo 1.22

Negar la proposición: $Q(x,y): \;\forall\, x \in \mathbb{N}\,[\,\underline{7x + 4 < 40} \;\vee\; \underline{\forall\, y \in \mathbb{N}\,(x + y \neq 5)}\,]$

Solución: $\neg\, Q(x,y) \;\equiv\; \exists\, x \in \mathbb{N}\,[\,7x + 4 \geq 40 \wedge \exists\, y \in \mathbb{N}\,(x + y = 5)\,]$

Ejercicios

1.2.1 ▶ Negar las siguientes proposiciones.

1) $\exists\, x \in \mathbb{N}\ \left[\, x > 4 \wedge x^2 \leq 7 \,\right]$

2) $\forall\, x \in \mathbb{Z}\ \left[x^2 + 2x - 3 > 0 \wedge x + 4 \leq 8\right]$

3) $\forall\, x \in \mathbb{Z}\ [(x + 1 = 4 \implies x \geq 3)]$

1.2.2 ▶ Sea $A = \{0, 3, 6, 9\}$ y $B = \{0, 1, 2, 3, 4, 5\}$. Determine el valor de verdad de las siguientes proposiciones

1) $(\forall y \in A)(\exists\, x \in B)[y = 3x]$

2) $(\exists\, x \in B)(\forall y \in A)\left[\dfrac{y}{x} \in B\right]$

1.2.3 ▶ **Paradoja de Epiménides:** Epiménides fue un legendario poeta filósofo del siglo VI a. C. a quien se le atribuye haber estado dormido durante cincuenta años. Se atribuye a Epiménides haber afirmado:

> "Todos los cretenses son unos mentirosos"

Sabiendo que él mismo era cretense, ¿decía Epiménides la verdad?

Bien, verifique que si definimos que un mentiroso sólo hace afirmaciones que son falsas, entonces si la afirmación de Epiménides es verdadera, llegamos a una contradicción, pero que sí podría ser falsa.

1.2.4 ▶ **Contraejemplos:** Dé un "contraejemplo" para la afirmación "Todo entero positivo es la suma de los cuadrados de tres enteros."

1.2.5 ▶ Determine el valor de verdad de las siguientes proposiciones, justificando cada respuesta:

a.) $(\forall x \in \mathbb{R})(\exists\, y \in \mathbb{R})\ \left[x^2 = y\right]$

b.) $(\forall x \in \mathbb{R})(\exists\, y \in \mathbb{R})\ \left[y^2 = x\right]$

c.) $(\forall x \in \mathbb{R})(\exists\, y \in \mathbb{R})\ [x + y = 2 \wedge 2x - y = 1]$

d.) $(\exists\, x \in \mathbb{R})(\forall y \in \mathbb{R})\ [y \neq 0 \implies xy = 1]$

e.) $(\exists\, x \in \mathbb{R})(\forall y \in \mathbb{R})\ [xy = 0]$

1.2.6 ▶ Determine el valor de verdad de las siguientes proposiciones, justificando cada respuesta:

a.) $(\forall x \in \mathbb{R})(\exists\, y \in \mathbb{R}\ \left[x^2 = y\right]$

b.) $(\exists\, y \in \mathbb{R})(\forall x \in \mathbb{R} - \{3\})\ \left[\dfrac{x - y}{3 - x} + x + 1 = x\right]$

1.2.7 ▶ Sean $A = \{1, 3, 5, 8, 9\}$ y $B = \{2, 3, 4, 5, 9\}$. Considere la proposición abierta:

$$P(x) : x \text{ es par}$$

Determine el valor de verdad de las siguientes proposiciones, justificando cada respuesta:

a.) $(\exists\, x \in A \cup B)\ [P(x)]$

b.) $(\forall x \in \mathbb{N})\ [x \in A \cap B \implies P(x+1)]$

c.) $(\exists\, x \in A)(\forall y \in A \cap B)\ [P(x+y)]$

1.2.8 ▶ **Pruebas por construcción:** Mostrar que existe un entero positivo que puede ser expresado como la suma de cubos de enteros positivos en dos diferentes formas (Hardy-Ramanujan), es decir, $(\exists\, n \in \mathbb{Z}^+)(\exists\, p,q,r,s \in \mathbb{Z}^+)[n = p^3 + q^3 \wedge n = r^3 + s^3]$. ¿Que tal $n = 1729$?

1.3 Inferencias lógicas

Las reglas de inferencia intentan capturar el modo en que naturalmente razonamos acerca de las conectivas lógicas. En las inferencias tenemos unas premisas y, aplicando las reglas de inferencia (y talvés alguna equivalencia), llegamos a una conclusión. En esta tabla, la notación $\therefore$ se puede leer "conclusión" o "por tanto"

Reglas	Premisas		Conclusión
Simplificación	$P \wedge Q$	$\therefore$	P
	$P \wedge Q$	$\therefore$	Q
Adjunción	P, Q	$\therefore$	$P \wedge Q$
Adición	P	$\therefore$	$P \vee Q$
Modus ponens	$P,\ P \to Q$	$\therefore$	Q
Modus tollens	$P \to Q,\ \neg Q$	$\therefore$	$\neg P$
Silogismo Disy	$P \vee Q,\ \neg P$	$\therefore$	Q
Silogismo Hip	$P \to Q,\ Q \to R$	$\therefore$	$P \to R$
Dilema Constructivo	$P \vee Q,\ P \to R,\ Q \to S$	$\therefore$	$R \vee S$
Dilema Destructivo	$\neg R \vee \neg S,\ P \to R,\ Q \to S$	$\therefore$	$\neg P \vee \neg Q$
Ley de casos	$P \to Q,\ \neg P \to R$	$\therefore$	$Q \vee R$

Observación 1. Al aplicar inferencias lógicas, podemos usar reglas de simplificación en pasos intermedios

Observación 2: No hay que confundir reglas de simplificación con inferencias lógicas. Por ejemplo

"$P,\ P \to Q \quad \therefore\ Q$" es una inferencia correcta, pero $(P \wedge\ (P \to Q)) \not\equiv Q$

Observación 3. Las inferencias se pueden poner en lenguaje de tautologías

$P,\ P \to Q \quad \therefore\ Q$ se puede expresar en la forma "tautológica" $((P \to Q) \wedge\ P) \to Q$

Sabores. Por supuesto, las leyes aparecen en distintos sabores. Por ejemplo

Modus ponens:	$P,\ P \to Q$	$\therefore\ Q$
	$\neg P,\ \neg P \to Q$	$\therefore\ Q$
	$(P \wedge R),\ (P \wedge R) \to Q$	$\therefore\ Q$

Ley de casos:	$P \to Q,\ \ \neg P \to R$	$\therefore\ Q \vee R$
	$\neg P \vee Q,\ P \vee R$	$\therefore\ Q \vee R$ (por ID)
	$P \to \neg Q,\ \ \neg P \to R$	$\therefore\ \neg Q \vee R$
	$P \to (Q \vee R),\ \ \neg P \to R$	$\therefore\ Q \vee R$ (por idempotecia)

Ejemplo 1.23

Demuestre $(M \vee R) \wedge (\neg R \vee \neg Q),\ Q,\ \ \therefore\ M$

Solución: Podemos poner las premisas en términos de "implicaciones" y usar Ley de casos.

Premisas			Ley
(1)	$(M \vee R) \wedge (\neg R \vee \neg Q)$		
(2)	Q		
Aplicando leyes			
(3)	$(M \vee R) \wedge (\neg R \vee \neg Q)\ \equiv\ \neg R \to M,\ R \to \neg Q$		ID, Adjunción
(4)	$\neg R \to M,\ R \to \neg Q$	$\therefore\ M \vee \neg Q$	Ley de casos
(5)	$M \vee \neg Q,\ Q$	$\therefore\ M$	Silogismo Disyuntivo

Ejemplo 1.24

Demuestre $(\neg P \vee \neg Q) \to (R \wedge S),\ R \to T,\ \neg T,\ \ \ \therefore\ P$

Solución: Plan: Como queremos obtener P, la idea es ver si podemos inferir $\neg(R \wedge S)$ para obtener, por MT, $\neg(\neg P \vee \neg Q)\ \equiv\ P \wedge Q$ en la primera premisa y concluir lo que necesitamos.

Primero usamos MT:	$R \to T,\ \neg T\ \ \therefore\ \neg R,$
tenemos ahora:	$(\neg P \vee \neg Q) \to (R \wedge S),\ \neg R,$
para negar $(R \wedge S)$ usamos adición:	$\neg R\ \ \therefore\ \neg R \vee \neg S\ \equiv\ \neg(R \wedge S),$
tenemos, usando MT,	$(\neg P \vee \neg Q) \to (R \wedge S),\ \neg R \vee \neg S\ \ \therefore\ \neg(\neg P \vee \neg Q)$
usamos DN, DM y simplificación:	$\neg(\neg P \vee \neg Q)\ \equiv\ P \wedge Q,\ P \wedge Q\ \ \therefore\ P$

Ejemplo 1.25

Demuestre $P \to Q,\ Q \to (R \wedge S),\ \neg R \vee \neg T \vee U,\ P \wedge T \quad \therefore U.$

Solución: Plan: Como $\neg R \vee \neg T \vee U \equiv \neg (R \wedge T) \vee U$, bastaría inferir $R \wedge T$ para que, usando SD, concluir U.

Primero usamos simplificación.:	$P \wedge T \quad \therefore P$
Ahora MP:	$P,\ P \to Q \quad \therefore Q.$
Ahora MP:	$Q,\ Q \to (R \wedge S) \quad \therefore R \wedge S.$
Ahora, usando simplificación:	$R \wedge S \quad \therefore R$ y $P \wedge T \quad \therefore T$
Tenemos entonces:	$R \wedge T$
Usando De Morgan:	$(\neg R \vee \neg T) \vee U \equiv \neg (R \wedge T) \vee U$
Ahora usamos SD:	$\neg (R \wedge T) \vee U,\ R \wedge T \quad \therefore U$

Ejemplo 1.26

Demuestre $P \to Q,\ \neg R \to (S \to T),\ R \vee P \vee S,\ \neg R \quad \therefore Q \vee T$

Solución: El plan es "extraer" $P \to Q$ y $S \to T$ y aplicar "dilema constructivo" para concluir $Q \vee T$.

$R \vee (P \vee S),\ \neg R$	$\therefore P \vee S$	Silogismo Disyuntivo
$\neg R,\ \neg R \to (S \to T)$	$\therefore S \to T$	Modus ponens
$S \to T,\ P \to Q,\ P \vee S$	$\therefore T \vee Q$	Dilema constructivo

Ejemplo 1.27

Demostrar la validez del siguiente argumento utilizando las reglas de inferencia y/o leyes de la lógica. Indique en cada paso la ley o la regla que utiliza.

$$
\begin{array}{ll}
1.) & \neg P \to Q \\
2.) & Q \to R \\
3.) & (P \wedge S) \to (\neg P \vee T) \\
4.) & \neg R \\
5.) & \neg Q \to (S \wedge M) \\
\hline
 & \therefore Q \vee T
\end{array}
$$

Solución:

Premisas		Inferencias		Leyes y/o reglas
1.)	$\neg P \to Q$	6.) $Q \to R,\ \neg R$	$\therefore\ \neg Q$	(MT)
2.)	$Q \to R$	7.) $\neg Q \to (S \wedge M),\ \neg Q$	$\therefore\ (S \wedge M)$	(MP)
3.)	$(P \wedge S) \to (\neg P \vee T)$	8.) $\neg P \to Q,\ \neg Q$	$\therefore\ P$	(MT)
4.)	$\neg R$	9.) *De* 7.) *y* 8.)	$\therefore\ P \wedge S$	(S)
5.)	$\neg Q \to (S \wedge M)$	10.) *De* 9.) *y* 3.)	$\therefore\ P \to T$	(MP, ID)
		11.) $\neg P \to Q,\ P \to T$	$\therefore\ Q \vee T$	(LC)

Ejemplo 1.28

Establezca la validez del siguiente razonamiento:

> No ocurre que $a+b=7$ y b sea positivo.
> Si b no es positivo, entonces $2a-3<0$.
> Si el problema no tiene solución única, entonces no ocurre que $a+b=7$ o que b sea postivo.
> Por tanto $a+b \neq 7$.

Solución: Convertimos el razonamiento a forma simbólica

Forma simbólica de las proposiciones	Razonamiento (y equivalencias)
$P:\ a+b=7$	(1.) $\neg(P \wedge Q) \equiv Q \to \neg P$
$Q:\ b$ es positivo	(2.) $\neg Q \to R \equiv \neg R \to Q$
$R:\ 2a-3<0$	(3.) $S \to \neg R$
$S:$ el problema tiene solución única	(4.) $\neg S \to \neg(P \vee \neg Q)$
$\therefore\ \neg P:\ a+b \neq 7$	$\therefore\ \neg P$

Demostración de la inferencia:

De (3.) y (2.) $\therefore\ S \to Q$ por SH

Con (1.) tenemos $S \to Q,\ Q \to \neg P \quad \therefore\ S \to \neg P$ por SH.

Con (4.): $S \to \neg P$ y $\neg S \to \neg(P \vee \neg Q) \quad \therefore\ \neg P \vee \neg(P \vee \neg Q)$ por Ley de casos.

Usando DM $\neg P \vee \neg(P \vee \neg Q) \equiv \neg P \vee (\neg P \wedge Q) \quad \therefore\ \neg P$ por Absorción.

Ejemplo 1.29

Establezca la validez del siguiente razonamiento:

Si estudio C entonces debo matricular un curso de M.
No estudio mucho o no tengo tiempo para leer o necesito vacaciones.
Estudio C y tengo tiempo para leer
Si matriculo un curso de M, entonces debo estudiar mucho y no puedo ir al estadio.
Por lo tanto necesito vacaciones.

Solución: Convertimos el razonamiento a forma simbólica

Forma simbólica de las proposiciones	Razonamiento (y equivalencias)
C : estudio C	(1.) $C \rightarrow M$
M : matriculo un curso de M	(2.) $\neg E \vee \neg L \vee V$
E : estudio mucho	(3.) $C \wedge L$
L : tengo tiempo para leer	(4.) $M \rightarrow (E \wedge \neg S)$
V : necesito vacaciones	$\therefore V$
S : voy al estadio	
$\therefore V$	

La demostración de la inferencia es un ejercicio.

Ejercicios

1.3.1 ▶ Demostrar la validez del siguiente argumento utilizando las reglas de inferencia y/o leyes de la lógica. Indique en cada paso la ley o la regla que utiliza.

$$\neg P \rightarrow Q,\ Q \rightarrow R,\ (P \wedge S) \rightarrow (\neg P \vee T),\ \neg R \wedge S \wedge M \quad \therefore Q \vee T$$

1.3.2 ▶ Demostrar $\neg A \vee \neg C$ a partir de $A \rightarrow B,\ C \rightarrow D,\ (\neg B \vee \neg D) \wedge (\neg A \vee \neg B)$

1.3.3 ▶ Demuestre que $\neg(S \wedge \neg Q)$ a partir de $\neg T, \neg P \rightarrow \neg S$, y $\neg P \vee T$

1.3.4 ▶ Demuestre que $R \rightarrow \neg Q$ a partir de $\neg(R \wedge S)$ y $\neg S \rightarrow \neg Q$

1.3.5 ▶ Demuestre que $\neg(S \vee \neg Q)$ a partir de $\neg S \rightarrow Q,\ \neg(T \wedge R), S \rightarrow T \wedge R$.

1.3.6 ▶ Demuestre P a partir de $(\neg P \vee \neg Q) \rightarrow (R \wedge S),\ R \rightarrow T,\ \neg T$.

1.3.7 ▶ Demuestre U a partir de $P \land T$, $P \to Q$, $Q \to (R \land S)$, $\neg R \lor \neg T \lor U$.

1.3.8 ▶ Por medio de las reglas de inferencia pruebe $\neg T$ a partir de $P \to \neg Q$, $Q \lor \neg R$, $P \land S$, $T \to R \land S$.

1.3.9 ▶ Demuestre la validez del argumento $\neg T \lor U$ a partir de las siguentes hipótesis y utilizando las reglas de inferencia y leyes de la lógica. Indique la ley o la inferencia que utiliza en cada paso.

a.) $R \land Q \to \neg T$

b.) $\neg(\neg P \lor R)$

c.) $\neg(P \land \neg Q)$

d.) $\neg P \lor (R \land S)$

1.4 Epílogo

¿Podríamos establecer el valor de verdad de cualquier proposición que involucre solo números enteros y las operaciones aritméticas usuales?.

El llamado "último teorema de Fermat" dice: Para todo entero ≥ 3, no existen tres enteros x, y y z tal que $x^n + y^n = z^n$. Este problema había estado abierto durante más de 350 años. Fue demostrado por Andrew Wildes (profesor de matemáticas en la Universidad de Princeton) en 1995.

La "Conjetura de Goldbach" dice: Todo entero $n \geq 2$ es la suma de dos números primos. Por ejemplo: $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, ..., $20 = 3+17$, $22 = 3+19 = 11+11$, etc. Se ha verificado que esta conjetura es verdadera para enteros hasta 1.6×10^{18}... pero no para todo $n \geq 2$!. El editor británico Tony Faber ofreció un premio de \$ 1000000 si se presentaba una prueba de esta conjetura antes de abril de 2002. El premio no fue reclamado y esta todavía hoy sin resolver.

¿Sera factible una prueba finita de este problema?[2]

El famoso matemático David Hilbert imaginó en 1900, que se podía establecer el valor de verdad de todas las proposiciones que implican sólo números enteros y operaciones aritméticas [3] Estas proposiciones incluirían las proposiciones de "el último teorema de Fermat" y la conjetura de Goldbach (y muchos otros problemas difíciles sin resolver). Pero, ... el "teorema de incompletitud de Gödel" (1931) dice que esto es una misión imposible!. Este teorema dice, que no hay un sistema de axiomas que describa totalmente a los números naturales, por lo tanto habrá enunciados en teoría de números que pueden ser intuitivamente correctos, pero que

[2] La "conjetura débil de Goldbach" si ha sido probada en 2013, por Harald Helfgott. Esta conjetura afirma que "cada número impar mayor que 5 puede expresarse como la suma de tres primos (un primo puede ser utilizado más de una vez en la misma suma).

[3] "Hilbert had a two-pronged proposal to save the day. First, he said, let's go all the way with the axiomatic method and with mathematical formalism. Let's eliminate from mathematics all the uncertainties and ambiguities of natural languages and of intuitive reasoning. Let's create an artifcial language for doing mathematics in which the rules of the game are so precise, so complete, that there is absolutely no uncertainty whether a proof is correct. In fact, he said, it should be completely mechanical to check whether a proof obeys the rules, because these rules should be completely syntactic or structural, they should not depend on the semantics or the meaning of mathematical assertions! In other words −words that Hilbert didn't use, but that we can use now− there should be a proof-checking algorithm, a computer program for checking whether or not a proof is correct." [9].

el sistema de axiomas que tenemos actualmente no permita probar su veracidad: Son enunciados indecidibles. No se se sabe si el teorema de Golbach será uno de estos enunciados. En el sentido del teorema de Gödel, podría pasar que este teorema no tiene una una "prueba finita" a partir de los axiomas usuales de la artimética.

Gregory Chaitin (1947−) produjo enunciados indecidibles en "teoría algorítmica de la información" y demostró otro teorema de la incompletitud en ese contexto. Afirma que sus resultados en lógica matemática y en teoría de la información algorítmica muestran que hay hechos matemáticos que son ciertos sin razón, por accidente. Son hechos matemáticos aleatorios. Chaitin propone que los matemáticos deberían abandonar toda esperanza de probarlos y adoptar una metodología cuasi-empírica [9].

Capítulo 2

Teoría intuitiva de conjuntos

"Later generations will regard set theory as a disease from which one has recovered!". **H. Poincaré**.

"No one shall expel us from the paradise which Cantor has created for us!". **D. Hilbert**.

2.1 Introducción

Intuitivamente, un conjunto es una colección de objetos. Los conjuntos se denotan con letras mayúsculas $A, B, C, \ldots$. Por ejemplo, $A = \{a, b, c\}$ es un conjunto de tres elementos, a saber, a, b y c.

- "$x \in A$" se lee "x es un elemento de A."

- $\varnothing$ o $\{\ \}$ denota el conjunto vacío (sin elementos)

- $A \subseteq B$ denota que A está incluido o es subconjunto de B.

En teoría (intuitiva) de conjuntos tenemos también, un conjunto de leyes similares a los de la lógica pero... los métodos de demostración son distintos. Para probar teoremas en teoría de conjuntos usamos las definiciones que siguen y estas leyes (las de teoría de conjuntos).

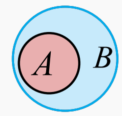
Debemos deternernos y observar que los métodos de prueba en esta teoría ya no es como los métodos de prueba que vimos en el capítulo anterior: Ahora razonamos con las leyes, las definiciones y *el significado* de los enunciados. Debemos detenernos y aprender los métodos de prueba en esta teoría.

Definición 2.1

Diagrama de Venn

• Inclusión
$A \subseteq B \iff (\forall x \in A \implies x \in B)$
En particular $\varnothing \subseteq A$

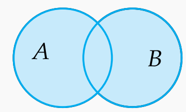
$A \subseteq B$



• Igualdad: $A = B \iff (A \subseteq B \wedge B \subseteq A)$

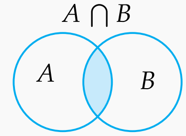
• Unión
$A \bigcup B = \{x \text{ tal que } x \in A \vee x \in B\}$

$A \bigcup B$



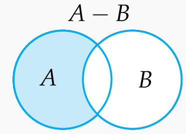
• Intersección
$A \bigcap B = \{x \text{ tal que } x \in A \wedge x \in B\}$

$A \bigcap B$



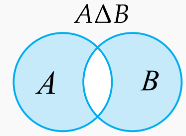
• Diferencia
$A - B = \{x \text{ tal que } x \in A \wedge x \notin B\}$

$A - B$



• Diferencia simétrica
$A \,\Delta\, B = \{x \text{ tal que } x \in A \bigcup B \wedge x \notin A \bigcap B\}$

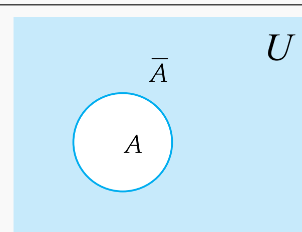
$A \Delta B$



• Complemento
U es el conjunto universal, es decir, un conjunto formado por todos los objetos del contexto. El complemento de A respecto a U es

$$\overline{A} = \{x \text{ tal que } x \in U - A\}.$$

En particular $\overline{\overline{A}} = A$ y $\overline{U} = \varnothing$



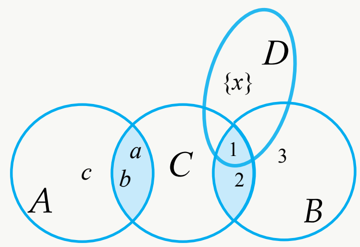
- Conjuntos Disjuntos: Dos conjuntos A y B son disjuntos si $A \bigcap B = \varnothing$

- Producto cartesiano: $A \times B = \{(a,b) \text{ tal que } a \in A \wedge b \in B\}$

- Conjunto de partes de A: $\mathcal{P}(A) = \{Q \text{ tal que } Q \subseteq A\}$. Observe que $Q \in \mathcal{P}(A) \iff Q \subseteq A$

Ejemplo 2.1

Sea $A = \{a,b,c\}$, $B = \{1,2,3\}$, $C = \{a,1,2,b\}$ y $D = \{\{x\},1\}$



a.) $A \cup C = \{a,b,c,1,2\}$ (los elementos repetidos se toman en cuenta solo una vez)

b.) $S = \{a,b\} \subseteq A$

c.) $A - B = A$ y $A - C = \{c\}$

d.) $\mathcal{P}(A) = \{\varnothing,\, A,\, \{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\}\}$. Observe que $\varnothing \subseteq \mathcal{P}(A)$ y que $\varnothing \in \mathcal{P}(A)$

e.) $\mathcal{P}(B) = \{\varnothing,\, B,\, \{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\}$

f.) Si $D = \{1,2\}$, entonces $D \in \mathcal{P}(B)$ pues $D \subseteq B$ y $D \notin \mathcal{P}(A)$ pues $D \not\subseteq A$

g.) $S = \{a,b,1,2\} \subseteq A \cup B \implies S \in \mathcal{P}(A \cup B)$ pero $S \notin \mathcal{P}(A)$ y $S \notin \mathcal{P}(B)$

h.) $\mathcal{P}(A) - \mathcal{P}(B) = \{A,\, \{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\}\}$. Observe que $\varnothing \subseteq \mathcal{P}(A) - \mathcal{P}(B)$ pero $\varnothing \notin \mathcal{P}(A) - \mathcal{P}(B)$

i.) $\{\{x\}\} \subseteq D$ y $\mathcal{P}(D) = \{\varnothing, D, \{\{x\}\}, \{1\}\}$

j.) El producto cartesiano se puede calcular con una tabla. Como convenio, en el producto $A \times B$, las filas son los elementos de A y las columnas, los elementos de B.

$A \times B$	1	2	3
a	$(a,1)$	$(a,2)$	$(a,3)$
b	$(b,1)$	$(b,2)$	$(b,3)$
c	$(c,1)$	$(c,2)$	$(c,3)$
d	$(d,1)$	$(d,2)$	$(d,3)$

$A \times B = \{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3),(c,1),(c,2),(c,3)\}$

k.) $D \times D = \{\ (\{x\}, \{x\}), (\{x\},1), (1,\{x\}), (1,1)\ \}$

l.) $\mathcal{P}(\{(1,1),(1,2)\}) = \{\ \varnothing, \{(1,1),(1,2)\}, \{(1,1)\}, \{(2,2)\}\ \}$

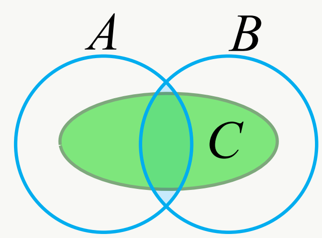
Ejemplo 2.2

Muestre, con un contraejemplo, que la siguiente afirmaciónes son falsas.

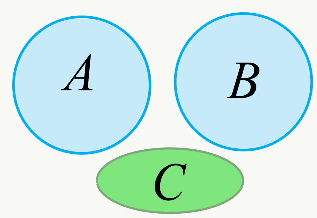
a.) $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$

b.) $(A \cup C) \cap (B \cup C) \subseteq A \cup B$

Demostración:



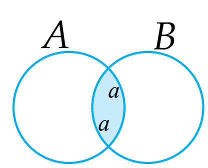
a.) Sea $A = \{a,b,c\}$, $B = \{1,2,3\}$ y $C = \{a,1,2,b\}$. Entonces $C \subseteq A \cup B \implies C \in \mathcal{P}(A \cup B)$ pero $C \notin \mathcal{P}(A)$ y $C \notin \mathcal{P}(B)$, es decir, $C \notin \mathcal{P}(A) \cup \mathcal{P}(B)$



b.) Sea $A = \{a,b,c\}$, $B = \{1,2,3\}$ y $C = \{\#,\%\}$. Entonces $(A \cup C) \cap (B \cup C) = C$ pero $C \not\subseteq A \cup B$.

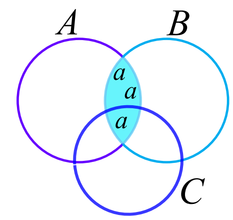
2.2 Cardinalidad

La cardinalidad de un conjunto A se denota $|A|$ y es el número o cantidad de elementos de un conjunto, sea esta cantidad finita o infinita.



1) $|A \cup B| = |A| + |B| - |A \cap B|$

2) Principio de inclusión-exclusión (caso particular)



$$\begin{aligned}|A \cup B \cup C| &= |A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C| \\ &\quad + |A \cap B \cap C|.\end{aligned}$$

Los elementos que están en $A \cap B \cap C$ se cuentan tres veces, pero solo debe eliminarse dos veces.

3) $|A \times B| = |A| \cdot |B|$

$A \times B$	1	2	3
a	$(a,1)$	$(a,2)$	$(a,3)$
b	$(b,1)$	$(b,2)$	$(b,3)$
c	$(c,1)$	$(c,2)$	$(c,3)$
d	$(d,1)$	$(d,2)$	$(d,3)$

4) $|A - B| = |A| - |A \cap B|$

5) $\mathcal{P}(A) = 2^{|A|}$

El teorema del binomio dice que

$$(x+y)^n = \binom{n}{0}x^ny^0 + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}x^1y^{n-1} + \binom{n}{n}x^0y^n.$$

En el caso de conjuntos, si $|A| = n$, el coeficiente binomial $\binom{n}{k}$ cuenta la cantidad subconjuntos de A con k elementos. Por tanto si ponemos $x = 1$ y $y = 1$ en el teorema del binomio, obtenemos

$$\mathcal{P}(A) = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = (1+1)^n = 2^{|A|}$$

Ejemplo 2.3

Sea $A = \{a,b,c\}$, $B = \{c,1,2\}$ y $C = \{a,1,3,4\}$ y $D = \{a,c,2,5\}$

1) En $|A| + |B|$ se cuenta c dos veces. $|A \cup B| = |\{a,b,c,1,2\}| = |A| + |B| - |A \cap B| = 3+3-1 = 5$

2) En $|A|+|B|+|C|$ se cuenta c dos veces, a dos veces y el 1 dos veces.

$|A \cup B \cup C| = |\{a,b,c,1,2,3,4\}| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| = 3+3+4-1-1-1 = 7$

3) En $|A|+|B|+|D|$ se cuenta a dos veces, c tres veces y el 2 dos veces.

$|A \cup B \cup C| = |\{a,b,c,1,2,5\}| = 6$ y

$|A|+|B|+|D|-|A \cap B|-|A \cap D|-|B \cap D|+|A \cap B \cap C| = 6.$

4) $\mathcal{P}(A) = 2^{|A|} = 2^3 = 8$

Ejemplo 2.4

Sean A, B y C conjuntos arbitrarios tales que: A y C son disjuntos, $|A \cup B| = 10$ y $|A \cap B| = 2$. Determine $|A - C| + |B|$.

Solución: Como $A \cap C = \varnothing$ entonces $A - C = A$. Luego, $|A - C| + |B| = |A| + |B|$.

Ahora, como $|A \cup B| = |A| + |B| - |A \cap B|$, entonces $|A| + |B| = |A \cup B| + |A \cap B| = 12$

Ejemplo 2.5

Sean A, B y C conjuntos no nulos tales que: A y C son disjuntos, $|A \cap B| = \dfrac{1}{3}|A|$ y $|B \cup C| = \dfrac{1}{5}|A|$. Pruebe que $|A \cup B \cup C| = \dfrac{13}{15}|A|$.

Solución: Tenemos $A \cap C = \varnothing$ y por tanto $A \cap B \cap C = \varnothing$.

$$
\begin{aligned}
|A \cup B \cup C| &= |A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C|+|A \cap B \cap C| \\
&= |A|+|B|+|C|-|A \cap B|-|B \cap C| \\
&= |A|+|B|+|C|-\frac{1}{3}|A|-|B \cap C| \\
&= |A|-\frac{1}{3}|A|+|B|+|C|-|B \cap C| \\
&= |A|-\frac{1}{3}|A|+|B \cup C| \\
&= |A|-\frac{1}{3}|A|+\frac{1}{5}|A| \;=\; \frac{13}{15}|A|
\end{aligned}
$$

Ejemplo 2.6

Sean A y B subconjuntos de un conjunto universo U el cual consta de N elementos. Si se sabe que $|A \cap B| = \frac{2N}{5}$, $|B| = \frac{N}{2}$ y $|A \cup B| = \frac{3N}{20}$, calcule $|A|$.

Solución: Solo debe despejar $|A|$ en la fórmula $|A \cup B| = |A| + |B| - |A \cap B|$.

Ejemplo 2.7

Si se sabe que $|A| = 2$, $|B| = 3$ y A y B son conjuntos disjuntos, entonces calcule $|P(A \times (A \cup B))|$

Solución: Como $A \cap B = \varnothing$ entonces $|A \cup B| = |A| + |B|$.

$$|P(A \times (A \cup B))| = 2^{|A \times (A \cup B)|} = 2^{|A| \cdot (|A| + |B|} = 2^{2 \cdot (2+3)}$$

2.3 Leyes de conjuntos (y sus análogas en lógica)

En teoria de conjuntos hay un conjunto de teoremas, las cuales les decimos “leyes” aquí, que muestran que en en diferentes contextos y con diferentes operaciones, la “estructura algebraica” es similar.

De Morgan	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$	$\overline{A \bigcap B} = \overline{A} \bigcup \overline{B}$ $\overline{A \bigcup B} = \overline{A} \bigcap \overline{B}$
Conmutatividad	$P \vee Q \equiv Q \vee P$ $P \wedge q \equiv Q \wedge P$	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Asociatividad	$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$	$A \cup (B \cup C) = (A \cup B) \cup C$ $P \cap (Q \cap R) = (P \cap Q) \cap R$
Distribuitividad	$P \vee (Q \wedge R) \equiv (p \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	$P \cup (Q \cap R) = (P \cup Q) \cap (P \cup R)$ $P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R)$
Idenpotencia	$P \wedge P \equiv P$ $P \vee P \equiv P$	$P \cap P = P$ $P \cup P = P$
Inversos	$P \vee \neg P \equiv V_0$ $P \wedge \neg P \equiv F_0$	$A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$
Neutro	$P \vee F_0 \equiv P$ $P \wedge V_0 \equiv P$	$P \cup \varnothing = P$ $P \cap U = P$
Dominación	$P \wedge F_0 \equiv F_0$ $P \vee V_0 \equiv V_0$	$P \cap \varnothing = \varnothing$ $P \cup U = U$
Absorción	$P \vee (P \wedge Q) \equiv P$ $P \wedge (P \vee Q) \equiv P$	$P \cup (P \cap Q) = P$ $P \cap (P \cup Q) = P$

Ejemplo 2.8

Probar que $(A \cup \overline{B}) \cap \left[\overline{(A \cup \overline{B})} \cup \overline{B}\right] = \overline{B}$

Solución:

$$\begin{aligned}
(A \cup \overline{B}) \cap \left[\overline{(A \cup \overline{B})} \cup \overline{B}\right] &= (A \cup \overline{B}) \cap \left[(\overline{A} \cap B) \cup \overline{B}\right] \text{ (usamos De Morgan)}\\
&= (A \cup \overline{B}) \cap \left[(\overline{A} \cup \overline{B}) \cap (B \cup \overline{B})\right] \text{ (Distributividad)}\\
&= (A \cup \overline{B}) \cap \left[(\overline{A} \cup \overline{B}) \cap U\right] \text{ (Inverso)}\\
&= (A \cup \overline{B}) \cap (\overline{A} \cup \overline{B}) \text{ (Neutro. } \overline{B} \text{ es “factor común”, lo sacamos...)}\\
&= (A \cap \overline{A}) \cup \overline{B} = \varnothing \cup \overline{B} = \overline{B}.
\end{aligned}$$

Ejemplo 2.9

Probar que $B \cup \overline{\left[\overline{[(A \cap B) \cup (A \cap \overline{B})]} \cup B\right] \cap A} = U$

Solución: Primero vamos a aplicar De Morgan,

$$B \cup \overline{\left[\overline{[(A \cap B) \cup (A \cap \overline{B})]} \cup B\right] \cap A} = B \cup \overline{\left[[(\overline{A} \cup \overline{B}) \cap (\overline{A} \cup B)] \cup B\right] \cap A}$$

En la expresión que acabamos de simplificar (en azul), $\overline{A}$ es “factor común”,

$$B \cup \overline{\left[[(\overline{A} \cup \overline{B}) \cap (\overline{A} \cup B)] \cup B\right] \cap A} = B \cup \overline{\left[[\overline{A} \cup (\overline{B} \cap B)] \cup B\right] \cap A} = B \cup \overline{\left[[\overline{A} \cup \varnothing] \cup B\right] \cap A}$$

Ahora volvemos a aplicar De Morgan. Luego aplicamos distribuitividad.

$$B \cup \overline{[\overline{A} \cup B] \cap A} = B \cup [(A \cap \overline{B}) \cup \overline{A}] = B \cup [(A \cup \overline{A}) \cap (\overline{B} \cup \overline{A})] = B \cup [U \cap (\overline{B} \cup \overline{A})]$$

$$= B \cup (\overline{B} \cup \overline{A}) = (B \cup \overline{B}) \cup \overline{A} = U \cup \overline{A} = U$$

2.4 Resultados y demostraciones

Para demostrar una proposición en teoría de conjuntos se deben usar las definiciones, las hipótesis de la proposición y posiblemente alguna equivalencia.

En cada caso, debemos acostumbrarnos al tipo de objeto que se debe manejar. Los conjuntos arbitarios manejan elementos genéricos, los productos cartesianos manejan pares ordenados y los conjuntos de partes, conjuntos. Por ejemplo,

a.) $x \in A \cup \overline{B} \implies x \in A \vee x \in \overline{B} \implies x \in A \vee x \notin B$

b.) $(a,b) \in A \times (B \cap \overline{C}) \Longrightarrow a \in A \wedge b \in (B \cap \overline{C}) \Longrightarrow a \in A \wedge (b \in B \wedge b \in \overline{C})$

c.) $S \in \mathcal{P}(A \cap B) \Longrightarrow S \subseteq A \wedge S \subseteq B$

d.) $x \notin A \cup B \Longrightarrow x \in \overline{A \cup B}$ o también $x \notin A \cup B \Longrightarrow x \notin A \wedge x \notin B$

e.) $x \notin A \cap B \Longrightarrow x \in \overline{A \cap B}$ o también $x \notin A \cap B \Longrightarrow \neg(x \in A \cap B) \Longrightarrow \neg(x \in A \wedge x \in B) \Longrightarrow x \notin A \vee x \notin B$

Ejemplo 2.10

Demostrar que $A - B \subseteq A$

Demostración: Debemos usar la definición de *subconjunto* y de la resta.

$x \in A - B \Longrightarrow x \in A \wedge x \notin B \Longrightarrow x \in A.$ ■

Ejemplo 2.11

Demostrar que $A \cap B \subseteq B$

Demostración: Debemos usar la definición de *subconjunto* y de la resta.

$x \in A \cap B \Longrightarrow x \in A \wedge x \in B \Longrightarrow x \in B.$ ■

Ejemplo 2.12

Demostrar que $(A - B) \cap B = \varnothing$

Demostración: Por reducción al absurdo, si asumimos que hay un elemento en $(A - B) \cap B$ entonces llegamos a algo falso.

si $\exists x \in (A - B) \cap B \Longrightarrow (x \in A \wedge x \notin B) \wedge x \in B \Longrightarrow (x \in A \wedge (x \notin B \wedge x \in B) \equiv F_0.$ ■

Ejemplo 2.13

Demostrar que si $A \subseteq B \Longrightarrow A \cup B = B$

Demostración: Recordemos que, por definición, $A \cup B = B \Longleftrightarrow (A \cup B \subseteq B \wedge B \subseteq A \cup B).$

$A \cup B \subseteq B$

$$\begin{aligned}
x \in A \cup B &\implies x \in A \vee x \in B \\
&\implies x \in A \vee x \in B
\end{aligned}$$

Por hipótesis, $x \in A \implies x \in B$, pues $A \subseteq B$,

$$\begin{aligned}
&\implies x \in B \vee x \in B \\
&\implies x \in B \text{ (por idempotencia)} \\
&\therefore\ A \cup B \subseteq B
\end{aligned}$$

$B \subseteq A \cup B$

$$\begin{aligned}
x \in B &\implies x \in B \vee x \in A \text{ (por adición)} \\
&\implies x \in A \cup B \\
&\therefore\ B \subseteq A \cup B
\end{aligned}$$

Ejemplo 2.14

Demostrar que si $A \subseteq B \implies A - B = \varnothing$

Demostración: Tenemos una hipótesis: $A \subseteq B$. Ahora procedemos por contradicción[1] : Supongamos que $A - B$ no es vacío.

Si $A - B$ no es vacío, $\exists\ x \in A - B \implies x \in A \wedge x \notin B$. Pero esto es una contradicción, pues por hipótesis, $A \subseteq B$, es decir, $x \in A \implies x \in B$.

■

[1] Las demostraciones "por contradicción", o por "reducción al absurdo", son demostraciones que en matemáticas se utilizan con gran libertad, pero no todas las escuelas de pensamiento matemático (por ejemplo el "intuicionismo") aceptan estas pruebas como universalmente válidas.

Ejemplo 2.15 (Demostración por casos).

Demuestre que si $S \subseteq A \vee S \subseteq B \implies S \subseteq A \cup B$

Demostración: Tenemos dos casos: $S \subseteq A$ o $S \subseteq B$

I Caso. Si $S \subseteq A$ entonces $\forall x \in S \implies x \in A \implies x \in A \vee x \in B$ por adición. $\therefore\ x \in A \cup B$, es decir $S \subseteq A \cup B$

II Caso. Si $S \subseteq B$ entonces $\forall x \in S \implies x \in B \implies x \in B \vee x \in A$ por adición. $\therefore\ x \in A \cup B$, es decir $S \subseteq A \cup B$

Hemos probado que en cualquier caso, $S \subseteq A \cup B$.

Ejemplo 2.16 **(Demostración por casos).**

Demuestre que si $A \cap B \subseteq \overline{D} \ \wedge \ \overline{B} \cap D = \varnothing$ entonces $A \subseteq \overline{D}$

Solución: Bien tenemos dos hipótesis (premisas) y un resultado para demostrar.

Hipótesis: $\left\{ \begin{array}{ll} A \cap B \subseteq \overline{D} & (H1) \\ \\ \overline{B} \cap D = \varnothing & (H2) \end{array} \right.$

Hay que mostrar que: $A \subseteq \overline{D}$

El esquema de la prueba es $x \in A \implies \ ... \implies x \in \overline{D}$

Si $x \in A$, podemos usar la hipotesis H1 solo si $x \in A \cap B$, entonces debemos hacer dos casos $x \in A \cap B$ y $x \notin A \cap B$.

Demostración.

$$\text{Sea } x \in A, \text{ entonces } \left\{ \begin{array}{lll} \text{si } x \in A \cap B & \implies & x \in A \cap B \\ & \implies & x \in \overline{D} \text{ por } (H1) \\ \\ \text{si } x \notin A \cap B & \implies & x \notin B \\ & \implies & x \in \overline{B} \\ & \implies & x \notin D \text{ pues } \overline{B} \cap D = \varnothing \ (H2) \\ & \implies & x \in \overline{D} \end{array} \right.$$

Entonces en ambos casos, si $x \in A$, concluimos que $x \in \overline{D}$, es decir, $\therefore A \subseteq \overline{D}$

Ejemplo 2.17

Demuestre que si $S \neq \varnothing$ y $S \subseteq A - B$ entonces $S \subseteq A \wedge S \not\subseteq B$.

Demostración: Por hipótesis, $\forall x \in S$ entonces $x \in A - B \implies x \in A \wedge x \notin B \quad \therefore S \subseteq A \wedge S \not\subseteq B$

Observe que $\varnothing \subseteq A - B$ y $\varnothing \subseteq A \wedge \varnothing \subseteq B$.

Ejemplo 2.18

Demuestre que $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

Demostración: HQM $\forall S \in \mathcal{P}(A) \cup \mathcal{P}(B) \Longrightarrow S \in \mathcal{P}(A \cup B)$

$\forall S \in \mathcal{P}(A) \cup \mathcal{P}(B) \Longrightarrow S \in \mathcal{P}(A) \vee S \in \mathcal{P}(B) \Longrightarrow S \subseteq A \vee S \subseteq B \Longrightarrow S \subseteq A \cup B$, por lo tanto $S \in \mathcal{P}(A \cup B)$

Ejemplo 2.19

Demostrar que $\mathcal{P}(A-B) \subseteq [\mathcal{P}(A) - \mathcal{P}(B)] \cup \{\varnothing\}$

Demostración: $\varnothing \in \mathcal{P}(A-B)$ pero $\varnothing \notin \mathcal{P}(A) - \mathcal{P}(B)$. Por eso hay que hacer dos casos.

I Caso. Si $S \neq \varnothing$ y $S \in \mathcal{P}(A-B) \Longrightarrow S \subseteq A-B \Longrightarrow S \subseteq A \wedge S \nsubseteq B$. Por tanto $S \in \mathcal{P}(A) \wedge S \notin \mathcal{P}(B)$, es decir, $S \in \mathcal{P}(A) - \mathcal{P}(B)$ y por tanto $S \in [\mathcal{P}(A) - \mathcal{P}(B)] \cup \{\varnothing\}$.

II Caso. Si $S = \varnothing$ entonces $S \in \mathcal{P}(A-B)$ y $S \in [\mathcal{P}(A) - \mathcal{P}(B)] \cup \{\varnothing\}$

Ejemplo 2.20

Demuestre que $A \times (B-C) = (A \times B) - (A \times C)$

Demostración: Hay que probar dos inclusiones. La naturaleza de la proposición no permite hacer un "$\Longleftrightarrow$". Observe que, por definición, $(x,y) \notin P \times Q$ si y solo si $x \notin P \vee y \notin Q$

I. $A \times (B-C) \subseteq (A \times B) - (A \times C)$.

Sea $(x,y) \in A \times (B-C) \Longrightarrow x \in A \wedge y \in (B-C) \Longrightarrow x \in A \wedge y \in B \wedge y \notin C$ entonces $(x,y) \in A \times B \wedge (x,y) \notin A \times C$, es decir, $(x,y) \in (A \times B) - (A \times C)$.

II. $(A \times B) - (A \times C) \subseteq A \times (B-C)$

Sea $(x,y) \in (A \times B) - (A \times C) \Longrightarrow (x,y) \in (A \times B) \wedge (x,y) \notin (A \times C)$ entonces usando distributividad y neutro, tenemos

$$x \in A \wedge y \in B \wedge (x \notin A \vee y \notin C) \equiv x \in A \wedge y \in B \wedge (x \in A \wedge y \notin C),$$

es decir $(x,y) \in A \times (B-C)$

Ejercicios

2.4.1 ▶ Sea $A = \{a,b\}$. Determine $\mathcal{P}(\mathcal{P}(A))$

2.4.2 ▶ Sea $D = \{\varnothing,\{a,b\}\}$. Determine $D \times D$

2.4.3 ▶ Sea $Q = \{\varnothing,a,b\}$. Calcule $|\mathcal{P}(\mathcal{P}(Q \times Q))|$

2.4.4 ▶ Sean $A = \{1,2,3,d\}$, $B = \{1,2,3,e\}$ y $D = \{2\}$. Determine el conjunto $(A \,\Delta\, B) \times \mathcal{P}(D)$.

2.4.5 ▶ Sean A, B y C tres conjuntos cualesquiera en el universo U. Se sabe que $|U| = 7$, $|C| = 4$, $|A| = 3$, $|A \cap B| = 2$, $|B| = 5$ y $|C - B| = 3$.
Determine la cantidad de elementos del conjunto $P\left((A \,\Delta\, B) \times \overline{(B \cap C)} \right)$.

2.4.6 ▶ Sean A,B y M conjuntos arbitrarios con A y M conjuntos disjuntos. Si $|A \cup B \cup M| = 17$, $|M| = 2$ y $|B - M| = 8$, determine la cardinalidad de $\mathcal{P}(\mathcal{P}(M)) \times (A - B)$

2.4.7 ▶ ¿Cuántos elementos debe tener A para que $|\mathcal{P}(\mathcal{P}(A))| = 65536$?

2.4.8 ▶ En un universo U considere tres conjuntos A, B, C tales que A y C son disjuntos y además $|A \cap B| = 5$, $|\overline{A}| = 24$, $|C| = 13$, $|B - A| = 15$, $|B \cap C| = 9$ y $|A \cup B \cup C| = 32$. Con estas condiciones determine

a.) $|A|$ b.) $|B|$ c.) $|U|$

2.4.9 ▶ Sean A,B y C conjuntos cualesquiera. Use las leyes de conjuntos para verificar la siguiente simplificación (indique en cada paso la ley que utiliza.)

$$(A \cap \overline{B}) \cap \overline{(B \cap \overline{C})} = A \cap \overline{B}$$

$$\begin{array}{rcll} (A \cap \overline{B}) \cap \overline{(B \cap \overline{C})} & = & (A \cap \overline{B}) \cap (\overline{B} \cup C) & \text{DM} \\ & = & A \cap [\overline{B} \cap (\overline{B} \cup C)] & \text{Asoc} \\ & = & = A \cap \overline{B} & \text{Absorción} \end{array}$$

2.4.10 ▶ Sean A,B,C conjuntos arbitrarios. Demuestre
$[\, A \cup B = C) \;\wedge\; (A \cup C) \cap B = C \,] \implies B = C$

2.4.11 ▶ Sean A,B,C conjuntos arbitrarios. Demuestre $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$

2.4.12 ▶ Sean A,B,C,D y M conjuntos arbitrarios. Demuestre

$$[\,(A \cup B = C) \;\wedge\; (A \cup C) \cap B = C \;\wedge\; (A \cap C) \cup B = A\,] \implies (B = C \;\wedge\; A = C)$$

2.4.13 ▶ Sean A,B,C,D y M conjuntos arbitrarios. Demuestre

$$[(M \subseteq A \cap \overline{B}) \wedge (D \subseteq A \cap B)] \implies M \cap D = \varnothing$$

2.4.14 ▶ Demuestre que $A \subseteq (B \cap D) \implies \overline{B} \subseteq (\bar{A} \cup C)$

2.4.15 ▶ Demuestre que $B - A \subseteq \overline{A \cap B}$

2.4.16 ▶ Demuestre que si $\overline{B} \cap D = \varnothing$ entonces $D \subseteq B$

2.4.17 ▶ Demuestre que si $A \subseteq B \wedge A \subseteq D$, entonces $\overline{B \cap D} \subseteq \overline{A}$

2.4.18 ▶ **Paradoja de Russel.** Sea M el "conjunto de todos los conjuntos que no se contienen a sí mismos como miembros". Hay conjuntos que se contienen a sí mismos, como el conjunto de "ideas abstractas" que en sí es una idea abstracta. Volviendo a M, entonces ¿$M \in M \iff M \notin M$?.

2.4.19 ▶ **Paradoja de Berry.** Sea A el "conjunto de enteros que se pueden definir con menos de quince palabras". Claramente A es finito pues el número de frases que se pueden formar con menos de quince palabras es finito y entonces $A \neq \mathbb{N}$. Algunas de estas frases pueden describir un entero positivo específico, por ejemplo "dosmil trescientos cuarenta", "el primer número primo mayor que veinte millones" o "dos elevado a la 20". Como A es finito, entonces $\overline{A}$ debe tener un elemento menor que todos los otros. Tiene que haber un número entero positivo N que sea el menor de todos los números enteros positivos que no están contenidos en A, es decir, $N \in \overline{A}$... pero entonces ¿$N \in A$ pues N es "el menor entero positivo que no se puede definir con menos de quince palabras"?

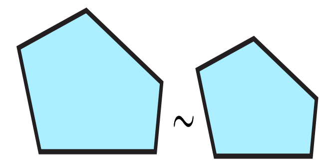
Capítulo 2 ——————————————————————————-

Capítulo 3

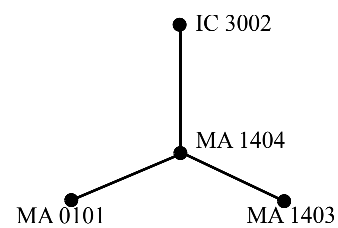
Relaciones binarias

Hay varias relaciones familiares, entre los objetos de un conjunto. Por ejemplo, la relación de orden " $\leq$ " en los números reales o la relación de similitud "$\sim$" en un conjunto de polígonos o la relación "=", etc.

La similitud es una de las propiedades más importantes de las figuras planas. Dos polígonos son similares si sus ángulos respectivos son iguales. En matemáticas hay muchas situaciones donde uno desea observar objetos diferentes como si esecialmente fueran el mismo, como en el caso de polígonos similares. Para hacer esta idea precisa generalizamos la idea de similitud y a estas relaciones las llamamos "relaciones de equivalencia."



Las relaciones de orden sobre un conjunto nos dan una noción de "precendencia". Esta idea tiene muchas aplicaciones. Por ejemplo, en la malla de cursos de una carrera, podríamos tener un conjunto de materias $\{\text{MA 0101}, \text{MA 1403}, \text{MA 0404}, \text{IC 3010}\}$. Una manera de ordenar este conjunto es definir un relación de orden, por ejemplo la relación "es requisito de"; esta relación induce un orden en este conjunto. El orden se puede representar con un diagrama.



Definición 3.1

1) Una relación $\mathcal{R}$ de un conjunto A en un conjunto B es un triple $(G_{\mathcal{R}}, A, B)$, donde $G_{\mathcal{R}} \subseteq A \times B$. $G_{\mathcal{R}}$ se llama *gráfico* de $\mathcal{R}$. El conjunto A se llama conjunto de partida y B es el conjunto de llegada.

2) La notación "$a\,\mathcal{R}\,b$" indica que $(a,b) \in G_{\mathcal{R}}$ y se lee "a se relaciona con b".

3) Si $A = B$, se dice que $\mathcal{R}$ es una relación sobre A.

Definición 3.2

Dada una relación $\mathcal{R}$ de A en B, el dominio y el rango de la relación se definen de la siguiente manera.

1) Dominio de la relación $\mathcal{R}$: $D_{\mathcal{R}} = \{a \in A \ \text{tal que} \ \exists\, b \in B \ \text{y} \ a\,\mathcal{R}\,b\}$

2) Rango de la relación $\mathcal{R}$: $\mathcal{R}[A] = \{b \in B \ \text{tal que} \ \exists\, a \in A \ \text{y} \ a\,\mathcal{R}\,b\}$

Ejemplo 3.1

Sea $A = \{1,2,3\}$ y $B = \{2,3,5\}$. La relación $\mathcal{R}$, de A en B, está definida por el criterio $a\mathcal{R}b \iff a+1=b$. Determine $G_\mathcal{R}$, $D_\mathcal{R}$ y $\mathcal{R}[A]$.

Solución: Por ejemplo, $2\mathcal{R}3$ pues $2+1=3$. $G_\mathcal{R} = \{(1,2),\ (2,3),\ (3,4).\}$
Para visualizar la relación, hacemos una tabla con el producto cartesiano, con los elementos de A en las filas.

$A\times B$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,1)	(3,2)	(3,4)

$G_\mathcal{R}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,1)	(3,2)	(3,4)

Como se observa, $G_\mathcal{R} = \{(1,2),\ (2,3),\ (3,4)\}$. En este caso, $D_\mathcal{R} = A$ y $\mathcal{R}[A] = B$

Ejemplo 3.2

Sea $A = \{1,2\}$ y $B = \{0,3\}$. La relación $\mathcal{R}$ sobre $A\times B$ está definida por el criterio $(a,b)\,\mathcal{R}\,(c,d) \iff ad \geq bc$. Determine $G_\mathcal{R}$, $D_\mathcal{R}$ y $\mathcal{R}[A]$.

Solución: Por ejemplo, $(1,2)\,\mathcal{R}\,(0,3)$ pues $1\cdot 3 \geq 2\cdot 0$. Para visualizar la relación, hacemos una tabla con el producto cartesiano. En la tabla ponemos 1 si hay relación entre los pares asociados y un 0 sino.

$G_\mathcal{R}$	(1,0)	(1,3)	(2,0)	(2,3)
(1,0)	1	1	1	1
(1,3)	0	1	0	0
(2,0)	1	1	1	1
(2,3)	0	1	0	1

Entonces,

$$\begin{array}{rcl} G_\mathcal{R} & = & \{((1,0),(1,0)),\ ((1,0),(1,3)),\ ((1,0),(2,0)),\ ((1,0),(2,3)),\ ((1,3),(1,3)),\\ & & ((2,0),(1,0)),\ ((2,0),(1,3)),\ ((2,0),(2,0)),\ ((2,0),(2,3)),\ ((2,3),(1,3)),\ ((2,3),(2,3))\}\\ D_\mathcal{R} & = & A\times B\\ \mathcal{R}[A\times B] & = & A\times B \end{array}$$

3.1 Operaciones con relaciones

Definición 3.3

Dadas las relaciones $\mathcal{R} = (G_{\mathcal{R}}, A, B)$ y $\mathcal{S} = (G_{\mathcal{S}}, A, B)$, se definen las nuevas relaciones

1) La relación unión: $\mathcal{R} \cup \mathcal{S} = (G_{\mathcal{R}\cup\mathcal{S}}, A, B)$ con $G_{\mathcal{R}\cup\mathcal{S}} = G_{\mathcal{R}} \cup G_{\mathcal{S}}$

   $a\mathcal{R} \cup \mathcal{S}b \iff a\mathcal{R}b \lor a\mathcal{S}b \iff (a,b) \in G_{\mathcal{R}} \cup G_{\mathcal{S}}$

2) La relación intersección: $\mathcal{R} \cap \mathcal{S} = (G_{\mathcal{R}\cap\mathcal{S}}, A, B)$ con $G_{\mathcal{R}\cap\mathcal{S}} = G_{\mathcal{R}} \cap G_{\mathcal{S}}$

   $a\mathcal{R} \cap \mathcal{S}b \iff a\mathcal{R}b \land a\mathcal{S}b \iff (a,b) \in G_{\mathcal{R}} \cap G_{\mathcal{S}}$

3) La relación diferencia: $\mathcal{R} - \mathcal{S} = (G_{\mathcal{R}-\mathcal{S}}, A, B)$ con $G_{\mathcal{R}-\mathcal{S}} = G_{\mathcal{R}} - G_{\mathcal{S}}$

   $a\mathcal{R} - \mathcal{S}b \iff a\mathcal{R}b \land a\not\mathcal{S}b \iff (a,b) \in G_{\mathcal{R}} - G_{\mathcal{S}}$

4) La relación inversa: $\mathcal{R}^{-1} = \left(G_{\mathcal{R}}^{-1}, B, A\right)$ con $G_{\mathcal{R}}^{-1} = \{(b,a) \in B \times A \text{ tal que } a\mathcal{R}b\}$

   $b\mathcal{R}^{-1}a \iff a\mathcal{R}b \iff (a,b) \in G_{\mathcal{R}}$

5) La relación complemento: $\overline{\mathcal{R}} = \left(\overline{G_{\mathcal{R}}}, A, B\right)$ con $\overline{G_{\mathcal{R}}} = A \times B - G_{\mathcal{R}}$

   $a\overline{\mathcal{R}}b \iff a\not\mathcal{R}b \iff (a,b) \in A \times B \land (a,b) \notin G_{\mathcal{R}}$

6) Composición: Si $\mathcal{R} = (G_{\mathcal{R}}, A, B)$ y $\mathcal{S} = (G_{\mathcal{S}}, B, C)$ entonces se define

   $\mathcal{S} \circ \mathcal{R} = (G_{\mathcal{S}\circ\mathcal{R}}, A, C)$ con $G_{\mathcal{S}\circ\mathcal{R}} = \{(a,c) \in A \times C \text{ tal que } \exists\, b \in B \text{ con } a\mathcal{R}b \land b\mathcal{S}c\}$

   $\mathcal{S} \circ \mathcal{R}$ es una relación de A en C. Observe que si $A = C$ entonces podemos definir $\mathcal{S} \circ \mathcal{R}$ tanto como $\mathcal{R} \circ \mathcal{S}$.

Ejemplo 3.3

Sean $A = \{1,2,3\}$ y $B = \{2,3,5\}$.

La relación $\mathcal{R}$, de A en B, está definida por el criterio $a\mathcal{R}b \iff a+1 = b$.

La relación $\mathcal{S}$, de A en B, está definida por el criterio $a\mathcal{S}b \iff \exists\, k \in \mathbb{N}$ tal que $a = bk+1$.

Por ejemplo, $2\mathcal{R}3$ pues $2+1=3$ y $3\mathcal{S}2$ pues $3=2\cdot 1+1$.

Para visualizar algunas operaciones con estas relaciones, hacemos una tabla con el producto cartesiano, con los elementos de A en las filas.

$G_{\mathcal{R}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$\overline{G_{\mathcal{R}}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{R}^{-1}}$	1	2	3
2	(2,1)	(2,2)	(2,3)
3	(3,1)	(3,2)	(3,3)
4	(4,1)	(4,2)	(4,3)

$G_{\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$\overline{G_{\mathcal{S}}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{S}^{-1}}$	1	2	3
2	(2,1)	(2,2)	(2,3)
3	(3,1)	(3,2)	(3,3)
4	(4,1)	(4,2)	(4,3)

$G_{\mathcal{R}\cup\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{R}\cap\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{R}-\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

Observe que $\mathcal{R}\cap\mathcal{S}=(G_{\mathcal{R}\cap\mathcal{S}},A,B)$ y $(\mathcal{R}\cap\mathcal{S})^{-1}=\left(G_{(\mathcal{R}\cap\mathcal{S})^{-1}},B,A\right)$. Entonces el complemento $\overline{(\mathcal{R}\cap\mathcal{S})^{-1}}$ se calcula en $B\times A$.

$G_{(\mathcal{R}\cap\mathcal{S})^{-1}}$	1	2	3
2	(2,1)	(2,2)	(2,3)
3	(3,1)	(3,2)	(3,3)
4	(4,1)	(4,2)	(4,3)

$G_{\overline{(\mathcal{R}\cap\mathcal{S})^{-1}}}$	1	2	3
2	(2,1)	(2,2)	(2,3)
3	(3,1)	(3,2)	(3,3)
4	(4,1)	(4,2)	(4,3)

El cálculo de $\left(\overline{\mathcal{R}\cap\mathcal{S}}\right)^{-1}$ se debe hacer en $B\times A$ pues $\overline{\mathcal{R}\cap\mathcal{S}}\subseteq A\times B$.

$G_{\mathcal{R}\cap\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\overline{\mathcal{R}\cap\mathcal{S}}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{(\overline{\mathcal{R}\cap\mathcal{S}})^{-1}}$	1	2	3
2	(2,1)	(2,2)	(2,3)
3	(3,1)	(3,2)	(3,3)
4	(4,1)	(4,2)	(4,3)

Ejemplo 3.4 (Composición)

Sea $A=\{1,2,3,4,5\}$ y sean $\mathcal{R}$, $\mathcal{S}$ y $\mathcal{T}$ relaciones sobre A definidas por

$G_\mathcal{R}=\{(1,2),\ (2,2),\ (2,3),\ (1,3)\}$,

$G_\mathcal{S}=\{(2,4),\ (2,5),\ (3,1)\}$ y

$G_\mathcal{T}=\{(3,1),\ (3,3),\ (3,4)\}$.

1) Cálculo de $G_{\mathcal{S}\circ\mathcal{R}}$ y $G_{\mathcal{T}\circ\mathcal{R}}$

Como en ambos casos, $\mathcal{R}$ es la primera relación que se aplica, la ponemos como primera columna de cada tabla. En la última columna aparece el resultado.
El método es: Para cada $(a,b)\in G_\mathcal{R}$, buscamos $(b,c)\in G_\mathcal{S}$ y obtenemos $(a,c)\in G_{\mathcal{S}\circ\mathcal{R}}$.

$G_{\mathcal{S}\circ\mathcal{R}}$

$G_\mathcal{R}$	$G_\mathcal{S}$	$G_{\mathcal{S}\circ\mathcal{R}}$
(1,2)	(2,4)	(1,4)
(2,2)	(2,5)	(1,5)
(2,3)	(3,1)	(2,4)
(1,3)		(2,5)
		(2,1)
		(1,1)

$G_{\mathcal{T}\circ\mathcal{R}}$

$G_\mathcal{R}$	$G_\mathcal{T}$	$G_{\mathcal{T}\circ\mathcal{R}}$
(1,2)	(3,1)	(2,1)
(2,2)	(3,3)	(2,3)
(2,3)	(3,4)	(2,4)
(1,3)		(1,1)
		(1,3)
		(1,4)

2) Contraejemplo: $(\mathcal{S}\cap\mathcal{T})\circ\mathcal{R}\neq(\mathcal{S}\circ\mathcal{R})\cap(\mathcal{T}\circ\mathcal{R})$

$G_{(\mathcal{S}\cap\mathcal{T})\circ\mathcal{R}}$

$G_\mathcal{R}$	$G_{\mathcal{S}\cap\mathcal{T}}$	$G_{(\mathcal{S}\cap\mathcal{T})\circ\mathcal{R}}$
(1,2)		(2,1)
(2,2)	(3,1)	(1,1)
(2,3)		
(1,3)		

$G_{(\mathcal{S}\circ\mathcal{R})\cap(\mathcal{T}\circ\mathcal{R})}$

$G_{\mathcal{S}\circ\mathcal{R}}$	$G_{\mathcal{T}\circ\mathcal{R}}$	$G_{(\mathcal{S}\circ\mathcal{R})}\cap G_{(\mathcal{T}\circ\mathcal{R})}$
(1,4)	(2,1)	(1,4)
(1,5)	(2,3)	(2,4)
(2,4)	(2,4)	(2,1)
(2,5)	(1,1)	(1,1)
(2,1)	(1,3)	
(1,1)	(1,4)	

Ejemplo 3.5

Sea $\mathcal{R}$ una relación definida sobre $A = \{1,2,3,4,5\}$, con criterio $a\,\mathcal{R}\,b \iff a+1 \leq b$.
Además sean $\mathcal{S}$ y $\mathcal{T}$ relaciones definidas sobre A cuyos gráficos son $G_{\mathcal{S}} = \{(2,4),\ (2,5),\ (3,1),\ (4,3)\}$ y $G_{\mathcal{T}} = \{(3,1),\ (3,3),\ (4,3)\}$.

a.) Determine el gráfico asociado a la relación $\mathcal{R}$

b.) Determine el gráfico asociada a la relación $(\mathcal{S} \cap \mathcal{T}) \circ \mathcal{R}$

Solución:

$G_{\mathcal{R}}$	1	2	3	4	5
1	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
2	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
3	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)
4	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)
5	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)

$G_{\mathcal{R}}$	$G_{\mathcal{S} \cap \mathcal{T}}$	$G_{(\mathcal{S} \cap \mathcal{T}) \circ \mathcal{R}}$
(1,2)	(3,1)	(1,1)
(1,3)	(4,3)	(2,1)
(1,4)		(1,3)
(1,5)		(2,3)
(2,3)		(3,3)
(2,4)		
(2,5)		
(3,4)		
(3,5)		
(4,5)		

Ejercicios

3.1.1 ▶ Considere el conjunto $A = \{2,4,6,8\}$, sobre el cual se definen dos relaciones $\mathcal{R}$ y $\mathcal{S}$.

- La relación $\mathcal{R}$ se define por: $a\mathcal{R}b \iff (b-a)^2 \in A$
- El gráfico de la relación $\mathcal{S}$ está dado por $G_{\mathcal{S}} = \{(2,4),\ (4,6),\ (6,2),\ (6,6),\ (8;2)\}$.

a.) Determine el gráfico de la relación $\mathcal{R}$

b.) Determine el gráfico de la relación $\overline{\mathcal{S} \circ \mathcal{R}} \cup \mathcal{R}^{-1}$.

3.1.2 ▶ Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones sobre $A = \{1,2,3,4\}$. $\mathcal{R}$ se define por el criterio:

$$a\mathcal{R}b \iff (a+b \text{ es par }) \vee (b \text{ es par }).$$

Y $\mathcal{S}$ la definimos con el gráfico $G_{\mathcal{S}} = \{(1,1),(1,4),(2,3),(4,2),(4,3)\}$.

a.) Determine el gráfico de $\mathcal{R}$

b.) Determine el gráfico de $\mathcal{S}^{-1} \cap \overline{\mathcal{R}}$

Ejemplo 3.6 (Demostraciones de resultados).

Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones definidas de A en B.

1) $\left(\mathcal{R}^{-1}\right)^{-1} = \mathcal{R}$

Prueba: $a\left(\mathcal{R}^{-1}\right)^{-1}b \iff b\mathcal{R}^{-1}a \iff a\mathcal{R}b.$

2) $(\mathcal{R} \cup \mathcal{S})^{-1} = \mathcal{R}^{-1} \cup \mathcal{S}^{-1}$

Prueba:

$$\begin{aligned} a(\mathcal{R} \cup \mathcal{S})^{-1}b &\iff b\,\mathcal{R} \cup \mathcal{S}a \iff b\,\mathcal{R}a \lor b\mathcal{S}a \iff a\mathcal{R}^{-1}b \lor a\mathcal{R}^{-1}b \\ &\iff a\,\mathcal{R}^{-1} \cup \mathcal{S}^{-1}b \end{aligned}$$

3) $(\mathcal{R} \cap \mathcal{S})^{-1} = \mathcal{R}^{-1} \cap \mathcal{S}^{-1}$

Prueba: Ejercicio

4) $(\mathcal{R} - \mathcal{S})^{-1} = \mathcal{R}^{-1} - \mathcal{S}^{-1}$

Prueba: Ejercicio

Ejemplo 3.7

Sean $\mathcal{R}$ relación definida de A en B, y las relaciones $\mathcal{S}$ y $\mathcal{T}$ definidas de B en C.

Recordemos que si $\exists\, b \in B$ tal que $a\,\mathcal{R}b \land b\,\mathcal{S}c$ entonces $a\,\mathcal{S} \circ \mathcal{R}c$ (observe el orden!)

1) $(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}$

Prueba: $\mathcal{S} \circ \mathcal{R}$ va de A en C y $(\mathcal{S} \circ \mathcal{R})^{-1}$ va de C en A y $\mathcal{R}^{-1} \circ \mathcal{S}^{-1}$ va de C en A.

$$\begin{aligned} c\,(\mathcal{S}\circ\mathcal{R})^{-1}a &\iff a\,\mathcal{S}\circ\mathcal{R}c \iff \exists\, b\in B \text{ tal que } a\,\mathcal{R}b \wedge b\,\mathcal{S}c \\ &\iff b\,\mathcal{R}^{-1}a \wedge c\,\mathcal{S}^{-1}b \\ &\iff c\,\mathcal{S}^{-1}b \wedge b\,\mathcal{R}^{-1}a \\ &\iff c\,\mathcal{R}^{-1}\circ\mathcal{S}^{-1}a \end{aligned}$$

2) $(\mathcal{S}\cup\mathcal{T})\circ\mathcal{R} = (\mathcal{S}\circ\mathcal{R})\cup(\mathcal{T}\circ\mathcal{R})$

Prueba: La relación $(\mathcal{S}\cup\mathcal{T})\circ\mathcal{R}$ va de A en C.

$$\begin{aligned} a(\mathcal{S}\cup\mathcal{T})\circ\mathcal{R}c &\iff \exists\, b\in B \text{ tal que } a\,\mathcal{R}b \wedge b\,\mathcal{S}\cup\mathcal{T}c \\ &\iff a\,\mathcal{R}b \wedge (b\,\mathcal{S}c \vee b\mathcal{T}c) \\ &\iff \text{...Ejercicio : completar la demostracin} \end{aligned}$$

3) $(\mathcal{S}\cap\mathcal{T})\circ\mathcal{R} \subseteq (\mathcal{S}\circ\mathcal{R})\cap(\mathcal{T}\circ\mathcal{R})$

Prueba: En el ejemplo 3.4 ya vimos un contraejemplo que muestra que estos dos conjuntos no son iguales. La relación $(\mathcal{S}\cup\mathcal{T})\circ\mathcal{R}$ va de A en C.

$$\begin{aligned} (a,c)\in G_{(\mathcal{S}\cap\mathcal{T})\circ\mathcal{R}} &\iff a\,(\mathcal{S}\cap\mathcal{T})\circ\mathcal{R}c \\ &\iff \exists\, b\in B \text{ tal que } a\,\mathcal{R}b \;\wedge\; b\,\mathcal{S}\cap\mathcal{T}c \\ &\iff \exists\, b\in B \text{ tal que } (a\,\mathcal{R}b \;\wedge\; b\,\mathcal{S}\,c) \;\wedge\; (a\,\mathcal{R}b \;\wedge\; b\,\mathcal{T}\,c) \\ &\implies a\,(\mathcal{S}\circ\mathcal{R})\,c \;\wedge\; a\,(\mathcal{T}\circ\mathcal{R})\,c \quad (*) \\ &\implies (a,c)\in G_{(\mathcal{S}\circ\mathcal{R})\cap(\mathcal{T}\circ\mathcal{R})} \end{aligned}$$

Observación. En el paso $(*)$ solo podemos usar " $\implies$ " porque en la otra dirección del razonamiento, no hay un "$b\in B$" sino $b_1, b_2\in B$. En efecto,

$$a\,(\mathcal{S}\circ\mathcal{R})\,c \;\wedge\; a\,(\mathcal{T}\circ\mathcal{R})\,c \implies \begin{cases} \exists\, b_1\in B \text{ tal que } a\,\mathcal{R}\,b_1 \;\wedge\; b_1\,\mathcal{S}\,c \\ \text{y} \\ \exists\, b_2\in B \text{ tal que } a\,\mathcal{R}\,b_2 \;\wedge\; b_2\,\mathcal{T}\,c \end{cases}$$

y *no* necesariamente $b_1 = b_2$, tal y como lo vimos en el ejemplo 3.4.

Ejemplo 3.8

Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones definidas de A en B.

1) $D_{\mathcal{R}\cup\mathcal{S}} = D_{\mathcal{R}} \cup D_{\mathcal{S}}$

Prueba:

$$\begin{aligned} a \in D_{\mathcal{R}\cup\mathcal{S}} &\iff \exists\, b \in B \text{ tal que } a\,(\mathcal{R} \cup \mathcal{S})\, b \\ &\iff \exists\, b \in B \text{ tal que } a\,\mathcal{R}\, b \;\vee\; a\,\mathcal{S}\, b \\ &\iff a \in D_{\mathcal{R}} \;\vee\; a \in D_{\mathcal{S}} \\ &\iff a \in D_{\mathcal{R}} \cup D_{\mathcal{S}} \end{aligned}$$

2) $D_{\mathcal{R}\cap\mathcal{S}} \subseteq D_{\mathcal{R}} \cap D_{\mathcal{S}}$

Prueba:

$$\begin{aligned} a \in D_{\mathcal{R}\cap\mathcal{S}} &\iff \exists\, b \in B \text{ tal que } a\,(\mathcal{R} \cap \mathcal{S})\, b \\ &\iff \exists\, b \in B \text{ tal que } a\,\mathcal{R}\, b \;\wedge\; a\,\mathcal{S}\, b \\ &\Longrightarrow a \in D_{\mathcal{R}} \;\wedge\; a \in D_{\mathcal{S}} \quad (*) \\ &\Longrightarrow a \in D_{\mathcal{R}} \cap D_{\mathcal{S}} \end{aligned}$$

Como en el ítem 3. del ejemplo 3.4, en el paso $(*)$ no podemos ir en la otra dirección del razonamiento, pues no hay un "$b \in B$" sino $b_1, b_2 \in B$. En efecto,

$$a \in D_{\mathcal{R}} \;\wedge\; a \in D_{\mathcal{S}} \Longrightarrow \begin{cases} \exists\, b_1 \in B \text{ tal que } a\,\mathcal{R}\, b_1 \\ \text{y} \\ \exists\, b_2 \in B \text{ tal que } a\,\mathcal{S}\, b_2 \end{cases}$$

y *no* necesariamente $b_1 = b_2$.

Ejercicios

3.1.3 ▶ Probar que $D_{\mathcal{R}} - D_{\mathcal{S}} \subseteq D_{\mathcal{R}-\mathcal{S}}$

3.1.4 ▶ Probar que $D_{\mathcal{R}} - D_{\mathcal{S}} \subseteq D_{\mathcal{R}-\mathcal{S}}$

3.1.5 ▶ Probar que $(\mathcal{R} \cap \mathcal{S})[A] \subseteq \mathcal{R}[A] \cap \mathcal{S}[A]$

3.2 Matrices y grafos asociados

Una matriz $A_{m\times n}$ es un arreglo rectangular de m filas y n columnas.

$$A = \begin{bmatrix} \boxed{a_{11}} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & \boxed{a_{mn}} \end{bmatrix}$$

Fila 1, Columna 1

Fila m, Columna n

A veces se escribe $A = (a_{ij})_{n\times m}$. La “entrada” a_{ij} está en la fila i y en la columna j.

Definición 3.4

La matriz transpuesta de $A = (a_{ij})_{n\times m}$ es la matriz $A^T = (a_{ji})_{m\times n}$.

Definición 3.5

Una matriz booleana es una matriz $A = (a_{ij})_{n\times m}$ con $a_{ij} = 0$ o $a_{ij} = 1$

Ejemplo 3.9 (Matriz booleana y su transpuesta)

$$A_{3\times 4} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad A^T_{4\times 3} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Definición 3.6

Sea $A = \{a_1, a_2, ..., a_n\}$ y $B = \{b_1, b_2, ..., b_m\}$ conjuntos de cardinalidad n y m respectivamente. Se define la matriz asociada a una relación $\mathcal{R}$ como la matriz booleana

$$M_{\mathcal{R}} = (m_{ij})_{n\times m} \text{ con } m_{ij} = \begin{cases} 1 & \text{si} \quad a_i\,\mathcal{R}\,b_j \\ 0 & \text{si} \quad a_i \not{\mathcal{R}}\, b_j \end{cases}$$

Ejemplo 3.10

Sean $A = \{1,2,3\}$ y $B = \{2,3,5\}$. Considere las relaciones $\mathcal{R}$ y $\mathcal{S}$ de A en B, definidas de la siguiente manera: $a\,\mathcal{R}b \iff a+1=b$ y $a\,\mathcal{S}b \iff \exists\, k \in \mathbb{N}$ tal que $a = bk+1$.

Ahora podemos visualizar la relación como un subconjunto de $A \times B$ y su representación con una matriz boolena.

$G_{\mathcal{R}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$$M_{\mathcal{R}} \quad \begin{array}{c c} & \begin{matrix} 2 & 3 & 4 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

$G_{\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$$M_{\mathcal{S}} \quad \begin{array}{c c} & \begin{matrix} 2 & 3 & 4 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array}$$

Ejemplo 3.11

Sea $A = \{\,\{1\},\,\{2\},\,\{3\},\,\{1,2\},\,\{1,3\},\,\{2,3\},\,\{1,2,3\}\,\}$. Sea $\mathcal{R}$ una relación sobre A, definida por el criterio $S\,\mathcal{R}\,T$ si y solo si el elemento mímimo de S es igual al elemento mínimo de T. Determine la matriz asociada a $\mathcal{R}$.

Solución: Por ejemplo, $\{2\}\mathcal{R}\{2,3\}$ pues $\text{mín}\{2\} = 2$ y $\text{mín}\{2,3\} = 2$.

$\mathcal{R}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$
$\{1\}$	1	0	0	1	1	0	1
$\{2\}$	0	1	0	0	0	1	0
$\{3\}$	0	0	1	0	0	0	0
$\{1,2\}$	1	0	0	1	1	0	1
$\{1,3\}$	1	0	0	1	1	0	1
$\{2,3\}$	0	1	0	0	0	1	0
$\{1,2,3\}$	1	0	0	1	1	0	1

Operaciones de relaciones vía operaciones con matrices booleanas. Se pueden definir operaciones sobre matrices booleanas para calcular la matriz booleana de las relaciones $\mathcal{R} \cup \mathcal{S}$, $\mathcal{R} \cap \mathcal{S}$, $\mathcal{R}^{-1}$ y $\mathcal{S} \circ \mathcal{R}$.

Definición 3.7

Sean $A = (a_{ij})_{n\times m}$ y $B = (b_{ij})_{n\times m}$ son matrices boolenas. Se define

a.) Conjunción: $A \wedge B = (c_{ij})_{n\times m}$ con

$$c_{ij} = \begin{cases} 1 & \text{si} \quad a_{ij} = 1 \wedge b_{ij} = 1 \\ 0 & \text{si} \quad a_{ij} = 0 \vee b_{ij} = 0 \end{cases}$$

b.) Disyunción: $A \vee B = (d_{ij})_{n\times m}$ con

$$c_{ij} = \begin{cases} 1 & \text{si} \quad a_{ij} = 1 \vee b_{ij} = 1 \\ 0 & \text{si} \quad a_{ij} = 0 \wedge b_{ij} = 0 \end{cases}$$

Teorema 3.1

Si $M_{\mathcal{R}}$ y $M_{\mathcal{S}}$ son las matrices booleanas que representan a las relaciones $\mathcal{R}$ y $\mathcal{S}$, entonces

$$\begin{aligned} M_{\mathcal{R}\cup\mathcal{S}} &= M_{\mathcal{R}} \vee M_{\mathcal{S}} \\ M_{\mathcal{R}\cap\mathcal{S}} &= M_{\mathcal{R}} \wedge M_{\mathcal{S}} \end{aligned}$$

Ejemplo 3.12

Consideremos las relaciones $\mathcal{R}$ y $\mathcal{S}$ del ejemplo 3.10. Vamos a calcular $M_{\mathcal{R}\cup\mathcal{S}}$ y $M_{\mathcal{R}\cap\mathcal{S}}$ de manera "manual" y usando las operaciones $\vee$ e $\wedge$

$G_{\mathcal{R}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{R}\cup\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_{\mathcal{S}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad M_{\mathcal{R}} \vee M_{\mathcal{S}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = M_{\mathcal{R}\cup\mathcal{S}}$$

$G_{\mathcal{R}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$G_{\mathcal{R}\cap\mathcal{S}}$	2	3	4
1	(1,2)	(1,3)	(1,4)
2	(2,2)	(2,3)	(2,4)
3	(3,2)	(3,3)	(3,4)

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_{\mathcal{S}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad M_{\mathcal{R}} \wedge M_{\mathcal{S}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = M_{\mathcal{R}\cap\mathcal{S}}$$

Definición 3.8

Sean $A = (a_{ij})_{n\times k}$ y $B = (b_{ij})_{k\times m}$ son matrices boolenas. Se define

$$\text{Producto: } A \odot B = (p_{ij})_{n\times m} \text{ con } p_{ij} = \begin{cases} 1 & \text{si} \quad \exists\, k \text{ tal que } a_{ik} = b_{kj} = 1 \\ 0 & \quad\text{en otro caso} \end{cases}$$

Es decir, si la fila F_i de A tiene *al menos una entrada* $a_{ik} = 1$ tal que la columna C_j tiene su respectiva entrada $b_{kj} = 1$, entonces $p_{ij} = 1$

Teorema 3.2

Si $M_{\mathcal{R}}$ y $M_{\mathcal{S}}$ son las matrices booleanas que representan a las relaciones $\mathcal{R}$ y $\mathcal{S}$, entonces

$$\begin{aligned} M_{\mathcal{R}^{-1}} &= M_{\mathcal{R}}^{T} \\ M_{\mathcal{S}\circ\mathcal{R}} &= M_{\mathcal{R}} \odot M_{\mathcal{S}} \end{aligned}$$

Ejemplo 3.13

Consideremos las relaciones $\mathcal{R}$ y $\mathcal{S}$ del ejemplo 3.10.

$$M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_{\mathcal{R}^{-1}} = M_{\mathcal{R}}^{T} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Ejemplo 3.14 (Composición)

Sea $A = \{1,2,3\}$ y sean $\mathcal{R}$, $\mathcal{S}$ relaciones sobre A definidas por $G_{\mathcal{R}} = \{(1,2),\ (2,2),\ (2,3),\ (1,3)\}$ y $G_{\mathcal{S}} = \{(2,1)\ (3,1),\ (3,3)\}$.

Vamos a usar la operación $\odot$ para calcular $G_{\mathcal{S}\circ\mathcal{R}}$. Matricialmente sería así: Si la fila F_i tiene al menos una "coincidencia" de $1's$ con la columna C_j, entonces la entrada $p_{ij} = 1$.

$G_{\mathcal{R}}$	1	2	3
1	(1,1)	(1,2)	(1,3)
2	(2,1)	(2,2)	(2,3)
3	(3,1)	(3,2)	(3,3)

$G_{\mathcal{S}}$	1	2	3
1	(1,1)	(1,2)	(1,3)
2	(2,1)	(2,2)	(2,3)
3	(3,1)	(3,2)	(3,3)

$\mathcal{S}\circ\mathcal{R}$	1	2	3
1	(1,1)		(1,3)
2			
3			

Ahora vamos a hacer el cálculo de $M_{\mathcal{S}\circ\mathcal{R}}$ como $M_{\mathcal{R}} \odot M_{\mathcal{S}}$.

Debemos buscar coincidencias de la fila F_1 de $M_{\mathcal{R}}$ con cada una de las columnas C_1, C_2 y C_3 de $M_{\mathcal{S}}$. Luego continuamos con la fila F_2 y las columnas C_1, C_2 y C_3 y lo mismo con la fila F_3

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad M_{\mathcal{S}} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

• La primera fila (p_{11}, p_{12}, p_{13}) de $M_{\mathcal{S}\circ\mathcal{R}}$ se calcula comparando la fila $F_1 = (0,1,1)$ con las columnas $C_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $C_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ y $C_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

La fila F_1 concide con C_1 al menos en $a_{12} = b_{21} = 1$. Entonces $p_{11} = 1$.

La fila F_1 no coincide en ninguna entrada con la columna C_2, entonces $p_{12} = 0$

La fila F_1 coincide con la columna C_3 en al menos la entrada $a_{13} = b_{31} = 1$. Entonces $p_{13} = 1$.

• Para calcular la fila La primera fila (p_{21}, p_{22}, p_{23}) de $M_{\mathcal{S}\circ\mathcal{R}}$ se comp[ara la fila F_2 con todas las columnas C_1, C_2 y C_3 como antes.

• Para calcular la fila La primera fila (p_{31}, p_{32}, p_{33}) de $M_{\mathcal{S}\circ\mathcal{R}}$ se compara la fila F_3 con todas las columnas C_1, C_2 y C_3 como antes.

$$M_{\mathcal{S}\circ\mathcal{R}} = M_{\mathcal{R}} \odot M_{\mathcal{S}} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Ejercicios

3.2.1 ▶ Considere las relaciones $\mathcal{R}$ y $\mathcal{S}$ definidas sobre A, con matrices asociadas

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad M_{\mathcal{S}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

a.) Determine $M_{\mathcal{R}} \vee M_{\mathcal{S}}$

b.) Determine $M_{\mathcal{R}} \wedge M_{\mathcal{S}}$

c.) Determine $M_{\mathcal{R}} \odot M_{\mathcal{S}}$

d.) Use operaciones con matrices boolenas para determinar la matriz asociada la relación $\mathcal{S}^{-1} \circ \overline{\mathcal{R}}$

3.2.1 Dígrafos (gráficos dirigidos)

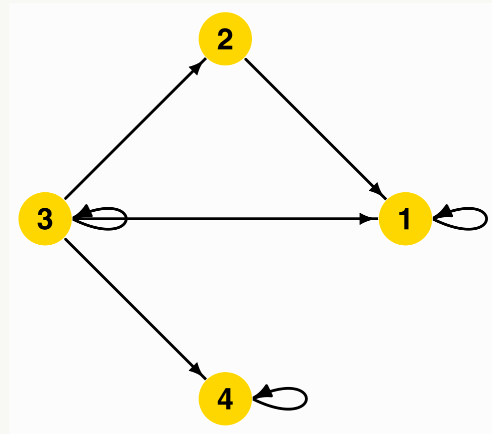
Una relación $\mathcal{R}$ de A en A se puede representar con un grafo dirigido (llamado también dígrafo). Los nodos o vértices, son los elementos de A y las flechas o aristas, conectan (de manera dirigida) los elementos de A que se relacionan de acuerdo con la relación $\mathcal{R}$.

Ejemplo 3.15

Sea $A = \{1,2,3,4\}$ y $\mathcal{R}$ una relación sobre A con

$G_{\mathcal{R}} = \{(1,1),\ (3,3),\ (2,1),\ (3,2),\ (3,1),\ (4,4),\ (3,4)\}$.

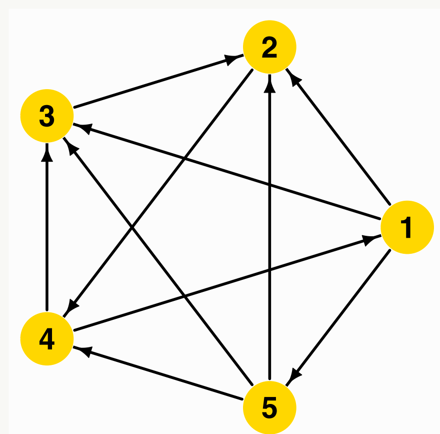
Entonces tenemos 4 nodos, 4 flechas y 3 lazos.



Ejemplo 3.16 **(Torneo "round-robin")**

Un torneo "round-robin" es un torneo "todos contra todos". Si no tomamos en cuenta los "marcadores", los resultados del torneo se pueden representar con un dígrafo. Consideremos cinco jugadores $A = \{1,2,3,4,5\}$ y la relación $\mathcal{R}$ sobre A definida por $i\,\mathcal{R}\,j \iff i$ i venció a j. Una posible matriz $M_{\mathcal{R}}$ (llamada matriz de adyacencia) y el dígrafo asociado se muestra a continuación

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$



Algunos jugadores están empatados en cantidad de victorias. Con el dígrafo podríamos visualizar las victorias directas e indirectas de cada jugador y decidir un método de desempate basado en esta consideración (sin considerar marcadores!).

Dígrafos con el lenguage R. Una manera sencilla de generar el dígrafo a aprtir de la matriz de adyancencia es usar el paquete `igraph` del lenguage **R**. El código para el ejemplo anterior es el que sigue.

■ **Código 3.1**: *Dígrafos con R*

```
install.packages("igraph")  #  instalar igraph (solo una vez!)
```

```
require(igraph)                 # solicitar igraph
#Ver parámetros en http://kateto.net/networks-r-igraph
adj.mat=matrix(c(1,   0,   0, 0,
                1,   0,   0, 0,
                1,   1,   1, 1,
                0,   0, 0, 1), nrow=4, byrow=TRUE)

g = graph.adjacency(adj.mat)
#Graph
par(bg=rgb(.99,.99,.99))    #color de fondo
plot(g, vertex.size = 30,
     vertex.color="gold",
     vertex.label.font=2,   #bold
     vertex.label.cex=2,    #font size
     vertex.frame.color=    "white",
     vertex.label.color =   "black",
     vertex.label.family = "sans",
     edge.width=4,
     edge.color="black",
     layout=layout_in_circle) #topología de nodos
```

3.3 Propiedades de las relaciones

Definición 3.9 (Reflexiva)

Sea $\mathcal{R}$ una relación definida sobre A. Esta relación es reflexiva si y solo si $\forall a \in A,\ a\mathcal{R}a$.

Ejemplo 3.17 (Reflexiva)

Sea $A = \{1,2,3,4,5\}$ y sea $\mathcal{R}$ una relación sobre A definida por

$G_{\mathcal{R}} = \{(1,2), (2,2), (2,3), (1,3), (2,1), (3,2), (1,4)\}$.
Entonces $\mathcal{R}$ es reflexiva.

$G_{\mathcal{R}}$	1	2	3	4
1	(1,1)	(1,2)	(1,3)	(1,4)
2	(2,1)	(2,2)	(2,3)	(2,4)
3	(3,1)	(3,2)	(3,3)	(3,4)
4	(4,1)	(4,2)	(4,3)	(4,4)

Definición 3.10 (Simétrica)

Sea $\mathcal{R}$ una relación definida sobre A. Esta relación es simétrica si y solo si

$$\forall a,b \in A,\ \text{si } a\mathcal{R}b \implies b\mathcal{R}a.$$

Ejemplo 3.18 (Reflexiva y Simétrica)

Sea $A = \{1,2,3,4,5\}$ y sea $\mathcal{R}$ una relación sobre A definida por

$G_{\mathcal{R}} = \{(1,2),\ (2,2),\ (2,3),\ (1,3),\ (2,1),\ (3,2),\ (1,4),\ (4,1)\}$. Entonces $\mathcal{R}$ es simétrica. Observe como la diagonal opera como un "espejo".

$G_{\mathcal{R}}$	1	2	3	4
1	(1,1)	(1,2)	(1,3)	(1,4)
2	(2,1)	(2,2)	(2,3)	(2,4)
3	(3,1)	(3,2)	(3,3)	(3,4)
4	(4,1)	(4,2)	(4,3)	(4,4)

Definición 3.11 (Transitiva)

Sea $\mathcal{R}$ una relación definida sobre A. Esta relación es transitiva si y solo si

$$\forall a,b,c \in A,\ \text{si } a\mathcal{R}b \wedge b\mathcal{R}c \Longrightarrow a\mathcal{R}c.$$

Ejemplo 3.19 (Reflexiva y transitiva)

Sea $A = \{1,2,3,4,5\}$ y sea $\mathcal{R}$ una relación sobre A definida por

$G_{\mathcal{R}} = \{(1,1),\ (2,2),\ (3,3),\ (4,4),\ (2,1),\ (1,2),\ (1,4),\ (4,3),$ $(1,3),\ (2,3),\ (2,4)\}$. Entonces $\mathcal{R}$ es transitiva.

$G_{\mathcal{R}}$	1	2	3	4
1	(1,1)	(1,2)	(1,3)	(1,4)
2	(2,1)	(2,2)	(2,3)	(2,4)
3	(3,1)	(3,2)	(3,3)	(3,4)
4	(4,1)	(4,2)	(4,3)	(4,4)

La transitividad no es tan evidente al observar el gráfico de $\mathcal{R}$. En el toerema que sigue tenemos una caracterización natural y práctica para establecer si una relación es reflexiva, simétrica o transitiva.

Teorema 3.3

Sea $\mathcal{R}$ una relación definida sobre A (finito). Si $|A| = n$, entonces

a.) $\mathcal{R}$ es reflexiva si y solo si $D \subseteq G_{\mathcal{R}}$ con $D = \{(a,a)$ tal que $a \in A\}$.

b.) $\mathcal{R}$ es simétrica si y solo si $G_{\mathcal{R}} = G_{\mathcal{R}}^{-1}$

c.) $\mathcal{R}$ es transitiva si y solo si $G_{\mathcal{R}\circ\mathcal{R}} \subseteq G_{\mathcal{R}}$

Prueba. Solo haremos la prueba de la c.). Esta equivalencia de demuestra en dos direcciones.

"$\Longrightarrow$". **Hipótesis:** $\mathcal{R}$ es transitiva. Hay que mostrar la inclusión $G_{\mathcal{R}\circ\mathcal{R}} \subseteq G_{\mathcal{R}}$.

$$\begin{array}{rcl} (a,c) \in G_{\mathcal{R}\circ\mathcal{R}} & \Longrightarrow & \exists\, b \in A \text{ tal que } a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,c, \\ & \Longrightarrow & \text{como } \mathcal{R} \text{ es transitiva, } a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,c \Longrightarrow a\,\mathcal{R}\,c \\ & \Longrightarrow & (a,c) \in G_{\mathcal{R}}. \end{array}$$

"$\Longleftarrow$". **Hipótesis:** $G_{\mathcal{R}\circ\mathcal{R}} \subseteq G_{\mathcal{R}}$. Hay que mostrar que $\mathcal{R}$ es transitiva.

Vamos directo a la definición de transitividad y usaremos la hipótesis en el camino.

Si $a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,c \Longrightarrow (a,c) \in G_{\mathcal{R}\circ\mathcal{R}}$ y por tanto $(a,c) \in G_{\mathcal{R}}$ por hipótesis. $\therefore\ a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,c \Longrightarrow a\,\mathcal{R}\,c$.

Ejemplo 3.20

Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones definidas sobre un conjunto no vacío A. Demuestre que si $\mathcal{R}$ y $\mathcal{S}$ son relaciones simétricas y si $\mathcal{R}\circ\mathcal{S} = \mathcal{S}\circ\mathcal{R}$, entonces $\mathcal{R}\circ\mathcal{S}$ es simétrica.

Solución:

Hipótesis: $\mathcal{R}$ y $\mathcal{S}$ son relaciones simétricas

$\mathcal{R}\circ\mathcal{S} = \mathcal{S}\circ\mathcal{R}$

Hay que demostrar que: $\mathcal{R}\circ\mathcal{S}$ es simétrica

$$\begin{array}{rcl} G_{(\mathcal{R}\circ\mathcal{S})^{-1}} & = & G_{\mathcal{S}^{-1}\circ\mathcal{R}^{-1}} \\ & = & G_{\mathcal{S}\circ\mathcal{R}}, \text{ pues ambas relaciones son simetricas} \\ & = & G_{\mathcal{R}\circ\mathcal{S}}, \text{ por hipótesis.} \end{array}$$

Ejemplo 3.21

Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones definidas en $A \neq \varnothing$ tal que $G_{\mathcal{R}} \subseteq G_{\mathcal{S}}$.

1) Muestre que si $\mathcal{R}$ es reflexiva, entonces $\mathcal{S}$ es reflexiva

Solución:

Hipótesis: $\mathcal{R}$ es reflexiva y $G_{\mathcal{R}} \subseteq G_{\mathcal{S}}$.

Hqm: $\mathcal{S}$ es reflexiva, es decir, $D \subseteq G_{\mathcal{S}}$

$$\begin{array}{rcl} \text{Como } \mathcal{R} \text{ es reflexiva} & \Longrightarrow & D \subseteq G_{\mathcal{R}} \\ & \Longrightarrow & D \subseteq G_{\mathcal{S}} \quad \text{pues } G_{\mathcal{R}} \subseteq G_{\mathcal{S}} \\ & \therefore & \mathcal{S} \text{ es reflexiva} \end{array}$$

2) Dé un contraejemplo de la afirmación "si $\mathcal{R}$ es simétrica, entonces $\mathcal{S}$ es simétrica"

Solución:

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

$G_{\mathcal{R}} = \{ (1,2),(2,1) \}$ $\quad\therefore\ \mathcal{R}$ es simétrica

$G_{\mathcal{S}} = \{ (1,2),(2,1),(3,1) \}$ $\quad G_{\mathcal{R}} \subseteq G_{\mathcal{S}}$ pero $\mathcal{S}$ no es simétrica pues $3\mathcal{S}1$ pero $1\not\mathcal{S}3$

El teorema 3.3 se puede plantear en términos de matrices asociadas.

Definición 3.12

Si $A = (a_{ij})_{n\times m}$ y $B = (b_{ij})_{n\times m}$ son matrices booleanas, entonces

$$A \leq B \iff a_{ij} \leq b_{ij}\ \forall i,j$$

Teorema 3.4

Sea $\mathcal{R}$ una relación definida sobre A (finito). Si $|A| = n$, entonces

a.) $\mathcal{R}$ es reflexiva si y solo si $I_n \leq M_{\mathcal{R}}$.

b.) $\mathcal{R}$ es simétrica si y solo si $M_{\mathcal{R}} = M_{\mathcal{R}}^T$

c.) $\mathcal{R}$ es transitiva si y solo si $M_{\mathcal{R}\circ\mathcal{R}} \leq M_{\mathcal{R}}$

Ejemplo 3.22

Considere la relación $\mathcal{R}$ sobre $A = \{a,b,c\}$ con matriz asociada $M_{\mathcal{R}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$. Entonces

a.) $\mathcal{R}$ no es reflexiva pues $I_3 \not\leq M_{\mathcal{R}}$ (la diagonal no tiene todos sus $1'$s).

b.) $\mathcal{R}$ es simétrica pues $M_{\mathcal{R}} = M_{\mathcal{R}}^T$

c.) $\mathcal{R}$ no es transitiva pues $M_{\mathcal{R}\circ\mathcal{R}} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \not\leq M_{\mathcal{R}}$. ¿Dónde falla la transitividad?.

pero

Ejercicios

3.3.1 ▶ Sea $A = \{1,2,3\}$ y sea la relación $\mathcal{R}$ sobre A, de gráfico $G_{\mathcal{R}} = \{(1,1), (2,2), (3,3), (3,1), (1,3)\}$. Determine la matriz asociada a $\mathcal{R}$ y use el teorema 3.4 para verificar que $\mathcal{R}$ reflexiva, simétrica y transitiva.

3.3.2 ▶ Sea $\mathcal{R}$ una relación con matriz asociada $M_{\mathcal{R}}$. Use el teorema 3.4 para determinar si $\mathcal{R}$ es transitiva.

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

3.4 Relaciones de equivalencia

Las relaciones de equivalencia son relaciones que generalizan relaciones tales como la relación "=" o la relación " $\sim$ " ("es similar") en geometría plana. Estas relaciones tienen tres propiedades muy conocidas

a.) **Reflexividad:** $\forall a \in \mathbb{R},\ a = a$

b.) **Simetría:** $\forall a,b \in \mathbb{R},\ a = b \implies b = a$

c.) **Transitividad**: $\forall a,b,c \in \mathbb{R},\ a = b \wedge b = c \implies a = c$

Definición 3.13 (Relación de equivalencia)
Una relación $\mathcal{R}$ sobre A es de equivalencia si y solo si $\mathcal{R}$ es reflexiva, simétrica y transitiva.

Para una relación $\mathcal{R}$ de equivalencia, si $a\,\mathcal{R}\,b$, entonces formalmente, desde el punto de $\mathcal{R}$, los objetos a y b son "de la misma clase" o "esencialmente similares" o también "congruentes". A veces de escribe $a \equiv_{\mathcal{R}} b$ en vez de $a\,\mathcal{R}\,b$. Los elementos que están relacionados se agrupan en "clases de equivalencia" y cualquier objeto de la clase puede ser representante de la clase.

Esta idea es muy provechosa porque, si $\mathcal{R}$ es una relación de equivalencia sobre A, en vez de analizar todo A, podemos solo analizar el conjunto de las "clases de equivalencia"; este conjunto es llamado "conjunto cociente" porque se escribe " $A/\mathcal{R}$ "

Definición 3.14 (Clases y conjunto cociente)
Si la relación $\mathcal{R}$ sobre A es de equivalencia, entonces todo elemento $a \in A$ está en un una "clase de equivalencia", denotada $\dot{a}$. Esta clase e define como

$$\dot{a} = \{b \in A \ \text{tal que}\ a\mathcal{R}b\}$$

El "conjunto cociente" es el conjunto de las clases de equivalencia y se denota $A/\mathcal{R}$.

$$A/\mathcal{R} = \{\dot{a} \text{ tal que } a \in A\}$$

A veces en vez de $\dot{a}$ se usa la notación $[a]$ o también $\bar{a}$.

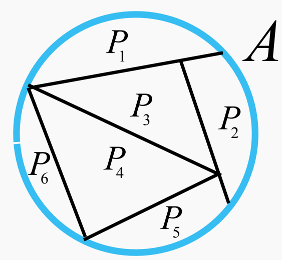
Teorema 3.5

Sea $\mathcal{R}$ una relación de equivalencia sobre A. Si $a\mathcal{R}b$ entonces $\dot{a} = \dot{b}$

Prueba: Ejercicio

Definición 3.15 (Partición)

Sea A un conjunto. Un conjunto $P \subseteq \mathcal{P}(A)$ es *una partición* de A si y solo si



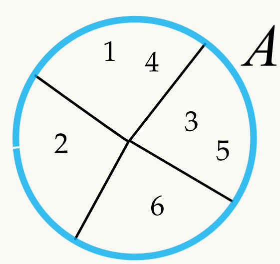
a.) $S \neq \varnothing \ \forall S \in P$.

b.) $\forall S, T \in P$, si $S \neq T \implies S \cap T = \varnothing$

c.) La unión de todos los elementos de P es A.

Ejemplo 3.23 (Particiones)

Sea $A = \{1,2,3,4,5,6\}$. Los siguientes conjuntos son particiones de A



a.) $P = \{\{1,4\},\{3,5\},\{2\},\{6\}\}$

b.) $P = \{\{1\},\{2\},\{3,5\},\{4\},\{6\}\}$

Teorema 3.6

Si $\mathcal{R}$ una relación de equivalencia sobre A, entonces el conjunto cociente $A/\mathcal{R}$ es una *partición* de A.

Si $\mathcal{T}$ es una partición de A, existe una relación de equivalencia $\mathcal{R}$ sobre A tal que $A/\mathcal{R} = \mathcal{T}$

Prueba: Ejercicio.

De acuerdo al teorema, dada un partición de A, existe una relación de equivalencia que induce esa partición. Entonces

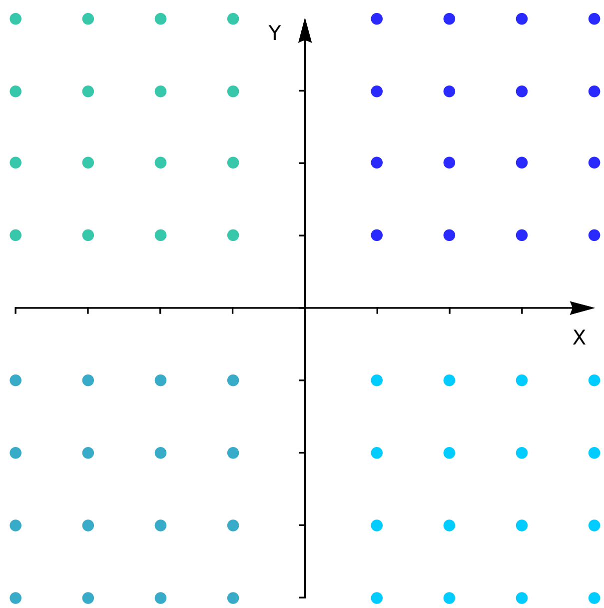
a.) Existe una relación de equivalencia que particiona $\mathbb{Z}$ en pares e impares.

b.) Existe una relación de equivalencia que particiona $\mathbb{R}^*$ en positivos y negativos

c.) Existe una relación de equivalencia que particiona $\mathbb{Z}$ en "paquetes" de dos elementos, por ejemplo

$$\mathbb{Z} = \{ \ldots \{-2,12\},\{-1,11\},\{0,10\},\{1,9\}, \ldots \}$$

d.) Existe una relación de equivalencia que particiona $\mathbb{Z}^* \times \mathbb{Z}^*$ en cuadrantes



Ejemplo 3.24

Sobre $A = \{1,2,3,4,5,6\}$ se tiene una relación de equivalencia $\mathcal{R}$, de gráfico

$G_{\mathcal{R}} = \{(1,1),(5,1),(1,5),(5,5),(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3),(4,4),(6,6)\}.$

Determine la partición (el conjunto cociente) inducida por esta relación.

Solución: Para obtener la partición revisamos las filas del gráfico (en configuración cartesiana) para determinar qué elementos están relacionados con cada elemento de A.

$G_{\mathcal{R}}$	1	2	3	4	5	6	Clases
1	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	$\to [1] = \{1,5\}$
2	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)	$\to [2] = \{2,3,4\}$
3	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)	$\to [3] = [2]$
4	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)	$\to [4] = [2]$
5	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)	$\to [5] = [1]$
6	(6,1)	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)	$\to [6] = \{6\}$

La partición sería $A/\mathcal{R} = \{\ \{1,5\},\ \{2,3,4\},\ \{6\}\ \}$

Ejemplo 3.25

Verifique que $P = \{\{1,4\},\{3,5\},\{2\},\{6\}\}$ es una partición de $A = \{1,2,3,4,5,6\}$ y determine el gráfico de la relación inducida sobre A.

Solución: P es una partición de A pues satisface la definición 3.15.

La relación inducida sobre A debe ser *de equivalencia*, según el teorema 3.6. Por lo tanto en su gráfico debe estar la diagonal D y debe ser simétrico.

Los objetos de A que se relacionan son los elementos de cada elemento de la partición. Como $\{1,4\}$ está en la partición, esos significa que $(1,1)$, $(1,4)$, $(4,4) \in G_{\mathcal{R}}$.

$G_{\mathcal{R}}$	1	2	3	4	5	6
1	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)
2	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)
3	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)
4	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)
5	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)
6	(6,1)	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)

Ejemplo 3.26

Sea $\mathcal{R}$ una relación sobre $\mathbb{R}^*$ definida por $x\,\mathcal{R}\,y \iff xy > 0$.

a.) Muestre que $\mathcal{R}$ es una relación de equivalencia.

b.) Determine las clases de equivalencia $[1]$ y $[-1]$.

c.) Determine $\mathbb{R}^*/\mathcal{R}$ (el conjunto cociente).

Solución:

a.) $\mathcal{R}$ es una relación de equivalencia.

I.) $\mathcal{R}$ es reflexiva pues $\forall a \in \mathbb{R}^*,\ a \cdot a > 0 \implies a\mathcal{R}a$.

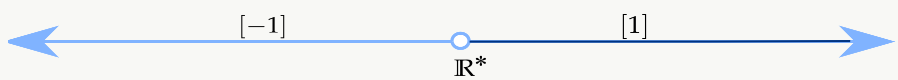
II.) $\mathcal{R}$ es simétrica pues si $a\mathcal{R}b \implies a \cdot b > 0 \implies b \cdot a > 0 \implies b\mathcal{R}a$

III.) $\mathcal{R}$ es transitiva pues si $a\mathcal{R}b \wedge b\mathcal{R}c \implies a \cdot b > 0 \wedge b \cdot c > 0$ por lo que a y c tienen el mismo signo que b, es decir, a y c tienen el mismo signo, $\therefore\ a \cdot c > 0 \implies a\mathcal{R}c$

Nota: También se puede demostrar así: $a \cdot b > 0$ y $b \cdot c > 0 \implies ab^2c > 0 \implies ac > 0$ pues $b^2 > 0$.

b.) $[1] = \{a \in \mathbb{R}^* \text{ tal que } a \cdot 1 > 0\} \implies [1] = \mathbb{R}^+$. $[-1] = \{a \in \mathbb{R}^* \text{ tal que } a \cdot -1 > 0\} \implies [-1] = \mathbb{R}^-$.

c.) Como $[1] \cup [-1] = \mathbb{R}^*$ entonces $\mathbb{R}^*/\mathcal{R} = \{[1], [-1]\}$.



Ejemplo 3.27

En $\mathbb{Z}$, si $m > 1$, la relación "*congruentes módulo* m" se define así: a y b son "*congruentes módulo* m" si y solo si $m|(b-a)$, es decir, m divide a $b-a$. Se escribe $a \equiv b \pmod{m}$ o también $a \equiv_m b$.

$$a \equiv b \pmod{m} \iff m|(b-a) \iff \exists\, k \in \mathbb{Z} \text{ tal que } b - a = mk$$

Por ejemplo

- Si $m = 2$ entonces $5 \equiv 7 \pmod{2}$ pues $7 - 5 = 2 \cdot 1$
- Si $m = 5$ entonces $27 \equiv 7 \pmod{5}$ $27 - 7 = 5 \cdot 4$.

---

a.) Demuestre que esta relación es de equivalencia (el conjunto cociente se denota $\mathbb{Z}_m$).

b.) Si $m = 2$, determine el conjuto cociente "$\mathbb{Z}_2$"

Solución:

a.) La relación es de equivalencia.

I.) **Reflexiva:** $\forall a \in \mathbb{Z}$, $a-a=m\cdot 0$, es decir, $a\equiv_m a$.

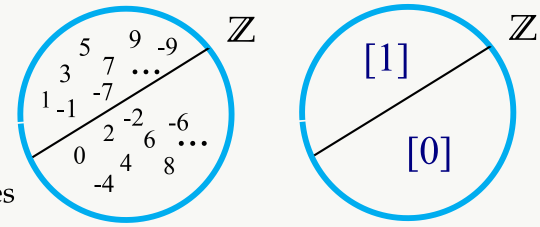
II.) **Simetría:** Si $a\equiv_m b \implies \exists\, k\in\mathbb{Z}$ tal que $b-a=mk \implies a-b=m(-k)$, por tanto $b\equiv_m a$

III.) **Transitiva:** $a\equiv_m b \,\wedge\, b\equiv_m c$ entonces $\exists\, k_1,k_2\in\mathbb{Z}$ tal que $b-a=mk_1$ y $c-b=mk_2$. Sumando obtenemos $c-a=m(k_1+k_2)$. Por tanto, $\exists\, k=k_1+k_2\in\mathbb{Z}$ tal que $c-a=mk$, es decir, $a\equiv_m c$.

b.) Si $m=2$ entonces

$$\begin{aligned}[0] &= \{a\in\mathbb{Z} \text{ tal que } a\equiv 0 \pmod 2\}\\ &= \{a\in\mathbb{Z} \text{ tal que } a=2k\}, \text{ es decir, los pares}\end{aligned}$$

$$\begin{aligned}[1] &= \{a\in\mathbb{Z} \text{ tal que } a\equiv 1 \pmod 2\}\\ &= \{a\in\mathbb{Z} \text{ tal que } a=2k+1\}, \text{ es decir, los impares}\end{aligned}$$



Como $[0]\cup[1]=\mathbb{Z} \implies \mathbb{Z}_2=\{[0],[1]\}$

Ejemplo 3.28

Sea $\mathcal{R}$ sobre $\mathbb{R}^*$ definida por $a\mathcal{R}b \iff a+\dfrac{1}{a}=b+\dfrac{1}{b}$.

1) $\mathcal{R}$ es de equivalencia

a) **Reflexiva:** $\forall a\in\mathbb{R}^*$, $a+\dfrac{1}{a}=a+\dfrac{1}{a} \implies a\mathcal{R}a$

b) **Simétrica:** $\forall a,b\in\mathbb{R}^*$, si $a\mathcal{R}b \implies a+\dfrac{1}{a}=b+\dfrac{1}{b} \implies b+\dfrac{1}{b}=a+\dfrac{1}{a} \implies b\mathcal{R}a$

c) **Transitiva:** $\forall a,b,c\in\mathbb{R}^*$, si $a\mathcal{R}b \,\wedge\, b\mathcal{R}c \implies a+\dfrac{1}{a}=b+\dfrac{1}{b} \,\wedge\, b+\dfrac{1}{b}=c+\dfrac{1}{c}$, entonces $a+\dfrac{1}{a}=c+\dfrac{1}{c}$, es decir, $a\mathcal{R}c$

2) $\left[\frac{1}{2}\right]=\{b\in\mathbb{R}^* \text{ tal que } \frac{1}{2}\mathcal{R}b\}$. Si $\frac{1}{2}\mathcal{R}b \implies \dfrac{1}{2}+\dfrac{1}{\frac{1}{2}}=b+\dfrac{1}{b} \implies \dfrac{-2b^2+5b-2}{2b}=0 \implies b=\frac{1}{2} \vee b=2$

$\therefore \left[\frac{1}{2}\right]=\{\frac{1}{2},2\}$

Ejemplo 3.29

En $\mathbb{N}^*\times\mathbb{N}^*$ se define la relación $\mathcal{R}$: $(a,b)\mathcal{R}(c,d) \iff ad=bc$

Verifique que es de equivalencia y determine las clases $[(2,2)]$ y $[7,4]$.

Solución:

a.) Es de equivalencia

I.) **Reflexiva:** $\forall n \in \mathbb{N}^*$, $(n,n)\,\mathcal{R}\,(n,n)$ pues $n^2 = n^2$.

II.) **Simétrica:** : $\forall a,b,c,d \in \mathbb{N}^*$, si $(a,b)\,\mathcal{R}\,(c,d)$ entonces $ad = bc \iff cb = da$, entonces $(c,d)\,\mathcal{R}\,(a,b)$

III.) **Transitividad**: $\forall a,b,c,d,p,q \in \mathbb{N}^*$, si $(a,b)\,\mathcal{R}\,(c,d) \wedge (c,d)\,\mathcal{R}\,(p,q)$ entonces $ad = bc \wedge cq = dp$.

Como $adcq = bcdp$ entonces $aq = bp$ (la cancelación es posible porque $cd \neq 0$). $\therefore\ (a,b)\,\mathcal{R}\,(p,q)$

b.) $[(2,2)] = \{\ (a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tal que $2a = 2b\ \} = \{\ (a,a)$ tal que $a \in \mathbb{N}^*\ \}$

$[(7,4)] = \{\ (a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tal que $7b = 4a\ \} = \{\ \left(a, \frac{4a}{7}\right)$ tal que $a \in \mathbb{N}^*\ \}$

Ejemplo 3.30

Sea E un conjunto y $H \subseteq E$. Sobre $\mathcal{P}(E)$ se define la relación $\mathcal{R}$ por

$$A\,\mathcal{R}\,B \iff A \cap H = B \cap H$$

a.) Demuestre que esta relación es de equivalencia

b.) Si $E = \{a,b,c\}$ y $H = \{a,\ b\}$, Determine el conjuto cociente "$\mathcal{P}(E)/\mathcal{R}$"

c.) En el caso general, ¿cuáles son las clases de equivalencia de $\mathcal{R}$?

Solución:

a.) Es de equivalencia

I.) **Reflexiva:** $\forall A \in \mathcal{P}(E)$, $A\mathcal{R}A$ pues $A \cap H = A \cap H$.

II.) **Simétrica:** : $\forall A,B \in \mathcal{P}(E)$, si $A\mathcal{R}B$ se tiene $A \cap H = B \cap H \implies B \cap H = A \cap H$ entonces $B\mathcal{R}A$

III.) **Transitividad**: $\forall A,B,C \in \mathcal{P}(E)$, si $A\mathcal{R}B \wedge B\mathcal{R}C$, se tiene $A \cap H = B \cap H = C \cap H$ entonces $A\mathcal{R}C$

b.) Si $E = \{a,b,c\}$ y $H = \{a,b\}$, Determine el conjunto cociente "$\mathcal{P}(E)/\mathcal{R}$"

Tenemos $\mathcal{P}(E) = \{\ \{\ \},\ \{a\},\ \{b\},\ \{c\},\ \{a,b\},\ \{a,c\},\ \{b,c\},\ \{a,b,c\}\}$. Hay tres clases (de equivalencia) en $\mathcal{P}(E)$:

I.) Los elementos de $\mathcal{P}(E)$ que contienen a $H = \{a,\, b\}$

$[H] = \{\ \{a,b\},\ \{a,b,c\}\}$

II.) Los elementos de $\mathcal{P}(E)$ disjuntos de H

$[\varnothing] = \{\ \varnothing,\ \{c\}\}$

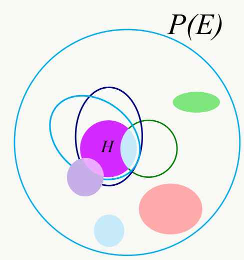
III.) Los elementos de $\mathcal{P}(E)$ que contienen un único elemento de $\mathcal{P}(H)^* = \mathcal{P}(H) - \{\varnothing, H\}$ (solo intersecan a H en subconjunto estricto y no vacío de H). Para obtener estos elementos hacemos lo siguiente: Cada $H_i \in \mathcal{P}(H)^*$ lo agregamos a cada uno de los elmentos de la clase $[\varnothing]$, de esta manera obtenemos una clase con elementos de $\mathcal{P}(E)$ cuya intersección con H es este H_i y por eso están relacionados.

Combinar $\mathcal{P}(H)^* = \{\ \{a\}, \{b\}\ \}$ con $[\varnothing] = \{\ \varnothing\ ,\ \{c\}\ \}$ nos produce dos clases:

$[\{a\}] = \{\ \{a\},\ \{c,a\}\ \}$ y $[\{b\}] = \{\ \{b\},\ \{c,b\}\}$

Finalmente, $\mathcal{P}(E)/\mathcal{R} = \{\ [H],\ [\varnothing],\ [\{a\}],\ [\{b\}]\ \}$ y es una partición de $\mathcal{P}(E)$.

c.) En el caso general, ¿cuáles son las clases de equivalencia de "$\mathcal{P}(E)/\mathcal{R}$"?. La respuesta está en el ítem anterior. Solo falta hacer una prueba formal. Queda como ejercicio.



Ejercicios

Sea $A = \{1,2,3\}$ y sea $\mathcal{R}$ una relación de gráfico $G_{\mathcal{R}} = \{(1,1),(2,2),(3,3,)\}$. Verifique que $\mathcal{R}$ es una relación de equivalencia.

3.4.1 ► Sea $A = \{a,b,c,d\}$ y sea $\mathcal{R}$ una relación de gráfico

$$G_{\mathcal{R}} = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,a),(a,c),(c,a),(a,d),(d,a),(b,c),(c,b),(b,d),(d,b),(c,d),(d,c)\}.$$

Determine si $\mathcal{R}$ es reflexiva, simétrica y/o transitiva.

3.4.2 ► Considere la relación $\mathcal{R}$ sobre $\mathbb{R} \times \mathbb{R}$, definida por $(x,y)\,\mathcal{R}\,(z,w) \iff x + z \leq y + w$. ¿Es $\mathcal{R}$ una relación de equivalencia?

3.4.3 ► En $\mathbb{Z}$ se define la relación $\mathcal{R}$: $a\mathcal{R}b \iff a = b \lor a + b = 10$

a.) Demuestre que esta relación es de equivalencia b.) Hacer una representación gráfica de la relación

c.) Determine el conjuto cociente "$\mathbb{Z}/\mathcal{R}$"

3.4.4 ▶ En $\mathbb{Z}^* \times \mathbb{Z}^*$ se define la relación $\mathcal{R}$: $(a,b)\mathcal{R}(c,d) \iff ac > 0 \wedge bd > 0$

a.) Demuestre que esta relación es de equivalencia

b.) Hacer una representación gráfica de la relación y determine el conjuto cociente "$\mathbb{Z}^* \times \mathbb{Z}^*/\mathcal{R}$"

3.4.5 ▶ En $\mathbb{N}$ se define la relación $\mathcal{R}$: $x\mathcal{R}y \iff x+y \in \{2n : n \in \mathbb{N}\}$

a.) Demuestre que esta relación es de equivalencia

b.) Determine el conjuto cociente "$\mathbb{N}/\mathcal{R}$"

3.4.6 ▶ En $\mathbb{Q}$ se define la relación $\mathcal{R}$: $\forall a,b \in \mathbb{Q} \quad a\mathcal{R}b \iff \quad \exists\, k \in \mathbb{Z}: \quad b = 2^k a$

a.) Demuestre que esta relación es de equivalencia

b.) Determine las clases $\dot{0}$ y $\dot{1}$

3.4.7 ▶ Sea E un conjunto y $H \in \mathcal{P}(E) - \{\varnothing\}$. Sobre $\mathcal{P}(E)$ se define la relación $\mathcal{R}$ por

$$A\,\mathcal{R}\,B \iff [A \cap H = B \cap H = \varnothing] \vee [A \cap H \neq \varnothing \wedge B \cap H \neq \varnothing]$$

a.) Demuestre que esta relación es de equivalencia

b.) Si $E = \{a,b,c\}$ y $H = \{a, b\}$, Determine el conjuto cociente "$\mathcal{P}(E)/\mathcal{R}$"

3.4.8 ▶ Sea $A = \{1,2,3\}$ y $B = \{1,2,3,4,5,6\}$.

a.) Sea $\mathcal{R}$ sobre A, de gráfico $G_{\mathcal{R}} = \{(1,1), (2,2), (3,3)\}$. $\mathcal{R}$ es de equivalencia (puede verificarlo usando el teorema 3.4). Determine el conjunto cociente $A/\mathcal{R}$ (una partición de A).

b.) Sea $\mathcal{R}$ sobre A, de gráfico $G_{\mathcal{R}} = \{(1,1), (2,2), (3,3), (3,1), (1,3)\}$. $\mathcal{R}$ es de equivalencia (puede verificarlo usando el teorema 3.4). Determine el conjunto cociente $A/\mathcal{R}$ (una partición de A).

c.) Sea $\mathcal{R}$ sobre B, de gráfico $G_{\mathcal{R}} = \{(1,1), (1,4), (2,2), (2,5), (3,3), (3,6), (4,1), (4,4), (5,2), (5,5), (6,3), (6,6)\}$. $\mathcal{R}$ es de equivalencia (puede verificarlo usando el teorema 3.4). Determine el conjunto cociente $B/\mathcal{R}$ (una partición de A).

3.4.9 ▶ Sea $A = \{\ \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. Sea $\mathcal{R}$ una relación sobre A, definida por el criterio $S\,\mathcal{R}\,T$ si y solo si el elemento mímimo de S es igual al elemento mínimo de T. Sabiendo que $\mathcal{R}$ es una relación de equivalencia, determine lel conjunto cociente $A/\mathcal{R}$.

$\mathcal{R}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$	Clases
$\{1\}$	1	0	0	1	1	0	1	
$\{2\}$	0	1	0	0	0	1	0	
$\{3\}$	0	0	1	0	0	0	0	
$\{1,2\}$	1	0	0	1	1	0	1	
$\{1,3\}$	1	0	0	1	1	0	1	
$\{2,3\}$	0	1	0	0	0	1	0	
$\{1,2,3\}$	1	0	0	1	1	0	1	

3.5 Relaciones de orden

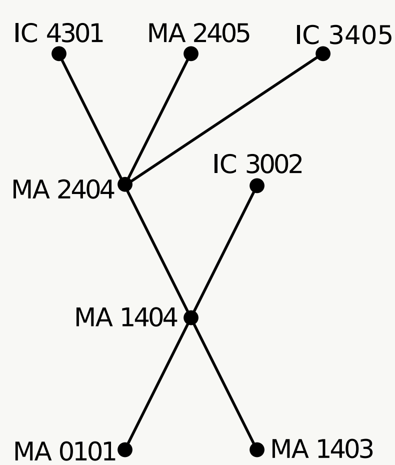
La noción intuitiva de "orden" se puede estudiar usando relaciones binarias. La idea es establecer un marco formal para poder describir nociones tales como "a es sucesor de b" o "b precede a a".

Ejemplo 3.31

Consideremos la relación de orden "Es requisito de", definida sobre un subconjunto C de los cursos de la carrera de Ingeniería en Computación

$$C = \{\ \text{MA 0101},\ \text{MA 1403},\ \text{MA 1404},\ \text{MA 2404},\ \text{IC 3002},\ \text{IC 4301},\ \text{MA 2405},\ \text{IC 3405}\ \}$$

Esta relación define una "relación de orden" en el conjunto C [1]. Una representación con un organigrama deja visualizar como la relación ordena al conjunto C



[1] Formalmente, debemos asumir que cada curso es requisito de sí mismo.

La relación de orden más conocida es posiblemente la relación " $\leq$ " sobre $\mathbb{R}$. Esta relación tiene tres propiedades muy bien establecidas,

a.) **Reflexiva:** $\forall a \in \mathbb{R},\ a \leq a$

b.) **Antisimétrica**: Si $a, b \in \mathbb{R},\ a \leq b \wedge b \leq a \Longrightarrow a = b$

c.) **Transitiva**: Si $a, b, c \in \mathbb{R},\ a \leq b \wedge b \leq c \Longrightarrow a \leq c$

Adicionalmente, $\forall a, b \in \mathbb{R},\ a \leq b \vee b \leq a$

Una relación de orden $\mathcal{R}$ es una generalización de la relación " $\leq$ ". En vez de escribir $a\mathcal{R}b$, a veces se escribe $a \preceq a$. Como tal, las relaciones de orden tiene las tres propiedades anteriores.

a.) **Reflexiva:** $a \preceq a$

b.) **Antisimétrica**: Si $a \preceq b \wedge b \preceq a \Longrightarrow a = b$

c.) **Transitiva**: Si $a \preceq b \wedge b \preceq c \Longrightarrow a \preceq c$

Un conjunto con un orden parcial $\preceq$ definido sobre él, se llama *un conjunto parcialmente ordenado* o simplemente un conjunto ordenado. La relación es un orden total si adicionalmente $\forall a, b \in A,\ a \preceq b \vee b \preceq a$

Definición 3.16

Sea $\mathcal{R}$ una relación definida sobre A.

a.) $\mathcal{R}$ es *antisimétrica* si y solo si $\forall a, b \in A$ se tiene que si $a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,a$ entonces $a = b$

b.) $\mathcal{R}$ es *total* si y solo si $\forall a, b \in A$ se tiene que $a\,\mathcal{R}\,b \vee b\,\mathcal{R}\,a$

Observación. Simetría y antisimetría no son nociones "opuestas".

a.) Existen relaciones que son simétricas y antisimétricas al mismo tiempo (como la relación "$=$")

b.) Existen relaciones que no son simétricas ni antisimétricas como la relación "divide a" en los enteros, por ejemplo, $-2|2$ y $2|-2$ pero $-2 \neq 2$. Además si $a|b$ no necesariamente $b|a$.

c.) Otras relaciones son simétricas pero no antisimétricas (como la relación de congruencia módulo n)

d.) Otras relaciones son antisimétricas pero no simétricas (como la relación " $\leq$ ").

A veces es útil ver la antisimetría desde el punto de vista de la contrapositiva:

$$\text{Es decir, si } a \neq b \text{ entonces } \neg\,[a\mathcal{R}b \wedge b\mathcal{R}a] \;\equiv\; a\not\mathcal{R}b \vee b\not\mathcal{R}a$$

Ejemplo 3.32

a.) Sea $\mathcal{R}$ una relación, definida sobre $\mathbb{Z}^*$, por la ley $a\mathcal{R}b \iff b$ divide a a, es decir, $\dfrac{a}{b} \in \mathbb{Z}$. Esta relación no es antisimétrica pues, por ejemplo, $-2|2$ y $2|-2$ pero $-2 \neq 2$.

b.) Sea $\mathcal{R}$ una relación, definida sobre $\mathbb{N}^*$, por la ley $a\mathcal{R}b \iff b$ divide a a, es decir, $\exists\, k \in \mathbb{Z}$ tal que $a = b \cdot k$. Esta relación es antisimétrica. En efecto:

Si $a\mathcal{R}b \wedge b\mathcal{R}a$ entonces existen $k_1, k_2 \in \mathbb{N}^*$ tal que $a = b \cdot k_1$ y $b = a \cdot k_2$. Por tanto $ab = ab \cdot k_1k_2 \implies k_1k_2 = 1 \implies k_1 = 1 = k_2$ pues estamos en $\mathbb{N}^*$, es decir, $a = b$.

Teorema 3.7

Sea $\mathcal{R}$ una relación definida sobre A con matriz asociada $M_{\mathcal{R}}$

a.) $\mathcal{R}$ es *antisimétrica* si y solo $M_{\mathcal{R}}^T \wedge M_{\mathcal{R}} \leq I_n$

b.) $\mathcal{R}$ es *total* si y solo $M_{\mathcal{R}}^T \vee M_{\mathcal{R}} = \mathbb{1}_n$ (matriz con todas sus entradas con 1.)

Ejemplo 3.33

Sea $\mathcal{R}$ definida sobre un conjunto A de cardinalidad 3. Se sabe que $M_{\mathcal{R}} = \begin{pmatrix} 1 & 1 & 1 \\ x & 1 & 0 \\ z & y & 1 \end{pmatrix}$. Determine x, y, z de tal manera $\mathcal{R}$ sea antisimétrica.

Solución: Como $\mathcal{R}$ sea antisimétrica, si $a \neq b$ entonces $\neg\,[a\mathcal{R}b \wedge b\mathcal{R}a] \equiv a\not\mathcal{R}b \vee b\not\mathcal{R}a$

Supongamos que $A = \{a, b, c\}$. Tenemos $M_{\mathcal{R}} = \begin{array}{c} \\ a \\ b \\ c \end{array}\!\!\begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ x & 1 & 0 \\ z & y & 1 \end{pmatrix} \end{array}$. Entonces,

$$\begin{cases} \text{Como } a\mathcal{R}b \wedge a \neq b, \implies b\not\mathcal{R}a \implies x = 0 \\ \text{Como } a\mathcal{R}c \wedge a \neq c, \implies c\not\mathcal{R}a \implies z = 0 \\ \text{Como } b\not\mathcal{R}c, \text{ no hay problema si } c\mathcal{R}b \text{ o si } c\not\mathcal{R}b \implies y = 0 \vee y = 1 \end{cases}$$

Otra manera: $\mathcal{R}$ es *antisimétrica* si y solo $M_{\mathcal{R}}^T \wedge M_{\mathcal{R}} \leq I_n$. Entonces

$$M_{\mathcal{R}}^T \wedge M_{\mathcal{R}} = \begin{pmatrix} 1 & x & z \\ 1 & 1 & y \\ 1 & 0 & 1 \end{pmatrix} \wedge \begin{pmatrix} 1 & 1 & 1 \\ x & 1 & 0 \\ z & y & 1 \end{pmatrix} \leq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies x = 0,\ z = 0 \text{ y } y = 0 \text{ o } y = 1.$$

Ejemplo 3.34

Consideremos tres relaciones sobre $A = \{1,2,3\}$, con matrices $M_{\mathcal{R}}$, $M_{\mathcal{S}}$ y $M_{\mathcal{T}}$

$$M_{\mathcal{R}} \quad \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \qquad M_{\mathcal{S}} \quad \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \qquad M_{\mathcal{T}} \quad \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \end{array}$$

La relación $\mathcal{R}$ es de equivalencia. $\mathcal{S}$ es antisimétrica pues $M_{\mathcal{S}}^T \wedge M_{\mathcal{S}} \leq I_n$. En $M_{\mathcal{S}}$, como $2 \neq 1$ entonces si aparece $(1,2)$ no puede parecer $(2,1)$ por la propiedad antisimétrica. Además $\mathcal{S}$ no es total, pues $1 \not{\mathcal{S}} 3$ y $3 \not{\mathcal{S}} 1$. En cambio $M_{\mathcal{T}}$ es antisimétrica y total.

Definición 3.17

Sea $\mathcal{R}$ una relación definida sobre A.

a.) $\mathcal{R}$ es *preorden* si y solo si $\mathcal{R}$ es reflexiva y transitiva.

b.) $\mathcal{R}$ es un *orden parcial u "orden sobre A"* si y solo si $\mathcal{R}$ es reflexiva, transitiva y antisimétrica.

c.) $\mathcal{R}$ es un un *orden total* si y solo si $\mathcal{R}$ es reflexiva, transitiva, antisimétrica y total.

Ejemplo 3.35

Considere la relación "$\preceq$" definida sobre $A = \{2,3,4,5,6\}$ con gráfico

$$G_{\mathcal{R}} = A = \{(2,2),(4,2),(6,2),(6,3),(3,3),(4,4),(5,5),(6,6)\}$$

a.) Esta relación es de orden.

I.) **Reflexiva**: La diagonal D está contenida en $\mathcal{R}$: $D \subseteq G_{\mathcal{R}}$

II.) **Antisimétrica**: Podemos usar el teorema 3.7. Hay que mostrar que $M_{\preceq}^T \wedge M_{\preceq} \leq I_n$.

$$\begin{array}{cc} M_{\preceq}^{T} & \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{array}{c} 2\\3\\4\\5\\6 \end{array} & \begin{pmatrix} 1&0&1&0&1\\0&1&0&0&1\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1 \end{pmatrix} \end{array} \wedge \begin{array}{cc} M_{\preceq} & \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{array}{c} 2\\3\\4\\5\\6 \end{array} & \begin{pmatrix} 1&0&0&0&0\\0&1&0&0&0\\1&0&1&0&0\\0&0&0&1&0\\1&1&0&0&1 \end{pmatrix} \end{array} = \begin{array}{cc} M_{\preceq\wedge\preceq} & \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{array}{c} 2\\3\\4\\5\\6 \end{array} & \begin{pmatrix} 1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1 \end{pmatrix} \end{array} \leq I_n$$

III.) **Transitiva**: Podemos usar el teorema 3.4. Hay que mostrar que $M_{\preceq\circ\preceq} = M_{\preceq} \odot M_{\preceq} \leq M_{\preceq}$.

$$\begin{array}{cc} M_{\preceq} & \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{array}{c} 2\\3\\4\\5\\6 \end{array} & \begin{pmatrix} 1&0&0&0&0\\0&1&0&0&0\\1&0&1&0&0\\0&0&0&1&0\\1&1&0&0&1 \end{pmatrix} \end{array} \odot \begin{array}{cc} M_{\preceq} & \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{array}{c} 2\\3\\4\\5\\6 \end{array} & \begin{pmatrix} 1&0&0&0&0\\0&1&0&0&0\\1&0&1&0&0\\0&0&0&1&0\\1&1&0&0&1 \end{pmatrix} \end{array} = \begin{array}{cc} M_{\preceq\circ\preceq} & \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{array}{c} 2\\3\\4\\5\\6 \end{array} & \begin{pmatrix} 1&0&0&0&0\\0&1&0&0&0\\1&0&1&0&0\\0&0&0&1&0\\1&1&0&0&1 \end{pmatrix} \end{array} \leq M_{\preceq}$$

b.) Esta relación no es de orden total. Por ejemplo $(3,5) \notin G_{\preceq}$ ni $(5,3) \notin G_{\preceq}$

Ejemplo 3.36

Consideremos tres relaciones sobre $A = \{1,2,3\}$, con matrices $M_{\mathcal{R}}$, $M_{\mathcal{S}}$ y $M_{\mathcal{T}}$

$$\begin{array}{cc} M_{\mathcal{R}} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1\\2\\3 \end{array} & \begin{pmatrix} 1&1&0\\1&1&1\\0&1&1 \end{pmatrix} \end{array} \qquad \begin{array}{cc} M_{\mathcal{S}} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1\\2\\3 \end{array} & \begin{pmatrix} 1&1&0\\0&1&1\\0&0&1 \end{pmatrix} \end{array} \qquad \begin{array}{cc} M_{\mathcal{S}} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1\\2\\3 \end{array} & \begin{pmatrix} 1&1&1\\0&1&0\\0&1&1 \end{pmatrix} \end{array}$$

La relación $\mathcal{R}$ es de equivalencia y $\mathcal{S}$ es un orden parcial. En $M_{\mathcal{S}}$, como $2 \neq 1$ entonces si aparece $(1,2)$ no puede aparecer $(2,1)$ por la propiedad antisimétrica. Además $\mathcal{S}$ no es un orden total, pues $1 \not\mathcal{S} 3$ y $3 \not\mathcal{S} 1$. En cambio $M_{\mathcal{T}}$ es una relación de orden total.

Ejemplo 3.37

Consideremos dos relaciones $\mathcal{R}$ y $\mathcal{S}$ sobre $A = \{1,2,4,5\}$. La relación $\mathcal{R}$ es la relación " $\leq$ ", es decir, $a\mathcal{R}b \iff a \leq b$. La relación $\mathcal{S}$ es la relación " $|$ ", es decir, $a\mathcal{R}b \iff a|b$ ("a divide a b", sin resto). $\mathcal{R}$ es un orden total sobre A y $\mathcal{S}$ es un orden parcial sobre A

Las matrices de adyacencia de estas relaciones son las matrices $M_{\mathcal{R}}$ y $M_{\mathcal{S}}$

$$\begin{array}{c|cccc} M_{\mathcal{R}} & 1 & 2 & 4 & 5 \\ \hline 1 & & & & \\ 2 & & & & \\ 4 & & & & \\ 5 & & & & \end{array}$$

$$\begin{array}{cc} & \begin{array}{cccc} 1 & 2 & 4 & 5 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 4 \\ 5 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \qquad M_{\mathcal{R}} \quad \begin{array}{cc} & \begin{array}{cccc} 1 & 2 & 4 & 5 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 4 \\ 5 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Ejemplo 3.38

Sean $\mathcal{R}$ una relación definida sobre un conjunto no vacío A, y sea $D(A) = \{(x,x) \text{ tal que } x \in A\}$. Muestre que $\mathcal{R}$ es antisimétrica si y solo si $G_{\mathcal{R} \cap \mathcal{R}^{-1}} \subseteq D(A)$

Solución:

"$\Longrightarrow$" **Hipótesis:** $\mathcal{R}$ es antisimétrica.

Hay que demostrar que $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq D(A)$.

$$\begin{aligned} (a,b) \in \mathcal{R} \cap \mathcal{R}^{-1} &\Longrightarrow a\,\mathcal{R}\,b \wedge a\,\mathcal{R}^{-1}\,b \\ &\Longrightarrow a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,a \\ &\Longrightarrow a = b \text{ por hipótesis.} \\ &\therefore \quad (a,b) = (a,a) \in D(A) \end{aligned}$$

- "$\Longleftarrow$" **Hipótesis:** $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq D(A)$.

Hay que demostrar que $\mathcal{R}$ es antisimétrica.

$$\begin{aligned} a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,a &\Longrightarrow a\,\mathcal{R}\,b \wedge a\,\mathcal{R}^{-1}\,b \\ &\Longrightarrow (a,b) \in \mathcal{R} \cap \mathcal{R}^{-1} \\ &\Longrightarrow (a,b) \in D(A) \text{ por hipótesis} \\ &\therefore \quad a = b \end{aligned}$$

Diagramas de Hasse. Al igual que con las relaciones, existe una manera conveniente de representar una relación de orden para visualizar de que manera induce un orden. Un Diagramna de Hasse es un dígrafo simplificado,

a.) Eliminamos todos los lazos.

b.) Eliminamos todos los "caminos transitivos".

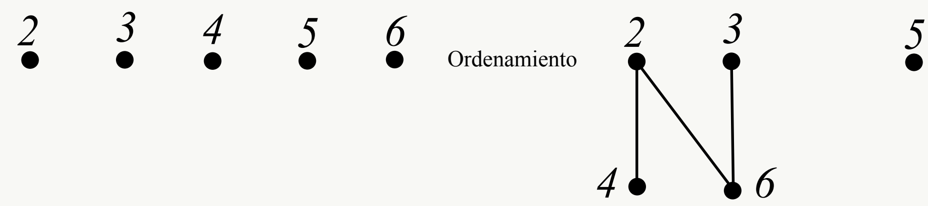
c.) El gráfico no tiene flechas, la dirección se asume "hacia arriba"

Ejemplo 3.39

Considere la relación "$\preceq$" definida sobre $A = \{2,3,4,5,6\}$ con gráfico

$$G_{\mathcal{R}} = A = \{(2,2),(4,2),(6,2),(6,3),(3,3),(4,4),(5,5),(6,6)\}$$

Ya probamos en el ejemplo 3.35 que esta relación es un orden parcial (no total). Los nodos en el diagrama de Hasse son $\{2,3,4,5,6\}$ y como se nota en el gráfico, $4 \preceq 2,\ 6 \preceq 2,\ 6 \preceq 3;$ entonces en el diagrama de Hasse, 2 va arriba de 4 y 6 y 3 va arriba de 6.

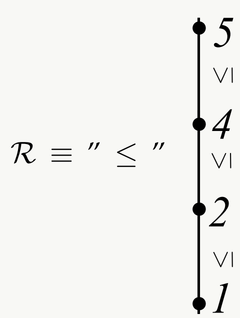


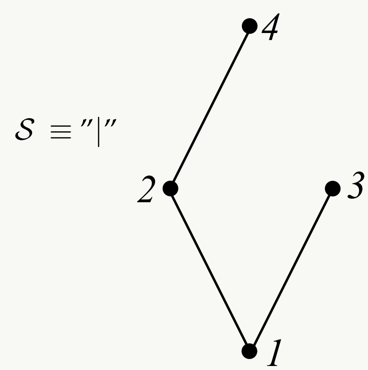
Ejemplo 3.40

Consideremos dos relaciones " $\leq$ " y "$|$" sobre $A = \{1,2,4,5\}$. Las matrices de adyacencia de estas relaciones son las matrices $M_{\mathcal{R}}$ y $M_{\mathcal{S}}$

$$
\begin{array}{c|c}
M_{\mathcal{R}} & \begin{array}{cccc} 1 & 2 & 4 & 5 \end{array} \\
\begin{array}{c} 1 \\ 2 \\ 4 \\ 5 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\end{array}
\qquad
\begin{array}{c|c}
M_{\mathcal{R}} & \begin{array}{cccc} 1 & 2 & 4 & 5 \end{array} \\
\begin{array}{c} 1 \\ 2 \\ 4 \\ 5 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\end{array}
$$

Sus digramas de Hasse serían





Ejemplo 3.41

Sea $A = \{x,y,z\}$. Sobre $\mathcal{P}(A) = \{\varnothing, \{x\}, \{y\}, \{z\}, \{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\}\}$ se define la relación $\mathcal{R}$ por $S\,\mathcal{R}\,T \iff S \subseteq T$.

a.) Muestre que $\mathcal{R}$ induce un orden parcial sobre $\mathcal{P}(A)$ pero no total.

b.) Determine la matriz $M_{\mathcal{R}}$

c.) Construya un diagrama de Hasse para la relación

Solución: En efecto.

a.) $\mathcal{R}$ es un orden parcial sobre $\mathcal{P}(A)$ pero no total

I.) **Reflexiva:** $\forall S \in \mathcal{P}(A)$, $S \subseteq S$. Por tanto $S \mathcal{R} S$.

II.) **Antisimétrica**: $\forall S, T \in \mathcal{P}(A)$, si $S \mathcal{R} T \wedge T \mathcal{R} S$ entonces $S \subseteq T \wedge T \subseteq S \implies S = T$.

III.) **Transitiva**: $\forall S, T, W \in \mathcal{P}(A)$, si $S \mathcal{R} T \wedge T \mathcal{R} W$ entonces $S \subseteq T \wedge T \subseteq W \implies S \subseteq W$, es decir, $S \mathcal{R} W$

Entonces la relación "$\subseteq$" induce un orden parcial sobre $\mathcal{P}(A)$ pero no lo ordena totalmente pues, por ejemplo $\{x\} \not\mathcal{R} \{z\}$ pues $\{x\} \not\subseteq \{z\}$.

b.) Para el cálculo de $M_{\mathcal{R}}$ podemos usar una representación cartesiana de la relación.

$\subseteq$	$\varnothing$	$\{x\}$	$\{y\}$	$\{z\}$	$\{x,y\}$	$\{x,z\}$	$\{y,z\}$	$\{x,y,z\}$
$\varnothing$	1	1	1	1	1	1	1	1
$\{x\}$	0	1	0	0	1	1	0	1
$\{y\}$	0	0	1	0	1	0	1	1
$\{z\}$	0	0	0	1	0	1	1	1
$\{x,y\}$	0	0	0	0	1	0	0	1
$\{x,z\}$	0	0	0	0	0	1	0	1
$\{y,z\}$	0	0	0	0	0	0	1	1
$\{x,y,z\}$	0	0	0	0	0	0	0	1

c.) Diagrama de Hasse

$\mathcal{R} \equiv$ "$\subseteq$"

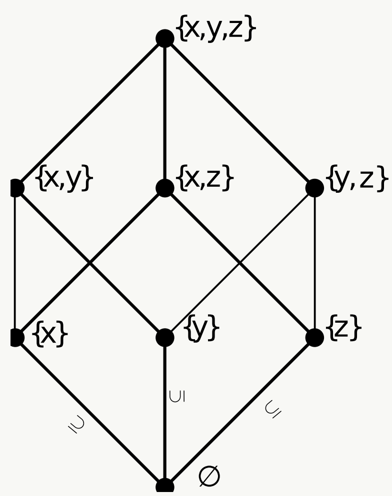


Diagrama de Hasse con Wolfram Mathematica

■ **Código 3.2**: *Diagramas de Hasse con Mathematica*

```
<< Combinatorica`;
am = {
   {1, 1, 1, 1, 1, 1, 1, 1},
   {0, 1, 0, 0, 1, 1, 0, 1},
   {0, 0 , 1, 0, 1, 0, 1, 1},
   {0, 0 , 0, 1, 0, 1, 1, 1},
   {0, 0, 0 , 0, 1, 0, 0, 1},
   {0, 0, 0, 0, 0 , 1, 0, 1},
   {0, 0, 0, 0, 0, 0, 1, 1},
   {0, 0, 0, 0, 0, 0, 0, 1}};

g = FromAdjacencyMatrix[am, Type -> Directed];
h = HasseDiagram[SetVertexLabels[g,
    {"   \[EmptySet]", "{x}", "{y}", "{z}", "{x,y}", "{x,z}", "{y,z}",
      "{x,y,z}"}
    ]];
ShowGraph[h, BaseStyle -> {FontSize -> 18}]
```

Para los ejemlos que siguen, necesitamos un par de recordatorios.

- $k_1,k_2 \in \mathbb{N}^*$ entonces, si $k_1 > 1 \implies k_1k_2 > 1$. En particular, si $k_1k_2 = 1 \implies k_1 = k_2 = 1$.
- Si $b,k \in \mathbb{N}^*$ y $b = b^k \implies \log_b(b) = \log_b(b^k) = k\log_b(b) \implies 1 = k$.

Ejemplo 3.42

Considere la relación $\mathcal{R}$ sobre $\mathbb{N}^*$ definida por $a\,\mathcal{R}\,b \iff \exists\, k \in \mathbb{N}$ tal que $a = bk$ (es decir, $b|a$). Muestre que $\mathcal{R}$ es un orden parcial. ¿Es un orden total?

Solución:

a.) **Reflexiva:** $\forall a \in \mathbb{N}^*,\ a = a \cdot 1$. Entonces $a\,\mathcal{R}\,a$.

b.) **Antisimétrica**: $\forall a,b \in \mathbb{N}^*$, si $a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,a$ entonces $\exists\, k_1,k_2 \in \mathbb{N}^*$ con $a = b \cdot k_1 \wedge b = a \cdot k_2$. Entonces, sustituyendo b, $a = (a \cdot k_2) \cdot k_1 \implies k_1k_2 = 1 \implies k_1 = k_2 = 1.\ \therefore\ a = b$.

c.) **Antisimétrica**: $\forall a,b \in \mathbb{N}^*$, si $a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,a$ entonces $\exists\, k_1,k_2 \in \mathbb{N}^*$ con $a = b^{k_1} \wedge b = a^{k_2}$. Entonces $\exists\, k_1,k_2 \in \mathbb{N}^*$ con $a = b \cdot k_1 \wedge b = c \cdot k_2$. Sustituyendo b, tenemos $a = (ck_2) \cdot k_1$. Por tanto existe $k = k_1k_2 \in \mathbb{N}^*$ tal que $a = c \cdot k.\ \therefore\ a\,\mathcal{R}\,c$.

d.) La relación es un orden parcial pero no es un orden total pues, por ejemplo, $2\not\mathcal{R}5$ y $5\not\mathcal{R}2$.

Ejemplo 3.43

Considere la relación $\mathcal{R}$ sobre $\mathbb{N}^*$ definida por $a\,\mathcal{R}\,b \iff \exists\, k \in \mathbb{N}$ tal que $a = b^k$.

a.) Muestre que $\mathcal{R}$ no es simétrica

b.) ¿Es $\mathcal{R}$ un orden parcial?. ¿Es un orden total?

Solución:

a.) $\mathcal{R}$ no es simétrica pues $4\mathcal{R}2$ pues $4 = 2^2$ pero $2\not\mathcal{R}4$ pues $2 = 4^k \implies k = \frac{1}{2} \notin \mathbb{N}^*$.

b.) ¿Es $\mathcal{R}$ un orden parcial?. ¿Es un orden total?

I.) **Reflexiva:** $\forall a \in \mathbb{N}^*,\ a = a^1$, es decir, $a\,\mathcal{R}\,a$

II.) **Antisimétrica**: $\forall a,b \in \mathbb{N}^*$, si $a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,a$ entonces $\exists\, k_1,k_2 \in \mathbb{N}^*$ con $a = b^{k_1} \wedge b = a^{k_2}$. Entonces

$$\begin{aligned} a = b^{k_1} \wedge b = a^{k_2} &\implies b = \left(b^{k_1}\right)^{k_2} \\ &\implies b = b^{k_1k_2} \\ &\implies k_1k_2 = 1 \\ &\implies k_1 = k_2 = 1, \text{ pues } k_1,k_2 \in \mathbb{N}^* \\ &\therefore\quad a = b^1 \end{aligned}$$

III.) **Transitiva**: $\forall a,b,c \in \mathbb{N}^*$, si $a\,\mathcal{R}\,b \wedge b\,\mathcal{R}\,c$ entonces $\exists\, k_1,k_2 \in \mathbb{N}^*$ con $a = b^{k_1} \wedge b = c^{k_2}$. Entonces

$$\begin{aligned} a = b^{k_1} \wedge b = c^{k_2} &\implies a = \left(c^{k_2}\right)^{k_1} \\ &\implies a = c^{k_1k_2} \\ &\therefore\quad a = c^k,\ \text{ es decir, } a\,\mathcal{R}\,c \text{ pues } k = k_1k_2 \in \mathbb{N}^* \end{aligned}$$

Ejemplo 3.44 **(Ordenamientos lexicográficos)**

El orden lexicográfico es el mismo que usamos en en un diccionario. Para comparar dos tiras (strings) a_1a_2 con $a_1'a_2'$ definimos una relación de orden de la siguiente manera,

Sea "$\preceq_1$" es una relación de orden sobre A_1 y "$\preceq_2$" es una relación de orden sobre A_2. El orden lexicográfico "$\preceq$" sobre $A_1 \times A_2$ es definido por

$$(a_1,a_2) \preceq (a_1',a_2') \text{ si } a_1 \preceq_1 a_1' \text{ o si } a_1 = a_1' \wedge a_2 \preceq_2 a_2'$$

Este orden se puede generalizar y aplicar al producto cartesiano de n conjuntos. Definimos " $\preceq$ " sobre $A_1 \times A_2, ..., \times A_n$ por

$$(a_1, a_2, ..., a_n) \preceq (b_1, b_2, ..., b_m) \iff a_1 \preceq b_1 \lor [\exists\, i \in \mathbb{N}^* \text{ tal que } a_1 = b_1, ..., a_i = b_i \text{ y } a_{i+1} \preceq b_{i+1}].$$

Este orden se puede usar para comparar tiras (strings) de caracteres no de la misma longitud. Consideremos dos tiras $a_1a_2...a_n$ con $b_1b_2...b_m$ en S.

Si $t = min\{n, m\}$ y $\preceq$ es el orden lexicográfico sobre $S^t = S \times ... \times S$, entonces $a_1a_2...a_n$ es menor o igual que $b_1b_2...b_m$ si y solo si

$$(a_1, a_2, ..., a_t) \preceq (b_1, b_2, ..., b_t) \lor [(a_1, a_2, ..., a_t) \preceq (b_1, b_2, ..., b_t) \land m < n]$$

Definición 3.18

Sea " $\preceq$ " una relación de orden sobre A. Sea $x \in A$.

a.) x es un "elemento minimal" de A si y solo si $\forall y \in A,\ y \preceq x \iff y = x$

b.) x es "primer elemento" de A si y solo si $\forall y \in A,\ x \preceq y$

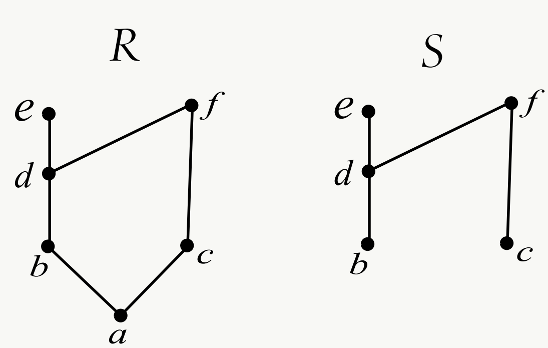
c.) x es "elemento maximal" de A si y solo si $\forall y \in A,\ x \preceq y \iff x = y$

d.) x es "último elemento" de A si y solo si $\forall y \in A,\ y \preceq x$

La definición dice que un "elemento minimal" no tiene predecesores y un "primer elemento" precede a todos (y es por tanto también minimal, pero no viceversa). Un "elemento maximal" no tiene sucesores y un "último elemento" sucede a todos los demás (y es por tanto también maximal, pero no viceversa).

Ejemplo 3.45

Consideremos la relaciones de orden $\mathcal{R}$ sobre $A\{a, b, c, d, e, f\}$, y $\mathcal{S}$ sobre $B\{b, c, d, e, f\}$. Sus diagramas de Hasse son



a.) a es un elemento minimal y también primer elemento de A.

b.) e y f son maximales de A, pero no hay último elemento.

c.) b y c son elementos minimales de B. No hay primer elemento.

d.) e y f son maximales de B, pero no hay último elemento.

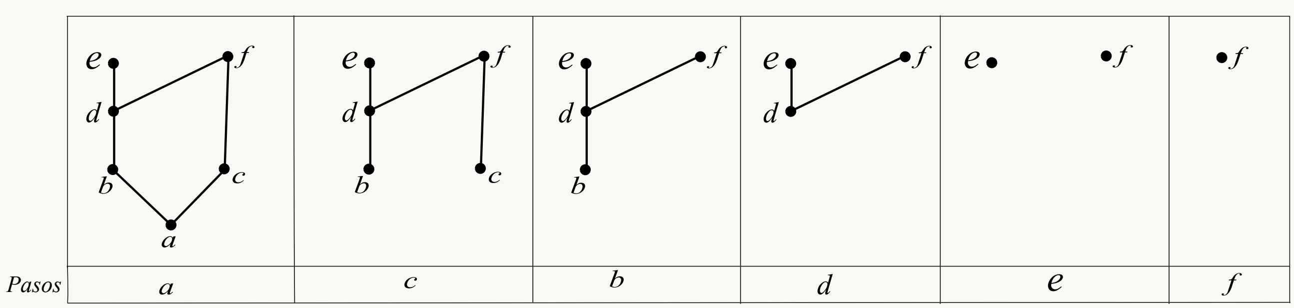
Ejemplo 3.46

Un algoritmo de "ordenamiento topológico" se puede aplicar si tenemos un conjunto A finito y un orden parcial $\mathcal{R}$ definido sobre él. El resultado final sería una subconjunto de elementos de A, totalmente ordenados: $a_1 \prec a_2 \prec ... \prec a_k$

El agoritmo es

```
Entrada: (R, A), A no vacío
k = 1
While A no sea vacío
     begin
     ak := un elemento minimal de A
     A  := A - {ak} (está parcialmente ordenado)
     k  := k+1
     end
Salida {a1,a2,...,an}
```

Por ejemplo, consideremos orden parcial $\mathcal{R}$ sobre $A\{a,b,c,d,e,f\}$. El algoritmo procedería como se muestra en la figura.



La salida es la lista ordenada $\{a,c,b,d,e,f\}$

Ejercicios

3.5.1 ▶ Considere el juego "Pi=piedra, Pa=papel, Ti=tijeras". Este juego es una relación sobre el conjunto $A = \{\text{Pi},\text{Pa},\text{Ti}\}$. La relación es $x\mathcal{R}y \iff$ "x es vencido por y" y por supuesto, suponemos que x se vence a sí mismo (empate). Determine la matriz de adyacencia es esta relación y preuebe que es simétrica, antisimétrica pero no transitiva.

3.5.2 ▶ Sea X una colección de conjuntos finitos y sea $\mathcal{R}$ una relación definida sobre X por

$$S\mathcal{R}T \iff |S| < |T| \vee S = T$$

a.) Mustre que $\mathcal{R}$ es una relación de orden. ¿Es un orden total?

b.) Si $X = \mathcal{P}(\{0,1,2\})$, realice un diagrama de Hasse de la relación $\mathcal{R}$ sobre X.

3.5.3 ▶ Sobre $\mathbb{Z} \times \mathbb{Z}^*$, se define la relación $\mathcal{R}$ de acuerdo al siguiente criterio,

$$(a,b)\mathcal{R}(c,d) \iff [b = d \wedge (a-c) \in \mathbb{N}]$$

Pruebe que $\mathcal{R}$ es una relación de orden. ¿Es R una relación de orden total?

3.5.4 ▶ Sobre $\mathbb{N}$ se define la relación $\mathcal{R}$ por $a\mathcal{R}b \iff \exists\, n \in \mathbb{N}$ tal que $b = a+n$. Muestre que $\mathcal{R}$ es un orden total.

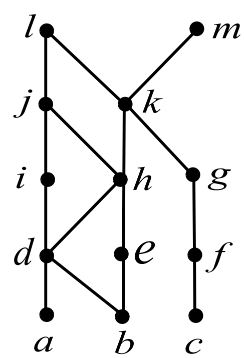
3.5.5 ▶ Sea $\mathcal{R}$ una relación de orden sobre A. Muestre que $\mathcal{R}$ es de orden total si y solo si $\mathcal{R} \cup \mathcal{R}^{-1} = A \times A$.

3.5.6 ▶ Sean $\mathcal{R}$ y $\mathcal{S}$ relaciones de orden sobre A. Muestre que

a.) $\mathcal{R}^{-1}$ es de orden

b.) Muestre que la relación $\mathcal{T}$, definida sobre A por $a\mathcal{T}b \iff a\mathcal{R}b \wedge a\mathcal{S}b$, es de orden

3.5.7 ▶ Considere el diagrama de Hasse que está a la derecha. Este diagrama corresponde a una relación de orden $\mathcal{R}$ definida sobre $A = \{a,b,c,d,e,f\}$. Si existen, determine los elementos maximales, minimales, primero y último elemento.



3.5.8 ▶ Sea $A = \{0,1,2,3\}$. Determine cuáles de las siguientes relaciones son de orden. En caso afirmativo, represente la relación con un diagrama de Hasse y, si existen, determine los elementos maximales, minimales, primero y último elemento.

a.) $G_{\mathcal{R}} = \{(0,0),(2,2),(3,3)\}$

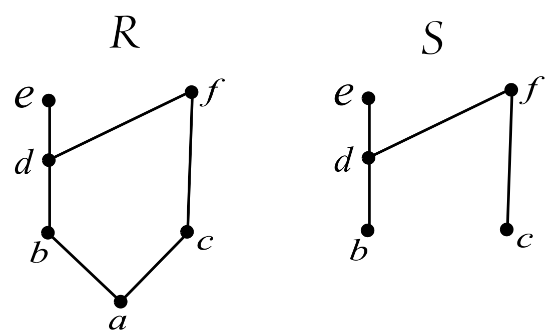
b.) $G_{\mathcal{R}} = \{(0,0),(1,1),(2,0),(2,2),(2,3),(3,3)\}$

c.) $G_{\mathcal{R}} = \{(0,0),(1,1),(1,2),(2,2),(3,1),(3,3)\}$

d.) $G_{\mathcal{R}} = \{(0,0),(1,1),(1,2),(1,3),(2,0),(2,2),(2,3),(3,0),(3,3)\}$

e.) $G_{\mathcal{R}} = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3),(2,0),(2,2),(3,3)\}$

3.5.9 ▶ Consideremos la relaciones de orden $\mathcal{R}$ sobre $A\{a,b,c,d,e,f\}$, y $\mathcal{S}$ sobre $B\{b,c,d,e,f\}$. Sus diagramas de Hasse son



Determine las matrices $M_{\mathcal{R}}$ y $M_{\mathcal{S}}$

Capítulo 4

Funciones

Definición 4.1

Se dice que la relación $f = (G_f, A, B)$ es una función de A en B y se denota $f : A \longrightarrow B$, si y solo si todo elemento de A esta relacionado con un único elemento de B, es decir,

$$\text{Si } (a,b) \in G_f \wedge (a,c) \in G_f \Longrightarrow b = c$$

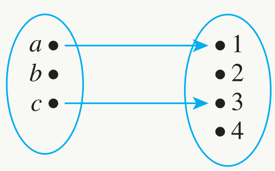
a.) A es el *dominio* o conjunto de partida,de f y se denota D_f. Los elementos de D_f se llaman "preimágenes".

b.) B es el *codominio* o conjunto de llegada de f. Sus elementos se llamam "imagenes"

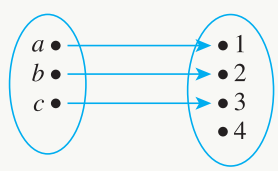
Ejemplo 4.1

Sea $A = \{a,b,c\}$ y $B = \{1,2,3,4\}$. La tres primeras figuras que que siguen, representan las funciones f, g y h. La cuarta figura es una relación $\mathcal{R}$ pero no una función, pues $(c,1),(c,3) \in G_{\mathcal{R}}$.

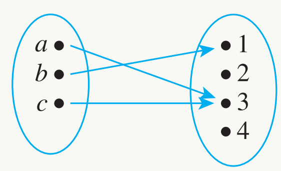
$f : A \longrightarrow B$



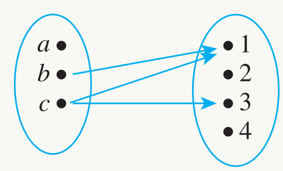
$g : A \longrightarrow B$



$h : A \longrightarrow B$



Relación $\mathcal{R}$



Definición 4.2 (Ámbito, imagen directa, imagen inversa).

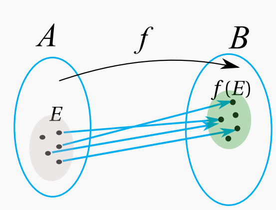
Sea $f : A \longrightarrow B$ una función.

a.) El "ámbito" (o rango) de f se denota A_f o también $f[A]$.

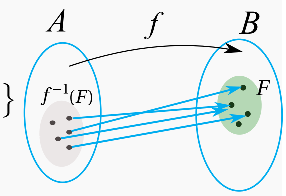
$$f[A] = \{y \in B \text{ tal que } \exists\, x \in A \text{ con } f(x) = y\}$$

b.) Si $f(x) = y$, "x" es la "preimagen" de y y "y" es la "imagen" de x bajo f

c.) La "imagen directa" de $E \subseteq A$ es $f(E) = \{b \in B \text{ tal que } \exists\, a \in E \text{ con } f(a) = b\}$



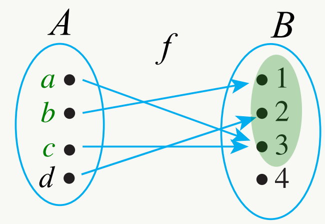
La "imagen inversa" de $F \subseteq B$ es $f^{-1}(F) = \{a \in A \text{ tal que } \exists\, b \in F \text{ con } b = f(a)\}$



En particular, $f^{-1}(b) := f^{-1}(\{b\})$

Ejemplo 4.2

Sean $A = \{a,b,c,d\}$ y $B = \{1,2,3,4\}$. Considere la función $f : A \longrightarrow B$ representada con la figura a la derecha. Entonces



a.) $f[A] = \{1,2,3\}$

b.) Si $E = \{a,b,c\}$, entonces $f(E) = \{1,3\}$

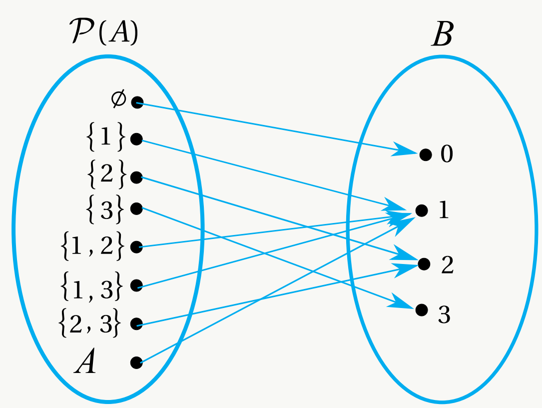
c.) $f^{-1}(B) = \{a,b,c,d\}$

d.) $f^{-1}(4) = \varnothing$

Ejemplo 4.3

Sean $A = \{1,2,3,\}$ y $B = \{0,1,2,3\}$. Sea f de $\mathcal{P}(A)$ en B, definida por

$$f(E)\begin{cases} = 0 & \text{si } \quad E = \varnothing \\ = \text{mín}(E) & \text{si } \quad E \neq \varnothing \end{cases}$$



a.) $f[\mathcal{P}(A)] = \{0,1,2,3\}$

b.) Si $F = \{2,3\}$, entonces $f^{-1}(F) = \{\{2\},\{2,3\},\{3\}\}$

c.) $f(\{\varnothing, A, \{1,2\}\}) = \{0,1\}$

Ejemplo 4.4

Sea $A = \{1,2,3,4,5\}$. Considere la función $f : A \times A \longrightarrow \mathcal{P}(\mathcal{P}(A))$ definida por $f(a,b) = \{\{a\}, \{a,b\}\}$.

a.) Determine $f(1,1)$

b.) Si $E = \{(1,2),(3,2),(1,1)\}$, Determine $f(E)$

c.) Si $F = \{ \{\{3\}, \{3,5\}\}, \{\{1\}, \{1,3\}\}, \{\{4\}\} \}$, determine $f^{-1}(F)$.

Solución:

a.) $f(1,1) = \{\{1\}, \{1,1\}\} \ = \ \{\{1\}\}$

b.) $f(E) = \{ \ \{\{1\}, \ \{1,2\}\}, \ \{\{3\}, \ \{3,2\}\}, \ \{\{1\}\} \ \}$

c.) $f^{-1}(F) = \{ \ (3,5), \ (1,3), \ (4,4) \ \}$

Ejemplo 4.5

Considere la función $f : A \longrightarrow B$. Sean $C, D \subseteq A$.

a.) $f(C \cap D) \subseteq f(C) \cap f(D)$

b.) $f(C) - f(D) \subseteq f(C - D)$

Solución:

a.) $f(C \cap D) \subseteq f(C) \cap f(D)$

$$
\begin{aligned}
\text{Sea } y \in f(C \cap D) & \implies \exists\, x \in C \cap D \text{ tal que } f(x) = y \\
& \implies \exists\, x \in C \text{ tal que } f(x) = y \ \wedge \ \exists\, x \in D \text{ tal que } f(x) = y \\
& \implies y \in f(C) \wedge y \in f(D) \\
& \implies y \in f(C) \cap f(D)
\end{aligned}
$$

b.) Ejercicio

Ejercicios

4.0.1 ▶ Sean $A = \{1,2,3\}$ y $B = \{2,3,4,5,6\}$, y sea $f : A \times A \longrightarrow B$, definida por $f(a,b) = a + b$.

a.) Determine $f[A \times A]$

b.) Determine $f(\{1,2\} \times \{2,3\})$.

c.) Determine $f^{-1}(\{3,4,5\})$.

4.1 Funciones inyectivas, sobreyectivas y biyectivas.

Definición 4.3 (Funciones inyectivas, sobreyectivas y biyectivas)

Consideremos la función $f : A \longrightarrow B$.

a.) f es "inyectiva" si cada imagen es asignada una única preimagen, es decir,

$$\text{si } f(a) = f(b) \implies a = b$$

b.) f es "sobreyectiva" si $f[A] = B$

c.) f es "biyectiva" si f es inyectiva y sobreyectiva.

Definición 4.4

a.) Una función $f : \mathbb{R} \longrightarrow \mathbb{R}$ es una función de variable real. Su *dominio máximo* es el mayor subconjunto posible de $\mathbb{R}$ cuyos valores no indefinen a $f(x)$

b.) Sean $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ funciones con dominios respectivos D_f y D_g. Se define

i. La función suma: $(f+g)(x) = f(x) + g(x)$ y su dominio es $D_f \cap D_g$

ii. La función resta: $(f-g)(x) = f(x) - g(x)$ y su dominio es $D_f \cap D_g$

ii. La función producto: $(fg)(x) = f(x) \cdot g(x)$ y su dominio es $D_f \cap D_g$

iv. La función cociente: $\left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)}$ y su dominio es $D_f \cap D_g - \{x \in D_g : g(x) = 0\}$

Ejemplo 4.6

a.) Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = \frac{x+1}{x^2-1}$. El dominio máximo de f es $D_f = \mathbb{R} - \{-1, 1\}$

b.) Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = \frac{x+1}{\sqrt{x+1}} + \frac{1}{x}$.

El dominio máximo de f requiere $x+1>0$ y $x\neq 0$, es decir, $x>-1$ pero $x\neq 0$. Entonces $D_f =]-1,\infty[-\{0\}$

Ejemplo 4.7

Sea $f:\mathbb{R}^+ \longrightarrow \mathbb{R}^+$ definida por $f(x)=x^2$.

a.) f es inyectiva. En efecto,

$$\begin{aligned} \text{si } f(a)=f(b) &\Longrightarrow a^2=b^2\\ &\Longrightarrow \sqrt{a^2}=\sqrt{b^2}\\ &\Longrightarrow |a|=|b|\\ &\Longrightarrow a=b \text{ pues } a,b\in\mathbb{R}^+\end{aligned}$$

b.) f es sobreyectiva. En efecto, hay que mostrar que $f[\mathbb{R}^+]=\mathbb{R}^+$.

$''\subseteq''$ $f[\mathbb{R}^+]=\{x^2 \text{ tal que } x\in\mathbb{R}^+\}\subseteq\mathbb{R}^+$

$$\begin{aligned} ''\supseteq'' \quad \forall y\in\mathbb{R}^+ &\Longrightarrow \exists\, x=\sqrt{y}\in\mathbb{R}^+(\text{ pues } y\in\mathbb{R}^+) \text{ tal que } x^2=y\\ &\Longrightarrow y\in f[\mathbb{R}^+]\\ &\therefore \quad f[A]\supseteq\mathbb{R}^+.\end{aligned}$$

c.) f es biyectiva

Ejemplo 4.8

Sea $f:\mathbb{R}-\{1\}\longrightarrow\mathbb{R}$, definida por $f(x)=\dfrac{x}{x-1}$.

a.) f es inyectiva. En efecto,

$$\begin{aligned} \text{si } f(a)=f(b) &\Longrightarrow \frac{a}{a-1}=\frac{b}{b-1}\\ &\Longrightarrow a(b-1)=b(a-1)\\ &\Longrightarrow ab-a=ba-b\\ &\Longrightarrow a=b.\end{aligned}$$

b.) ¿f es sobreyectiva?. Mmmmm veamos, hay que analizar si $f\left[\mathbb{R}-\{1\}\right]=\mathbb{R}$.

$''\subseteq''$ Por definición $f\left[\mathbb{R}-\{1\}\right]\subseteq\mathbb{R}$

¿$''\supseteq''$?. Debemos analizar si $\forall y\in\mathbb{R}$, $\exists\, x\in\mathbb{R}-\{1\}$ tal que $f(x)=y$. Veamos

$$
\begin{aligned}
y = f(x) \quad &\Longrightarrow \quad y = \frac{x}{x-1} \\
&\Longrightarrow \quad y(x-1) = x \\
&\Longrightarrow \quad yx - y = x \\
&\Longrightarrow \quad x(y-1) = y \\
&\Longrightarrow \quad x = \frac{y}{y-1}
\end{aligned}
$$

Por tanto, como $y = 1$ no tiene preimagen en el dominio de f. $\therefore$ la función no es sobreyectiva.

c.) Si restringimos el codominio de f así: $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{1\}$, entonces f si sería biyectiva.

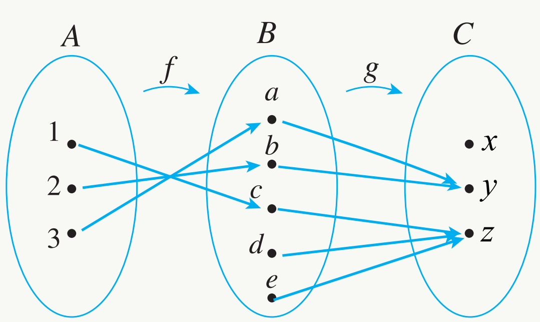
Definición 4.5 (Composición).

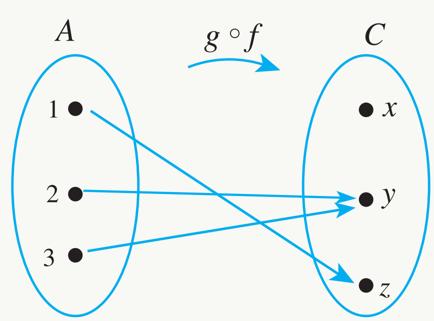
Consideremos dos funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$. La composición de f y g es un función denotada $g \circ f$. La función $g \circ f : A \longrightarrow C$, se define como

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

Ejemplo 4.9

Sea $A = \{1,2,3\}$, $B = \{a,b,c,d\}$ y $C = \{x,y,z\}$. Sean f y g funciones definidas por el diagrama que sigue.





Entonces

$$
\begin{aligned}
(g \circ f)(1) &= g(f(1)) &= g(c) &= z \\
(g \circ f)(2) &= g(f(2)) &= g(b) &= y \\
(g \circ f)(3) &= g(f(3)) &= g(a) &= y
\end{aligned}
$$

Teorema 4.1

a.) Si $h: S \to T$, $g: T \to U$ y $f: U \to V$, entonces $f \circ (g \circ h) = (f \circ g) \circ h$

b.) Si $g: A \to B$ y $f: B \to C$ son ambas inyectivas, entonces $f \circ g: A \to C$ es inyectiva.

c.) Si $g: A \to B$ y $f: B \to C$ son ambas sobreyectivas, entonces $f \circ g: A \to C$ es sobreyectiva.

d.) Si $g: A \to B$ y $f: B \to C$ son ambas biyectivas, entonces $f \circ g: A \to C$ es biyectiva.

Ejemplo 4.10

Sean $f: \mathbb{R} \longrightarrow \mathbb{R}$, $g: \mathbb{R} \longrightarrow \mathbb{R}$ y $g: \mathbb{R}^* \longrightarrow \mathbb{R}$ definidas por $f(x) = \dfrac{x+1}{x^2+4}$, $g(x) = 2x - 4$ y $h(x) = \dfrac{1}{x}$.

a.) $(g \circ f)(x) \; = \; g(f(x)) \; = \; 2(f(x)) - 4 \; = \; 2\left(\dfrac{x+1}{x^2+4}\right) - 4$

b.) $(f \circ g)(x) \; = \; f(g(x)) \; = \; \dfrac{g(x)+1}{[g(x)]^2+4} \; = \; \dfrac{2x-4+1}{(2x-4)^2+4}$

c.) $(f \circ f)(x) \; =$

d.) $(g \circ g)(x) \; =$

e.) $(h \circ g \circ h)(x) \; =$

Ejemplo 4.11

Sea $f, g: \mathbb{R} \longrightarrow \mathbb{R}$ funciones definidas por $f(x) = \begin{cases} x^2 & \text{si} \quad x < -1 \\ 2x & \text{si} \quad -1 \leq x \leq 2 \\ |x-4| - 2 & \text{si} \quad x > 2 \end{cases}$, $g(x) = x + 1$.

a.) $(f \circ f \circ f)(2) \; = \; f(f(f(2)) \; = \; f(f(4)) \; = \; f(-2) \; = \; 4$

b.) $(g \circ f \circ g)(1) \; =$ ____________________

c.) $(g \circ g \circ g)(-1) \; =$ ____________________

Ejemplo 4.12

Sean $A = \{1,2,3,4,5,6\}$ y $B = \{2,3,4,5\}$ y sea $f : A \to B$. Sea $G_f = \{(1,3),\ (2,5),\ (3,4),\ (4,3),\ (5,4),\ (6,3)\}$. Muestre que f no es inyectiva ni sobreyectiva y calcule $f^{-1}(\{4,5\})$, $f^{-1}(\{2\})$ y $f(\{1,5\}) \cap f(\{2,3\})$

Solución:

1) f no es inyectiva pues, por ejemplo, $f(1) = f(4) = 3$ pero $1 \neq 4$.

2) f no es sobreyectiva pues $2 \in B$, pero no tiene preimagen. De esta manera $f[A] \neq B$.

3) $$\begin{cases} f^{-1}(\{4,5\}) & = & \{3,5,2\} \\ f^{-1}(\{2\}) & = & \varnothing \\ f(\{1,5\}) \cap f(\{2,3\}) & = & \{4\} \end{cases}$$

Ejemplo 4.13

Sean A, B, C y D conjuntos no vacíos. Sean $f : A \to B$ y $g : C \to D$. Sea $h : A \times C \to B \times D$, $h(x,y) = (\,f(x),\ g(y)\,)$. Si f y g ambas son biyectivas, muestre que h es biyectiva.

1) **Inyectividad:** **Hipótesis:** f y g ambas son biyectivas

Hqm: Si $h(a,b) = h(p,q)$ entonces $(a,b) = (p,q)$

$$h(a,b) = h(p,q) \implies (f(a),\, g(b)) = (f(p),\, g(q)) \implies \begin{cases} f(a) & = & f(p) \implies a = p \text{ pues } f \text{ es inyectiva} \\ g(b) & = & g(q) \implies b = q \text{ pues } g \text{ es inyectiva} \\ & \therefore & (a,b) = (p,q) \end{cases}$$

2) **Sobreyectividad:** **Hipótesis:** f y g ambas son biyectivas

Hqm: $\forall (p,q) \in B \times D\ \ \exists\, (x,y) \in A \times C$ tal que $h(x,y) = (p,q)$

$$(p,q) \in B \times D \implies \begin{cases} p \in B & \implies & \exists\, x \in A \text{ con } f(x) = p, \text{ pues } f \text{ es sobreyectiva} \\ q \in D & \implies & \exists\, y \in C \text{ con } g(y) = q, \text{ pues } g \text{ es sobreyectiva} \\ & \therefore & \exists\, (x,y) \in A \times C \text{ tal que } h(x,y) = (f(x), g(y)) = (p,q). \end{cases}$$

Ejemplo **4.14**

Sea X un conjunto no vacío y sea $H \subseteq X$. Sea $f : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ definida por el criterio $f(A) = A \cap H$.

a.) Si $X = \{1,2,3\}$, determine H de tal manera que f **no** sea inyectiva

b.) Determine X y H de tal manera que f **no** sea sobreyectiva.

Solución:

a.) Si $X = \{1,2,3\}$ y $H = \{1\}$ entonces $f(\{1\}) = f(\{1,2\}) = \{1\}$, pero $\{1\} \neq \{1,2\}$.

b.) Si $X = \{1,2,3\}$ y $H = \{1\}$ entonces $\forall A \in X,\ f(A) = A \cap \{1\} \neq \{2\}$, es decir, $\{2\}$ no tiene preimagen.

4.2 Función invertible.

Si $f : A \to B$ es biyectiva entonces f^{-1} se puede convertir en una función usando el criterio

$$f^{-1}(y) := f^{-1}(\{y\})$$

En este caso f^{-1} sería "la función inversa" de f y como tal

$$(f^{-1} \circ f)(x) = x \text{ y } (f \circ f^{-1})(y) = y$$

Se requiere que f sea inyectiva para que f^{-1} esté bien definida y se requiere que f sea sobreyectiva porque si existe un $b \in B$ sin preimagen, entonces $f^{-1}(b) = \varnothing$ y entonces $(f \circ f^{-1})(b) \neq b$.

Por ejemplo, $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R}$, definida por $f(x) = \dfrac{x}{x-1}$, no es sobreyectiva, en particular $f^{-1}(1) = \varnothing$

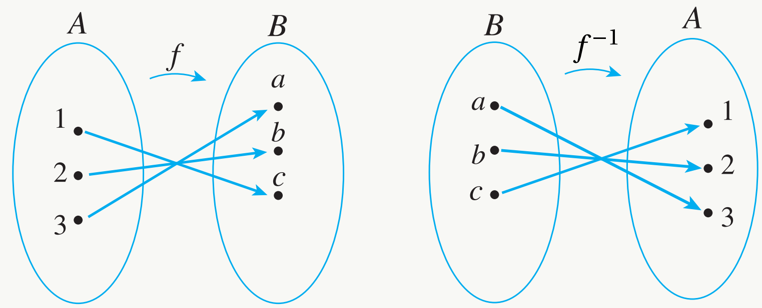
Pero $f : \mathbb{R} - \{1\} \to \mathbb{R} - \{1\}$, con $f(x) = \dfrac{x}{x-1}$ es biyectiva, f es invertible y su inversa es $f^{-1}(x) = \dfrac{x}{x-1}$. En efecto, $(f^{-1} \circ f)(x) = (f \circ f^{-1})(x) = x$.

Teorema 4.2 (Función inversa)

Si la función $f : A \longrightarrow B$ es biyectiva si y solo si f es invertible, es decir, $(f^{-1} \circ f)(x) = x$ y $(f \circ f^{-1})(y) = y$.

Ejemplo **4.15**

Sea $A = \{1,2,3\}$, $B = \{a,b,c\}$. En el diagrama que sigue se muestra una función $f : A \longrightarrow B$ biyectiva, y su inversa.



Ejemplo 4.16

Sea $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{1\}$, definida por $f(x) = \dfrac{x}{x-1}$. f es biyectiva. Calcular f^{-1} y $(f^{-1} \circ f^{-1} \circ f^{-1})(x)$

Solución:

$$\begin{aligned} y = f(x) &\implies y = \frac{x}{x-1} \\ &\implies y(x-1) = x \\ &\implies yx - y = x \\ &\implies x(y-1) = y \\ &\implies x = \frac{y}{y-1.} \quad \therefore\ f^{-1}(x) = \frac{x}{x-1} \end{aligned}$$

$(f^{-1} \circ f^{-1} \circ f^{-1})(x) =$ ____________________

Ejemplo 4.17

Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$, definida por $f(x) = \sqrt[3]{1-x^3}$.

a.) Muestre que f es biyectiva.

b.) Determine $(f^{-1} \circ f^{-1} \circ f^{-1})(x)$

Solución:

a.) **Inyectividad:** Si $f(a) = f(b) \implies \sqrt[3]{1-a^3} = \sqrt[3]{1-b^3} \implies 1-a^3 = 1-b^3 \implies a = b$

Sobreyectiva: Si $y \in \mathbb{R}$ entonces $f(x) = y$ con $x = \sqrt[3]{1-y^3}$. En efecto

$$\begin{aligned} y &= \sqrt[3]{1-x^3} \\ \implies y^3 &= 1-x^3 \\ \implies x^3 &= 1-y^3 \\ \implies x &= \sqrt[3]{1-y^3} \end{aligned}$$

b.) Como $f^{-1}(x) = \sqrt[3]{1-x^3}$, entonces $(f^{-1} \circ f^{-1} \circ f^{-1})(x) = (f^{-1}(f^{-1}(f^{-1}(x))) = \sqrt[3]{1-x^3}$

Ejemplo **4.18**

Sean $f,g: A \longrightarrow A$ funciones biyectivas.

a.) Muestre que $g\circ f$ es inyectiva

b.) Muestre que $g\circ f$ es sobreyectiva

c.) Muestre que $g\circ f$ es invertible y que $(g\circ f)^{-1} = f^{-1}\circ g^{-1}$

Solución:

a.) $g\circ f$ es inyectiva. En efecto,

$$\begin{aligned}
\text{Si } (g\circ f)(x) = (g\circ f)(y) &\Longrightarrow g(f(x)) = g(f(y)) \\
&\Longrightarrow f(x) = f(y), \text{ por ser } g \text{ inyectiva} \\
&\Longrightarrow x = y, \text{ por ser } f \text{ inyectiva.}
\end{aligned}$$

b.) $g\circ f$ es sobreyectiva: Ejercicio

c.) $g\circ f$ es invertible y $(g\circ f)^{-1} = f^{-1}\circ g^{-1}$: En efecto, como $g\circ f$ es biyectiva, es invertible. Recordemos que la función ID es $\mathrm{Id}(x) = x$, entonces $(g^{-1}\circ g)(x) = \mathrm{Id}(x)$

$$\begin{aligned}
(f^{-1}\circ g^{-1})\circ(g\circ f)(x) &= (f^{-1}\circ(g^{-1}\circ g)\circ f)(x), \text{ pues la composición es asociativa} \\
&= (f^{-1}\circ \mathrm{Id}\circ f)(x) \\
&= (f^{-1}\circ f)(x) = x
\end{aligned}$$

Es decir, $(g\circ f)^{-1} = f^{-1}\circ g^{-1}$.

Ejercicios

4.2.1 ▶ Sea $f: \mathbb{R}-\{2\} \longrightarrow \mathbb{R}-\{3\}$, definida por $f(x) = \dfrac{3x+1}{x-2}$.

a.) Probar que f es inyectiva

b.) Probar que f es sobreyectiva

c.) Calcule f^{-1}

4.2.2 ▶ Sea $f: \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = \sqrt{x^2-1}$. Determine su dominio máximo.

4.2.3 ▶ Sea $f: [1,\infty[\longrightarrow]-\infty,2]$ definida por $f(x) = -x^2+2x$. Muestre que f es biyectiva y calcule f^{-1}.

4.2.4 ▶ Sea $f:[-1,\infty[\ \longrightarrow\ [-2,\infty[$ definida por $f(x)=x^2+2x-1$. Muestre que f es biyectiva y determine su inversa.

4.2.5 ▶ Considere los conjuntos $A=\{3,4,5,6\}$ y $B=\{1,2,3\}$. Sea $f:\to A\times B\to[1,2]$, definida por $f((a,b))=\dfrac{a}{b}$.

a.) Calcule $f(6,2)$ y $f(3,1)$

b.) Calcule $f[A\times B]$

c.) Calcule $f(D)$ donde $D=\{(a,b)\in A\times B$ tal que $a+b=6\}$

d.) Calcule $f^{-1}(\{1,2,3\})$

e.) ¿Es f inyectiva? ‘Es f sobreyectiva?

4.2.6 ▶ Si A,B son conjuntos no vaciíos y $f:A\to B$, considere D, $E\subseteq B$ con $D\subseteq E$. Mostrar que $f^{-1}(E)\subseteq f^{-1}(D)$

En los ejercicios que siguen, se asume que $f:A\to B$ y $g:B\to C$ y que f y g están definidas en todo su dominio.

4.2.7 ▶ Muestre que si $g\circ f$ es inyectiva, entonces f es inyectiva

4.2.8 ▶ Muestre que si $g\circ f$ es sobreyectiva, entonces g es sobreyectiva

4.2.9 ▶ Muestre que si $g\circ f$ es sobreyectiva y g es inyectiva, entonces f es sobreyectiva

4.2.10 ▶ Muestre que si $g\circ f$ es inyectiva y f es sobreyectiva, entonces g es inyectiva

Capítulo 5

Inducción Matemática

5.1 Introducción

El principio de *inducción matemática* es un método de demostración, se usa comúnmente para demostrar la veracidad de una proposición $P(n)$ para todos los números naturales. También puede usarse para probar proposiciones sobre cualquier conjunto bien ordenado.

Principio del Buen Orden: Todo conjunto no vacío de números naturales contiene un elemento mínimo.
En particular, si $S \subset \mathbb{Z}$ y si S tiene al menos un elemento positivo, entonces S tiene un entero positivo mínimo.

Principio del palomar: Si k es un entero positivo y $k+1$ o más objetos son asignados a k cajas, entonces hay al menos alguna caja a la que se le asignaron dos o más objetos.

Ejemplo 5.1

En un grupo de 367 personas, debe haber al menos dos que cumplen años el mismo día, porque hay solo 366 posibles días para cumplir años.

Principio de Inducción: Para probar que una proposición $P(n)$ es verdadera para todo entero positivo n, se deben ejecutar los dos pasos siguientes:

1) Verificar que $P(n)$ se cumple para $n = 1$,

2) Probar que si se cumple $P(k)$ (hipótesis de inducción), entonces se cumple $P(k+1)$

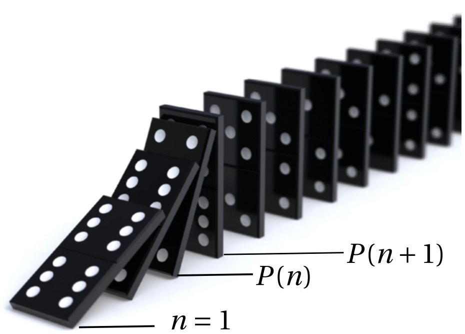


Figura 5.1: Idea de inducción matemática usando un juego de domino.

Se puede probar que el principio de inducción es un método válido de prueba si asumimos el principio del buen orden como un axioma.

Históricamente, el primer ejemplo que se conoce en el que se usó inducción matemática aparece en el libro "Arithmeticorum Libri Duo" de Francesco Maurolico (1494-1575). En este libro, entre otras cosas, Maurolico presenta gran variedad de propiedades de los enteros y las pruebas de estas propiedades. Para las demostraciones, él ideo el método de inducción matemática. La primera vez que se usa el método, es para probar que la suma de los primeros n enteros impares es n^2. El nombre "inducción matemática", lo usó por primera vez el matemático inglés John Wallis.

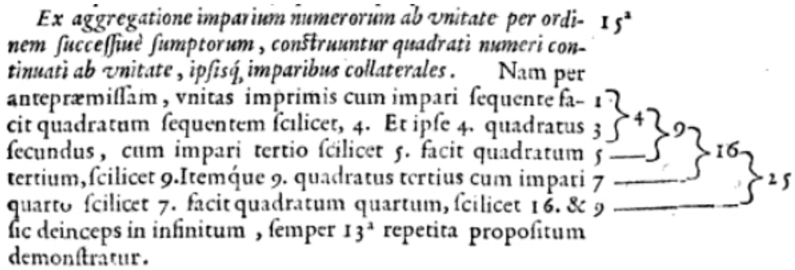

Ex aggregatione imparium numerorum ab vnitate per ordinem ſucceſſiuè ſumptorum, conſtruuntur quadrati numeri continuati ab vnitate, ipſiſq; imparibus collaterales. Nam per antepræmiſſam, vnitas imprimis cum impari ſequente facit quadratum ſequentem ſcilicet, 4. Et ipſe 4. quadratus ſecundus, cum impari tertio ſcilicet 5. facit quadratum tertium, ſcilicet 9. Itemque 9. quadratus tertius cum impari quarto ſcilicet 7. facit quadratum quartum, ſcilicet 16. & ſic deinceps in infinitum, ſemper 13ª repetita propoſitum demonſtratur.

Figura 5.2: Francesco Maurolico. "Arithmeticorum Libri Duo", pág 7. En `www.books.google.com`

Ejemplo 5.2

Probar que $1+3+5+...+(2n-1)=n^2$

Solución: En este caso, n indica el número de sumandos.

a.) La proposición es correcta para $n=1$ pues $1=1^2$

b.) **Hipótesis de inducción:** La proposición es cierta para $n=k$, es decir, $1+3+5+...+2k-1=k^2$.

Hay que mostrar que: La proposición es cierta para $n=k+1$, es decir, $1+3+5+...+2k+1 = (k+1)^2$.

Tomemos la hipotesis de inducción y sumemos el siguiente impar, $2k-1\ +2\ =2k+1$, a ambos lados,

$$\overbrace{1+3+5+...+2k-1}^{k^2}\ +\ 2k+1=k^2+2k+1=(k+1)^2.$$

Por lo tanto, hemos demostrado que si la proposición es correcta para $n=k$, es correcta para $n=k+1$. Entonces, la fórmula es válida para todo $n\in\mathbb{N}^*$, por el principio de inducción.

Ejemplo 5.3

Probar que si $r\neq -1$, entonces $\displaystyle\sum_{k=1}^{n} r^{k-1}=\frac{1-r^n}{1-r}$

Solución: Hay que probar que $1+r^1+r^2+...+r^{n-1}=\dfrac{1-r^n}{1-r}$ para $n\geq 1$.

a.) La proposición es correcta para $n=1$ pues $r^0=\dfrac{1-r^1}{1-r}\ =\ 1$ pues $r-1\neq 0$.

b.) **Hipótesis de inducción:** $1+r^1+r^2+...+r^{n-1} = \dfrac{1-r^n}{1-r}$

Hay que mostrar que: $1+r^1+r^2+...+r^{n} = \dfrac{1-r^{n+1}}{1-r}$

$$\begin{aligned}
1+r^1+r^2+...+r^{n-1} &= \frac{1-r^n}{1-r}, \text{ por hipótesis de inducción.}\\
1+r^1+r^2+...+r^{n-1}+r^n &= \frac{1-r^n}{1-r}+r^n\\
1+r^1+r^2+...+r^{n} &= \frac{1-r^n+(1-r)r^n}{1-r}\\
&= \frac{1-r^{n+1}}{1-r}
\end{aligned}$$

Ejemplo **5.4**

Probar que $2^n \geq 2n$ para todo $n \in \mathbb{N},\ n \geq 2$

Solución:

a.) La proposición es correcta para $n=2$ pues $2^2 \geq 2\cdot 2$.

b.) **Hipótesis de inducción:** $2^n \geq 2n$

Hay que mostrar que: $2^{n+1} \geq 2(n+1)$

$$\begin{aligned}
2^n &\geq 2n, \text{ por hipótesis de inducción.}\\
2^n\cdot 2 &\geq 2n\cdot 2 = 2n+2n\\
2^{n+1} &\geq 2n+2, \text{ pues } 2n\geq 2 \text{ si } n\geq 2.
\end{aligned}$$

Ejemplo **5.5**

Probar que $n^2 \geq 2n$ para todo $n \in \mathbb{N},\ n \geq 2$

Solución:

a.) La proposición es correcta para $n=2$ pues $2^2 \geq 2\cdot 2$.

b.) **Hipótesis de inducción:** $n^2 \geq 2n$

Hay que mostrar que: $(n+1)^2 \geq 2(n+1)$

$$
\begin{aligned}
(n+1)^2 &= n^2+2n+1\\
&\geq 2n+2n+1, \text{ por hipótesis de inducción.}\\
&\geq 2n+2, \text{ pues } 2n+1\geq 2 \text{ si } n\geq 2.
\end{aligned}
$$

Ejemplo 5.6

Probar que $1+\dfrac{1}{2}+\dfrac{1}{3}+\cdots+\dfrac{1}{n} \leq \dfrac{n}{2}+1$ para todo $n\in\mathbb{N},\ n\geq 1$

Solución:

a.) La proposición es correcta para $n=1$ pues $1 \leq \dfrac{1}{2}+1$.

b.) **Hipótesis de inducción:** $1+\dfrac{1}{2}+\dfrac{1}{3}+\cdots+\dfrac{1}{n} \leq \dfrac{n}{2}+1$

Hay que mostrar que: $1+\dfrac{1}{2}+\dfrac{1}{3}+\cdots+\dfrac{1}{n}+\dfrac{1}{n+1} \leq \dfrac{n+1}{2}+1$

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}+\frac{1}{n+1} \leq \frac{n}{2}+1+\frac{1}{n+1}, \text{ por hipótesis de inducción.}$$

$$\text{Como } n\geq 1 \implies \frac{1}{n+1}\leq\frac{1}{2}, \quad \therefore \quad \frac{n}{2}+1+\frac{1}{n+1} \leq \frac{n}{2}+1+\frac{1}{2}$$

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n+1} \leq \frac{n}{2}+1+\frac{1}{2} = \frac{n+1}{2}+1$$

Ejemplo 5.7

Verifique que $7^{2n}+16n-1$ es divisible por 64 para todo $n\geq 2$.

Solución:

a.) La proposición es correcta para $n=2$ pues $7^{2\cdot 2}+16\cdot 2-1 = 64\cdot 38 = 2432$

b.) **Hipótesis de inducción:** $7^{2n}+16n-1=64k$ para algún $k\in\mathbb{Z}$

Hay que mostrar que: $7^{2(n+1)}+16(n+1)-1=64k_1$ para algún $k_1\in\mathbb{Z}$

$$
\begin{aligned}
7^{2(n+1)}+16(n+1)-1 &= 7^{2n+2}+16n+16-1\\
&= 7^2\cdot 7^{2n}+16n+16-1\\
&= 7^2\cdot(64k-16n+1)+16n+16-1, \text{ por hipótesis de inducción.}\\
&= 64k\cdot 7^2 - 64\cdot 12\cdot n+64 = 64k_1
\end{aligned}
$$

Ejemplo 5.8

Verifique que $\forall n \in \mathbb{N}^* : 4^{2n} + 4 = 20k$ para algún $k \in \mathbb{Z}$.

Solución:

a.) La proposición es correcta para $n = 1$ pues $4^2 + 4 = 20 \cdot 1$

b.) **Hipótesis de inducción:** $4^{2n} + 4 = 20k$ para algún $k \in \mathbb{Z}$

Hay que mostrar que: $4^{2(n+1)} + 4 = 20k_1$ para algún $k_1 \in \mathbb{Z}$

$$\begin{aligned} 4^{2(n+1)} + 4 &= 4^2 4^n + 4 \quad \text{Complete el razonamiento!} \\ &= \ldots \\ &= \ldots \\ &= 20k_1 \end{aligned}$$

Ejemplo 5.9

Utilice la fórmula $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + (n-1)(n+1) = \dfrac{n(n-1)(2n+5)}{6}$ para calcular el valor exacto de la suma

$$S = 121 \cdot 123 + 122 \cdot 124 + 123 \cdot 123 + \cdots + 35343$$

Solución: Resolvemos $35343 = (n-1)(n+1) \implies n = 188$. Ahora aplicamos la fórmula con $n = 121$ y $n = 188$,

$$\begin{aligned} 1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + 120 \cdot 122 + 121 \cdot 123 + 122 \cdot 124 + 123 \cdot 123 + \cdots + 187 \cdot 189 &= \frac{188(188-1)(2 \cdot 188 + 5)}{6} \\ \frac{121(121-1)(2 \cdot 121 + 5)}{6} + 121 \cdot 123 + 122 \cdot 124 + 123 \cdot 123 + \cdots + 187 \cdot 189 &= 2232406 \\ 597740 + 121 \cdot 123 + 122 \cdot 124 + 123 \cdot 123 + \cdots + 187 \cdot 189 &= 2232406 \\ 121 \cdot 123 + 122 \cdot 124 + 123 \cdot 123 + \cdots + 187 \cdot 189 &= 1634666 \end{aligned}$$

Ejercicios

5.1.1 ▶ Probar que $2^n < n!$ para todo natural $n \geq 4$

5.1.2 ▶ Probar que $n^2 + 3n + 1 < 2(3^n) \ \forall\, n \geq 4$

5.1.3 ▶ Probar que $n^3 < 3^n \ \forall\, n \geq 4$

5.1.4 ▶ Probar que 31 divide a $5^{n+1} + 6^{2n-1} \ \forall\, n \in \mathbb{N}^*$

5.1.5 ▶ Probar que 3 divide a $12^n - 7^n - 4^n - 1, \ \forall\, n \in \mathbb{N}^*$

Principio de Inducción Completa: Para probar que una proposición $P(n)$ es verdadera para todo entero positivo n, se deben ejecutar los dos pasos siguientes:

a.) Verificar que $P(n)$ se cumple para $n=1$,

b.) Probar que si se cumple $P(1) \wedge P(2) \wedge \ldots \wedge P(k)$ (hipótesis de inducción), entonces se cumple $P(k+1)$

Se puede probar que el principio de inducción completa es equivalente al principio de inducción. Es decir, cada principio puede ser demostrado asumiendo el otro. La ganancia es que el principio de inducción completa es más flexible. A el principio de inducción completa también se le llama "principio de inducción fuerte" o "segundo principio de inducción".

Capítulo 6

Relaciones de recurrencia

6.1 Introducción

Sucesiones. Consideremos la sucesión $1,\ 0, 1,\ 0, 1,\ 0, \ldots$. Si denotamos con $a_0 = 1,\ a_1 = 0,\ a_2 = 1, etc.$ entonces se podría deducir que

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

a_n es el término general de la sucesión.

Sucesiones definidas por recurrencia. Algunas sucesiones están definidas por una relación de recurrencia, por ejemplo

$$a_n = a_{n-1} + na_{n-2} + 1,\ \text{ con } \ a_0 = 1 \ \text{ y } \ a_1 = 2$$

Entonces

$a_2 = a_1 + 2 \cdot a_0 + 1 = 5$

$a_3 = a_2 + 3 \cdot a_1 + 1 = 12$

En algunos casos podemos, dada una relación de recurrencia, deducir una fórmua para el término general a_n.

Ejemplo 6.1

La sucesión (aritmética) definida por $a_k = a_{k-1} + d,\ \forall k \geq 1$ y $a_0 = a$, tiene término general $a_n = a + n \cdot d\ \ \forall n \geq 0$

Ejemplo 6.2

La sucesión (geométrica) definida por $a_k = r \cdot a_{k-1},\ \forall k \geq 1$ y $a_0 = a$, tiene término general $a_n = a \cdot r^n\ \ \forall n \geq 0$

Sucesiones de recurrencia homogéneas de orden dos, con coeficientes constantes. Son relaciones del tipo

$$a_n = Aa_{n-1} + Ba_{n-2} \quad \forall n \geq N \ \text{ con constantes } \ A, B \neq 0$$

Ecuación característica. Si para algún $t \neq 0$ se tiene que $a_n = t^n$ es solución de la relación $a_n = Aa_{n-1} + Ba_{n-2}$, entonces

$$t^n \quad = \quad At^{n-1} + Bt^{n-2} \ \forall n \geq 2$$

Si $n = 2$, tenemos $t^2 = At + B$ o también $t^2 - At + B = 0$. Esta es la llamada "ecuación característica" de la relación $a_n = Aa_{n-1} + Ba_{n-2}$.

Teorema 6.1

Consideremos una relación de recurrencia de la forma $a_n = Aa_{n-1} + Ba_{n-2}$ con A, B constantes y $B \neq 0$. Ahora consideremos su ecuación característica $t^2 - At + B = 0$.

a.) Si la ecuación característica tiene dos raíces reales distintas r_1 y r_2, entonces

$$a_n = C \cdot r_1^n + D \cdot r_2^n$$

donde los números C y D se determinan con las condiciones iniciales de la relación

b.) Si la ecuación característica tiene solo una raíz real r_1 entonces

$$a_n = C \cdot r_1^n + D \cdot n \cdot r_1^n$$

donde los números C y D se determinan con las condiciones iniciales de la relación

Y en general,

Teorema 6.2

Una relación de recurrencia de la forma $a_n = A_1 a_{n-1} + A_2 a_{n-2} + ... + A_{n-k} a_{n-k}$ con las A_i constantes y $A_{n-k} \neq 0$, tiene ecuación característica a $t^k - A_1 t^{k-1} - \ ... \ - A_{n-k} = 0$.

a.) Si la ecuación característica tiene k raíces distintas $r_1, ..., r_k$ entonces

$$a_n = C_1 \cdot r_1^n + C_2 \cdot r_2^n + ... + C_k \cdot r_k^n$$

Los números C_i se determinan con las condiciones iniciales de la relación.

b.) Si la ecuación característica una raíz r de multiplicidad $m + 1$ entonces en vez de agregar el sumando $B_0 r^n$ a la solucion general, agregamos el sumando $B_0 r^n + B_1 n r^n + B_3 n^2 r^n + ... + B_m n^m r^n$. Los números B_i se determinan con las condiciones iniciales de la relación

Ejemplo 6.3

Resolver $a_n = 5a_{n-1} - 6a_{n-2}$ con condiciones iniciales $a_0 = 1, \ a_1 = 4$.

Solución:

Ecuación característica: $t^2 - 5t + 6 = 0 \implies t = 2$ y $t = 3$.

Solución general: $a_n = C \cdot 2^n + D \cdot 3^n$

Aplicamos condiciones iniciales:

$$\begin{cases} a_0 &= C\cdot 2^0 + D\cdot 3^0 = C + D = 1 \\ a_1 &= C\cdot 2^1 + D\cdot 3^1 = 2C + 3D = 1 \end{cases} \implies C = -1 \wedge D = 2.$$

$\therefore\ a_n = -1\cdot 2^n + 2\cdot 3^n$

Ejemplo 6.4

Considere la relación a_n definida por recurrencia por $a_n = a_{n-1} + a_{n-2} - a_{n-3}$ si $n \geq 4$, con $a_1 = 6$, $a_2 = 1$ y $a_3 = 12$

a.) Determine a_5 con esta fórmula

b.) Determine una fórmula explícita para a_n y utilice esta fórmula para calcular a_5

Solución:

a.) $a_4 = a_3 + a_2 - a_1 = 7$ y $a_5 = a_4 + a_3 - a_2 = 18$

b.) Fórmula explícita para a_n

Ecuación característica: $t^3 - t^2 - t + 1 = (t-1)^2(t+1)$

Solución general: $a_n = A_1(1)^n + A_2 n(1)^n + A_3(-1)^n$

Aplicando condiciones iniciales: $\begin{cases} A_1 + A_2 - A_3 &= 6 \\ A_1 + 2A_2 + A_3 &= 1 \\ A_1 + 3A_2 - A_3 &= 12 \end{cases} \implies A_1 = -1,\ A_2 = 3,\ A_3 = -4.$

$\therefore\ a_n = -1 + 3n - 4(-1)^n$ y $a_5 = 18.$

Ejemplo 6.5

Si $a_n = (1+2n)2^n + n(-2)^n$ para $n \geq 4$, determine una relación de recurrencia para esta relación.

Solución: Las condiciones iniciales se obtiene evaluando en la relación: Serían $a_0 = 1$, $a_1 = 4$, $a_2 = 28$ y $a_3 = 32$.

La relación es $a_n = 1\cdot 2^n + 2n\cdot 2^n + n(-2)^n$. Por la forma de esta relación, la ecuación característica tendría dos raíces, $t = 2$ y $t = -2$, ambas de multiplicidad dos. Es decir, la ecuación característica es $(t-2)^2(t+2)^2 = t^4 - 8t^2 + 16 = 0$ y

$$a_n = 1\cdot 2^n + 2n\cdot 2^n + 0\cdot(-2)^n + n(-2)^n$$

La relación de recurrencia es $a_n = 8a_{n-2} - 16a_{n-4}$ para $n \geq 4$ y las condiciones iniciales $a_0 = 1$, $a_1 = 4$, $a_2 = 28$ y $a_3 = 32$.

Ejemplo 6.6

Resolver $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ con condiciones iniciales $a_0 = 1,\ a_1 = -2$ y $a_2 = -1$.

Solución:

Ecuación característica: $t^3 - 3t^2 + 3t + 1 = (t+1)^3 = 0 \implies t = -1$ (de multiplicidad 3)

Solución general: $a_n = B_0(-1)^n + B_1 n(-1)^n + B_2 n^2(-1)^n$

Aplicando condiciones iniciales: $a_n = (1 + 3n - 2n^2)(-1)^n$

Ejemplo 6.7

Resolver $a_n = 6a_{n-1} - 9a_{n-2}$ con condiciones iniciales $a_0 = 4,\ a_1 = 6$.

Solución:

Ecuación característica: $t^2 - 6t + 9 = 0 \implies t = 3$

Solución general: $a_n = C \cdot 3^n + D \cdot n \cdot 3^n$

Aplicando condiciones iniciales: $a_n = 4 \cdot 3^n - 2 \cdot n \cdot 3^n$

Ejemplo 6.8 (Fibonacci)

Resolver $a_n = a_{n-1} + a_{n-2}$ con condiciones iniciales $a_0 = 0,\ a_1 = 1$.

Solución:

Ecuación característica: $t^2 - t - 1 = 0 \implies t = ...$ y $t = ...$

Solución general: $a_n = ...$

Aplicando condiciones iniciales: $a_n = ...$

Ejemplo 6.9

Resolver $a_n = 2a_{n-1} + 12a_{n-2} - 40a_{n-3} + 32a_{n-4}$ con condiciones iniciales $a_0 = 1,\ a_1 = -2$ y $a_2 = -1$ y $a_3 = 0$

Solución:

Ecuación característica: $-32+40t-12t^2-2t^3+t^4=(t-2)^3(t+4)=0 \implies t=2$ y $t=-4$

Solución general: $a_n=C_1(-4)^n+C_2 2^n+C_3 n 2^n+C_4 n^2 2^n$

Aplicando condiciones iniciales: $a_n=\ldots$

Ejercicios

6.1.1 ▶ Resolver la relación de recurrencia $a_n=6a_{n-1}+7a_{n-2}$ donde $a_0=344$ y $a_1=2400$.

6.1.2 ▶ Resolver la relación de recurrencia $a_n=2a_{n-1}+5a_{n-2}-6a_{n-3}$ donde $a_0=1, a_1=2, a_2=1$.

6.1.3 ▶ Si $a_n=2(-4)^n+2^{n+1}-n2^n+n^2 2^n$, determine una relación de recurrencia para esta relación

6.1.4 ▶ Resolver la relación de recurrencia $a_n=11a_{n-1}-39a_{n-2}+45a_{n-3}$ donde $a_0=5, a_1=11, a_=25$

Capítulo 7

Estructuras algebraicas

Podemos ver las propiedades de la suma de enteros (asociatividad, existencia de neutro e inversos) no como propiedades que tengan que ver con los enteros propiamente sino que como un reflejo de su *estructura algebraica.*

Las propiedades de una operación definida sobre un conjunto es lo que define la *estructura algebraica del conjunto bajo esta operación.*

La estructura algebraica más importante es la estructura de *grupo.* Un grupo es un conjunto en el que se ha definido una regla de composición interna (una operación) que, esencialmente tiene las mismas propiedades algebraicas que la suma en los enteros (cerradura, asociatividad, existencia de neutro e inversos).

7.1 Ley de composición interna

Definición 7.1

Sea $A \neq \varnothing$. Una ley de composición interna es una función $\circledast : A \times A \longrightarrow A$. La función $\circledast$ es una operación binaria y escribimos $\circledast(a,b) = a \circledast b$. La operación es cerrada, es decir, $\forall\, a,b \in A,\ a \circledast b \in A$.

Ejemplo 7.1

a.) En $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$ las operaciones $+$ y $\cdot$ son leyes de composición interna.

b.) La operación $a \circledast b = b - a$ no es cerrada en $\mathbb{N}$. Por ejemplo, $5 \circledast 4 = 4 - 5 = -1 \notin \mathbb{N}$

c.) La operación $a \circledast b = \dfrac{a+b}{2}$ es cerrada en $\mathbb{Q}$.

d.) La operación $(a,b) \circledast (p,q) = \left(ap, \dfrac{1}{bq}\right)$ es cerrada en $\mathbb{Q} \times \mathbb{Q}^*$.

Ejemplo 7.2

Si A es finito, a veces una operación se define sobre A usando una tabla para operar (como las tablas de multiplicar).

Sea $A = \{i, a, b, c\}$ y una operación $*$ sobre A es definida por la tabla

$*$	i	a	b	c
i	i	a	b	c
a	a	c	i	b
b	b	i	c	a
c	c	b	a	i

Como se observa, $i * i = i$, $a * a = c$, $a * c = b$, etc. La operación es cerrada.

Definición 7.2 (Propiedades de las operaciones binarias)

Sea $\circledast$ una operación sobre G. A la dupla $(G, \circledast)$ le llamamos una estructura algebraica.

a.) La operación es **cerrada** si $a \circledast b \in G$, para todo $a, b \in G$

b.) La operación es **asociativa** si $a \circledast (b \circledast c) = (a \circledast b) \circledast c$, para todo $a, b, c \in G$

c.) Elemento **neutro:** Si existe $e \in G$ tal que $a \circledast e = e \circledast a = a$, para todo $a \in G$, a e se le llana *neutro.*

d.) **Inversos:** Si para $a \in G$ existe $b \in G$ tal que $a \circledast b = b \circledast a = e$, entonces b es inverso de a y se escribe $b = a^{-1}$.

e.) La operación es **conmutativa** si $a \circledast b = b \circledast a$ para todo $a, b \in G$

Otras definiciones. Consideremos la estructura algebraica $(G, \circledast)$

a.) $a \in G$ es *idempotente* si $a \circledast a = a$

b.) Si la operación $\circledast$ admite un neutro en G, se dice que $a \in G$ es *involutivo* si $a \circledast a = e$

c.) $a \in G$ es *absorbente* en G si $a \circledast x = x \circledast a = a, \quad \forall\, x \in G$

Ejemplo 7.3

a.) La operación $a \circledast b = \dfrac{a+b}{2}$, ¿es asociativa en $\mathbb{Q}$?.

Solución: Hay que verificar si se cumple o no se cumple la condición de asociatividad.

$$a \circledast (b \circledast c) = a \circledast \frac{b+c}{2} = \frac{a + \dfrac{b+c}{2}}{2} = \frac{2a+b+c}{4}$$

$$(a \circledast b) \circledast c = \frac{a+b}{2} \circledast c = \frac{\frac{a+b}{2}+c}{2} = \frac{a+b+2c}{4}$$

Así que si $a \neq c$ entonces $a \circledast (b \circledast c) \neq (a \circledast b) \circledast c$. La operación no es asociativa.

b.) Sobre $\mathbb{R}$ se define la operación $a \circledast b = a + b + ab$. ¿Existe un elemento neutro?

Solución: Si un neutro $e \in \mathbb{R}$ existe, debería cumplir $e \circledast a = a \circledast e = a$. Veamos

$e \circledast a = e + a + ea = a \implies e(1+a) = 0$. $\therefore$ $\forall a \in \mathbb{R}$, $e \circledast a = a$ si $e = 0$.

$a \circledast 0 = 0 + a + 0 \cdot a = a$

$\therefore$ $e = 0$ es el elemento neutro en la estructura algebraica $(\mathbb{R}, \circledast)$.

7.2 Grupos

Definición 7.3

La estructura algebraica $(G, *)$ es un grupo si

1) $*$ es cerrada en G

2) $*$ es asociativa en G

3) Existe $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$. Al elemento e se le llama "elemento neutro" de G respecto a $*$ y se demuestra, más adelante, que es único.

4) Para todo $a \in G$ existe un inverso, $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$, donde e es *el* elemento neutro.

Si $*$ es conmutativa, $(G, *)$ se dice "grupo abeliano"

Teorema 7.1

Si $(G, *)$ es un grupo, entonces

a.) El neutro e es único

b.) El inverso a^{-1} de $a \in G$ es único

c.) Si $ab = a \implies b = e$ y si $a^2 = a * a = a \implies a = e$.

d.) $(a^{-1})^{-1} = a$

e.) $(ab)^{-1} = b^{-1}a^{-1}$

Demostración:

a.) El neutro e es único pues si hubiera otro neutro $e' \in G$, entonces $e * e' = e = e' * e = e'$. $\therefore\ e = e'$

La demostración de las otras afirmaciones queda como ejercicio.

Potencias. Cuado el grupo es “multiplicativo”, entonces la notación a^n se usa para las potencias usuales, es decir,

$$a^n = \underbrace{a * a * \cdots a}_{n \text{ veces}}$$

En particular, $a^{-n} = (a^n)^{-1}$

Ejemplo 7.4

Sobre $\mathbb{R}^*$ se define la operación $a * b = 2ab$. Verifique que $(\mathbb{R}^*, *)$ es un grupo conmutativo.

Solución:

a.) **Cerradura:** $a * b = 2ab \in \mathbb{R}^*$ pues $a, b \neq 0$.

b.) **Asociatividad:** $\left\{\begin{array}{lclcl} a * (b * c) & = & a * 2bc & = & 4abc \\ (a * b) * c & = & 2ab * c & = & 4abc \end{array}\right. \checkmark$

c.) **Neutro:** $\left\{\begin{array}{lcl} a * e & = & a \Longrightarrow a = 2ae \Longrightarrow e = \dfrac{1}{2}. \\ \dfrac{1}{2} * a & = & a \end{array}\right.$

d.) **Inversos:** $\left\{\begin{array}{lcl} a * a' & = & 2aa' = \dfrac{1}{2} \Longrightarrow a' = \dfrac{1}{4a} \text{ pues } a \neq 0. \\ \\ \dfrac{1}{4a} * a & = & 2\dfrac{1}{4a}a = \dfrac{1}{2}.\quad \therefore\ \forall a \in \mathbb{R}^*,\ a^{-1} = \dfrac{1}{4a}. \end{array}\right. \checkmark$

e.) El grupo $(G, *)$ es conmutativo pues $a * b = b * a = 2ab$.

Ejemplo 7.5

Sea $G = \{(a,b) \in \mathbb{R} \times \mathbb{R} \text{ tal que } a \neq 0\}$ y $(a,b) * (c,d) = (ac, ad + b)$. Verifique que $(G, *)$ es un grupo no conmutativo.

Solución:

a.) **Cerradura:** $(a,b) * (c,d) = (ac, ad + b) \in G$ pues $ac \neq 0$.

b.) **Asociatividad:** $\left\{\begin{array}{lcl} (a,b) * ((c,d) * (p,q)) & = & (acp,\ acq + ad + b) \\ ((a,b) * (c,d)) * (p,q) & = & (acp,\ acq + ad + b) \end{array}\right. \checkmark$

c.) **Neutro:** $\begin{cases} (a,b)*(e_1,e_2) &= (a,b) \implies (a\cdot e_1,\, a\cdot e_2+b) = (a,b) \implies (e_1,e_2)=(1,0) \\ (e_1,e_2)*(a,b) &= (1,0)*(a,b) = (a,b) \end{cases}$

d.) **Inversos:** $\begin{cases} (a,b)*(a',b') &= (1,0) \implies (a',b') = \left(\dfrac{1}{a},-\dfrac{b}{a}\right) \text{ pues } a,b\neq 0. \\ & \checkmark \\ \left(\dfrac{1}{a},-\dfrac{b}{a}\right)*(a,b) &= (1,0). \quad \therefore\ \forall (a,b)\in G,\ (a,b)^{-1} = \left(\dfrac{1}{a},-\dfrac{b}{a}\right). \end{cases}$

e.) El grupo $(G,*)$ no es conmutativo pues $(a,b)*(c,d)=(ac,ad+b)$ pero $(c,d)*(a,b)=(ac,bc+d)$

Ejemplo 7.6

Sea $A=\{i,a,b,c\}$ y una operación $*$ sobre A es definida por la tabla que sigue. Verifique que $(A,*)$ es un grupo conmutativo y calcule $(a*b^3)^{-2}*c^3$

*	i	a	b	c
i	i	a	b	c
a	a	c	i	b
b	b	i	c	a
c	c	b	a	i

Solución:

a.) **Cerradura:** En la tabla se observa que la operación solo da como resultados elementos de A.

b.) **Asociatividad:** Se requiere verificar las 4^3 ID es $a_i*(a_j*a_k)=(a_i*a_j)*a_k$.

Hay una algoritmo para hacer esto, llamado "Light's associativity test" ([7, pp. 7]). El algoritmo compara las tablas de las operaciones "$\circ$" y "$\odot$" definidas por $x\circ y = x*(a*y)$ y $x\odot y=(x*a)*y$, para todos los $a\in A$. Si coinciden, la operación es asociativa. Sin embargo no hay que hacer todas las tablas, porque se pueden ver usando las filas $x*a$ y las columnas $a*y$ y hay simplificaciones adicionales usando propiedades de semigrupos.

c.) **Neutro:** Debemos buscar en la tabla una fila y la respectiva columna donde se hay una copia de $i\ a\ b\ c$

*	i	a	b	c
i	i	a	b	c
a	a	c	i	b
b	b	i	c	a
c	c	b	a	i

Por tanto $e = i$ es el elemento neutro.

d.) **Inversos:** Para obtener los inversos, debemos buscar el neutro en la tabla

$*$	i	a	b	c
i	i	a	b	c
a	a	c	i	b
b	b	i	c	a
c	c	b	a	i

De esta manera obtenemos que $i^{-1} = i,\ a^{-1} = b,\ b^{-1} = a$ y $c^{-1} = c$

e.) La conmutatividad se sigue de la simetría de la tabla respecto a a la diagonal

f.) Observemos que $c^2 = i \implies c^{2k} = (i)^{2k} = i,\ c^{2k+1} = c^{2k} * c = c$ y $c^{-1} = c$. Ahora,

$$(a * b^3)^{-50} * c^3 = (a * a)^{-50} * c^3 = (c)^{-50} * c^3 = i * c = c.$$

Ejemplo 7.7

Verifique que $\mathbb{R} - \{-1\}$ con la operación $a \circledast b = a + b + ab$, es un grupo abeliano.

Solución:

a.) **Cerradura:** Si $a, b \in \mathbb{R} - \{-1\}$ es claro que $a \circledast b = a + b + ab \in \mathbb{R}$. Solo falta probar que $a \circledast b = a + b + ab \in \mathbb{R} - \{-1\}$, es decir, $a + b + ab \neq -1$. Para probar esto, observe que

$a + b + ab = -1 \iff a + b + ab + 1 = 0 \iff (a + 1)(b + 1) = 0$, lo cual es imposible, pues $a, b \in \mathbb{R} - \{-1\}$.

b.) **Asociatividad:** $\begin{cases} (a \circledast b) \circledast c = (a + b + ab) \circledast c = a + b + ab + c + (a + b + ab)c \\ a \circledast (b \circledast c) = a \circledast (b + c + bc) = a + b + c + bc + a(b + c + bc) \end{cases}$

Desarrollando se verifica que las os expresiones son iguales.

c.) **Conmutatividad:** $a \circledast b = a + b + ab = b + a + ba = b \circledast a$ pues la suma y el producto son conmutativas en $\mathbb{R}$.

d.) **Neutro:** Por el ítem anterior, solo necesitamos resolver la ecuación $a \circledast e = a$.

$a \circledast e = a \iff a + e + ae = a \iff e(a + 1) = 0 \iff e = 0$ pues $a \in \mathbb{R} - \{-1\}$.

e.) **Inversos:** Por el ítem anterior, solo necesitamos resolver la ecuación $a \circledast \overline{a} = e = 0$.

$a \circledast \overline{a} = 0 \iff a + \overline{a} + a\overline{a} = 0 \iff \overline{a}(1+a) = -a \implies \overline{a} = -\dfrac{a}{1+a} \in \mathbb{R} - \{-1\}$ pues $-\dfrac{a}{1+a} \neq -1$.
Como $a \neq -1$, todos los elementos de $\mathbb{R} - \{-1\}$ tienen inverso.

Ejemplo 7.8

En $\mathbb{R} \times \mathbb{R}^*$ se define la operación $*$ como

$$(a,b) * (c,d) = (a + c + 3, 2bd)$$

Si se sabe que $(\mathbb{R} \times \mathbb{R}^*, *)$ es un grupo abeliano, calcule

$$(-4,1)^3 * \left[\left(1, \frac{4}{3}\right) * (2,-3)^{-2}\right]^2$$

Solución:

$(-4,1)^3 = (-4,1) * (-4,1) * (-4,1) = (-4 + -4 + 3,\ 2 \cdot 1 \cdot 1) * (-4,1) = (-5,\ 2) * (-4,1) = (-6,\ 4)$.

Para calcular $(2,-3)^{-2}$ requerimos calcular el neutro (e_1, e_2) para poder calcular inversos.

a.) **Neutro:** $(a,b) * (e_1,e_2) = (a,b) \implies (e_1,e_2) = \left(-3,\ \dfrac{1}{2}\right)$

b.) **Inversos:** $(a,b) * (a',b') = \left(-3,\ \dfrac{1}{2}\right) \implies (a',b') = (a,b)^{-1} = \left(-6 - a,\ \dfrac{1}{4b}\right)$ pues $b \in \mathbb{R}^*$

c.) $(-4,1)^3 * \left[\left(1, \dfrac{4}{3}\right) * (2,-3)^{-2}\right]^2 = (-6,4) * \left[\left(1, \dfrac{4}{3}\right) * \left(-13, \dfrac{1}{72}\right)\right]^2 = (-6,4) * \left(-9, \dfrac{1}{27}\right)^2 = \left(-18, \dfrac{16}{729}\right)$

7.2.1 Los grupos $(\mathbb{Z}_m, +)$ y $(\mathbb{Z}_m^*, \cdot)$

Recordemos que sobre $\mathbb{Z}$, si $m > 1$, la relación "$a \equiv_m b$" (a es congruente con "b" módulo m), es una relación de equivalencia. Dos enteros están relacionados si dejan el mismo residuo positivo al dividir por m.

El "Algoritmo de Euclides", establece que si $n, m \in \mathbb{Z}$ con $m > 1$, entonces existe un "residuo"[1] $r \in \mathbb{N}$ tal que $n = qm + r$ con $0 \leq r < m$. El "Algoritmo de Euclides" dice que al dividir n por m, solo hay $m-1$ posibles residuos no negativos, a saber: $\{0, 1, 2, ..., m-1.\}$

Por ejemplo, en el contexto del algoritmo de Euclides,

a.) Al dividir por n por $m = 2$ solo se puede tener a $r = 0$ como residuo (si n es par) o $r = 1$ (si n es impar).

[1]En este caso usamos un sistema de residuos ≥ 0 (en otros contextos, otro tipo de residuos puede ser mejor).

b.) Al dividir por n por $m=3$ solo se puede tener a $r=0$ como residuo (si $n=3k$), $r=1$ (si $n=3k+1$) o $r=2$ (si $n=3k+2$).

Observemos que $a\equiv_m b$ si y solo si a y b dejan el mismo residuo, al divirlos por m. En efecto, si $a=mk_1+r$ y $b=mk_2+r$ entonces $b-a=m\cdot(k_2-k_1)$. Además, usando el criterio de la relación,

Un entero es congruente con el residuo que deja al dividir por m : $a\equiv_m r$

En conclusión, si $a=mk+r$ con $0\leq r<a$, entonces $a\in\overline{r}$. Por ejemplo,

a.) Si $m=2$, entonces los pares están en la clase $\overline{0}$ y los impares en la clase $\overline{1}$

b.) Si $m=7$, entonces $9\equiv_7 2$ pues $9=7\cdot 1+2$. y $11\equiv_7 4$ pues $11=7\cdot 1+4$.

El conjunto cociente de la relación $\equiv_m$ son los residuos, es decir, $\mathbb{Z}/\equiv_m=\{\overline{0},\overline{1},\overline{2},...,\overline{m-1}.\}$

Se acostumbra escribir $\mathbb{Z}_m$ en vez de $\mathbb{Z}/\equiv_m$. Es decir,

$$\mathbb{Z}_m=\{\overline{0},\overline{1},\overline{2},...,\overline{m-1}\}\ \text{ o simplemente }\ \mathbb{Z}_m=\{0,1,2,...,m-1\}$$

Adición y multiplicación en $\mathbb{Z}_m$

a.) La adición en $\mathbb{Z}_m$ es $\overline{a}+\overline{b}=\overline{a+b}$.

Por ejemplo en $\mathbb{Z}_5=\{\overline{0},\overline{1},\overline{2},\overline{4}\}$,

- $\overline{2}+\overline{3}=\overline{0}$ pues $5\equiv_5 0$
- $\overline{4}+\overline{2}=\overline{1}$ pues $6\equiv_5 1$
- $\overline{1}+\overline{2}=\overline{3}$ pues $3\equiv_5 3$

  La tabla de sumar completa sería

$(\mathbb{Z}_5,+)$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

b.) La multiplicación en $\mathbb{Z}_m$ es $\overline{a}\cdot\overline{b}=\overline{a\cdot b}$.

Por ejemplo en $\mathbb{Z}_7^*=\{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\}$,

- $\overline{2}\cdot\overline{3}=\overline{6}$ pues $6\equiv_7 6$
- $\overline{4}\cdot\overline{2}=\overline{1}$ pues $8\equiv_7 1$
- $\overline{4}\cdot\overline{3}=\overline{5}$ pues $12\equiv_7 5$

  La tabla de multilicar completa sería

$(\mathbb{Z}_7^*,\cdot)$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Orden de un grupo. El orden de un grupo finito $(G,*)$ es $\mathrm{ord}(G)=|G|$, es decir, su cardinalidad.

Teorema 7.2

Sea $m \in \mathbb{N},\ m > 1.$

a.) $(\mathbb{Z}_m, +)$ es un grupo "aditivo" de orden m

b.) $(\mathbb{Z}_m^*, \cdot)$ es un grupo "multiplicativo" de orden $m-1$

En $(\mathbb{Z}_m, +)$ el neutro es $\overline{0}$ y en $(\mathbb{Z}_m^*, \cdot)$ el neutro es $\overline{1}$.

Ejercicios

7.2.1 ▶ En $\mathbb{N}$ se define la operación $a \vee b = \text{mín}\{a, b\}$. ¿Es $(\mathbb{N}, \vee)$ un grupo?

7.2.2 ▶ Sea $A \neq \varnothing$. En el conjunto de partes $\mathcal{P}(A)$ se define la operación $A \,\Delta\, B = (A \bigcup B) - (A \bigcap B)$ ¿Es $(\mathcal{P}(A), \Delta)$ un grupo?

7.2.3 ▶ Sean $(G_1, *)$ y $(G_2, \circ)$ grupos. Sobre $G_1 \times G_2$ se define la operación $(a, b) \odot (p, q) = (a * p, b \circ q)$. ¿Es $(G_1 \times G_2, \odot)$ un grupo?

7.2.4 ▶ Sobre $A = \{a, b, c, d\}$ se define la operación $*$ por medio de las tabla que sigue. ¿Es $(A, *)$ un grupo?

$*$	a	b	c	d
a	c	d	b	a
b	d	c	a	b
c	b	a	d	c
d	a	b	c	d

7.2.5 ▶ Verifique, usando las tablas, que $(\mathbb{Z}_5, +)$ y $(\mathbb{Z}_7^*, \cdot)$ son grupos.

$(\mathbb{Z}_5, +)$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(\mathbb{Z}_7^*, \cdot)$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

7.2.6 ▶ Realice la tabla de multiplicación para $(\mathbb{Z}_4^*, \cdot)$ y determine si es un grupo.

7.2.7 ▶ Realice la tabla de adición para $(\mathbb{Z}_4' +)$ y determine el neutro y los inversos.

7.2.8 ▶ Sea $A = \{a, b, c\}$ con la operiación $x * y = y$. Realice la tabla de operación para $(A, *)$. ¿Qué propiedades tiene esta operación?

7.2.9 ▶ Sea $F = \{p + q\sqrt{2}$ tal que $p, q \in \mathbb{Q}\}$. Considere la estructura $(F, \cdot)$, es decir, F con la multiplicación usual.

a.) Verifique que *no existen* $p, q \in \mathbb{Q}$ tal que $\dfrac{p}{q} = \sqrt{2}$. (Sugerencia: Razone por contradicción, suponga que la fracción está totalmente simplificada y que $\dfrac{p^2}{q^2} = 2$. Luego deduzca que p, q deberían ser pares!).

b.) Hay elemento neutro, determine cuál es.

c.) Verifique que el inverso de $p + q\sqrt{2}$ es $\dfrac{p}{p^2 - rq^2} + \dfrac{-q}{p^2 - rq^2}\sqrt{2}$. Observe que por el ítem a.), este inverso está bien definido para cuaquier $p, q \in \mathbb{Q}$.

7.3 Subgrupos

Definición 7.4

Consideremos un grupo $(G, \circ)$. Si H es subconjunto no vacío de G, tal que $(H, \circ)$ es grupo, entonces decimos que H es subgrupo del grupo G y usamos la notación $H \leq G$.

Subgrupos triviales. Los subgrupos triviales de $(G, \circ)$ son $H = \{e\}$ y $H = G$.

Los subconjuntos de G "heredan" la asociatividad, entonces en principio, para probar que H es subgrupo de G, se requiere que la operación sea cerrada en H, que el neutro esté en H y que los inversos de los elementos de H estén en H.

Ejemplo 7.9

Consideremos el grupo $(A, *)$

$*$	i	a	b	c
i	$\boldsymbol{i}$	a	b	c
a	a	c	$\boldsymbol{i}$	b
b	b	$\boldsymbol{i}$	c	a
c	c	b	a	$\boldsymbol{i}$

Determinemos los subgrupos propios de $(A, *)$

a.) $H_1 = \{i\}$ pues i es el neutro.

b.) $H_2 = \{i, c\}$ pues c es inverso de sí mismo. De esta manera, en este conjunto la operación es cerrada pues $c * i \in H_2$, y $c * c \in H_2$

c.) $H_3 = \{i, a, b\}$ no es subgrupo pues aunque b es el inverso de a, sucede que $a * a = c$ y $c \notin H_3$

En el siguientes teoremas establecen criterios para decidir si un subconjunto es un subgrupo o no.

Teorema 7.3

Sea $(G, *)$ un grupo. Entonces $H \leq G$ si y sólo si $a * b^{-1} \in H$ para todo $a, b \in H$

Teorema 7.4 (Teorema de Lagrange)

a.) Si a es elemento de un grupo finito $(G, *)$ de orden n entonces $a^n = e$.

b.) Si $(G, *)$ es un grupo de orden n y si $H \leq G$ entonces el orden de H divides el orden de G.

Si H es unsubconjunto de G y el orden de H divide el orden de G, no significa que sea un subgrupo! El teorema solo da condiciones necesarias para que H sea subgrupo de G.

En cálculos de potencias de elementos de G se puede usar $a^{\text{Ord}(G)} = e$.

Ejemplo 7.10

a.) $(\mathbb{Z}_5, +)$ tiene 5 elementos, por lo tanto, de acuerdo al teorema de Lagrange, solo tiene subgrupos de orden 1 y de orden 5, es decir $H_1 = \{0\}$ pues 0 es el neutro y $H = \mathbb{Z}_5$.

b.) Consideremos los subgrupos de $(\mathbb{Z}_7^*, \cdot)$: Como este grupo tiene orden 6, cualquier subgrupo debe tener orden 1, 2, 3 o 6.

$(\mathbb{Z}_7^*, \cdot)$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

i.) Los subgrupos triviales son $H = \{1\}$ y $H = \mathbb{Z}_7^*$

ii.) Subgrupos de orden 2:
$H_2 = \{1, 6\}$ pues 6 es inverso de sí mismo.

iii.) Habría que analizar los subconjuntos de 3 elementos. Deben tener el neutro, otro elemento y su inverso, pero la operación debe ser cerrada. Solo hay dos candidatos. Para aceptar un candidato como subgrupo podemos hacer una subtabla o usar el teorema 7.3.

$H_3 = \{1,2,4\}$ es subgrupo pues $2 * (4)^{-1} = 2 * 2 \equiv_7 4$ y $4 * (2)^{-1} = 4 * 4 \equiv_7 2$ y ambos elementos están en H_3

$H_3 = \{1,3,5\}$ no es subgrupo. Observemos su tabla de multiplicar

$\cdot$	1	3	5
1	1	3	5
3	3	2	1
5	5	1	4

c.) Consideremos los subgrupos de $(\mathbb{Z}_{13}^*, \cdot)$: Como este grupo tiene orden 12, cualquier subgrupo debe tener orden 1, 2, 3, 4, 6 o 12.

$(\mathbb{Z}_{13}^*, \cdot)$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

Subgrupos

$$\begin{aligned}
H &= \mathbb{Z}_{13}^* \\
H_1 &= \{1\} \\
H_2 &= \{1,12\} \\
H_3 &= \{1,3,9\} \\
H_4 &= \{1,5,8,12\} \\
H_6 &= \{1,3,4,9,10,12\}
\end{aligned}$$

Ejemplo 7.11

Sea $A=\{a,b,c,m,n,o\}$. Si se sabe que $(A,*)$ es un grupo con tabla de "multiplicación" dada por

$*$	a	b	c	m	n	o
a	b	c	a	n	o	m
b	c	a	b	o	m	n
c	a	b	c	m	n	o
m	n	o	m	a	b	c
n	o	m	n	b	c	a
o	m	n	o	c	a	b

a.) Encuentre todos los subgrupos de A

b.) Calcule $\left(m^{-46}*o^4\right)^2*\left(b*n^{-1}\right)^{-1}$

Solución:

a.) Subgrupos de A. El neutro es $e=c$. El orden de A es 6. Por tanto tenemos que analizar los subconjuntos de orden 1, 2, 3 y 6

i.) Subgrupos triviales $H=c$ y $H=A$

ii.) Subgrupos de orden $2:$ $H=\{c,n\}$ pues n es su propio inverso

iii.) Subgrupos de orden $3:$ Necesitamos analizar conjuntos con el neutro y dos elementos, uno inverso del otro. Solo hay dos posibilidades

$H=\{c,a,b\}$. Su tabla es

$*$	c	a	b
c	c	a	b
a	a	b	c
b	b	c	a

$\therefore$ $H=\{c,a,b\}$ es subgrupo de A

$H=\{c,m,o\}$. Su tabla es

$*$	c	m	o
c	c	m	o
m	m	a	c
o	o	c	b

$\therefore$ $H=\{c,m,o\}$ no es subgrupo de A.

b.) Primero calculamos algunas potencias de $m:$ $o^5=m$ y $o^6=c$ y $m^{-46}=(m^{-1})^{46}=o^{46}$. Entonces

$$\left(m^{-46}*o^4\right)^2*\left(b*n^{-1}\right)^{-1} = (o^{50})^2*(m)^{-1} = o^{101} = o^{6\cdot 16+5} = o^6*o^5 = m$$

Para obtener los subgrupos de $(\mathbb{Z}_m,\cdot)$, en particular cuando m es primo, podemos usar la teoría de grupos cíclicos para simplificar la labor.

7.3.1 (*) Grupos cíclicos

Definición 7.5

Consideremos el grupo "multiplicativo" $(G,*)$. Si existe un $a \in G$ tal que $G = \{a^n \text{ tal que } n \in \mathbb{Z}\}$ entonces decimos que G es cíclico y se escribe $G =< a >$

Teorema 7.5

Si $(G,*)$ es cíclico y finito con $\text{Ord}(G) = m$, entonces todos los subgrupos H de G son cíclicos
Si $d_1, d_2, ..., d_k$ son los divisores positivos de m, los subgrupos de G son

$$H_1 =< a^{d_1} >, \quad H_2 =< a^{d_2} >, \quad ..., \quad H_k =< a^{d_k} >$$

Ejemplo 7.12

Consideremos el grupo multiplicativo $(\mathbb{Z}_{13}^*, \cdot)$.

a.) $(\mathbb{Z}_{13}^*, \cdot)$ es un grupo cíclico y $\mathbb{Z}_{13}^* =< 2 >$. En efecto,

$$\mathbb{Z}_{13}^* = \{2,2^2,2^3,2^4,2^5,2^6,2^7,2^8,2^9,2^{10},2^{11},2^{12}\} = \{2,4,8,3,6,12,11,9,5,10,7,1\}$$

b.) Como $\text{Ord}(\mathbb{Z}_{13}^*) = 12$ entonces los subgrupos de $\mathbb{Z}_{13}^*$ son

$$\begin{array}{lllll} < 2^1 > & = & \mathbb{Z}_{13}^* & & \\ < 2^2 > & = & < 4 > & = & \{4,3,12,9,10,1\} = \{1,3,4,9,10,12\}, \\ < 2^3 > & = & < 8 > & = & \{8,12,5,1\} = \{1,5,8,12\}, \\ < 2^4 > & = & < 3 > & = & \{3,9,1\} = \{1,3,9\}, \\ < 2^6 > & = & < 12 > & = & \{12,1\} = \{1,12\}, \\ < 2^{12} > & = & < 1 > & = & \{1\}. \end{array}$$

Ejemplo 7.13

Consideremos el grupo multiplicativo $(\mathbb{Z}_7^*, \cdot)$.

a.) $(\mathbb{Z}_7^*, \cdot)$ es un grupo cíclico y $\mathbb{Z}_7^* =< 3 >$. En efecto,

$$\mathbb{Z}_7^* = \{3^1,3^2,3^3,3^4,3^5,3^6\} = \{3,2,6,4,5,1\}$$

b.) Como $\text{Ord}(\mathbb{Z}_7^*) = 6$ entonces los subgrupos de $\mathbb{Z}_6^*$ son

$$
\begin{array}{rcccl}
< 3^1 > & = & \mathbb{Z}_7^* & & \\
< 3^2 > & = & < 9 > & = & \{1,2,4\} \\
< 3^3 > & = & < 27 > & = & \{1,6\} \\
< 3^6 > & = & < 1 > & = & \{1\}
\end{array}
$$

Ejercicios

7.3.1 ▶ Determine los subgrupos de $(\mathbb{Z}_5,+)$ y $(\mathbb{Z}_5^*,\cdot)$.

7.3.2 ▶ Consideremos $A = \{a,b,c,d\}$ y la operación $*$, sobre A, definida por medio de la tabla que sigue.

$*$	a	b	c	d
a	c	d	b	a
b	d	c	a	b
c	b	a	d	c
d	a	b	c	d

Si se sabe que grupo $(A,*)$ es un grupo,

a.) Determine el elemento neutro

b.) Determine el inverso de cada uno de los elementos de A

c.) Usando el teorema de Lagrange, determine toso los subgrupos de A. Excepto para los subgrupos triviales, debe mostrar una subtabla de "multiplicar" para justificar que los subconjuntos cuyo orden dividen al orden de A, son o no son grupos.

7.3.3 ▶ Consideremos $A = \{1,2,3,4,5,6\}$ y la operación $*$, sobre A, definida por medio de la tabla que sigue.

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	1	5	6	4
4	4	6	5	1	3	2
5	5	4	6	2	1	3
6	6	5	4	3	2	1

Si se sabe que grupo $(A,*)$ es un grupo,

a.) Determine el elemento neutro

b.) Determine el inverso de cada uno de los elementos de A

c.) Usando el teorema de Lagrange, determine toso los subgrupos de A. Excepto para los subgrupos triviales, debe mostrar una subtabla de "multiplicar" para justificar que los subconjuntos cuyo orden dividen al orden de A, son o no son grupos.

7.3.4 ▶ Verifique que $(\mathbb{R}, \circledast)$ es grupo abeliano si $a \circledast b = a + b + 5$.

7.3.5 ▶ Verifique que $(\mathbb{R} \times \mathbb{R}^{+}, *)$ es grupo abeliano si $(a,b) * (c,d) = (a + c + 5, 3bd)$.

7.3.6 ▶ Verifique que $(\mathbb{R} \times \mathbb{R}^{*}, \circledast)$ es grupo abeliano si $(a,b) \circledast (c,d) = (a + c - 3, bd/2)$.

Bibliografía

[1] Susanna S. Epp. *Discrete Mathematics with Applications.* Brooks/Cole Cengage Learning, 1995.

[2] G. Haggard, J. Schlipf, S. Whitesides. *Discrete Mathematics for Computer Science.* Thomson, 2006.

[3] K. Rosen. *Discrete Mathematics and Its Applications.* McGraw Hill. 2007

[4] M. Murillo. *Introducción a la Matemática Discreta.* Cartago, Editorial Tecnológica de Costa Rica. 4ta. Edición

[5] G. Sanabria B. "Apuntes de Relaciones Binarias". Folleto ITCR.

[6] L. Marranghello M. "Principios de Matemática I". Folleto. UCR, 1983.

[7] A. H. Clifford *The Algebraic Theory of Semigroup.* American Mathematical Society. 1961.

[8] W. Mora F. *Introducción a la teoría de números. Ejemplos y Algoritmos.* ITCR. 2010. http://tecdigital.tec.ac.cr/revistamatematica/Libros/index.htm

[9] Gregory J. Chaitin. *The Unknowable (Discrete Mathematics and Theoretical Computer Science)*. Springer. 1999 edition.

[10] L.E.Carrera, R. Solís O., J. L. Chinchilla V. "Matemática Discreta: Ejercicios y soluciones". Folleto. Escuela de Matemática. Instiuto Tecnológico de Costa Rica. 2017.