Contenido

Notas de Matemáticas Discretas

César Bautista Ramos
Facultad de Ciencias de la Computación
Benemérita Universidad Autónoma de Puebla

CAPíTULO 1

Lógica de Predicados y Proposiciones

1. Proposiciones, predicados y paradojas

DEFINICIÓN 1. *Una proposición es una afirmación de la qiue se puede decir sin ambiguedad y de manera excluyente que es cierta o falsa.*

EJEMPLO 2.

(1) El hierro es un metal.
(2) $2 + 2 = 5$
(3) x es un número entero.

Las dos primeras son proposiciones, la tercera, como depende de x se llama función proposicional.

DEFINICIÓN 3. *Una* **función proposicional** *es una expresión que contiene variables $x, y, z, \ldots$, de manera que cuando $x, y, z, \ldots$ se sustituyen por objetos de un cierto* **referencial** *o* **universo de discurso** *(***conjunto universal***), se convierte en una proposición.*

EJEMPLO 4. Sea $E = \{4, 8, 12, 16, 20, 24\}$. Sean las funciones proposicionales

$$p(x) : x \text{ es múltiplo de } 2$$
$$q(x) : x \text{ es múltiplo de } 3.$$

entonces, $p(8)$ es cierta y $q(20)$ es falsa.

El *predicado* de $p(x)$ es "múltiplo de 2" y el de $q(x)$ es "múltiplo de 3". Tales se acostumbran identificar con p y q respectivamente.

DEFINICIÓN 5. *Sea E el universo de discurso de una función proposicional $p(x)$. Con la notación*

$$P = \{x \in E \,|\, p(x)\} = \{x \in E \,:\, p(x)\}$$

se simboliza al conjunto P formado por los elementos x del referencial E para los cuales $p(x)$ es cierta. Aquí se dice que P está definido por **comprensión**.

A veces, E se sobrerentiende y entonces se puede omitir:

$$P = \{x \,|\, p(x)\}.$$

Un conjunto también se puede definir por **extensión** encerrando sus elementos entre llaves.

DEFINICIÓN 6. *Si el elemento x del universo E está en el conjunto P entonces se escribe $x \in P$ que se lee "equis pertenece a P"; y si x no está en P se escribe $x \notin P$ que se lee "equis no pertenece a P". Esto es*

(1) $x \in P \Leftrightarrow p(x)$

(2) $x \notin P \Leftrightarrow \neg p(x)$

DEFINICIÓN 7. *Si se tiene que*

$$P = \{x \in E \,|\, p(x)\} = \{x \in E \,:\, p(x)\}$$

y se cumple $\forall x, \neg p(x)$ *es decir que siempre* $p(x)$ *es falso, entonces se dice que* P *es vacío y se pone*

$$P = \varnothing$$

(1) Si $P = E$ entonces P se llama **conjunto universal**.
(2) Si P tiene un solo elemento, se llama **conjunto unitario**.
(3) Los términos **familia, clase** son usados como sinónimos de conjunto.
(4) En ciertos contextos, por **clase** se entiende una generalización del término "conjunto": todo conjunto es una clase, pero no toda clase es un conjunto. Esta distinción se hace para evitar *paradojas.* Una paradoja es una afirmación que es al mismo tiempo verdadera y falsa.

EJEMPLO 8 (Paradoja de Russel (1902)). Sabemos que un conjunto es una colección de objetos, por ejemplo P el conjunto de enteros pares o C el conjunto de músicos que tocan cumbias en Acajete, Puebla. También se pueden formar colecciones de conjuntos, por ejemplo,

$$D = \{\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{N}\}$$

así, $\mathbb{R} \in D$, $\mathbb{Z} \in D$, $\mathbb{N} \in D$. O por ejemplo $\mathcal{P}(\mathbb{Z})$ el conjunto de todos los subconjuntos de números enteros:

$$\{1, 2, 3\} \in \mathcal{P}(\mathbb{Z}), \quad \mathbb{Z} \in \mathcal{P}(\mathbb{Z}).$$

Muchas veces los conjuntos no son miembros de ellos mismos. Por ejemplo si P es el conjunto de los perros, entonces Manchitas $\in P$ (Manchitas es un perro), pero $P \notin P$ pues el conjunto de los perros no es un perro. Sin embargo podría haber conjuntos que pertenezcan a sí mismos: por ejemplo si E es *el conjunto de todos los conjuntos* entonces $E \in E$.

Consideremos el conjunto

$$A = \{X \text{ conjunto} \,|\, X \notin X\}$$

nos preguntamos: ¿$A \in A$?.

Si $A \in A$ entonces A es un conjunto tal que $A \notin A$. Pero si $A \notin A$ entonces A cumple con las condiciones de los elementos que pertenecen a A; por lo que $A \in A$. En resumen

$$\begin{cases} \text{si } A \in A \Rightarrow A \notin A \\ \text{si } A \notin A \Rightarrow A \in A \end{cases}$$

Hemos obtenido una paradoja!

EJEMPLO 9 (Paradoja de Grellings (1908)).

(1) Un adjetivo se llama *autológico* si el adjetivo se cumple para el mismo adjetivo.
(2) Un adjetivo se lama *heterológico* si la propiedad denotada por el adjetivo no se cumple para el mismo adjetivo.

Por ejemplo

(1) polisilábico es autológico
(2) español es autológico

(3) inglés es heterológico
(4) monosilábico es heterológico

¿heterológico es heterológico?

Si heterológico fuera heterológico entonces debería ser autológico y así no heterológico.

Si heterológico es no heterológico , entonces no tiene la propiedad descrita por él mismo luego es heterológico.

De nuevo una paradoja.

La paradoja de Russel se llama *sintáctica* porque resulta del uso de la sintaxis, de los símbolos; mientras que la de Grelling es de carácter *semántico* pues resulta de la interpretación (semántica) que le damos a las palabras.

Tales paradojas resultan de la *autorecurencia* de las definiciones: para definir el conjunto de la paradoja de Russell se hace uso del mismo conjunto. Similarmente, para definir los adjetivos como autológicos o heterológicos se hace referencia a los mismos adjetivos. Tal fenómeno de autorecurrencia se puede visualizar en los grabados del holandés M. C. Escher. Las paradojas son indeseables en Matemáticas,

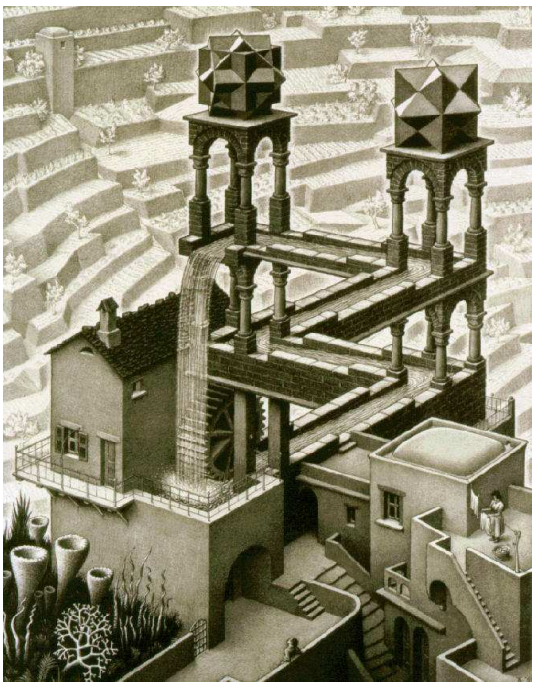


FIGURA 1. Cascada (litografía) por M. C. Escher; http://www.mcescher.com.

CAPíTULO 2

Conjuntos y Clases

1. Axiomas de la Teoría de Conjuntos

Para evitar las paradojas existen reglas para la formación de los conjuntos. Un ejemplo de tales son los *axiomas de Zermelo-Fraenkel*. En general, estos axiomas tienen la forma "si tal conjunto existe entonces tal otro existe" y tales presuponen el conocimiento de la lógica de predicados. Los axiomas de Zermelo-Fraenkel son

- Extensionalidad
- Reemplazo
- Conjunto potencia
- Conjunto unión (suma)
- Infinitud
- Elección
- Regularidad

Por ejemplo, el axioma de extensionalidad dice que si dos conjuntos X, Y son iguales entonces ellos pueden pertenecer a un mismo conjunto Z; en símbolos

$$(\forall X)(\forall Y)((X = Y) \Rightarrow (\forall Z)((X \in Z) \Rightarrow (Y \in Z)))$$

No es la intención en este curso desarrollar axiomaticamente la teoría de conjuntos. Nuestro objetivo es más modesto. Trataremos a los conjuntos desde el *punto de vista inocente* (naive set theory). Sin embargo conviene destacar ciertos hechos de la teoría axiomática de conjuntos.

Como consecuencia de tales axiomas se puede demostrar, por ejemplo, la existencia del conjunto vacío $\varnothing$, así como el siguiente teorema:

TEOREMA 1 (de Separación). *Si E es un conjunto y $p(x)$ una función proposicional, el conjunto*

$$\{x \in E \,|\, p(x)\}$$

existe.

Formalmente el teorema de separación se escribe como

TEOREMA 2 (de Separación).

$$(\forall E)(\exists P)(\forall x)((x \in P) \Leftrightarrow ((x \in E) \wedge p(x)))$$

En otras palabras, lo que el teorema de separación asegura es que si de antemano sabemos que tenemos un universo de discurso como un conjunto entonces podemos formar conjuntos por comprensión.

Examinemos el conjunto A que conduce a la paradoja de Russell. Tal es

$$A = \{X \in E \,|\, X \notin X\}$$

donde tomamos como referencial E el *conjunto* de todos los conjuntos. Según el teorema de separación, A es conjunto a condición de que E lo sea. Pero E que es la

colección de todos los conjuntos no sabemos de antemano que *sea un conjunto*. De hecho no puede serlo, pues la suposición de que lo es conduce a contradicciones en la construcción de A. *No existe el conjunto de todos los conjuntos.*

Si la colección de todos los conjuntos no es un conjunto, entonces ¿qué es? Respuesta: es una *clase*.

2. Axiomas de clases NBG (Neumann-Bernays-Gödel)

Como pudo notarse de la discusión anterior, no definimos formalmente lo que es un conjunto. Los axiomas de Zermelo-Fraenkel sólo dicen cómo, si ya se tiene un conjunto, se pueden construir otros. Es decir, el concepto de "conjunto" se deja indefinido.

Una alternativa a los axiomas de Zermelo-Fraenkel para explicar la teoría de conjuntos, son los axiomas BNG ([**3**]). En la teoría BNG se deja como concepto indefinido "clase".

DEFINICIÓN 10. *X es un conjunto si existe una clase $\mathcal{Y}$ tal que X pertenece a tal clase, i.e., si*

$$(\exists \mathcal{Y})(X \in \mathcal{Y})$$

Las clases que no son conjuntos se llaman *clases propias*. Luego $\mathcal{A}$ la clase de todos los conjuntos es una clase propia.

Los axiomas BNG son

(1) T
(2) P (paridad)
(3) N (conjunto vacío)
(4) Existencia de clases
(5) U (suma de conjuntos)
(6) W (potencia de conjuntos)
(7) R (reemplazo)
(8) I (infinito)

Por ejemplo el axioma T dice que

$$\mathcal{X}_1 = \mathcal{X}_2 \Rightarrow (\mathcal{X}_1 \in \mathcal{Z} \Leftrightarrow \mathcal{X}_2 \in \mathcal{Z})$$

que es una modificación del axioma de extensionalidad. Mientras que el axioma N dice que existe una clase vacía:

$$(\exists \mathcal{X})(\forall \mathcal{Y})(\mathcal{Y} \notin \mathcal{X})$$

Luego se puede mostrar que tal $\mathcal{X}$ es un conjunto y tal se denota con $\varnothing$.

3. Álgebra de conjuntos

3.1. Teoría de conjuntos ingenua (Naive set theory). A pesar de que existen serias formalizaciones de la teoría de conjuntos, nos contentaremos con desarrolar su álgebra usando el punto de vista inocente.

EJEMPLO 11.

(1) $2\mathbb{N} = \{x \in \mathbb{N} \,|\, x = 2h, \text{ para algún } h \in \mathbb{N}\} = \{0, 2, 4, 6, \ldots\}$ que es el conjunto de números naturales pares.
(2) $\{x \in \mathbb{N} \,|\, 1 < x < 2\} = \varnothing$ conjunto vacío.
(3) $\{x \in \mathbb{Z} \,|\, 7 < x^2 < 16 \wedge x > 0\} = \{3\}$ conjunto unitario.
(4) $V = \{a, e, i, o, u\}$ conjunto definido por extensión.

El símbolo $\in$ no es transitivo. Por ejemplo: para

$$P = \{r \,|\, r \text{ es una recta del plano}\}$$

tomemos $\ell \in P$, i.e. ℓ una recta del plano y p un punto en tal recta. Luego,

$$p \in \ell \in P$$

pero $p \notin P$ pues p no es una recta.

DEFINICIÓN 12. *Sean P, Q dos conjuntos con conjunto unversal E. Se dice que P está* **contenido (incluido)** *en Q si*

$$\forall x \in E \, x \in P \Rightarrow x \in Q$$

en tal caso se escribe

$$P \subset Q$$

o bien

$$P \subseteq Q$$

y se dice que P es subconjunto de Q.

Notemos que si

$$P = \{x \in E \,|\, p(x)\} \text{ y } Q = \{x \in E \,|\, q(x)\}$$

entonces

$$P \subset Q \Leftrightarrow \forall x \in E, p(x) \Rightarrow q(x)$$

EJEMPLO 13. Sean

$$P = \{x \in \mathbb{N} \,|\, x \text{ es múltiplo de } 10\}, \quad Q = \{x \in \mathbb{N} \,|\, x \text{ es múltiplo de } 2\}$$

Entonces

$$P \subset Q$$

pues si x es múltiplo de 10 natural entonces existe un natural h que cumple

$$x = 10h = 2(5h)$$

luego x es también múltiplo de 2.

PROPIEDAD 1. *Sean P, Q, R conjuntos con conjunto universal E. Entonces*

(1) $\varnothing \subseteq P$
(2) $P \subseteq P$
(3) $P \subseteq E$
(4) $P \subseteq Q$ *y* $Q \subseteq R \Rightarrow P \subseteq R$

DEM.

(1) Tenemos que demostrar que

$$\forall x \in E, x \in \varnothing \Rightarrow x \in P.$$

La proposición $x \in \varnothing \Rightarrow x \in P$ tiene antecedente falso, luego siempre es verdadera.

(2) Se cumple trivialmente que

$$\forall x \in E, x \in P \Rightarrow x \in P$$

(3) Tenemos que checar que

$$\forall x \in E, x \in P \Rightarrow x \in E$$

lo cual es obvio.

(4) Tenemos que demostrar que

$$\forall x \in E, x \in P \Rightarrow x \in R.$$

lo cual haremos *elemento a elemento*:

si $x \in P$ entonces $x \in Q$ pues $P \subseteq Q$ por hipótesis. Luego $x \in R$ pues $Q \subseteq R$ por hipótesis. Hemos probado que $x \in P \Rightarrow x \in R$;

$$\therefore P \subseteq R.$$

□

Ejemplo 14.

(1) $\varnothing \subseteq \varnothing$ pues un conjunto siempre es subconjunto de sí mismo.
(2) $\varnothing \subseteq \{\varnothing\}$ pues el conjunto vacío siempre es subconjunto de cualquier otro conjunto.
(3) $\varnothing \in \{\varnothing\}$ pues $\varnothing$ que aparece del lado izquierdo está en la descripción del conjunto del lado derecho.
(4) $\varnothing \notin \varnothing$ pues el conjunto vacío no tiene elementos.

Definición 15. *$P \nsubseteq Q$ significa que P no es subconjunto de Q.*

Ejemplo 16.

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

Definición 17. *Se dice que $\varnothing$ y P son* **subconjuntos impropios** *de P; los otros subconjuntos de P se llaman* **propios**.

Definición 18. *Sea Q un conjunto. Se define el conjunto*

$$2^Q = \mathcal{P}(Q)$$

como el conjunto de todos los subconjuntos de Q y se llama **conjunto potencia** *o* **conjunto de partes** *de P.*

Que tal colección es realmente un conjunto lo asegura el axioma del conjunto potencia según Zermelo-Fraenkel o bien el axioma W según los axiomas NBG.

Ejemplo 19.

(1) Sea $Q = a, b, c$. Entonces

$$\mathcal{P}(Q) = \{\varnothing, \{a\}, \{b\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

(2) Sea $R = \{a\}$. Entonces

$$\mathcal{P}(R) = \{\varnothing, \{a\}\}$$

(3) $\mathcal{P}(\varnothing) = \{\varnothing\}$

Definición 20. *Si P es un conjunto con $|P|$ se denota al número de elementos de P y tal se llama la* **cardinalidad** *del conjunto.*

En los ejemplos anteriores

$$|2^Q| = 8 = 2^{|Q|}$$
$$|2^R| = 2 = 2^{|R|}$$
$$|2^\varnothing| = 1 = 2^{|\varnothing|}$$

Posteriormente se demostrará que, en general si Q es un conjunto finito entonces

$$|2^Q| = 2^{|Q|}$$

TAREA 1. *¿Cuál es la cardinalidad de estos conjuntos?*

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

TAREA 2. *¿Cuál es la cardinalidad de estos conjuntos?*

(1) $\varnothing$
(2) $\{\varnothing\}$
(3) $\{\varnothing, \{\varnothing\}\}$
(4) $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$

TAREA 3. *Obtener el conjunto potencia de*

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

TAREA 4. *¿Cuántos elementos tiene el conjunto* 2^A*?*

(1) $A = \{a, b, \{a, b\}\}$
(2) $A = \{\varnothing, a\}$
(3) $A = \{\varnothing, \{a\}, \{\varnothing, a\}\}$
(4) $A = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$
(5) $A = 2^{\varnothing}$

TAREA 5. *Determinar si alguno de los siguientes es el conjunto potencia de algún conjunto (¿cuál?).*

(1) $\varnothing$
(2) $\{\varnothing, \{a\}\}$
(3) $\{\varnothing, \{a\}, \{\varnothing, a\}\}$
(4) $\{\varnothing, \{a\}, \{b\}, \{a, b\}\}$

DEFINICIÓN 21. *Sean* P, Q *conjuntos con conjunto universal* E*. Se dice que* P *y* Q *son* **iguales** *si* $P \subseteq Q$ *y* $Q \subseteq P$*. En tal caso se escribe* $P = Q$*. Es decir*

$$P = Q \Leftrightarrow P \subseteq Q \wedge Q \subseteq P.$$

EJEMPLO 22.

$$\{a, a\} = \{a\}$$

pues si $\{a, a\} \subseteq \{a\}$ porque si $x \in \{a, a\}$ entonces $x = a \in \{a\}$; y recíprocamente, $\{a\} \subseteq \{a, a\}$.

EJEMPLO 23.

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

pues $\{a, b\} \subseteq \{b, a\}$ pues si $x \in \{a, b\}$ entonces $x = a \vee x = b$ y en cualquiera de estos dos casos $x \in \{b, a\}$; similarmente $\{b, a\} \subseteq \{a, b\}$.

Como puede notarse de los ejemplos, en conjuntos no importan las redundancias, ni el orden de los elementos que las forman.

TAREA 6. *Describir los siguientes conjuntos por extensión:*

(1) $\{x \in \mathbb{R} \mid x^2 = 1\}$
(2) $\{x \in \mathbb{Z} \mid 0 < x < 12\}$

(3) $\{x \in \mathbb{R} \,|\, x \text{ es el cuadrado de un entero y } x < 100\}$
(4) $\{x \in \mathbb{Z} \,|\, x^2 = 2\}$

TAREA 7. *Describir por comprensión los siguientes conjuntos*

(1) $\{0, 3, 6, 9, 12\}$
(2) $\{-3, -2, -1, 0, 1, 2, 3\}$
(3) $\{m, n, o, p\}$

TAREA 8. *Determinar si los siguientes pares de conjuntos son iguales.*

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

TAREA 9. *Supongamos que* $A = \{2, 4, 6\}$, $B = \{2, 6\}$, $C = \{4, 6\}$ *y* $D = \{4, 6, 8\}$. *Determinar cuáles de estos conjuntos son subconjuntos de cuáles.*

TAREA 10. *Determinar si 2 es un elemento del conjunto.*

(1) $\{x \in \mathbb{R} \,|\, x \text{ es entero mayor que } 1\}$
(2) $\{x \in \mathbb{R} \,|\, x \text{ es el cuadrado de un entero}\}$
(3) $\{2, \{2\}\}$
(4) $\{\{2, \{2\}\}\}$
(5) $\{\{2\}, \{2, \{2\}\}\}$
(6) $\{\{\{2\}\}\}$

TAREA 11. *Determinar si es cierto o falso.*

(1) $0 \in \varnothing$
(2) $\{0\} \subseteq \varnothing$
(3) $\varnothing \in \{0\}$
(4) $\{0\} \in \{0\}$
(5) $\{\varnothing\} \subseteq \{\varnothing\}$
(6) $\varnothing \subseteq \{0\}$

TAREA 12. *Determinar si es cierto o falso.*

(1) $\varnothing \in \{\varnothing\}$
(2) $\{\varnothing\} \in \{\varnothing\}$
(3) $\{\varnothing\} \subseteq \{\varnothing, \{\varnothing\}\}$
(4) $\{\{\varnothing\}\} \subseteq \{\{\varnothing\}, \{\varnothing\}\}$
(5) $\varnothing \in \{\varnothing, \{\varnothing\}\}$

TAREA 13. *Determinar cierto o falso*

(1) $x \in \{x\}$
(2) $\{x\} \in \{\{x\}\}$
(3) $\{x\} \subseteq \{x\}$
(4) $\{x\} \in \{x\}$
(5) $\varnothing \subseteq \{x\}$
(6) $\varnothing \in \{x\}$

TAREA 14. *Encontrar dos conjuntos* A, B *tales que*

(1) $A \subseteq B$
(2) $A \in B$.

TAREA 15. *Sean* A, B *conjuntos con conjunto universal* E. *Demostrar que si* $2^A = 2^B$ *entonces* $A = B$.

DEFINICIÓN 24. *Si P es un conjunto con conjunto universal E entonces el* **complemento** *de P es*

$$P^c = \{x \in E \,|\, x \notin P\}$$

es decir, P^c consta de los elementos que no están en P.

EJEMPLO 25. *Sea $E = \{a, e, i, o, u\}$ y $P = \{a, e, o\}$. Entonces $P^c = \{i, u\}$.*

PROPIEDAD 2. *Sean A, B conjuntos con conjunto universal E. Entonces*

(1) $E^c = \varnothing$
(2) $\varnothing^c = E$
(3) $A^c = B^c \Leftrightarrow A = B$
(4) $A \subseteq B \Leftrightarrow B^c \subseteq A^c$
(5) $A^{cc} = A$

DEM.

(1) Por contradicción: si $E^c \neq \varnothing$ entonces existe $z \in E^c = \{x \in E \,|\, x \notin E\}$, luego $z \in E$ y $z \notin E$, lo cual es absurdo.

$$\therefore E \neq \varnothing$$

(2) Por contenciones, esto es probaremos que
   (a) $\varnothing^c \subseteq E$;
   (b) $E \subseteq \varnothing^c$.
   (a) Esto es porque cualquier conjunto está contenido en el conjunto universal.
   (b) Checaremos, por definición de contención, que

$$\forall x \in E, x \in E \Rightarrow x \in \varnothing^c$$

   en efecto, si $x \in E$ entonces $x \in \varnothing \vee x \notin \varnothing$ (recordemos que $p \vee \neg p$ es una tautología, para cualquier proposición p). El primer caso no se puede dar luego $x \notin \varnothing$, por lo que $x \in \varnothing^c$:

$$\therefore E \subseteq \varnothing^c$$

(3) Tarea.
(4) ($\Rightarrow$) Supongamos que $A \subseteq B$. Por demostrar que $B^c \subseteq A^c$ lo cual haremos elemento a elemento: es decir tenemos que checar que

$$\forall x \in E, x \in B^c \Rightarrow x \in A^c$$

   En efecto, si $x \in B^c$ entonces $x \notin B$ luego $x \notin A$, pues en caso contrario $x \in A$ lo cual implicaría $x \in B$ (por hipótesis $A \subseteq B$). Por lo que $x \in A^c$:

$$\therefore B^c \subseteq A^c$$

   ($\Leftarrow$) Supongamos $B^c \subseteq A^c$. Por demostrar ahora que $A \subseteq B$ lo cual haremos, de nuevo, elemento a elemento, esto es

$$\forall x \in E, x \in A \Rightarrow x \in B$$

   Si $x \in A$ entonces $x \in B \vee x \notin B$; si ocurriera lo segundo entonces $x \in B^c$ luego $x \in A^c$ (recordar la hipótesis $B^c \subseteq A^c$) y entonces $x \notin A$ lo que contradeciría nuestra suposición. Por tanto $x \in B$.

$$\therefore A \subseteq B.$$

(5) Tarea.

□

Notemos que si

$$A = \{x \in E \,|\, p(x)\} \text{ y } B = \{x \in E \,|\, q(x)\}$$

entonces

$$A = B \text{ si y sólo si } \forall x \in E, p(x) \Leftrightarrow q(x).$$

Tal hecho lo podemos usar en la demostración del siguiente.

TEOREMA 3. *Sean A, B, C conjuntos con conjunto universal E.*

(1) $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ *(asociativa)*
(2) $A \cup B = B \cup A$, $A \cap B = B \cap A$ *(conmutativa)*
(3) *(asociativa)*
   (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(4) $A \cup \varnothing = A$, $A \cap E = A$ *(neutro)*
(5) $A \cup A^c = E$, $A \cap A^c = \varnothing$ *(complemento)*

DEM.

(1) Tarea
(2) Tenemos que, para p, q proposiciones se cumple que

$$p \vee q \Leftrightarrow q \vee p \quad \text{y} \quad p \wedge q \Leftrightarrow q \wedge p$$

son tautologías, por que lo se cumplen

$$\forall x \in E, x \in A \vee x \in B \Leftrightarrow x \in B \vee x \in A$$

y

$$\forall x \in E, x \in A \wedge x \in B \Leftrightarrow x \in B \wedge x \in A$$

de donde $A \cup B = B \cup A$ y $A \cap B = B \cap A$.
(3) Tarea.
(4) (a) $A \cup \varnothing = A$: que $A \subseteq A \cup \varnothing$ es por una propiedad anterior. Y si $x \in A \cup \varnothing$ entonces $x \in A \vee x \in \varnothing$; como el segundo caso es imposible, entonces $x \in A$. por lo tanto $A \cup \varnothing \subseteq A$. Concluimos

$$A \cup \varnothing = A$$

   (b) $A \cap E = A$: tarea.
(5) Tarea.

□

TEOREMA 4 (Leyes de De Morgan). *Sean A, B conjuntos con conjunto universal E.*

(1) $(A \cup B)^c = A^c \cap B^c$
(2) $(A \cap B)^c = A^c \cup B^c$

DEM.

(1)

$$\begin{aligned} z \in (A \cup B)^c &\Rightarrow z \notin A \cup B \\ &\Leftrightarrow \neg(z \in A \cup B) \\ &\Leftrightarrow \neg(z \in A \vee z \in B) \\ &\Leftrightarrow \neg(z \in A) \wedge \neg(z \in B) \qquad \text{pues } \neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q) \\ &\Leftrightarrow z \in A^c \wedge z \in B^c \\ &\Leftrightarrow z \in A^c \cap B^c \end{aligned}$$

Hemos probado que $\forall z \in E, z \in (A \cup B)^c \Leftrightarrow z \in A^c \cap B^c$:

$$\therefore (A \cup B)^c = A^c \cap B^c$$

(2) Tarea.

□

DEFINICIÓN 26. *Sea I una familia de índices y A_i un conjunto con conjnto universal E para cada $i \in I$.*

(1) *La* **unión** *de los A_i con $i \in I$ es*

$$\bigcup\{A_i \mid i \in I\} = \bigcup_{i \in I} A_i = \{x \in E \mid \exists i \in I \text{ tal que } x \in A_i\}$$

(2) *La* **intersección** *de los A_i con $i \in I$ es*

$$\bigcap\{A_i \mid i \in I\} = \bigcap_{i \in I} A_i = \{x \in E \mid \forall i \in I, x \in A_i\}$$

Para ejemplificar necesitamos la *propiedad arquimediana* de los números reales:

$$(\forall x > 0)(\forall y)(\exists m \in \mathbb{N})(mx > y)$$

EJEMPLO 27. Tomemos como conjunto universal $E = \mathbb{R}$. Probaremos $\bigcup_{i \in \mathbb{N}}[i, i] = \mathbb{R}$: (aquí $[-i, i]$ es un intervalo cerrado, $[-i, i] = \{x \in \mathbb{R} \mid -i \leq x \leq i\}$) por contenciones

(1) $\bigcup_{i \in \mathbb{N}}[-i, i] \subseteq \mathbb{R}$; esto es porque cualquier conjunto es subconjunto del conjunto universal.
(2) $\mathbb{R} \subseteq \bigcup_{i \in \mathbb{N}}[i, i]$; si $x \in \mathbb{R}$ entonces, por la propiedad arquimediana existe $m \in \mathbb{N}$ tal que $m > |x|$, luego $x \in [-m, m]$; es decir, $\exists m \in \mathbb{N}$ tal que $x \in [-m, m]$. Luego, por definición

$$x \in \bigcup_{i \in \mathbb{N}}[i, i]$$

$$\therefore \mathbb{R} \subseteq \bigcup_{i \in \mathbb{N}}[i, i]$$

$$\therefore \mathbb{R} = \bigcup_{i \in \mathbb{N}}[i, i]$$

EJEMPLO 28. $E = \mathbb{R}$. Probaremos que

$$\bigcap_{i \in \mathbb{N}} \left[-\frac{1}{i+1}, \frac{1}{i+1}\right] = \{0\}.$$

Tenemos que

$$-\frac{1}{i+1} \leq 0 \leq \frac{1}{i+1}, \quad \forall i \in \mathbb{N}$$

entonces

$$(\forall i \in \mathbb{N}) \quad 0 \in \left[-\frac{1}{i}, \frac{1}{i}\right]$$

luego por definición

$$0 \in \bigcap_{i\in\mathbb{N}} \left[-\frac{1}{i+1}, \frac{1}{i+1}\right].$$

$$\therefore \{0\} \subseteq \bigcap_{i\in\mathbb{N}} \left[-\frac{1}{i+1}, \frac{1}{i+1}\right]$$

Reciprocamente: sea

$$x \in \bigcap_{i\in\mathbb{N}} \left[-\frac{1}{i+1}, \frac{1}{i+1}\right]. \tag{1}$$

Tenemos dos casos: $x = 0$ o $x \neq 0$. En el segundo caso $|x| > 0$, luego existe $m \in \mathbb{N}$ tal que $(m+1)|x| > 1$, según la propiedad arquimediana; lo que implica $|x| > 1/(m+1)$, por lo que

$$x > \frac{1}{m+1} \vee x < -\frac{1}{m+1}$$

entonces

$$x \notin \left[-\frac{1}{m+1}, \frac{1}{m+1}\right]$$

lo que contradice (1). Por lo tanto $x = 0$,

$$\therefore \bigcap_{i\in\mathbb{N}} \left[-\frac{1}{i+1}, \frac{1}{i+1}\right] \subseteq \{0\}$$

$$\therefore \bigcap_{i\in\mathbb{N}} \left[-\frac{1}{i+1}, \frac{1}{i+1}\right] = \{0\}.$$

Tarea 16. *Pruebe que*

(1)

$$\bigcap_{i\in\mathbb{N}} [-i-1, i+1] = [-1, 1]$$

(2)

$$\bigcup_{i\in\mathbb{N}} [-i-2, i+2] = \mathbb{R}$$

(3)

$$\bigcap_{i\in\mathbb{N}} [-i, i] = \{0\}$$

(4)

$$\bigcap_{i\in\mathbb{N}} \left(0, \frac{1}{i+1}\right] = \varnothing$$

(5)

$$\bigcap_{i\in\mathbb{N}} \left(-\frac{1}{i+1}, \frac{1}{i+1}\right) = \varnothing$$

DEFINICIÓN 29.

(1) *La negación de*

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

es

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

(2) *La negación de*

$$(\exists x)p(x)$$

es

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

TEOREMA 5 (De Morgan). *Sea A_i, $i \in I$ una familia de conjuntos con conjunto universal E.*

(1)

$$(\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} A_i^c$$

(2)

$$(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c$$

DEM.

(1)

$$\begin{aligned} x \in (\bigcup_{i\in I} A_i)^c &\Leftrightarrow x \notin \bigcup_{i\in I} A_i \\ &\Leftrightarrow \neg\left(x \in \bigcup_{i\in I} A_i\right) \\ &\Leftrightarrow \neg\left((\exists i \in I) \quad x \in A_i\right) \\ &\Leftrightarrow (\forall i \in I) \quad x \notin A_i \\ &\Leftrightarrow (\forall i \in I) \quad x \in A_i^c \\ &\Leftrightarrow x \in \bigcap_{i\in I} A_i^c \end{aligned}$$

$$\therefore (\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} A_i^c$$

(2) Tarea.

□

CAPíTULO 3

Funciones y Relaciones

1. Producto cartesiano y relaciones

DEFINICIÓN 30. *Sean A, B conjuntos.*

(1) *Si $a \in A$ y $b \in B$ entonces (a, b) se dice* **par ordenado**.
(2) *Se pone $(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$.*
(3) *Se define el* **producto cartesiano** *de A con B como*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

EJEMPLO 31.

(1) $(1, 2) \neq (2, 1)$
(2) $\{1, 2\} = \{2, 1\}$
(3) $\left(\frac{2}{\sqrt{2}}, \frac{\sqrt{2}}{2}\right) = \left(\sqrt{2}, \frac{2}{\sqrt{2}}\right)$ pues

$$\begin{aligned} \frac{2}{\sqrt{2}} &= \frac{\sqrt{2}\sqrt{2}}{\sqrt{2}} \\ &= \sqrt{2} \end{aligned}$$

y

$$\begin{aligned} \frac{\sqrt{2}}{2} &= \frac{\sqrt{2}\sqrt{2}}{2} \\ &= \frac{2}{\sqrt{2}} \end{aligned}$$

EJEMPLO 32. $A = \{a, b, b\}$, $B = \{1, 2\}$. Entonces

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

que se puede representar graficamente por un *diagrama cartesiano*:

PROPIEDAD 3. *Sean A, B, C conjuntos.*

(1) $(A \cup B) \times C = (A \times C) \cup (B \times C)$
(2) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

DEM.

(1)

$$\begin{aligned} x \in (A \cup B) \times C &\Leftrightarrow x = (r,s) \wedge r \in A \cup B \wedge s \in C \\ &\Leftrightarrow x = (r,s) \wedge (r \in A \vee r \in B) \wedge s \in C \\ &\Leftrightarrow x = (r,s) \wedge ((r \in A \wedge s \in C) \vee (r \in B \wedge s \in C)) \\ &\Leftrightarrow (x = (r,s) \wedge (r \in A \wedge s \in C)) \vee (x = (r,s) \wedge r \in B \wedge s \in C) \\ &\Leftrightarrow x \in A \times C \vee x \in B \times C \\ &\Leftrightarrow x \in (A \times C) \cup (B \times C) \end{aligned}$$

(2) Tarea.

□

DEFINICIÓN 33. *Sean A, B conjuntos. Si $f \subseteq A \times B$ entonces f se llama* **relación** *o* **correspondencia** *entre A y B. En tal caso f se denota como*

$$f : A \to B$$

DEFINICIÓN 34. *Si $f : A \to B$ es relación y $(a,b) \in f$ entonces*

(1) *b se llama* **imagen** *de a*
(2) *a se llama* **anti-imagen** *o* **preimagen** *de b*
(3) *si $a \in A$ arbitrario el* **conjunto de im'agenes** *de a es*

$$f(a) = \{b \in B \,|\, (a,b) \in f\}$$

(4) *si $b \in B$ arbitrario, el conjunto de pre-imágenes de b es*

$$f^{-1}(b) = \{a \in A \,|\, (a,b) \in f\}$$

(5) *El* **dominio** *de f es*

$$Dom\, f = \{a \in A \,|\, existe\ b \in B\ con\ (a,b) \in f\}$$

(6) *El* **rango, recorrido, imagen** *de f es*

$$Im\, f = \{b \in B \,|\, existe\ a \in A\ con\ (a,b) \in f\}$$

EJEMPLO 35. Sea A el conjunto de nombres de las ciudades, B el conjunto de nombres de países. Se define una relación entre A y B como

$$f = \{(a,b) \,|\, a \text{ está en } b\}$$

Entonces, (Rosario,Argentina)$\in f$, (Barranquilla,Colombia)$\in f$, (Paris, Francia)$\in f$, (Paris,Hilton)$\notin f$, (Mérida,México)$\in f$, (Córdoba,Argentina)$\in f$, (Cŕdoba,México)$\in f$, (Córdoba,España)$\in f$;

- f^{-1}(México) son todos los nombres de las ciudades que están en México
- f(Paris) todos los nombres de los países que tienen a Paris como una ciudad.

EJEMPLO 36. Sean $A = \{0,1,2\}$, $B = \{a,b\}$. Se define la relación

$$f = \{(0,a),(0,b),(1,a),(2,b)\}$$

Nótese que f es un subconjunto propio de $A \times B$. Luego,

(1) $f(0) = \{a,b\}$
(2) $f(1) = \{a\}$
(3) $f(2) = \{b\}$
(4) $f^{-1}(a) = \{0,1\}$

(5) $f^{-1}(b) = \{0\}$
(6) $Dom\, f = \{0, 1, 2\}$
(7) $Im\, f = \{a, b\}$

EJEMPLO 37. Sean $A = \{a, b, b\}$, $B = \{1, 2, 3, 4\}$. Se puede definir una correspondencia $f : A \to B$ por

$$f(a) = \{1, 2\}, \quad f(b) = \varnothing, \quad f(c) = \{3\}$$

esto es,

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

Tal correspondencia se puede visualizar por sus diagramas *sagital* o *cartesiano*. Como podemos ver

$$Im\, f = \{1, 2, 3\}, \quad Dom\, f = \{a, c\}$$

DEFINICIÓN 38. *Una relación R sobre un conjunto A es una relación de A en A. En tal caso, si $(a, b) \in R$ entonces se escribe aRb. Esto es:*

$$aRb \Leftrightarrow (a, b) \in R.$$

Si $(a, b) \notin R$ se escribe $a \not R b$.

EJEMPLO 39. Sea $A = \{1, 2, 3, 4, 5\}$. Se define una relación en A mediante

$$xRy \Leftrightarrow y = 2x$$

entonces $1R2$ pues $2 = 2 * 1$ y $2R4$ pues $4 = 2 * 2$:

$$R = \{(1, 2), (2, 4)\}$$

EJEMPLO 40. Sea S la siguiente relación en $\mathbb{N}$:

$$aSb \Leftrightarrow a \leq b$$

así $(1, 2) \in S$ pues $1 \leq 2$, $(2, 3) \in S$, $(2, 40) \in S$ pero $(40, 2) \notin S$.

EJEMPLO 41. $\varnothing$ es una relación sobre cualquier conjunto.

TAREA 17. *Enumerar los pares ordenados de la relación R de $A = \{0, 1, 2, 3, 4\}$ en $B = \{0, 1, 2, 3\}$ donde aRb si y sólo si*

(1) $a = b$
(2) $a + b = 4$
(3) $a > b$
(4) *el máximo común divisor entre a y b es 1*

Representar tales relaciones mediante su diagrama cartesiano.

TAREA 18. *Escribir por extensión los pares ordenados de la relación R sobre $\{1, 2, 3, 4, 5, 6\}$:*

$$aRb \Leftrightarrow \ a \text{ divide a } b$$

2. Relaciones de equivalencia. Particiones

DEFINICIÓN 42. *Sea R una relación sobre A. Se dice que R es*

(1) **reflexiva** *si* $(\forall a \in A)(aRa)$
(2) **simétrica** *si* $(\forall a \in A)(\forall b \in B)(aRb \Rightarrow bRa)$
(3) **antisimétrica** *si* $(\forall a \in A)(\forall b \in B)(aRb \wedge bRa \Rightarrow a = b)$
(4) **transitiva** *si* $(\forall a \in A)(\forall b \in A)(\forall c \in C)(aRb \wedge bRc \Rightarrow aRc)$

EJEMPLO 43. Sea R la relación en $\mathbb{Z}$ definida por

$$xRy \Leftrightarrow xy > 0.$$

(1) R no es reflexiva pues $0 \not R 0$ porque $0 * 0 \not> 0$.
(2) R es simétrica pues

$$aRb \Rightarrow ab > 0 \Rightarrow ba > 0 \Rightarrow bRa$$

(3) R no es antisimétrica pues $1R2$ y $2R1$ pero $2 \neq 1$.
(4) R es transitiva pues

$$\begin{aligned} aRb \wedge bRc &\Rightarrow ab > 0 \text{ y } bc > 0 \\ &\Rightarrow \ a \text{ y } b \text{ tienen el mismo signo además } b \text{ y } c \text{ tienen el mismo signo} \\ &\Rightarrow a \text{ y } c \text{ tienen el mismo signo} \\ &\Rightarrow ac > 0 \\ &\Rightarrow aRc \end{aligned}$$

EJEMPLO 44. Sea R la relación en $\mathbb{Z}$ definida por

$$xRy \Leftrightarrow xy \geq 0.$$

(1) R es reflexiva: $\forall x \in \mathbb{Z}$ se cumple xRx pues $xx \geq 0$.
(2) R es simétrica:

$$xRy \Rightarrow xy \geq 0 \Rightarrow yx \geq 0 \Rightarrow yRx$$

(3) R no es antisimétrica: $4R3$ y $3R4$ pero $4 \neq 3$.
(4) R no es transitiva: $(-1)R0$ pues $-1 * 0 \geq 0$ y $0R1$ pues $0 * 1 \geq 0$ pero $(-1) \not R 1$.

EJEMPLO 45. Considérese las siguientes relaciones en $\{1, 2, 3, 4\}$:

$$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$$
$$R_2 = \{(1,1), (1,2), (2,1)\}$$
$$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$$
$$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$$
$$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4)\}$$
$$R_6 = \{(3,4)\}$$

¿Qué propiedades tienen las relaciones anteriores?

SOL.

R_1 : (a) no es reflexiva pues $3 \not R_1 3$ (i.e. $(3,3) \notin R_1$)
(b) no es simétrica: $3R_1 4$ pero $4 \not R_1 3$
(c) no es antisimétrica: $1R_1 2$ y $2R_1 1$ pero $1 \neq 2$
(d) no es transitiva: $4R_1 1$ y $1R_1 2$ pero $4 \not R_1 2$

R_2: (a) no reflexiva: $2 \not R_2 2$
(b) sí simétrica:

$$1R_2 1 \Rightarrow 1R_2 1$$
$$1R_2 2 \Rightarrow 2R_2 1$$
$$2R_2 1 \Rightarrow 1R_2 1$$

(c) no antisimétrica: $1R_2 2$ y $2R_2 1$ pero $1 \neq 2$.
(d) transitiva: $2R_2 1$ y $1_R R_2 2$ pero $2 \not R_2 2$

R_3: (a) sí reflexiva: $1R-31$, $2R_32$, $3R_33$, $4R_34$.
(b) simétrica:

$$1R_32 \Rightarrow 2R_31$$
$$1R_34 \Rightarrow 4R_31$$
$$2R_31 \Rightarrow 1R_32$$
$$2R_32 \Rightarrow 2R_32$$
$$3R_33 \Rightarrow 3R_33$$
$$4R_31 \Rightarrow 1R_34$$

(c) no antisimétrica: $1R_32$ y $2R_31$ pero $1 \neq 2$.
(d) no transitiva: $4R_31$ y $1R_32$ pero $4\not{R}_32$

□

TAREA 19. *Sea $X = \{a, b, c, d\}$ y considérese las relaciones sobre X:*

$$S_1 = \{(a, c), (b, a), (b, c), (c, d), (d, d)\}$$
$$S_2 = \{(a, a), (a, b), (b, a), (b, c), (c, d), (d, d)\}$$
$$S_3 = \{(a, a), (b, b), (c, c), (d, d), (c, d), (d, c)\}$$

Indique qué propiedades verifican dichas relaciones.

TAREA 20. *Determinar si la relación R en el conjunto de todas las personas es reflexiva, simétrica, antisimétrica, y/o transitiva, donde aRb si*

(1) *a es más alto que b*
(2) *a y b nacieron el mismo día*
(3) *a tiene el mismo nombre de pila que b*
(4) *a y b tienen un abuelo o abuela en común*

Finaliza 1er. parcial 2013 verano

DEFINICIÓN 46. *Sea $A \neq \varnothing$. Una relación R sobre A se dice que es de* **equivalencia** *si es reflexiva, simétrica y transitiva.*

EJEMPLO 47. Sea R la relación en $\mathbb{Z}$ dada por

$$aRb \Leftrightarrow a = b \vee a = -b.$$

Demostrar que es de equivalencia.

DEM.

(1) R es reflexiva: $\forall a \in \mathbb{Z}$, aRa pues $a = a$.
(2) R es simétrica: si aRb entonces $a = b$ o $a = -b$, luego $b = a$ o $b = -a$ lo que implica bRa.
(3) R transitiva: si aRb y bRc entonces ($a = b$ o $a = -b$) y ($b = c$ o $b = -c$) lo que implica $|a| = |b|$ y $|b| = |c|$ entonces $|a| = |c|$ de donde se sigue que $a = c$ o $a = -c$ por lo que aRc.

□

EJEMPLO 48. Sea R la relación de equivalencia en $\mathbb{Q}$ (conjunto de números racionales) dada por

$$aRb \Leftrightarrow a - b \in \mathbb{Z}.$$

(ejemplos de parejas relacionadas son: $(1/2)R(1/2)$ pues $1/2-1/2 \in \mathbb{Z}$, $(3/2)R(1/2)$ pues $3/2-1/2=1\in\mathbb{Z}$, $(1/2)R(3/2)$ pues $1/2-3/2=-1\in\mathbb{Z}$, etc.) Demostrar que R es de equivalencia.

Dem.

(1) R es reflexiva: $\forall a\in\mathbb{Q}$, $a-a=0$ luego aRa.
(2) R es simétrica: $\forall a\in\mathbb{Q}$, $\forall b\in\mathbb{Q}$

$$\begin{aligned} aRb &\Rightarrow a-b\in\mathbb{Z}\\ &\Rightarrow \underbrace{-(a-b)}_{b-a}\in\mathbb{Z}\\ &\Rightarrow b-a\in\mathbb{Z}\\ &\Rightarrow bRa \end{aligned}$$

(3) R es transitiva: $\forall a\in\mathbb{Q}$, $\forall b\in\mathbb{Q}$

$$aRb\wedge bRc \Rightarrow a-b\in\mathbb{Z}\wedge b-c\in\mathbb{Z}$$

$$\begin{aligned} &\underbrace{(a-b)+(b-c)}_{a-c}\in\mathbb{Z}, && \text{pues suma de enteros es entero;}\\ &\Rightarrow a-c\in\mathbb{Z}\\ &\Rightarrow aRc. \end{aligned}$$

□

Ejemplo 49. Se define la siguiente relación en $\mathbb{Z}$:

$$a|b \Leftrightarrow \exists k\in\mathbb{Z} \text{ tal que } b=ka$$

El símbolo "|" se lee "divide". Esto es

$$a \text{ divide a } b \Leftrightarrow b \text{ es múltiplo de } a$$

Por ejemplo:

(1) $3|6$ pues existe $2\in\mathbb{Z}$ tal que $6=2*3$;
(2) $7|21$ pues $\exists 3\in\mathbb{Z}$ tal que $21=3*7$;
(3) $5|-50$ pues $\exists -10\in\mathbb{Z}, -50=(-10)*5$;
(4) $37|0$ pues $\exists 0\in\mathbb{Z}, 0=0*37$;
(5) $3\nmid 4$ pues no existe $k\in\mathbb{Z}$ tal que $4=k*3$. De hecho tal k tiene que ser $k=4/3\notin\mathbb{Z}$.
(6) $0|0$ pues $\exists 1\in\mathbb{Z}$ tal que $0=1*0$.

Como puede notarse, la relación de divisibilidad no es de equivalencia pues no es simétrica: $3|6$ pero $6\nmid 3$. Sin embargo es reflexiva y transitiva:

(1) reflexiva: $\forall a\in\mathbb{Z}$: como $a=1*a$ entonces $a|a$;
(2) transitiva: $\forall a,b,c\in\mathbb{Z}$:

$$\begin{aligned} a|b\wedge b|c &\Rightarrow (\exists k_1\in\mathbb{Z}, b=k_1a)\wedge(\exists k_2\in\mathbb{Z}, c=k_2b)\\ &\Rightarrow c=k_2(k_1a) && \text{sustituyendo } b;\\ &\Rightarrow c=(k_2k_1)a && \text{asociando con } k_2k_1\in\mathbb{Z}\\ &\Rightarrow c \text{ es múltiplo de } a\\ &\Rightarrow a|c \end{aligned}$$

$\therefore$ "$|$" no es relación de equivalencia

EJEMPLO 50. Se define la relación en $\mathbb{Z}$:

$$a \equiv b \Leftrightarrow 4|(a-b)$$

(por ejemplo $32 \equiv 8$ pues $4|(32-8) = 24$, $7 \equiv 3$ pues $4|(7-3) = 4$, $4 \equiv 0$ pues $4|(4-0)$, $4 \not\equiv 1$ pues $4 \nmid (4-1) = 3$). ¿Es $\equiv$ relación de equivalencia?

SOL. Si:

(1) reflexiva: $\forall a \in \mathbb{Z}$, $a \equiv a$ pues $4|(a-a) = 0$.
(2) simétrica:

$$\begin{aligned} a \equiv b &\Rightarrow 4|(a-b) \\ &\Rightarrow \exists k \in \mathbb{Z}, a-b = 4k \\ &\Rightarrow \exists k \in \mathbb{Z}, -(a-b) = -4k && \text{multiplicando por } -1 \\ &\Rightarrow \exists -k \in \mathbb{Z}, b-a = 4(-k) \\ &\Rightarrow 4|(b-a) \\ &\Rightarrow b \equiv a \end{aligned}$$

(3) transitiva:

$$\begin{aligned} a \equiv b \wedge b \equiv c &\Rightarrow 4|(a-b) \wedge 4|(b-c) \\ &\Rightarrow a-b \text{ es múltiplo de 4 y } b-a \text{ es múltiplo de 4} \\ &\Rightarrow \underbrace{(a-b)+(b-c)}_{a-c} \text{ es múltiplo de 4} \end{aligned}$$

pues suma de múltiplos de 4 resulta en un múltiplo de 4.

□

TAREA 21. *¿Cuáles de las siguientes relaciones en* $\{0,1,2,3\}$ *son de equivalencia? ¿Qué propiedades faltan para que lo sean?*

(1) $\{(0,0),(1,1),(2,2),(3,3)\}$
(2) $\{(0,0),(0,2),(2,2),(2,3),(3,2),(3,3)\}$
(3) $\{(0,0),(1,1),(1,2),(2,1),(2,2),(3,3)\}$
(4) $\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,2),(3,3)\}$

TAREA 22. *Lo mismo que el anterior para las siguientes relaciones entre el conjunto de personas.*

(1) $\{(a,b) \mid a$ *y* b *tienen la misma edad*$\}$
(2) $aRb \Leftrightarrow a$ *y* b *tienen los mismos padres.*
(3) $aRb \Leftrightarrow a$ *y* b *tienen un padre en común.*
(4) $aRb \Leftrightarrow a$ *y* b *hablan un mismo idioma.*

DEFINICIÓN 51. *Sea* $n \in \mathbb{Z}$, $n \neq 0$. *Se define la relación de* **congruencia módulo** n *en* $\mathbb{Z}$ *como*

$$a \equiv b \pmod{n} \Leftrightarrow n|(a-b)$$

EJEMPLO 52.

(1) $5 \equiv 1 \pmod 4$ pues $4|(5-1)$.
(2) $21 \equiv 0 \pmod 7$ pues $7|(21-0)$.

(3) $28 \equiv 8 \pmod 5$ pues $5|(28-8)$

TAREA 23. *Demuestre que la relación de congruencia módulo n es de equivalencia.*

TAREA 24. *Determinanr el número de relaciones de equivalencia distintas que puede haber en un conjunto de tres elementos enumerándolas todas.*

TAREA 25. *Sea R la relación en $\mathbb{Z} \times \mathbb{Z}$ definida por*

$$(a,b)R(c,d) \Leftrightarrow ad = bc.$$

Demostrar que R es de equivalencia.

DEFINICIÓN 53. *Sea R una relación de equivalencia sobre A. Si $a \in A$, la* **clase de equivalencia de** *a es*

$$\bar{a} = [a] = \{x \in A \,|\, xRa\}$$

El elemento a se llama **representante** *de la clase de equivalencia.*

EJEMPLO 54. Sea R la relación de equivancia en $\mathbb{Z}$ dada por $aRb \Leftrightarrow a = b$ o $a = -b$. Entonces

$$[1] = \{x \in \mathbb{Z} \,|\, xR1\}$$

pero $xR1 \Leftrightarrow x = 1$ o $x = -1$. Así

$$\begin{aligned}[1] &= \{1, -1\} \\ [2] &= \{2, -2\} \\ [0] &= \{0\}\end{aligned}$$

EJEMPLO 55. Consideremos la relación en $\mathbb{Z}$ de congruencia módulo 4:

$$a \equiv b \pmod 4 \Leftrightarrow 4|(a-b)$$

entonces

$$[0] = \{x \in \mathbb{Z} \,|\, x \equiv 0 \pmod 4\}$$

pero

$$\begin{aligned}x \equiv 0 \pmod 4 &\Leftrightarrow 4|(x-0) = x \\ &\Leftrightarrow x = 4k \text{ para algún } k \in \mathbb{Z}.\end{aligned}$$

esto es

$$\begin{aligned}[0] =& \{x \in \mathbb{Z} \,|\, \text{existe } k \in \mathbb{Z} \text{ con } x = 4k\} \\ =& \{\ldots, -4, 0, 4, 8, 12, \ldots\}\end{aligned}$$

Similarmente

$$[1] = \{x \in \mathbb{Z} \,|\, x \equiv 1 \pmod 4\}$$

pero

$$\begin{aligned}x \equiv 1 \pmod 4 &\Leftrightarrow x - 1 = 4k \text{ para algún } k \in \mathbb{Z}; \\ &\quad x = 4k + 1 \text{ para algún } k \in \mathbb{Z}\end{aligned}$$

i.e.,

$$\begin{aligned}[1] &= \{x \in \mathbb{Z} \,|\, x = 4k+1 \text{ para algún } k \in \mathbb{Z}\} \\ &= \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\}\end{aligned}$$

y de forma análoga

$$[2] = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$$

$$[3] = \{\ldots, -4, -1, 3, 7, 11, 15, 19, \ldots\}$$

$$[4] = \{\ldots, -4, 0, 4, 8, 12, \ldots\} = [0]$$

y $[-1] = [3]$, $[-2] = [2]$, etc.

Ejemplo 56. En $\mathbb{Q}$ se define la relación

$$xRy \Leftrightarrow \exists h \in \mathbb{Z}, \quad x = \frac{3y+h}{3}.$$

(1) Demostrar que R es de equivalencia.
(2) Hallar la clase de $2/3$.

Sol.

(1) (a) Reflexiva: notemos que

$$xRx \Leftrightarrow x = \frac{3x+h}{3} \Leftrightarrow h = 0$$

luego $\forall x \in \mathbb{Q}$, xRx pues existe $h = 0 \in \mathbb{Z}$ tal que $x = \frac{3x+0}{3}$

(b) Simétrica:

$$\begin{aligned} xRy &\Rightarrow \exists h \in \mathbb{Z}, \quad x = \frac{3y+h}{3} \\ &\Rightarrow 3x = 3y + h \\ &\Rightarrow \frac{3x-h}{3} = y \\ &\Rightarrow y = \frac{3x+(-h)}{3} \text{ con } -h \in \mathbb{Z} \\ &\Rightarrow yRx \end{aligned}$$

(c) Transitiva: si xRy y yRz, por demostrar xRz. Tenemos

$$x = \frac{3y+h_1}{3} \text{ y } y = \frac{3z+h_2}{3}$$

sustituyendo y dado por la segunda ecuación en la primera:

$$x = \frac{3\frac{3z+h_2}{3} + h_1}{3} = \frac{(3z+h_2)+h_1}{3}$$

entonces

$$x = \frac{3z+(h_1+h_2)}{3}$$

con $h_1 + h_2 \in \mathbb{Z}$. Lo que implica

$$xRz$$

(2) Por definición de clase

$$[2/3] = \{x \in \mathbb{Q} \mid xR(2/3)\}$$

pero

$$xR(2/3) \Leftrightarrow x = \frac{3(2/3)+h}{3} = \frac{2+h}{3}$$

con $2+h \in Z$. Pero $h \in \mathbb{Z} \Leftrightarrow 2+h \in \mathbb{Z}$; por lo que podemos renombrar $h' = h+2$ y escribir

$$\begin{aligned}[2/3] &= \{z \in \mathbb{Q} \mid z = h'/3 \text{ con } h' \in \mathbb{Z}\} \\ &= \{\ldots, -3/3, -2/3, -1/3, 0, 1/3, 2/3, 3/3, 4/3, \ldots\}\end{aligned}$$

□

PROPIEDAD 4. *Sea R una relaciń de equivalencia sobre A y $a, b \in A$ cualesquiera.*

$$[a] = [b] \Leftrightarrow aRb$$

DEM.

($\Rightarrow$) Supongamos que $[a] = [b]$. Por la propiedad reflexiva $a \in [a] = [b]$ luego $a \in [b] = \{x \in A \mid xRa\}$ entoncesaRb.

($\Leftarrow$) Supongamos aRb. Por demostrar $[a] = [b]$, lo cual haremos por contenciones:

(1) $[a] \subseteq [b]$: si $z \in [a]$ entonces zRa, pero como por hipótesis aRb entonces zRb por transitiva. Luego $z \in [b]$.

(2) $[b] \subseteq [a]$: si $z \in [b]$ entonces zRb, pero bRa por simétrica, luego, por transitiva, zRa; lo que implica $z \in [a]$

□

PROPIEDAD 5. *Sea R una relación de equivalencia sobre un conjunto A, entonces las clases de equivalencia constituyen una partición de A. Esto es:*

(1) $\bigcup_{a \in A} [a] = A$

(2) *si* $[a] \neq [b]$ *entonces* $[a] \cap [b] = \varnothing$.

DEMOSTRACIÓN.

(1) Por contenciones:

$\subseteq$: Como cada clase se forma con conjunto universal A, tenemos que $(\forall a \in A)\, [a] \subseteq A$, luego

$$\bigcup_{a \in A} [a] \subseteq A.$$

$\supseteq$: si $z \in A$ entonces zRz por reflexiva, luego $z \in [z]$ por lo que

$$z \in \bigcup_{a \in A} [a]$$

$$\therefore A \subseteq \bigcup_{a \in A} [a]$$

$$\therefore \bigcup_{a \in A} [a] = A$$

(2) Por contrarrecíproca, tal propiedad es equivalente a

$$[a] \cap [b] \neq \varnothing \Rightarrow [a] = [b]$$

demostraremos ésta.

Si $[a] \cap [b] \neq \varnothing$ entonces $\exists z \in [a] \cap [b]$, esto es $z \in [a]$ y $z \in [b]$; por lo que zRa y zRb. Luego por simétrica aRz y zRb y entonces, por transitiva aRb lo que implica $[a] = [b]$.

□

Ejemplo 57. Consideremos la relación de equivalencia llamada congruencia módulo 4 sobre $\mathbb{Z}$. Entonces

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$$

y

$$\begin{array}{ll} [0] \cap [1] = \varnothing & [1] \cap [2] = \varnothing \\ [0] \cap [2] = \varnothing & [1] \cap [3] = \varnothing \\ [0] \cap [3] = \varnothing & [2] \cap [3] = \varnothing \end{array}$$

Definición 58. *Si R es una relación de equivalencia sobre A entonces*

$$A/R = \{[a] \,|\, a \in A\}$$

se llama **conjunto cociente**.

Ejemplo 59. En el ejemplo inmediato anterior,

$$\mathbb{Z}/ \equiv = \{[0], [1], [2], [3]\}$$

Ejemplo 60. *Si consideramos ahora la congruencia módulo 2 en los enteros obtenemos*

$$\mathbb{Z}/ \equiv = \{[0], [1]\}$$

donde $[1]$ *es el conjunto de enteros impares y* $[0]$ *es el conjunto de enteros pares.*

Ejemplo 61. Sea la relación en $A = \{1, 2, 3, 4\}$:

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

S es una relación de equivalencia. Entonces el conjunto cociente est'a formado por

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

luego,

$$A/S = \{[1], [2], [3]\} = \{\{1\}, \{2\}, \{3, 4\}\}$$

Ejemplo 62. Sea $X = \{a, b, c\}$. Definimos una relación de equivalencia en el conjunto potencia 2^X mediante $(A, B \in 2^X)$:

$$ARB \Leftrightarrow A \cap \{a, c\} = B \cap \{a, c\}.$$

Evidentemente R es de equivalencia. Calculemos el conjunto cociente $2^X/R$. Primero recordemos que

$$2^X = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

entonces, por definción de clase

$$\begin{aligned}[\varnothing] &= \{A \subseteq X \mid A \cap \{a,c\} = \underbrace{\varnothing \cap \{a,c\}}_{\varnothing}\} \\ &= \{A \subseteq X \mid A \cap \{a,c\} = \varnothing\} \\ &= \{\varnothing, \{b\}\}\end{aligned}$$

$$\begin{aligned}[\{a\}] &= \{A \subseteq X \mid A \cap \{a,c\} = \underbrace{\{a\} \cap \{a,c\}}_{\{a\}}\} \\ &= \{A \subseteq X \mid A \cap \{a,c\} = \{a\}\} \\ &= \{\{a\}, \{a,b\}\}\end{aligned}$$

$$[\{b\}] = [\{a\}]$$

pues $\{b\}R\{a\}$;

$$\begin{aligned}[\{c\}] &= \{A \subseteq X \mid A \cap \{a,c\} = \{c\}\} \\ &= \{\{c\}, \{b,c\}\}\end{aligned}$$

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

pues $\{a,b\}R\{a\}$.

$$\begin{aligned}[\{a,c\}] &= \{A \subseteq X \mid A \cap \{a,c\} = \{a,c\}\} \\ &\quad \{\{a,c\}, \{a,b,c\}\}.\end{aligned}$$

Finalmente

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

pues $\{b,c\}R\{c\}$ y $\{a,b,c\}R\{a,c\}$. Por tanto, el conjunto cociente es

$$2^X/R = \{[\varnothing], [\{a\}], [\{c\}], [\{a,c\}]\}$$

DEFINICIÓN 63. *Sea $\equiv$ la relación de congruencia módulo n. El conjunto de* **enteros gaussianos** *se denota con $\mathbb{Z}_n$ o $\mathbb{Z}/n\mathbb{Z}$ y este es el cociente $\mathbb{Z}/\equiv$,*

$$\mathbb{Z}_n = \mathbb{Z}/\equiv = \{[0], [1], [2], \ldots, [n]\}$$

Resulta que el conjunto cociente $\mathbb{Z}_n$ tiene una estructura aritmética definida por las siguientes operaciones:

$$[a] + [b] = [a+b], \quad [a][b] = [ab].$$

Por ejemplo, en $\mathbb{Z}_3$

$$[2][2] = [2 * 2] = [4] = [1]$$

pues 4 y 1 están relacionados: $4 \equiv 1 \pmod 3$. Y similarmente

$$[2] + [3] = [5] = [2]$$

pues $5 \equiv 2 \pmod 3$. De esta forma tenemos las siguientes tablas de suma y producto en $\mathbb{Z}_3$.

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$*$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

La aritmética de $\mathbb{Z}_n$ tiene uso en criptografía.

DEFINICIÓN 64. *Una partición de un conjunto B es una familia A_i, $i \in I$ de subconjuntos de B tales que*

(1) $B = \bigcup_{i\in I} A_i$
(2) $(\forall i \in I)(\forall j \in I)(B_i \cap B_j \neq \varnothing \Rightarrow B_i = B_j)$

Sabemos que una relación de equivalencia induce una partición, siendo la familia de tal partición las clases de equivalencia. Reciprocamente: una partición induce una relación de equivalencia.

PROPIEDAD 6. *Si A_i, $i \in I$, forman una partición de un conjunto B entonces esta induce una relación de equivalencia:*

$$aRb \Leftrightarrow \exists i \in I \text{ tal que } a \in A_i \wedge b \in A_i$$

DEM. Probaremos que R es relación de equivalencia:

(1) Reflexiva: si $a \in B$ entonces $a \in \bigcup_{i\in I} A_i$, luego existe $j \in I$ tal que $a \in A_j$. Así $a \in A_j$ y $a \in A_j$, luego aRa.
(2) Simétrica: si aRb entonces existe $i \in I$ tal que $a \in A_i$ y $b \in A_i$; luego $b \in A_i$ y $a \in A_i$ entonces bRa.
(3) Transitiva: si aRb y bRc entonces existe $i \in I$ tal que $a, b \in A_i$ y existe $j \in I$ tal que $b, c \in A_j$. Luego $b \in A_i \cap A_j$, esto es $A_i \cap A_j \neq \varnothing$ lo que implica $A_i = A_j$. Entonces $a \in A_i$ y también $c \in A_i$. Por lo tanto aRc.

□

EJEMPLO 65. La población de la ciudad de Puebla está dividida por colonias; luego la siguiente es una relación de equivalencia entre la población de Puebla:

$$aRb \Leftrightarrow a \text{ y } b \text{ vivien en la misma colonia}$$

y la ciudad queda dividida en clases:

$$P = \underbrace{[\text{José Doger}]}_{\text{Bosques de la Calera}} \cup \underbrace{[\text{ yo }]}_{\text{La Vista}} \cup \underbrace{[\text{E. Aguera}]}_{\text{Valsequillo}} \cup \ldots$$

EJEMPLO 66. Sea $B = \{a, b, c, d, e\}$. Una partición de B viene dada por

$$B = \underbrace{\{a\}}_{A_1} \cup \underbrace{\{b, c\}}_{A_2} \cup \underbrace{\{d, e\}}_{A_3}$$

Luego una relación de equivalencia en A es

$$xSy \Leftrightarrow \text{existe } i \text{ con } 1 \leq i \leq 3 \text{ tal que } x \in A_i \text{ y } y \in A_i$$

luego $[a] = \{a\}$, $[b] = \{b, c\}$ y $[d] = \{d, e\}$ y el conjunto cociente es

$$A/S = \{\underbrace{[a]}_{A_1}, \underbrace{[b]}_{A_2}, \underbrace{[d]}_{A_3}\}$$

EJEMPLO 67. En $\mathbb{Z}_6$ (la relación es $x \equiv y \pmod 6 \Leftrightarrow x - y$ es múltiplo de 6con $x, y \in \mathbb{Z}$) tenemos que

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

y las clases forman una partición de $\mathbb{Z}$:

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5]$$

TAREA 26. *Sea A u conjunto no vacío con conjunto universal E. En 2^X se define la relación R como*

$$XRY \Leftrightarrow X \cap A \subseteq Y \cap A$$

¿Qué propiedades verifica R? ¿Es relación de equivalencia? ¿Y si en la difinición se cambia $\subseteq$ por $=$? En éste último caso calcular $[\varnothing]$ y $[E]$.

TAREA 27.

(1) *Considere el conjunto de enteros gaussianos $\mathbb{Z}_5$ y la clase $[3]$. Encontrar una clase $[x]$ tal que $[3x] = [1]$.*
(2) *¿Es posible repetir el ejercicio anterior con $\mathbb{Z}_6$?*

TAREA 28. *Describir $[4] \in \mathbb{Z}_n$ si*

(1) $n = 2$
(2) $n = 3$
(3) $n = 6$
(4) $n = 8$.

TAREA 29. *Sea R la relación de equivalencia en $\mathbb{Z} \times \mathbb{Z}$ definida por*

$$(a, b)R(c, d) \Leftrightarrow ad = bc.$$

Describir $[(1, 2)]$.

TAREA 30. *¿Cuáles de estas colecciones de subconjuntos son particiones de $\{1, 2, 3, 4, 5, 6\}$?*

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

TAREA 31. *¿Cuáles de estas colecciones de subconjuntos son particiones del conjunto de cadenas de bits de longitud 8?*

(1) *El conjunto de cadenas de bits que empiezan por 1, el conjunto de cadenas de bits que empiezan por 00 y el conjunto de cadenas de bits que empiezan por 01.*
(2) *El conjunto de cadenas de bits que contienen la cadena 00, el conjunto de cadenas de bits que contienen la cadena 10 y el conjunto de cadenas de bits que contienen a la cadena 11.*
(3) *El conjunto de cadenas de bits que terminan en 00, el conjunto de cadenas de bits que que terminan en 01, el conjunto de cadenas de bits que terminan en 10 y el conjunto de cadenas de bits que terminan en 11.*
(4) *El conjunto de cadenas de bits que terminan en 111, el conjunto de cadenas de bits que terminan en 011 y el conjunto de cadenas de bits que terminan en 00.*
(5) *El conjunto de cadenas de bits que tienen $3k$ unos, donde k es un entero no negativo, el conjunto de cadenas de bits que tienen $3k+1$ unos, donde k es un entero no negativo, el conjunto de cadenas de bits que tienen $3k+2$ unos, donde k es un entero no negativo.*

TAREA 32. *Enumerar los pares ordenados de las relaciones de equivalencia producidas por las siguientes particiones de $\{0, 1, 2, 3, 4, 5\}$:*

(1) $\{0\}, \{1, 2\}, \{3, 4, 5\}$
(2) $\{0, 1\}, \{2, 3\}, \{4, 5\}$
(3) $\{0, 1, 2\}, \{3, 4, 5\}$
(4) $\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}$

3. Algunas aplicaciones de $\mathbb{Z}_n$

3.1. Protocolo Diffie-Hellman para intercambio de claves secretas. Sabemos que los enteros gaussianos $\mathbb{Z}_n$ tienen una aritmética. Entonces, en particular se pueden calcular potencias de sus elementos: $[a]^0 = 1$ y si $n > 0$

$$[a]^n = \underbrace{[a] \dots [a]}_{n-\text{veces}}.$$

Por ejemplo, en $\mathbb{Z}_3$,

$$[2]^4 = [2]^2[2]^2 = [4][4] = [1][1] = [1].$$

Luego entonces se puede calcular logaritmos, pues los logaritmos no son mas que potencias:

$$\log_b(a) = x \Leftrightarrow b^x = a.$$

Por ejemplo, de nuevo en $\mathbb{Z}_3$: podemos poner $\log_{[2]}[1] = 4$ pues $[2]^4 = [1]$. Nótese que también $[2]^8 = [1]$ por lo que, para evitar conflictos ponemos

$$\log_{[b]}[a] = x \Leftrightarrow x = \min\{x \in \mathbb{N} \,|\, x > 0 \text{ y } [b]^x = [a]\}.$$

Esta clase de logaritmos, si se calcula en $\mathbb{Z}_n$, se llama *logaritmo discreto módulo* n.

Una de las ideas detrás del protocolo Diffie-Hellman es la creencia de que calcular logaritmos discretos es "difícil".

Necesitamos de la siguiente definición.

DEFINICIÓN 68. *Sea n entero positivo. Una raíz primitiva módulo n es una clase $[\alpha]$ en $\mathbb{Z}_n$ tal que*

$$\{[\alpha]^0, [\alpha]^1, \dots, [\alpha]^{p-2}\} = \{[1], [2], \dots, [p-1]\} = \mathbb{Z}_n \backslash \{[0]\}.$$

EJEMPLO 69. La clase $[2]$ es raíz primitiva módulo 13 porque en $\mathbb{Z}_{13}$:

$$[2]^0 = [1], [2]^1 = [2], [2]^2 = [4], [2]^3 = [8], [2]^4 = [3], [2]^5 = [6], [2]^6 = [12]$$
$$[2]^7 = [11], [2]^8 = [9], [2]^9 = [5], [2]^{10} = [10], [2]^{11} = [7], [2]^{12} = [1], [2]^{13} = [2].$$

Pero la clase $[3]$ no es raíz primitiva módulo 13 porque

$$\{[3]^0, \dots, [3]^{p-1}\} = \{[1], [3], [9]\}.$$

Supóngase que se tienen dos partes A y B. Usualmente a éstas se les llama Alicia y Beto (Alice, Bob).

Problema: Entre A y B quieren intercambiar claves secretas por un canal inseguro.

El canal inseguro podría ser una línea telefónica o bien Internet.

Solución: El protocolo Diffie-Hellman que consiste de los siguientes pasos:

(1) Entre A y B eligen un número primo p y $[\alpha]$ una raíz primitiva módulo p. Tal información la intercambian por el canal inseguro.
(2) A elige un número entero x al azar tal que $1 < x < p - 1$. Tal número A lo mantiene en secreto.
(3) B eleige un número entero y al azar tal que $1 < y < p - 1$. Tal número B lo mantiene en secreto.

(4) A calcula $[\alpha]^x$ y hace reducciones módulo p (i.e., en $\mathbb{Z}_p$) para obtener a tal que
$$[\alpha]^x = [a]$$
con $1 \leq a \leq p-1$. El número a que A obtiene se lo envia a B por el canal inseguro.
(5) B calcula $[\alpha]^y$ y hace reducciones módulo p (i.e., en $\mathbb{Z}_p$) para obtener b tal que
$$[\alpha]^y = [b]$$
con $1 \leq b \leq p-1$. El número b que B obtiene se lo envia a A por el canal inseguro.
(6) Con el número b que A recibió, la misma A calcula $[b]^x$ y hace reducciones en $\mathbb{Z}_p$ para calcular r_A entero tal que
$$[b]^x = [r_A]$$
y $1 \leq r_A \leq p-1$.
(7) Con el número a que B recibió, el mismo B calcula $[a]^y$ y hace reducciones en $\mathbb{Z}_p$ para calcular r_B entero tal que
$$[a]^y = [r_B]$$
y $1 \leq r_B \leq p-1$.
(8) Fin: la clave secreta intercambiada es r_A para Alicia y r_B para Beto, pues resulta que $r_A = r_B$.

Que al final del protocolo $r_A = r_B$ es gracias al siguiente teorema

TEOREMA 6.
$$r_A = r_B$$

DEM. Tenemos, por definición que
$$\begin{aligned}[r_A] &= [b]^x \\ &= ([\alpha]^y)^x \\ &= [\alpha]^{yx}.\end{aligned}$$

Similarmente
$$\begin{aligned}[r_B] &= [a]^y \\ &= ([\alpha]^x)^y \\ &= [\alpha]^{xy}.\end{aligned}$$

Luego, como $xy = yx$, se sigue que $[r_A] = [r_B]$. Luego r_A y r_B están relacionados, esto es, $r_A \equiv r_B \pmod{p}$, lo que implica que $p|(r_A - r_B)$. Es decir $r_A - r_B$ es múltiplo de p, entonces también $|r_A - r_B|$ es múltiplo de p. Pero como $0 \leq |r_A - r_B| \leq p-1$ entonces se sigue que $|r_A - r_B| = 0$, es decir $r_A = r_B$. □

EJEMPLO 70. Alicia y Beto desean intercambiar una clave secreta por e-mail.
(1) Para esto eligen al primo 47 y raíz primitiva [5] módulo 47. Intercambian esta información por e-mail, el cual es un canal inseguro. Así que una tercera parte E (Eva) conoce esta información.
(2) Alicia elige un número x al azar con $1 < x < 47$, digamos $x = 30$ y lo mantiene en secreto.

(3) Beto elige un número y al azar con $1 < y < 47$, digamos $y = 4$, y lo mantiene en secreto.
(4) Alicia calcula $[5]^x = [5]^{30}$ en $\mathbb{Z}_{13}$: $[5]^{30} = [36]$. Alicia envia el número 36 a Beto por e-mail. Nótese que E se entera de este número.
(5) Beto calcula $[5]^y = [5]^4$ en $\mathbb{Z}_{13}$: $[5]^4 = [14]$ y envia 14 por e-mail a Alicia. De nuevo E se entera de éste número.
(6) Con el número 14 que Alicia recibió de Beto ella calcula $[14]^x = [14]^30$ en $\mathbb{Z}_{13}$: $[14]^{30} = [24]$.
(7) Con el número 36 que Beto recibió de Alicia, el calcula $[36]^y = [36]^4$ en $\mathbb{Z}_{13}$: $[36]^4 = [24]$.
(8) Fin: Alicia y Beto tienen una misma clave secreta: 24, de la cual E no se enteró.

4. Una aplicación de digrafos: GooglePage Rank

Idea: desplegar los resultados de búsquedas según su importancia.
Algoritmo de Google:

- Definir la importancia de las páginas web.
- Calcular la importancia de cada página.

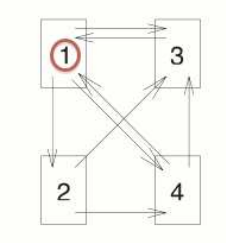
Considerar el grafo de internet:

- Vértices: páginas web;
- Aristas: $a \to b$ si hay un hyperlink de a apuntando hacia b y $a \neq b$.

DEFINICIÓN 71. *Sea x_k la importancia (no normalizada) del vértice (página) k y L_k el conjunto de vértices que inciden en k. Entonces*

$$x_k = \sum_{j \in L_k} \frac{1}{\delta^-(j)} x_j$$

EJEMPLO 72. Supongamos que el grafo de internet es:



entonces

$$x_1 = \frac{1}{1}x_3 + \frac{1}{2}x_4, \quad x_2 = \frac{1}{3}x_1$$

En total:

$$\begin{array}{rcccccccc} x_1 & = & & & & & \frac{1}{1}x_3 & + & \frac{1}{2}x_4 \\ x_2 & = & \frac{1}{3}x_1 & & & & & & \\ x_3 & = & \frac{1}{3}x_1 & + & \frac{1}{2}x_2 & & & + & \frac{1}{2}x_4 \\ x_4 & = & \frac{1}{3}x_1 & + & \frac{1}{2}x_2 & & & & \end{array}$$

i.e.,

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 1/2 \\ 1/3 & 0 & 0 & 0 \\ 1/3 & 1/2 & 0 & 1/2 \\ 1/3 & 1/2 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

Se tiene un sistema de ecuaciones del tipo

$$AX = \lambda X$$

en tal caso, el vector X se llama *eigenvector* del *eigenvalor* λ.

Despejando

$$(A - \lambda I)X = 0$$

donde I es matriz identidad. En nuestro ejemplo:

$$\begin{pmatrix} -1 & 0 & 1 & 1/2 \\ 1/3 & -1 & 0 & 0 \\ 1/3 & 1/2 & -1 & 1/2 \\ 1/3 & 1/2 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

y por Gauss-Jordan:

$$x_1 = 2r, x_2 = \frac{2}{3}r, x_3 = \frac{3}{2}r, x_4 = r$$

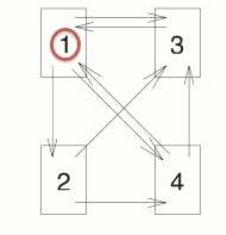
con $r \in \mathbb{R}$ variable libre.

DEFINICIÓN 73. *La importancia normalizada x'_k del vertice k es*

$$x'_k = \frac{x_k}{\sum_j x_j}$$

Por ejemplo, las importancias normalizadas, en nuestro ejemplo, son:

- $x'_1 = \frac{x_1}{x_1+x_2+x_3+x_4} = \frac{2r}{2r+(2/3)r+(3/2)r+r} = 12/31 \approx .3870967741935484$
- $x'_2 = \frac{x_2}{x_1+x_2+x_3+x_4} = 4/31 \approx .1290322580645161$
- $x'_3 = \frac{x_3}{x_1+x_2+x_3+x_4} = 9/31 \approx .2903225806451613$
- $x'_4 = \frac{x_4}{x_1+x_2+x_3+x_4} = 6/31 \approx .1935483870967742$



Google:

- 1
- 3
- 4
- 2

Aclaración: Google no usa el método de Gauss-Jordan, sino el *método de la potencia* que se basa en el teorema de Perron-Frobenius.

5. Relaciones de Orden. Retículos

DEFINICIÓN 74.

(1) *Una relación R sobre el conjunto A se dice de* **orden** *si R es reflexiva, antisimétrica y transitiva. En tal caso R se escribe como $\leq$ y al par $(A, \leq)$ se le llama* **conjunto (parcialmente) ordenado**.

(2) *Si* $(A, \leq)$ *es conjunto parcialmente ordenado como en el inciso anterior y* $a, b \in A$*, entonces*

$$\begin{aligned} a < b &\Leftrightarrow a \leq b \wedge a \neq b \\ &\Leftrightarrow aRb \wedge a \neq b \end{aligned}$$

Ejemplo 75. La relación S en $\mathbb{R}$ dada por

$$xSy \Leftrightarrow x \leq y$$

es un orden pues

(1) reflexiva: $(\forall x \in \mathbb{R})$, xSx pues $x \leq x$
(2) antisimétrica: si xSy y ySx entonces $x \leq y$ y $y \leq x$ entonces $x = y$.
(3) transitiva: si xSy y ySz entonces $x \leq y$ y $z \leq z$ luego $x \leq z$.

Ejemplo 76. Sea E un conjunto. Se define la relación en 2^E por

$$ARB \Leftrightarrow A \subseteq B$$

R es un orden pues:

(1) reflexiva: $\forall A \subset E$, $A \subseteq A$
(2) antisimétrica: si ARB y BRA entonces $A \subseteq B$ y $B \subseteq A$ entonces $A = B$ según la definición de igualdad de conjuntos.
(3) transitiva: si ARB y BRC entonces $A \subseteq B$ y $B \subset C$ entonces, por porpiedad anterior $A \subseteq C$, i.e., ARC.

Definición 77.

$$\mathbb{N}^* = \mathbb{N} \backslash \{0\}$$

Ejemplo 78. En $\mathbb{N}^*$ se define la relación

$$aSb \Leftrightarrow a|b$$

entonces S es un orden:

(1) reflexiva: $\forall a \in \mathbb{N}^*$ $a|a$ luego aSa.
(2) antisimétrica:

$$\begin{aligned} aSb \wedge bSa &\Rightarrow a|b \wedge b|a \\ &\Rightarrow b \text{ es múltiplo de } a \text{ y } a \text{ lo es de } b \\ &\Rightarrow b = k_1 a \wedge a = k_2 b \text{ para ciertos } k_1, k_2 \in \mathbb{Z} \\ &\Rightarrow b = k_1 k_2 b \text{ sustituyendo } a \text{ en la primer ecuación} \\ &\Rightarrow k_1 k_2 = 1 \\ &\Rightarrow k_1 = 1 = k_2 \vee k_1 = -1 = k_2 \end{aligned}$$

si ocurriera lo segundo entonces $a = -b < 0$ lo cual es absurdo pues $a \in \mathbb{N}^*$. Por tanto el segundo caso es imposible. Luego $k_1 = 1 = k_2$ lo que implica $a = b$.

(3) transitiva:

$$\begin{aligned} aSb \wedge bSc &\Rightarrow a|b \wedge b|c \\ &\Rightarrow b = k_1 a \wedge c = k_2 b \text{ para ciertos } k_1, k_2 \in \mathbb{Z} \\ &\Rightarrow \text{ sustituyendo } b \text{ en la segunda ecuación:} c = k_2 k_1 a \\ &\Rightarrow c = k_3 a \text{ con } k_3 = k_2 k_1 \in \mathbb{Z} \\ &\Rightarrow a|c \\ &\Rightarrow aSc \end{aligned}$$

TAREA 33. *¿Cuáles de los siguientes conjuntos son parcialmente ordenados? Demuestre.*

(1) $(\mathbb{Z}, =)$
(2) $(\mathbb{Z}, \geq)$
(3) $(\mathbb{Z}, \neq)$
(4) $(\mathbb{Z}, \not|)$

DEFINICIÓN 79. *Sea $(A, \leq)$ un conjunto parcialmente ordenado. Se dice que $(A, \leq)$ está* **totalmente ordenado** *o* **orden lineal** *si*

$$(\forall x \in A)(\forall y \in A)(x \leq y \vee y \leq z)$$

EJEMPLO 80. $(\mathbb{R}, \leq)$ es totalmente ordenado.

EJEMPLO 81. $(\mathbb{N}^*, |)$ no es totalmente ordenado pues existen $2, 3 \in \mathbb{N}^*$ tales que

$$2 \nmid 3 \text{ y } 3 \nmid 2$$

EJEMPLO 82. Si $X = \{a, b, c\}$, entonces $(2^X, \subseteq)$ no es totalmente ordenado pues

$$\{a\} \not\subseteq \{b\} \text{ ni } \{b\} \not\subseteq \{a\}$$

TAREA 34. *Encontrar dos elementos no comparables en*

(1) $(2^{\{0,1,2\}}, \subseteq)$
(2) $(\{1, 2, 3, 4, 6, 8\}, |)$

DEFINICIÓN 83. *Sea $(A, \leq)$ parcialmente ordenado y $B \subseteq A$. Los siguientes se llaman* **elementos notables***:*

(1) *Un $k \in A$ se dice* **cota superior** *de B si*

$$(\forall b \in B)(b \leq k)$$

(2) *Un $\ell \in A$ se dice* **cota inferior** *de B si*

$$(\forall b \in B)(\ell \leq b)$$

(3) *La más pequeña de las cotas inferiores M de B se llama* **supremo** *de B:*

$$(\forall k \text{ cota superior de } B)(k \leq M).$$

Se pone

$$M = \sup B$$

Si el supremo M pertenece a B entonces M se llama **máximo** *de B.*

(4) *La más grande de las cotas inferiores m de B se llama* **ínfimo** *de B:*

$$(\forall \ell \text{ cota inferior de } B)(\ell \leq m).$$

Se pone

$$m = \inf B.$$

Si el ínfimo de B pertenece a B éste se llama **mínimo** *de B.*

(5) *Un elemento $c \in A$ se dice* **maximal** *de A si*

$$(\forall a \in A)(c \leq a \Rightarrow c = a)$$

(6) *Un elemento $c \in A$ se dice* **minimal** *de A si*

$$(\forall a \in A)(a \leq c \Rightarrow c = a)$$

EJEMPLO 84. Sea $E = \{a, b, c\}$. Hallaremos elementos notables de $(2, \subseteq)$. Tenemos que

$$2^X = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

luego tenemos que

$$\varnothing \subseteq \{a\} \subseteq \{a, b\} \subseteq \{a, b, c\}$$

pero también

$$\varnothing \subset \{b\} \subseteq \{b, c\} \subseteq \{a, b, c\}$$

etcétera. Ponemos toda esta información en un diagrama:(ver Figura 1). En tal

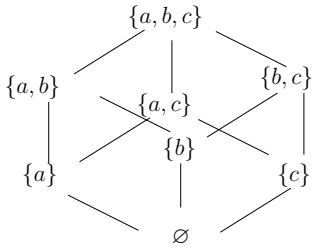


FIGURA 1. Diagrama de Hasse de $(2^{\{a,b,c\}}, \subseteq)$

diagrama, una raya de abajo hacia arriba significa $\subseteq$. Luego

- $\{a, b, c\}$ es cota superior de $\{\varnothing, \{a\}, \{b, c\}\}$
- $\varnothing$ es cota inferior de $\{\{a\}, \{b\}, \{b, c\}, \{a, b, c\}\}$.

De hecho,

- $\{a, b, c\}$ es cota superior de 2^E
- $\varnothing$ es cota inferior de 2^E
- $\{a, b, c\}$ es máximo de 2^E
- $\varnothing$ es mínimo de 2^E

Mientras que

- $\{a\}$ es minimal de la cadena $\{a\} \subseteq \{a, c\} \subseteq \{a, b, c\}$
- $\{a, b, c\}$ es maximal de la cadena $\{a\} \subseteq \{a, c\} \subseteq \{a, b, c\}$

En un diagrama de Hasse se pone:

para indicar que $x \leq y$; pero se debe de cumplir que

$$\nexists\, z,\ x \leq z \leq y \text{ con } z \neq x, z \neq y.$$

EJEMPLO 85. Sea $A = \{2, 4, 5, 10, 12, 20, 25\}$. ¿Qué elementos en $(A, |)$ son maximales y cuáles son minimales? ¿Cuáles son cotas superiores, supremo, ínfimo?

SOL. Calculemos el diagrama de Hasse de $(A, |)$: □

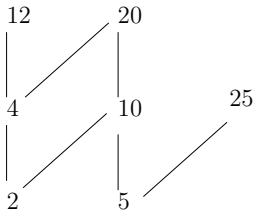


FIGURA 2. El diagrama de Hasse de $(\{2, 4, 5, 10, 20, 25\}, |)$.

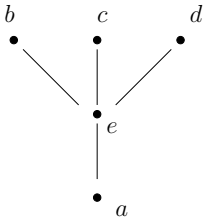
Luego

- $12, 20, 25$ son maximales
- $2, 5$ son minimales

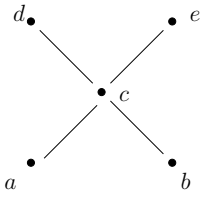
y tal conjunto no tiene cotas superiores ni inferiores, en consecuencia no hay máximos ni mínimos.

EJEMPLO 86. Calcular los máximos y mínimos de los conjuntos parcialmente ordenados representados por su diagrama de Hasse siguientes:

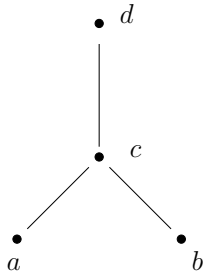
(1)



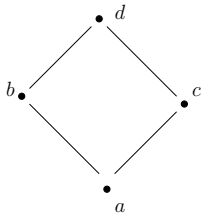
(2)



(3)



(4)



Sol.

(1) No hay cotas superiores, luego no hay máximo; a es cota inferior y ésta es la mínima cota inferior (de hecho, la única), por lo que a es el supremo; además a está en el conjunto. Por lo tanto a es mínimo.
(2) No hay cotas inferiores, ni superiores; así no hay ni máximos ni mínimos.
(3) El elemento d es cota superior y d es la más pequeña de éstas, luego d es máximo; no hay cotas inferiores, luego no hay mínimo.
(4) d es máximo, a es mínimo.

□

Ejemplo 87. ¿Hay máximos o mínimos en el conjunto parcialmente ordenado $(\mathbb{N}^*, |)$?

Sol. Tenemos que

$$(\forall n \in \mathbb{N}^*)(1|n)$$

luego 1 es cota inferior. También es la mayor de las cotas inferiores: pues si m es otra cota inferior entonces se tiene que cumplir

$$(\forall n \in \mathbb{N}^*)(m|n)$$

en particular para $n = 1 \in \mathbb{N}^*$:

$$m|1$$

es decir 1 es la mayor de las cotas inferiores:

$$\therefore 1 = \inf \mathbb{N}^*$$

y como $1 \in \mathbb{N}^*$ se sigue que

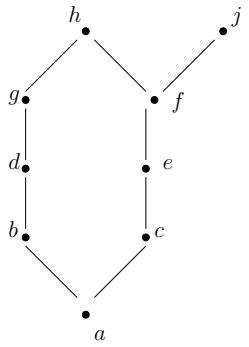
$$1 = \min \mathbb{N}^*$$

El conjunto ordenado $(\mathbb{N}^*, |)$ no tiene máximo, pues si lo tuviera entonces debería de ser cota superior. Denotemos a esta cota con k. Luego, por definición de cota superior

$$(\forall n \in \mathbb{N}^*)(n|k)$$

es decir k debe ser múltiplo de todos los enteros positivos, lo que implica $k = 0$ pero $k \notin N^*$, lo que contradice la definición de "máximo" (el máximo debe de estar en el conjunto). □

EJEMPLO 88. Considere el diagrama de Hasse



Calcular el ínfimo y el supremo de $A = \{b, d, g\}$.

SOL. Las cotas superiores de A son: g, h. La menor de éstas es g, luego

$$g = \sup A.$$

Las cotas inferiores de A son: b, a. La mayor es b. Por lo que

$$b = \inf A.$$

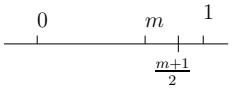
□

EJEMPLO 89. Sea $A = (0, 1)$ intervalo cerrado en $\mathbb{R}$ con orden parcial $\leq$. Calcular $\sup A$ e $\inf A$.

SOL. Si $x \in A$ entonces $x \leq 1$. Luego 1 es cota superior. Probaremos que es la menor cota inferior. Sea m otra cota inferior de A. Entonces

$$(\forall x \in A)(x \leq m) \tag{2}$$

en particular para $x = .5 \in A$ tenemos que $.5 \leq m$, por lo que $m > 0$. Queremos demostrar que $1 \leq m$. Si ocurriera lo contrario: $1 > m > 1$, luego



el número $(m + 1)/2$ es tal que

$$0 < m < \frac{m+1}{2} < 1 \tag{3}$$

de donde $(m + 1)/2 \in A$, entonces, según (2),

$$\frac{m+1}{2} \leq m$$

lo que contradice (3).

Por lo tanto $1 \leq m$.

$$\therefore 1 = \sup A.$$

Similarmente $0 = \inf A$ (tarea). □

EJEMPLO 90. Hallar el ínfimo y supremo, si existen, de $\{3, 9, 12\}$ en $(\mathbb{N}^*, |)$.

Sol.

(1) Ínfimo: una cota inferior m es un número tal que

$$m|3, \quad m|9 \text{ y } m|12$$

Como los divisores positivos de 3 son $1, 3$, los de 9 son $1, 3, 9$ y los de 12 son $1, 2, 3, 4, 6$ entonces

$$m = 1 \vee m = 3$$

Pero como $1|3$, 3 es la mayor cota inferior:

$$\therefore 3 = \inf\{3, 9, 12\}.$$

(2) Supremo: una cota superior es un número m tal que

$$3|m, \quad 9|m \text{ y } 12|m.$$

Es decir m es un múltiplo común de $3, 9, 12$. Tales deben de ser múltiplos de 36, esto es $36|m$; luego 36 es la menor cota superior:

$$36 = \sup\{3, 9, 12\}.$$

□

Si $s = \sup B$ entonces se debe de cumplir que

$$(\forall k \text{ cota superior de } B)(s \leq k).$$

En particular, el supremo siempre tiene que estar relacionado con todas las cotas superiores.

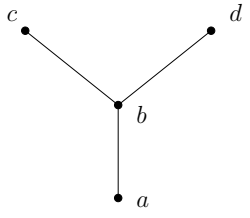
Similarmente para el ínfimo.

Tarea 35.

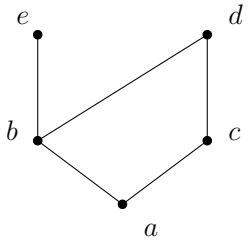
(1) *Dibujar el diagrama de Hasse de la relación "mayor o igual" en el conjunto* $\{0, 1, 2, 3, 4\}$
(2) *Dibujar el diagrama de Hasse de la relación de divisibilidad en el conjunto*
   (a) $\{1, 2, 3, 4, 5, 6\}$
   (b) $\{3, 5, 7, 11, 13, 16, 17\}$
   (c) $\{2, 3, 5, 10, 11, 15, 25\}$
   (d) $\{1, 3, 9, 27, 81, 243\}$
(3) *Dibujar el diagrama de Hasse de* $(2^S, \subseteq)$ *con* $S = \{a, b, c, d\}$.

Tarea 36. *Enumerar todos los pares ordenados de cada uno de los órdenes parciales que corresponden a los diagramas de Hasse que se muestran.*

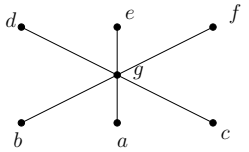
(1)



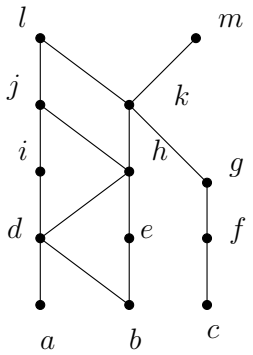
(2)



(3)



TAREA 37. *Considerar el siguiente diagrama de Hasse:*



(1) *Hallar los elementos maximales.*
(2) *Hallar los elementos minimales.*
(3) *¿Hay máximo?*
(4) *¿Hay mínimo?*
(5) *Hallar todas las cotas superiores de* $\{a, b, c\}$
(6) *Hallar el supremo de* $\{a, b, c\}$*, si es que existe.*
(7) *Hallar todas las cotas inferiores de* $\{f, g, h\}$
(8) *Hallar el ínfimo de* $\{f, g, h\}$*, si es que existe.*

TAREA 38. *Considérese el conjunto parcialmente ordenado*

$$(\{3, 5, 9, 15, 24, 45\}, |)$$

(1) *Hallar los elementos maximales.*
(2) *Hallar los elementos minimales.*
(3) *¿Hay máximo?*
(4) *¿Hay mínimo?*
(5) *Hallar todas las cotas superiores de* $\{3, 5\}$
(6) *Hallar el supremo de* $\{3, 5\}$*, si es que existe.*
(7) *Hallar todas las cotas inferiores de* $\{15, 45\}$
(8) *Hallar el ínfimo de* $\{15, 45\}$*, si es que existe.*

TAREA 39. *Considerar el conjunto parcialmente ordenado*

$$(\{2, 4, 6, 9, 12, 18, 27, 36, 48, 60, 72\}, |)$$

(1) *Hallar los elementos maximales.*
(2) *Hallar los elementos minimales.*
(3) *¿Hay máximo?*
(4) *¿Hay mínimo?*
(5) *Hallar todas las cotas superiores de* $\{2, 9\}$
(6) *Hallar el supremo de* $\{2, 9\}$*, si es que existe.*
(7) *Hallar todas las cotas inferiores de* $\{60, 72\}$
(8) *Hallar el ínfimo de* $\{60, 72\}$*, si es que existe.*

TAREA 40. *Considérese el conjunto*

$$(P, \subseteq)$$

donde

$$P = \{\{1\}, \{2\}, \{4\}, \{1, 2\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$$

(1) *Hallar los elementos maximales.*
(2) *Hallar los elementos minimales.*
(3) *¿Hay máximo?*
(4) *¿Hay mínimo?*
(5) *Hallar todas las cotas superiores de* $\{\{2\}, \{4\}\}$
(6) *Hallar el supremo de* $\{\{2\}, \{4\}\}$*, si es que existe.*
(7) *Hallar todas las cotas inferiores de* $\{\{1, 3, 4\}, \{2, 3, 4\}\}$.
(8) *Hallar el ínfimo de* $\{\{1, 3, 4\}, \{2, 3, 4\}\}$*, si es que existe.*

TAREA 41. *Hallar un conjunto parcialmente ordenado que*

(1) *tenga un elemento minimal y que no tenga ningún elemento maximal.*
(2) *tenga un elemento maximal y no tenga ningún elemento minimal.*
(3) *no tenga ni elementos maximales ni minimales.*

DEFINICIÓN 91. *Un conjunto* $(A, \leq)$ *se llama* **retículo** *si*

$$(\forall x \in A)(\forall y \in A)(\text{ existen } \sup\{x, y\} \text{ e } \inf\{x, y\})$$

EJEMPLO 92. $(\mathbb{R}, \leq)$ es un retículo, pues si $x, y \in \mathbb{R}$, entonces, por tricotomía $x \leq y$ o $y \leq x$:

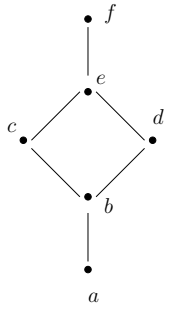
- Caso $x \leq y$: $\sup\{x, y\} = y$ y $\inf\{x, y\} = x$.
- Caso $y \leq x$: $\sup\{x, y\} = x$ y $\inf\{x, y\} = y$.

El mismo argumento prueba que

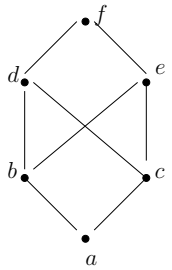
PROPIEDAD 7. *Si* $(A, \leq)$ *es totalmente ordenado entonces es un retículo.*

EJEMPLO 93. Considérese los siguientes diagramas de Hasse:

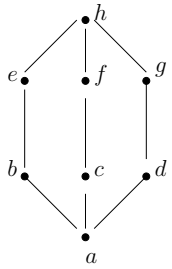
(1)



(2)



(3)



que representan ordenes parciales. Determinar si son retículos.

Sol. Tenemos que mostrar que cada pareja tiene supremo e ínfimo. Pondremos tal información en una tabla. Como $\sup\{x, y\} = \sup\{y, x\}$ sólo llenaremos la mitad de tal tabla.

(1) Nótese que $\sup\{a, b\} = b$ pues b, c, d, e, f son cotas superiores y la menor de éstas es b. Similarmente $\sup\{b, e\} = f$:

sup	a	b	c	d	e	f
a	a	b	c	d	e	f
b		b	c	d	e	f
c			c	e	e	f
d				d	e	f
e					e	f
f						f

inf	a	b	c	d	e	f
a	a	a	a	a	a	a
b		b	b	b	b	b
c			c	b	c	c
d				d	d	f
e					e	e
f						f

Por lo tanto tenemos un retículo.

(2) Las cotas superiores de $\{b, c\}$ son: d, e, f y de éstas, para calcular el supremo, debemos tomar la menor, pero d y e no son comparables. Por lo tanto no existe supremo de $\{b, c\}$. Luego no tenemos un retículo.

(3)

sup	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b		b	h	h	e	h	h	h
c			c	h	h	f	h	h
d				d	h	h	g	h
e					e	h	h	h
f						f	h	h
g							g	h
h								h

Nótese que las cotas superiores de $\{b, c\}$ son: h. Luego $\sup\{b, c\} = h$.

inf	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b		b	a	a	b	a	a	b
c			c	a	a	c	a	c
d				d	a	a	d	a
e					e	a	a	a
f						f	a	f
g							g	g
h								h

Por lo tanto tenemos un retículo.

□

Ejemplo 94. Sea E un conjunto. Determinar si $(2^E, \subseteq)$ es un retículo.

Sol. Sean $A, B \in 2^E$. Entonces $A \subseteq E$ y $B \subseteq E$. Probaremos que

(1) $\sup\{A, B\} = A \cup B$
(2) $\inf\{A, B\} = A \cap B$

(1) Sabemos que $A \subseteq A \cup B$ y $B \subseteq A \cup B$, esto es, $A \cup B$ es cota superior del conjunto $\{A, B\}$; probaremos que esta es la mínima cota superior. Supongamos que C es cota superior de $\{A, B\}$. Luego, $A \subseteq C$ y $B \supseteq C$, entonces $A \cup B \subseteq C$.

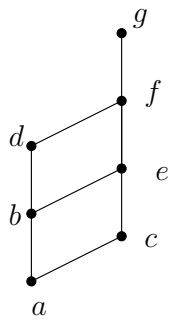
$$\therefore \sup\{A, B\} = A \cup B.$$

(2) Tarea.

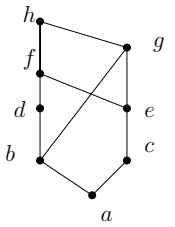
Por lo tanto $(2^E, \subseteq)$ es un retículo. □

Tarea 42. *Determinar si los conjuntos parcialmente ordenados con estos diagramas de Hasse son o no retículos.*

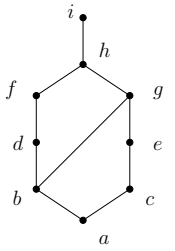
(1)



(2)



(3)



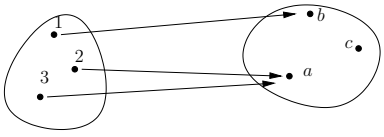
6. Funciones

Definición 95. *Sea $f : A \to B$ una relación de A en B. La relación f se llama* **función** *si*

(1) $Dom\, f = A$
(2) $(\forall a \in A)(\forall b \in B)(\forall c \in C)(((a, b) \in f \wedge (a, c) \in f) \Rightarrow b = c)$.

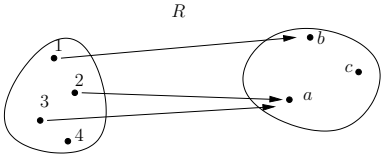
Ejemplo 96.

(1)



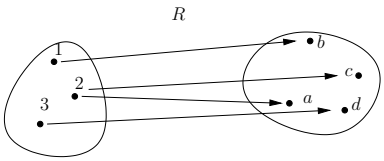
representa una función.

(2)



no es una función pues $Dom\, R \neq \{1, 2, 3, 4\}$.

(3)



no es función pues $(2, c) \in R$ y $(2, a) \in R$ pero $c \neq a$.

Ejemplo 97. Sea A el conjunto de mujeres con novio, B el conjunto de hombres. Se define una relación f de A en B como

$$afb \Leftrightarrow a \text{ es novia de } b$$

Tal f resulta una función si *creemos que las mujeres no pueden tener más de un novio*:

(1) $Dom\, f = A$: recordemos que

$$Dom\, f = \{a \in A \,|\, \exists b \in B \text{ tal que } afb\}$$

es decir $Dom\, f$ es el conjunto de mujeres que tienen novio, siendo este precisamente A.

(2) Si $(a, b) \in f$ y $(a, c) \in f$ entonces a es novia de b y también a es novia de c. Según nuestra creencia, se debe de seguir que $a = c$.

Ejemplo 98. Sea $f : \mathbb{R} \to \mathbb{R}$ relación definida por

$$xfy \Leftrightarrow x^2 = y$$

f es función pues

(1) $Dom\, f = \mathbb{R}$: recordemos que, por definición,

$$Dom\, f = \{x \in \mathbb{R} \,|\, \exists y \in \mathbb{R}, xfy\} = \{x \in \mathbb{R} \,|\, \exists y \text{ tal que } x^2 = y\}$$

Luego $Dom\, f \subseteq \mathbb{R}$ evidentemente. Mientras que $\mathbb{R} \subseteq Dom\, f$ es porque si $x \in \mathbb{R}$ entonces $(x, x^2) \in f$, luego $x \in Dom\, f$.

$$\therefore Dom\, f = \mathbb{R}.$$

(2) Supongamos que $(a, b) \in f$ y $(a, c) \in f$ entonces $a^2 = b$ y $a^2 = c$, de donde $b = c$.

Ejemplo 99. Sea $f : \mathbb{R} \to \mathbb{R}$ relación definida por

$$xfy \Leftrightarrow x = y^2$$

f no es función pues $Dom\, f \neq \mathbb{R}$. En efecto, $-1 \in \mathbb{R}$ pero si $-1 \in Dom\, f$ entonces existe $y \in \mathbb{R}$ tal que $-1 = y^2$ lo cual es imposible. Por lo que $-1 \notin Dom\, f$. Por lo tanto $\mathbb{R} \neq Dom\, f$.

EJEMPLO 100. Sea $f : [0, \infty)$ relación definida por

$$xfy \Leftrightarrow y = \sqrt{x} \vee y = -\sqrt{y}$$

f no es función, pues

$$(1, 1) \in f \text{ y } (1, -1) \in f \text{ pero } 1 \neq -1.$$

DEFINICIÓN 101. *Si $f : A \to B$ función y $a \in A$, se define*

$$f(a) = b \Leftrightarrow (a, b) \in f \Leftrightarrow afb$$

en tal caso b se llama **imagen** *de a bajo f.*

EJEMPLO 102. Sean $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$. La siguiente relación

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

es una función, donde $f(1) = b$, $f(2) = c$, $f(3) = b$ y $f(4) = a$.

PROPIEDAD 8. *Sea A un conjunto y $Id_A : A \to A$ relación definida por*

$$aId_Ab \Leftrightarrow a = b$$

entonces Id_A es una función (llamada **función identidad***). Además*

$$(\forall a \in A)(Id_A(a) = a)$$

DEMOSTRACIÓN.

(1) $Dom\, f = A$: que $Dom\, f \subseteq A$ es por definición. Por demostrar que $A \subseteq Dom\, f$. Sea $a \in A$, entonces afa, luego $a \in Dom\, f$.
(2) Supongamos que $(a, b) \in f$ y $(a, c) \in f$ entonces $b = a$ y $c = a$, DE DONDE $b = c$.

Notemos, además que $\forall a \in A$ se cumple que $(a, a) \in Id_A$, luego por definiciń $Id_A(a) = a$. □

DEFINICIÓN 103. *Sean $R : A \to B$, $S : B \to C$ relaciones. Se define la* **relación composición** *como la relación $S \circ R$,*

$$aS \circ Rc \Leftrightarrow \exists b \in B \text{ tal que } aRb \wedge bSc.$$

EJEMPLO 104. Sean

$$A = \{1, 2, 3, 4\}, \quad B = \{a, b, c\}, \quad C = \{\alpha, \beta, \delta, \gamma\}$$

y relaciones

$$R : A \to B, \quad S : B \to C.$$

definidas por

$$R = \{(1, a), (1, b), (3, c)\}, \quad S = \{(a, \alpha), (a, \delta), (b, \alpha), (c, \gamma)\}.$$

Entonces

$$S \circ R = \{(1, \delta), (1, \alpha), (3, \gamma)\}$$

pues

- $(1, \delta) \in S \circ R$ pues $\exists a \in B$ tal que $1Ra$ y $aS\delta$;
- $(1, \alpha) \in S \circ R$ porque $\exists a \in B$ con $1Ra$ y $aS\alpha$;
- $(3, \gamma) \in S \circ R$ pues $existsc \in B$ tal que $3Rc$ y $cS\gamma$.

TEOREMA 7. *Si $f : A \to B$ y $g : B \to C$ son funciones, entonces la relación composición $g \circ f$ es una función. Además*

$$(\forall a \in A)\, (g \circ f)(a) = g(f(a)).$$

Dem.

(1) Por definición

$$Dom\, g \circ f = \{a \in A \,|\, \exists c \in C,\, a\, g \circ f\, c\}$$

de donde $Dom\, g \circ f \subseteq A$. Recíprocamente, que $A \subseteq Dom\, g \circ f$ es porque si $a \in A$ como $A = Dom\, f$ entonces existe $b \in B$ tal que afb. Pero $B = Dom\, g$, luego existe $c \in C$ tal que bgc. Tenemos

$$afb \text{ y } bgc$$

entonces, por definición de composición, $a\, g \circ f\, c$. Esto es $a \in Dom\, g \circ f$.

(2) Supongamos que $a\, g \circ f\, c_1$ y $a\, g \circ f\, c_2$. Por demostrar que $c_1 = c_2$. Como $g \circ f\, c_1$ entonces existe $b_1 \in B$ tal que

$$afb_1 \text{ y } b_1gc_1$$

y como $a\, g \circ\, c_2$ existe $b_2 \in B$ tal que

$$afb_2 \text{ y } b_2gc_2$$

Notemos que tenemos afb_1 y afb_2 luego, como f es función se sigue que $b_1 = b_2$. De donde

$$b_1gc_2 \text{ y } b_1gc_2$$

y como g es función se sigue que $c_1 = c_2$.

$$\therefore f \text{ es función.}$$

Tomemos $a \in A$ arbitrario. Entonces, por definición de imagen

$$(a, (g \circ f))(a)) \in g \circ f.$$

También $(a, f(a)) \in f$ y $(f(a), g(f(a))) \in g$; por lo que

$$(f(a), g(f(a))) \in g \circ f.$$

Entonces, como $g \circ f$ es función,

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

□

Definición 105. *Sea $f : A \to B$ función.*

(1) *f se dice* **inyectiva** *si* $(\forall x \in A)(\forall y \in B)(x \neq y \Rightarrow f(x) \neq f(y))$.
(2) *f se dice* **suprayectiva** *si $f(A) = B$, es decir si*

$$(\forall b \in B)(\exists x \in A)\, f(x) = b$$

(3) *f es biyectiva si es inyectiva y suprayectiva.*

Notemos que

$$f \text{ es inyectiva } \Leftrightarrow (f(x) = f(y) \Rightarrow x = y)$$

Ejemplo 106. ¿Qué tipo de funciones son las siguientes?

(1) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$
(2) $f : \mathbb{R} \to [0, \infty)$, $f(x) = x^2$
(3) $f :\to [0, \infty)$, $f(x) = x^2$
(4) $f : [0, \infty) \Rightarrow [0, \infty)$, $f(x) = x^2$
(5) $g : \mathbb{N} \to \mathbb{N}$, $g(n) = 2n$.

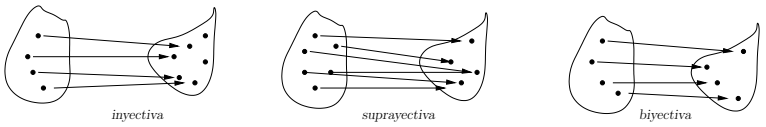


FIGURA 3. Algunos tipos de funciones

SOL.

(1) No es inyectiva pues $f(-1) = 1 = f(1)$ y $-1 \neq 1$. Tampoco es sobre pues $\exists -1 \in \mathbb{R}$ que hace la ecuación

$$\underbrace{f(x)}_{x^2} = -1$$

imposible de resolver para $x \in \mathbb{R}$.

(2) Como en el ejemplo anterior f no es inyectiva, pero ahora f sí es sobre. Pues $\forall b \in [0, \infty)$, i.e., $b \geq 0$ tenemos que existe $x = \sqrt{b}$ que es solución de $f(x) = b$.

(3) f es inyectiva: $\forall x \geq 0$, $\forall y \geq 0$ tenemos que

$$\begin{aligned} f(x) = f(y) &\Rightarrow x^2 = y^2 \\ &\Rightarrow \sqrt{x^2} = \sqrt{y^2} \\ &|x| = |y|, \text{ pues, en general } \sqrt{x^2} = |x|, \\ &x = y, \text{ pues } x \geq 0, y \geq 0. \end{aligned}$$

g es sobre: Sea $b \in [0, \infty)$ entonces $\exists x = \sqrt{b}$ tal que resuelve la ecuación

$$\underbrace{f(x)}_{(\sqrt{b})^2} = b$$

Por lo tanto f es biyectiva.

(4) g es inyectiva: $\forall x \in \mathbb{N}$, $\forall y \in \mathbb{N}$

$$\begin{aligned} g(x) = g(y) &\Rightarrow 2x = 2y \\ &x = y \text{ multiplicando por } 1/2; \end{aligned}$$

g no es sobre: pues para $b = 1 \in \mathbb{N}$ la ecuación

$$\underbrace{g(x)}_{2x} = 1$$

es imposible de resolver en $x \in \mathbb{N}$: su solución es $x = 1/2 \notin \mathbb{N}$.

□

EJEMPLO 107. Sea

$$f : \{a, b, c, d\} \to \{1, 2, 3\}$$

definida por $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, $f(d) = 3$. ¿Es f suprayectiva?

SOL. Tenemos que $Im\, f = \{1, 2, 3\}$. Luego f es sobreyectiva.

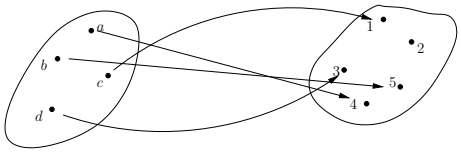
□

Ejemplo 108. Determinar si la función

$$f : \{a, b, c, d\} \to \{1, 2, 3, 4, 5\}$$

con $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, $f(d) = 3$ es inyectiva.

Sol. El diagrama sagital de f es



de donde se puede ver a f toma diferentes valores en diferentes elementos. □

Ejemplo 109. Determinar si la función $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 3x + 2$ es inyectiva, ¿es biyectiva?

Sol.

- Inyectiva:

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow 3x_1 + 2 = 3x_2 + 2 \\ &\Rightarrow 3x_1 = 3x_2 \text{ sumando -2} \\ &\Rightarrow x_1 = x_2 \text{ multiplicando por } 1/3 \end{aligned}$$

- Suprayectiva: sea $b \in \mathbb{R}$. Tratamos de resolver la ecuación

$$f(x) = b$$

es decir

$$3x + 2 = b$$

cuya solución es

$$x = \frac{b-2}{3}$$

esto es

$$f\left(\frac{b-2}{3}\right) = b$$

por lo tanto f es sobre.

$$\therefore f \text{ es biyectiva.}$$

□

Teorema 8. *Sean $R : A \to B$, $S : B \to C$, $T : C \to D$ relaciones. Entonces*

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Demostración. Tenemos que

$$S \circ R : A \to C, \quad T \circ S : B \to D.$$

Demostraremos que

(1) $T \circ (S \circ R) \subseteq (T \circ S) \circ R$
(2) $(T \circ S) \circ R \subseteq T \circ (S \circ R)$

(1) Sea $(a,d) \in T \circ (S \circ R)$ entonces existe $c \in C$ tal que

$$a\, S \circ R\, c \text{ y } cTd$$

en particular $(a,c) \in S \circ R$, luego existe $b \in B$ tal que

$$aRb \text{ y } bSc.$$

Tenemos bSc y cTd, luego $(b,d) \in T \circ S$; pero también $(a,b) \in R$ y $(b,d) \in T \circ S$, lo que implica

$$a \in (T \circ S) \circ R$$

(2) Tarea.

□

Como consecuencia tenemos la propiedad de asociatividad para la composición de funciones:

COROLARIO 1. *Si $f : A \to B$, $g : B \to C$, $h : C \to D$ son funciones, entonces*

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

El siguiente teorema da la relación entre el concepto de función biyectiva y el concepto de función inversa.

TEOREMA 9. *Sea $f : A \to B$ una función. Entonces*

$$f^{-1} : B \to A \text{ es función } \Leftrightarrow f \text{ es biyectiva.}$$

DEMOSTRACIÓN.

(⇒) Supongamos que $f^{-1} : B \to A$ es función. Demostraremos que f es biyectiva.

(1) f es inyectiva: supongamos que $f(x) = f(y)$. Por demostrar que $x = y$. Tenemos que $(x, f(x)) \in f$ y $(y, \underbrace{f(y)}_{=f(x)}) \in f$. Luego, por definición de relación inversa,

$$(f(x), x) \in f^{-1} \text{ y } (f(x), y) \in f^{-1}$$

de donde, como f es función, se obtiene que $x = y$.

(2) f es sobre: sea $b \in B$. Por demostrar que existe $x \in A$ tal que

$$f(x) = b.$$

Como f^{-1} es función, $(b, f^{-1}(b)) \in f^{-1}$. Luego, por definición de relación inversa, $(f^{-1}(b), b) \in f$. Definimos $x = f^{-1}(b)$. Luego, por definición de imagen $(x, f(x)) \in f$, pero también tenemos que $(x,b) \in f$. Luego $f(x) = b$.

$$\therefore f \text{ es biyectiva.}$$

(⇐) Supongamos que f es biyectiva. Por demostrar que $f^{-1} : B \to A$ es función.

(1) $Dom\, f^{-1} = B$: tenemos que, por definición de dominio, $Dom\, f^{-1} \subseteq B$. Recíprocamente: sea $b \in B$, como f es suprayectiva existe $x \in A$ tal que $f(x) = b$, esto es $xfb \in f$; se sigue que $bf^{-1}x$, lo que implica $b \in Dom\, f^{-1}$, por definición de dominio:

$$\therefore B \subseteq Dom\, f.$$

$$\therefore Dom\, f = B.$$

(2) Supongamos que $(a, b) \in f^{-1}$ y $(a, c) \in f^{-1}$. Por demostrar que $b = c$. Por definición de relación inversa, tenemos que $(b, a) \in f$ y $(c, a) \in f$, esto es, $f(b) = a$ y $f(c) = a$ por lo que $f(b) = f(c)$; ahora usmos la definición de función inyectica para obtener que $b = c$ como queríamos.

□

TAREA 43. *En cada inciso dar un ejemplo de una función $f : A \to B$ tal que*

(1) *sea inyectiva pero no sobre;*
(2) *sobre pero no inyectiva;*
(3) *inyectiva y sobre;*
(4) *ni inyectiva ni sobre.*

TAREA 44. *Determinar si las siguientes reglas de correspondencia definen funciones $f : \mathbb{Z} \to \mathbb{Z}$ inyectivas.*

(1) $f(n) = n - 1$
(2) $f(n) = n^3$
(3) $f(n) = n^2 + 1$

TAREA 45. *¿Cuáles de los incisos del ejercicio anterior definen funciones suprayectivas?*

TAREA 46. *Determinar si las siguientes funciones $f : \mathbb{R} \to \mathbb{R}$ son biyectivas.*

(1) $f(x) = -3x + 4$
(2) $f(x) = 3x^2 + 7$
(3) $f(x) = \frac{x^2+1}{x^2+2}$
(4) $f(x) = x^3 + 1$

TEOREMA 10. *Sean $f : A \to B$, $g : B \to C$ funciones.*

(1) *Si f y g son inyectivas entonces $g \circ f$ es inyectiva.*
(2) *Si f y g son suprayectivas entonces $g \circ f$ es suprayectiva.*
(3) *Si f y g son biyectivas entonces $g \circ f$ es biyectiva.*

DEMOSTRACIÓN.

(1) Tarea
(2) Tenemos que

$$g \circ f : A \to C.$$

Sea $c \in C$. Queremos mostrar que la ecuacón

$$(g \circ f)(x) = c$$

es soluble en x.

Como g es sobre, existe $y \in B$ tal que $g(y) = c$. A su vez, como f es sobre, existe $x \in A$ tal que $f(x) = y$. Luego

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(y) \\ &= c.\end{aligned}$$

(3) Como f y g son inyectivas y suprayectivas, entonces, según el inciso anterior $g \circ f$ es inyectiva y suprayectiva. Esto es $g \circ f$ es biyectiva

□

TAREA 47. *Sea $f : A \to B$ relación. Demostrar que*

(1) *$Dom\, f^{-1} = Im\, f$*
(2) *$Im\, f^{-1} = Dom\, f$.*

TAREA 48. *Muestre que si $f : A \to B$, $g : B \to C$ son funciones tales que $g \circ f = Id_A$ entonces f es inyectiva y g es suprayectiva.*

TAREA 49. *Sean $f : A \to B$ y $g : B \to C$ funciones.*

(1) *Si f y $g \circ f$ son inyectivas, ¿es g inyectiva? Explicar.*
(2) *Si f y $g \circ f$ son suprayectivas, ¿es g suprayectiva?. Explicar*

TAREA 50. *Sea $f : A \to B$ una relación tal que es función y $f^{-1} : B \to A$ relación inversa. Demostrar que*

(1)
$$f^{-1} \circ f = Id_A \Leftrightarrow f \text{ es inyectiva.}$$
(2)
$$f \circ f^{-1} = Id_B \Leftrightarrow f \text{ es sobreyectiva.}$$

TAREA 51. *En criptografía una encriptación de un conjunto de textos T es una función $E_k : T \to C$ donde C es un conjunto de cadenas llamadas* **encriptamientos** *y k es la* **clave** *de encriptación. Una* **desencriptación** *es una función $D_k : C \to T$ tal que*

$$(\forall t \in T) D_k(E_k(t)) = t$$

Demostrar que la encriptación no puede encriptar dos textos diferentes de la misma forma y que cualquier texto puede ser la descriptación de algúna cadena.

CAPíTULO 4

Teoría de Números

En teoría de números el universo del discurso es el conjunto de números enteros $\mathbb{Z}$. Muchas de sus propiedades tienen que ver con divisibilidad.

1. Divisibilidad y primos

DEFINICIÓN 110. *Si $a \mid b$ entonces a se llama divisor (ó factor) de b y b se llama múltiplo de a.*

Nótese que la relación de *múltiplo* es la recación inversa de divisibilidad. Esto es

$$a \mid b \Leftrightarrow b \text{ es múltiplo de } a \Leftrightarrow b \mid^{-1} a.$$

TEOREMA 11. *Sean $a, b, c \in \mathbb{Z}$. Entonces*

(1) *si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$;*
(2) *si $a \mid b$ entonces $a \mid bc$;*
(3) *si $a \mid b$ y $b \mid c$ entonces $a \mid c$.*

DEMOSTRACIÓN.

(1) Tenemos que existen $k_1, k_2 \in \mathbb{Z}$ tales que $b = k_1 a$ y $c = k_2 a$, luego
$$\begin{aligned} b + c &= k_1 a + k_2 a \\ &= (k_1 + k_2)a \end{aligned}$$
con $k_1 + k_2 \in \mathbb{Z}$. Entonces, por definición, $a \mid (b + c)$.
(2) Tarea.
(3) Tarea.

□

COROLARIO 2. *Sean $a, b, c \in \mathbb{Z}$. Si $a \mid b$ y $a \mid c$ entonces $a \mid (mb + nc)$, para cualesquiera $m, n \in \mathbb{Z}$.*

DEMOSTRACIÓN. Si $a \mid b$ y $a \mid c$ entonces $a \mid mb$ y $a \mid nc$ por (2) del teorema inmediato anterior. Luego, por (1) del mismo teorema, $a \mid (mb + nc)$. □

Recordemos:

DEFINICIÓN 111. *Un número $p \in \mathbb{N}$ es primo si cumple:*

(1) *$p > 1$;*
(2) *los únicos divisores positivos de p son 1 y p.*

EJEMPLO 112. El número 7 es primo porque $7 > 1$ y además sus únicos divisores positivos son 1 y 7.

EJEMPLO 113. Son primos: $2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43, 47$.

DEFINICIÓN 114. *Un número $n \in \mathbb{N}$ se dice compuesto si cumple que*

(1) $n > 1$
(2) n *no es primo*

EJEMPLO 115. *El número* 9 *es compuesto porque* $9 > 1$ *y* $3 \mid 9$ *por lo que* 9 *no es primo.*

TEOREMA 12 (Fundamental de la Aritmética). *Sea* $n \in \mathbb{Z}$ *tal que* $n > 1$. *Entonces* n *se puede escribir como un producto de números primos de forma única.*

La razón de ser del teorema fundamental del la aritmética es que, dado un $n \in \mathbb{Z}$ con $n > 1$, cumple uno de dos casos: n es primo ó compuesto.

- Si $n = p$ es primo, entonces n se considera el producto de un sólo primo: p.
- Si n es compuesto entonces se puede escribir como un producto de enteros $n = m_1 m_2$ con $1 < m_1 < n$ y $1 < m_2 < n$. Entonces a cada uno de éstos factores se le puede aplicar el mismo razonamiento recursivamente. Eso es, m_1 es primo o compuesto; similarmente m_2 es primo o compuesto. Etc.

Para la unicidad del teorema fundamental de la aritmética se requiere más trabajo.

El producto del teorema fundamental de la aritmética se conoce como *factorización prima*.

EJEMPLO 116. Encontrar la factorización prima de 100.

SOL.

$$\begin{aligned} 100 &= 2 * 50 \\ &= 2 * 2 * 25 \\ &= 2 * 2 * 5 * 5 \end{aligned}$$

Luego la factorización prima de 100 es:

$$100 = 2^5 * 5^2.$$

□

EJEMPLO 117. Encontrar la factorización prima de 999.

SOL.

$$\begin{aligned} 999 &= 3 * 333 \\ &= 3 * 3 * 111 \\ &= 3 * 3 * 3 * 37, \end{aligned}$$

entonces, como 37 es primo, la factorización prima de 999 es

$$999 = 3^3 * 37.$$

□

EJEMPLO 118. *Encontrar la factorización prima de* 641.

SOL. La factorización prima de 641 es

$$641 = 641$$

pues 641 es primo. □

Para verificar que 641 es primo con relativa facilidad se puede usar el *criterio de la raíz*.

TEOREMA 13 (Criterio de la raíz). *Si $n \in \mathbb{N}$ es un número compuesto, entonces existe p primo tal que $p \mid n$ y $p \leq \sqrt{n}$.*

DEMOSTRACIÓN. Si n es compuesto entonces tiene un divisor a tal que $1 < a < n$. Entonces existe $k \in \mathbb{N}$ tal que $n = ka$. Nótese que $k > 1$.

Si ocurriera que $k > \sqrt{n}$ y $a > \sqrt{n}$ entonces, multiplicando lado a lado éstas desigualdades obtenemos que

$$\underbrace{ak}_{n} > \underbrace{\sqrt{n}\sqrt{n}}_{n}$$

es decir, $n > n$: absurdo.

Así, necesariamente ocurre que $k \leq \sqrt{n}$ ó $a \leq \sqrt{n}$:

(1) Si $k \leq \sqrt{n}$ entonces, por el teorema fundamental de la aritmética, existe p primo tal que $p \mid k$. Además, por definición de k, $k \mid n$, luego por transitividad $p \mid n$. También $p \leq k \leq \sqrt{n}$. En resumen, hemos obtenido:

$$p \text{ primo, } p \leq \sqrt{n} \text{ y } p \mid n.$$

(2) Si $a \leq \sqrt{n}$, entonces, de nuevo por el teorema fundamental de la aritmética, existe q primo tal que $q \mid a$ y se procede como en el caso anerior para obtener

$$q \text{ primo, } q \leq \sqrt{n} \text{ y } q \mid n.$$

□

EJEMPLO 119. El número 641 es primo porque si fuera compuesto existiría un primo p tal que $p \mid 641$ y $p \leq \sqrt{641} \approx 25.31$, de donde $p = 2, 3, 7, 11, 13, 17, 19$ ó 23. Pero ninguno de éstos primos divide a 641. Por lo tanto 641 es primo.

La relación de divisivilidad y el *algoritmo de la división* están a su vez relacionados.

TEOREMA 14 (Algoritmo de la división). *Sea $a \in \mathbb{Z}$ y d un entero positivo. Entonces existen q, r enteros tales que*

$$a = qd + r \text{ y } 0 \leq r < d.$$

Tales enteros q, r son únicos.

Notación: El número $q = a$ **div** v se llama el *cociente* al dividir a por d. Mientras que $r = a$ **mod** d se llama el *residuo* al dividir a por d.

El algoritmo de la divisón no es ás que la notación de "casita" al dividir enteros:

$$\begin{array}{rl} & q \\ d & \overline{)\,a} \\ & r \end{array}$$

EJEMPLO 120. Tenemos que

$$\begin{array}{rlll} & 1 & 2 & 8 \\ 5 & \overline{)\,6} & 4 & 1 \\ & 1 & 4 & \\ & & 4 & 1 \\ & & & 1 \end{array}$$

que se obtuvo con el llamado *algoritmo largo de la división*. Esto indica la siguiente ecuación:

$$641 = 128 * 5 + 1.$$

De donde

$$128 = 641 \textbf{ div } 5, \quad 1 = 641 \textbf{ mod } 5.$$

Nótese que se cumplen las siguientes equivalencias:

$$d \,|\, a \Leftrightarrow 0 = a \textbf{ mod } d \Leftrightarrow a/d \in \mathbb{Z}.$$

Ejemplo 121.

$$2 \nmid 641 \text{ pues } 0 \neq 641 \textbf{ mod } 2 = 1;$$
$$3 \nmid 641 \text{ pues } 641/3 \notin \mathbb{Z};$$
$$7 \nmid 641 \text{ pues } 641/7 \notin \mathbb{Z}.$$

Ejemplo 122. calcular el residuo de -11 dividido por 3.

Sol. Tenemos que

$$\begin{array}{r|l} & -4 \\ \hline 3 & -11 \\ & 1 \end{array}$$

esto es:

$$-11 = -4 * 3 + 1.$$

Entonces

$$1 = -11 \textbf{ mod } 3.$$

□

Obsérvese que el poner

$$\begin{array}{r|l} & -3 \\ \hline 3 & -11 \\ & -2 \end{array}$$

es incorrecto porque el residuo NO cumple $0 \leq -2 < 3$, a pesar de que es correcta la ecuación

$$-11 = -3 * 3 - 2$$

Teorema 15. *Hay una infinidad de números primos.*

Ejemplo 123. Muestre que el número 101 es primo.

Sol. Por el criterio de la raíz: si 101 fuera compuesto entonces existiría un primo p tal que $p|101$ y $p \leq \sqrt{101} \approx 10.05$. Entonces $p = 2, 3, 5$ ó 7. Pero $2 \nmid 101$ pues $101/2 \notin \mathbb{Z}$, $3 \nmid 101$ pues $101/3 \notin \mathbb{Z}$, $5 \nmid 101$ pues $101/5 \notin \mathbb{Z}$, y ni $7 \nmid 101$ pues $101/7 \notin \mathbb{Z}$. En cualquier caso se obtiene una contradicción. Por lo tanto 101 es primo. □

2. Máximo común divisor

Definición 124. *Sean $a, b \in \mathbb{Z}$. Un número d se llama divisor común de a y b si*

$$d \,|\, a \text{ y } d \,|\, b.$$

EJEMPLO 125. El conjunto de divisores de 24 es

$$\{-24, -12, -8, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 8, 12, 24\}$$

mientras que el conjunto de divisores de 36 es

$$\{-36, -18, -12, -9, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 9, 12, 18, 36\}.$$

El conjunto de divisores comunes de 24 y 36 es

$$\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}.$$

Nótese que el máximo de los divisores comunes es 12.

DEFINICIÓN 126. *Sean $a, b \in \mathbb{Z}$. El máximo común divisor de a y b se denota con* $\gcd(a, b)$.

EJEMPLO 127. $\gcd(24, 36) = 12$.

Es evidente que, para cualesquiera enteros a, b se cumple $\gcd(a, b) = \gcd(b, a)$. También que sólo necesitamos de los divisores positivos.

EJEMPLO 128. ¿Cuál el el máximo común divisor de 17 y 22?

SOL. El conjunto de divisores positivos de 17 es:

$$\{1, 17\}$$

y los divisores positivos de 22 son

$$\{1, 2, 11, 22\}$$

entonces el conjunto divisores positivos comunes es: $\{1\}$, cuyo máximo es 1. Por lo tanto

$$\gcd(17, 22) = 1.$$

□

DEFINICIÓN 129. *Sean $a, b \in \mathbb{Z}$. Se dice que a es corprimo con b si* $\gcd(a, b) = 1$.

EJEMPLO 130. *Los números* 17 *y* 22 *son coprimos, también* 2 *y* 3 *son coprimos.*

LEMA 1. *Si $a \in \mathbb{Z}$, entonces* $\gcd(a, 0) = |a|$.

DEMOSTRACIÓN. Podemos poner como divisores positivos de a a

$$D = \{1, \ldots, |a|\}.$$

Mientras que los divisores positivos de 0 son todos los naturales no cero: $\mathbb{N}^*$. Luego, el conjunto de divisores comunes es $D \cap \mathbb{N}^* = D$ cuyo máximo es $|a|$. □

Calcular el máximo común divisor usando sólo la definición como lo hemos estado haceindo es ineficiente. Es mejor usar el *algorimo de Euclides* para el cálculo de gcd. Por ejemplo, digamos que queremos calcular $\gcd(91, 287)$. Deberíamos encontrar todos los d divisores comunes de 91 y 287, i.e.,

$$d \in \mathbb{Z} \text{ tales que } d \,|\, 91 \text{ y } d \,|\, 287.$$

En lugar de escribir la lista de tales, le aplicamos el algoritmo de la división a 91 y 287:

$$287 = 3 * 91 + 14.$$

Esto es útil porque entonces se obtiene que los divisores comunes de 91 y 287 son los mismos que los divisores comunes de 91 y el residuo 14. En efecto: si $d \,|\, 91$ y $d \,|\, 287$

entonces $d \mid \underbrace{287 - 3 * 91}_{14}$ (por Corolario 2) y $d \mid 91$. Recíprocamente, si $d \mid 14$ y $d \mid 91$ entonces, del Corolario 2 obtenemos que $d \mid \underbrace{(3 * 91 + 14)}_{287}$ y $d \mid 91$.

Por lo anterior podemos poner

$$\gcd(287, 91) = \gcd(91, 14).$$

Hemos reducido el problema a calcular $\gcd(91, 14)$. Repetimos el mismo argumento ahora para 91 y 14. Le aplicamos el algoritmo de la división a 91 y 14:

$$91 = 6 * 14 + 7.$$

Entonces los divisores comunes de 91 y 14 son los mismos divisores comunes que los de 7 y 14. En efecto, si $d \mid 91$ y $d \mid 14$ entonces $d \mid \underbrace{91 - 6 * 14}_{7}$ (por el Corolario 2) y $d \mid 14$. Recíprocamente, si $d \mid 7$ y $d \mid 14$ entonces $d \mid \underbrace{(6 * 14 + 7)}_{7}$ y $d \mid 14$.

Por lo tanto $\gcd(91, 14) = \gcd(14, 7)$. Ahora aplicamos el algoritmo de la división a 14 y 7:

$$14 = 2 * 7 + 0,$$

y procedemos como antes, para obtener que $\gcd(14, 7) = \gcd(7, 0)$. Pero sabemos del Lema 1 que $\gcd(7, 0) = 7$ y ya terminamos.

En resumen, obtuvimos la siguiente cadena de igualdades:

$$\begin{aligned} \gcd(287, 91) &= \gcd(91, 14) \\ &= \gcd(14, 7) \\ &= \gcd(7, 0) \\ &= 7. \end{aligned}$$

Nótese que finalmente el máximo común divisor se obtuvo del residuo antes de obtener residuo cero.

El procedimiento anterior es esencialmente el algoritmo de Euclides que hace uso repetitivo del siguiente hecho.

LEMA 2. *Sean a, b, q, r enteros tales que*

$$a = qb + r.$$

Entonces

$$\gcd(a, b) = \gcd(b, r).$$

DEMOSTRACIÓN. Sea D_1 el conjunto de divisores comunes de a y b. Sea D_2 el conjunto de divisores comunes de b y r. Proberemos primero que $D_1 = D_2$ por contenciones. En efecto:

$D_1 \subseteq D_2$: si $d \in D_1$ entonces $d \mid a$ y $d \mid b$, luego por el Corolario 2, $d \mid \underbrace{a - qb}_{r}$ y $d \mid b$, esto es d es un divisor común de d y r, lo que indica $d \in D_2$.

$D_2 \subseteq D_1$: si $d \in D_2$ entonces $d \mid b$ y $d \mid r$ y de nuevo, por el Corolario 2, obtenemos que $d \mid \underbrace{qb + r}_{a}$ y $d \mid b$. Lo que significa que d es divisor común de a y b, i.e., $d \in D_1$.

Por lo tanto

$$\begin{aligned}\gcd(a,b) &= \max D_1, && \text{por definición de gcd,}\\ &= \max D_2\\ &= \gcd(b,r).\end{aligned}$$

□

EJEMPLO 131. Encontrar el máximo comúnn divisor de 414 y 662.

SOL. Usamos el algorimo de Euclides:

$$\begin{array}{rr} & 1\\ 414 & |\overline{662}\\ & 248\end{array}$$

$$\begin{array}{rr} & 1\\ 248 & |\overline{414}\\ & 166\end{array}$$

$$\begin{array}{rr} & 1\\ 166 & |\overline{248}\\ & 82\end{array}$$

$$\begin{array}{rr} & 2\\ 82 & |\overline{166}\\ & 2\end{array}$$

$$\begin{array}{rr} & 41\\ 2 & |\overline{82}\\ & 0\end{array}$$

Por lo tanto

$$\gcd(414, 662) = 2.$$

□

TAREA 52.

(1) *¿A cuáles de los siguientes* 17 *divide?* $68, 84, 357, 1001$.
(2) *Sean* a, b, c, d *enteros.*
   (a) *Muestre que si* $a \mid b$ *y* $b \mid a$ *entonces* $a = b$ *ó* $a = -b$.
   (b) *Muestre que si* $a \mid b$ *y* $c \mid d$ *entonces* $ac \mid bd$.
   (c) *Muestre que si* $ac \mid bc$ *y* $c \neq 0$ *entonces* $a \mid c$.

   Cuáles son el cociente y el residuo cuando
   (a) 44 *is dividido por* 88*?*
   (b) -123 *es dividido por* 19*?*
   (c) -1 *es dividido por* 23*?*
   (d) 0 *es dividido por* 17*?*
(3) *Evaluar*
   (a) $-17 \mod 2$
   (b) $144 \mod 7$
   (c) $-101 \mod 13$
(4) *¿Qué secuencia de de números pseudoaleatorios es generada usando la congruencia lineal* $x_{n+1} = (4x_n + 1) \mod 7$ *con semilla* $x_0 = 3$*?*
(5) *¿Qué secuencia de de números pseudoaleatorios es generada usando la congruencia lineal* $x_{n+1} = 3x_n \mod 11$ *con semilla* $x_0 = 2$*?*

(6) *Determine cuáles de los siguientes números es primo:* $19, 27, 93, 101, 107, 113$
(7) *Encuentre la factorización en primos de cada uno de los siguientes:* $88, 126, 729, 1001, 1111$
(8) *Encuentre la factorización en primos de* $10!$

CAPíTULO 5

Combinatoria

Para contar hay dos principios básicos:

- regla del producto
- regla se la suma

1. Regla del producto

Regla del producto: supóngase que una tarea se puede dividir en dos tareas consecutivas. Si hay n formas de realizar la primera tarea y m formas de hacer la segunda tarea después de que se ha completado la primera tarea, entonces hay nm formas de completar la tarea original.

EJEMPLO 132. Si se quiere etiquetar las butacas de un auditorio con una letra (del alfabeto inglés) y un número entero positivo ≤ 100 ¿cuál es el número máximo de butacas que se les puede asignar una etiqueta diferente?

SOL. La tarea de etiquetar las butacas se puede dividir en dos partes:

(1) poner una letra;
(2) poner un número positivo ≤ 100.

La primera tarea se puede completar de 26 formas y la segunda de 100. Luego hay 26*100=2,600 butacas diferentes. □

EJEMPLO 133. En una sala hay 32 computadoras. Cada computadora tiene 24 puertos. ¿Cuántos puertos diferentes hay en la sala?

SOL. La tarea de contar los puertos se puede dividir en dos:

(1) elegir computadora;
(2) elegir los puertos.

La primera tarea se completa de 32 formas, y la segunda de 24 formas. Por lo tanto, según la regla del producto hay 32*24=768 puertos. □

Regla del producto generalizada: supóngase que una tarea T requiere de realizar sucesivamente las tareas $T_1, T_2, \ldots, T_m$. Si cada tarea T_i puede realizarse de n_i formas después de completar las tareas $T_1, T_2, \ldots, T_{i-1}$, entonces hay $n_1 * n_2 * \cdots * n_m$ formas de hacer la tarea T.

EJEMPLO 134. ¿Cuántas cadenas de bits diferentes hay de longitud 7?

SOL. El primer bit se puede elegir de dos formas, el segundo de dos foarmas también, el tercer de dos,...,el séptimo también. Luego el número de bits de longitud 8 es

$$\underbrace{2 * 2 * \cdots * 2}\, 7 \text{ veces} = 2^7 = 128$$

□

Ejemplo 135. ¿Cuántas matrículas están disponibles si cada una contiene una serie de tres letras seguidas de tres dígitos?

Sol. El matricular se puede hacer en varias etapas: poner la primera letra, la segunda y luego la tercera. Entonces poner el primer, segundo y tercer dígito.

La primera letra se puede poner de 26 formas, igual que la segunda y tercera. Mientras que el primer dígito se puede poner de 10 formas diferentes, igual que el segundo y el tercer. Así, el total de matrículas es

$$26^3 * 10^3 = 17,576,000.$$

□

Ejemplo 136. Sea A un conjunto con m elementos y B un conjunto con n elementos. ¿Cuántas funciones $f : A \to B$ se pueden definir?

Sol. Supongamos que

$$A = \{a_1, \ldots, a_m\}, \quad B = \{b_1, \ldots, b_n\}$$

con $|A| = m$ y $|B| = n$.

La tarea de definir una función $f : A \to B$ se puede hacer en varias etapas:

$$\begin{gathered} 1) \text{ definir } f(a_1) \\ 2) \text{ definir } f(a_2) \\ \vdots \\ m) \text{ definir } f(a_m) \end{gathered}$$

La primera de estas tareas se puede hacer de n formas, la segunda de n,..., la m-ésima de n formas. Luego el total de funciones pedidas es

$$n \cdots n = n^m = |B|^{|A|}.$$

Por ejemplo hay 5^3 funciones de $\{1, 2, 3\}$ en $\{a, b, c, d, e\}$. □

Ejemplo 137. ¿Cuántas funciones inyectivas de $\{a, b, c, d\}$ en $\{1, 2, 3\}$ se pueden definir?

Sol. Ninguna, pues si $f : \{a, b, c, d\} \to \{1, 2, 3\}$ es inyectiva entonces, el conjunto de imágenes cumple

$$\{f(a), f(b), f(c), f(d)\} \subseteq \{1, 2, 3\}$$

siendo que el conjunto del lado izquierdo tiene cuatro elementos diferentes dentro de un conjunto de tres elementos: un absurdo. □

El mismo argumento muestra la siguiente propiedad.

Propiedad 9. *Si $f : A \to B$ es función inyectva y A tiene m elementos y B tiene n. Entonces $m \leq n$.*

Demostración. Sea $A = \{a_1, \ldots, a_m\}$, entonces $\{f(a_1), \ldots, f(a_m)\} \subseteq B$ donde B tiene m elementos; luego $m \leq n$. □

Ejemplo 138. ¿Cuántas funciones inyectivas de $\{a, b, c\}$ en $\{1, 2, 3, 4\}$ se pueden definir?

Sol. Primero podemos elegir $f(a)$ de 4 formas, luego $f(b)$ no debe repetirse de la elección anterior luego $f(b)$ puede elegirse de 3 formas y $f(c)$ de 2. Por lo que hay $4 * 3 * 2 = 24$ funciones inyectivas. □

Propiedad 10. *Si A es conjunto con m elementos, B conjunto con n elementos y $m \leq n$, entonces hay*

$$n(n-1)\cdots(n-m+1)$$

funciones inyectivas $f : A \to B$ inyectivas.

Demostración. Sea $A = \{a_1, a_2, \ldots, a_m\}$ y $B = \{b_1, \ldots, b_n\}$. Luego para definir $f : A \to B$ inyectiva primero se tiene que definir $f(a_1)$ de n formas, $f(a_2)$ de $n-1$ formas,..., $f(a_m)$ de $n-m+1$. Luego hay

$$n(n-1)\cdots(n-m+1)$$

funciones inyectivas. □

Propiedad 11. *Si $f : A \to B$ es función biyectiva con A y B finitos, entonces $|A| = |B|$.*

Demostración. Tenemos que $f : A \to B$ es inyectiva, luego $|A| \leq |B|$; pero también que $f^{-1} : B \to A$ es función y además inyectiva (pues $(f^{-1})^{-1} = f$). Entonces $|B| \leq |A|$.

$$|A| = |B|$$

□

Teorema 16. *Si A es un conjunto finito entonces $|2^A| = 2^{|A|}$.*

Demostración. Sea $\mathcal{C}$ el conjunto de cadenas de bits de longitud $|A| = n$. Sea $A = \{a_1, a_2, \ldots, a_n\}$. Definiremos una función

$$f : 2^A \to \mathcal{C}$$

de la siguiente manera: si $B \subseteq A$ se define $f(B) = c_1 \cdots c_n$ donde cada c_i es 0 ó 1 elegido de la forma

$$c_1 = \begin{cases} 0 & \text{si } a_1 \notin B \\ 1 & \text{si } a_1 \in B \end{cases}$$

$$c_2 = \begin{cases} 0 & \text{si } a_2 \notin B \\ 1 & \text{si } a_2 \in B \end{cases}$$

$$\vdots$$

$$c_n = \begin{cases} 0 & \text{si } a_n \notin B \\ 1 & \text{si } a_n \in B \end{cases}$$

(Por ejemplo, si $A = \{a, b, c\}$ entonces

$$f(\varnothing) = 000 \qquad f(\{a, b\}) = 110$$
$$f(\{a\}) = 100 \qquad f(\{a, c\}) = 101$$
$$f(\{b\}) = 010 \qquad f(\{b, c\}) = 011$$
$$f(\{a, b, c\}) = 111)$$

Claramente f es biyectiva, luego

$$|2^A| = |\mathcal{C}| = 2^n = 2^{|A|}.$$

□

TAREA 53. (1) *En cierta universidad hay 18 estudiantes de ingeniería y 325 de licenciatura.*
   (a) *¿De cuántas maneras se pueden escoger dos representantes, de forma que uno de ellos sea estudiantes de ingeniería y el otro de licenciatura?*
   (b) *¿De cuantas maneras se puede escoger un representante que sea estudiante de ingeniería o de licenciatura?*
(2) *Un edificio tiene 27 pisos y cada piso tiene 37 oficinas ¿Cuántas oficinas tiene el edificio?*
(3) *Un cuestionario se compone de diez preguntas, cada una de las cuales tiene una de cuatro posibilidades.*
   (a) *¿De cuántas formas puede contestar un estudiante al cuestionario si responde a todas las respuestas?*
   (b) *¿De cuantas formas puede contestar un estudiante si puede dejar preguntas sin contestar?*
(4) *Cierta marca de camiseta se fabrica en 12 colores en tres tallas distintas y tiene modelos diferentes para hombre y mujer. ¿Cuántos modelos diferentes de camiseta se fabrican?*
(5) *¿Cuántas cadenas distintas de tres mayúsculas se pueden formar?*
(6) *¿Cuntas cadenas de 8 bits existen?*
(7) *¿Cuántas cadenas de diez bits empiezan y terminan en 1?*
(8) *Cuántas cadenas de bits hay de longitud seis o menor?*
(9) *¿Cuántas cadenas de n bits donde n es un entero positivo empiezan y terminan con 1?*

2. Regla de la suma

Regla de la suma: si una primera primera tarea se puede realizar de n_1 formas y un segunda tarea se puede realizar de n_2 formas y si las dos tareas son ajenas (intersección vacía) entonces hay $n_1 + n_2$ formas de realizar una u otra tarea.

EJEMPLO 139. Supongamos que para elegir un representante de la facultad en una comisión universitaria se puede elegir entre un profesor y un estudiante de maestría ¿de cuántas formas se puede elegir el representante si hay 37 profesores y 83 estudiantes de maestría.

SOL. La tarea de elegir el profesor se puede hacer de 37 formas y la del estudiante de 83 formas. Como no hay un profesor que sea estudiante de maestría en esta facultad y no hay estudiantes de maestría que sea profesor, entonces hay 37+83 formas de elegir el representante. □

Regla de la suma generalizada: Supóngase que las tareas $T_1, T_2, \ldots, T_m$ se pueden hacer respectivamente de $n_1, n_2, \ldots, n_m$ formas y que éstas tareas son ajenas dos a dos ($T_1 \cap T_2 = \varnothing$, $T_1 \cap T_3 = \varnothing$, $\ldots$, $T_1 \cap T_n = \varnothing$, $T_2 \cap T_3 = \varnothing$,$\ldots$)

Ejemplo 140. Un estudiante puede elegir un proyecto de trabajo de entre tres listas. Cada una contiene, respectivamente, 23, 15 y 19 propuestas de trabajo. ¿Cuántos posibles proyetos tiene el estudiante para elegir?

Sol. El estudiante puede elegir la primera lista 23 opciones, de la segunda 15 y 19 de la tercera. Como estas opciones son ajenas, entonces hay 23+15+19=57 proyectos a elegir. □

Ejemplo 141. En una versión del lenguaje BASIC el nombre de una variable es una cadena de dos caracteres alfanuméricos (caracter alfanuméricos = dígitos ó una de las 26 letras del alfabeto inglés). Además, un nombre de una variable debe de empezar con una letra y debe de ser diferente a cinco cadenas de dos carcateres que están reservados por el lenguaje ¿Cuántos nombres de variables diferentes hay en dicha versión del lenguaje BASIC?

Sol. Sea n_1 el número de variables compuestas por un sĺo caracter y n_2 el número de variables compuestos por dos caracteres. El número total de variables será

$$n = n_1 + n_2$$

por la regla de la suma.

Tenemos $n_1 = 26$ por definición. Además cada caracter de dos letras está compuesto de

(1) una letra (26 formas)
(2) caracter alfanumérico (26 letas + 10 dígitos = 36 formas)

luego por la regla del producto

$$n_2 = 26 * 36 - 5 = 931.$$

Por lo que el número de variables es

$$n = 931 + 26 = 957.$$

□

Ejemplo 142. En cierto computador cada usario tiene una contraseña, con una longitud de entre 6 y 8 caracteres, cada una de las cuales es un dígito o una letra mayúscula. Cada contrasenña debe contener al menos un dígito ¿Cuántas contraseñas admite el sistema?

Sol. Sea P_6 el número de contraseñas de 6 caracteres, P_7, P_8 definidos similarmente. Según la regla de la suma generalizada, el número total de contraseñas es

$$P = P_6 + +P_7 + P_8.$$

Contaremos P_6 indirectamente: el número de contraseñas de 6 caracteres es de 36^6 y el número de contraseñas sin dígitos es 26^6, luego

$$P_6 = 36^6 - 26^6 = 1,867,866,560.$$

Similarmente:

$$P_7 = 36^7 - 26^7 = 70,332,353,920 P_8 \qquad = 36^8 - 26^8 = 2,612,282,842,880$$

de donde

$$P = 2,684,483,063,360.$$

□

TAREA 54. (1) *¿Cuántas cadenas de cuatro letras minúsculas hay que contengan la letra x?*
(2) *¿Cuántas cadenas de cuatro letras minúsculas hay que contengan la letra x?*
(3) *¿Cuántas cadenas de cinco caracteres ASCII contienen el caracter @ al menos una vez? (Hay 128 caracteres ASCII).*
(4) *De las cadenas de tres dígitos decimales,*
   (a) *¿Cuántas no contiene el mismo dígito tres veces?*
   (b) *¿Cuántas comienzan con un dígito impar?*
   (c) *¿Cuántas contienen exactamente dos cuatros?*
   (d) *¿Cuántas matrículas se pueden formar utilizando bien tres dígitos seguidos de tres letras mayúsculas o bien tres letras mayúsculas seguidas de tres dígitos?*
(5) *De entre un alfabeto de 26 letras mayúsculas y 26 minúsculas, ¿cuántas cadenas de ocho caracteres existen si*
   (a) *si las letras se pueden repetir?*
   (b) *si ninguna letra se puede repetir?*
   (c) *que empiecen por X si ninguna letra se puede repetir?*
   (d) *que empiecen y terminen en X si las letras se pueden repetir?*
   (e) *que empiecen y terminen en la cadena BO si las letras se pueden repetir?*
   (f) *que empiecen o terminen en la cadena BO si las letras se pueden repetir?*
   (g) *¿Cuántas funciones hay entre el conjunto 1, 2, . . . , n y el conjunto 0, 1?*
(6) *Un palíndromo es una cadena que se lee igual de derecha a izquierda que de izquierda a derecha. ¿Cuántas cadenas de n caracteres son palíndromos?*

Cuando las tareas no son ajenas se puede usar el principio de inclusión-exclusión. La idea es que bajo estas condiciones el simple uso de la regla de la suma cuenta doble las tareas repetidas. Por lo que, de la suma, se deben de restar los elementos de la intersección.

TEOREMA 17 (inclusión-exclusión). *Sean A, B conjuntos con conjunto universal E. Entonces*

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

DEMOSTRACIÓN. Tenemos que

$$(A \cap B^c) \cup B = A \cup B \tag{4}$$

pues

$$\begin{aligned} A \cup B &= (A \cap E) \cup B \\ &= (A \cap (B \cup B^c)) \cup B \\ &= ((A \cap B) \cup (A \cap B^c)) \cup B && \text{distributiva,} \\ &= (A \cap B^c) \cup ((A \cap B) \cup B), && \text{conmutativa y asociativa} \\ &= (A \cap B^c) \cup B, && \text{pues } A \cap B \subseteq B \end{aligned}$$

Similarmente se demuestra que

$$(A^c \cap B) \cup A = A \cup B. \tag{5}$$

Además se cumple que

$$(A \cap B^c) \cup (A^c \cap B) \cup (A \cap B) = A \cup B \tag{6}$$

pues

$$\begin{aligned}(A \cap B^c) \cup (A^c \cup B) \cup (A \cap B) &= (A \cap B^c) \cup ((A^c \cup A) \cap B) \\ &= (A \cap B^c) \cup B \\ &= A \cup B \qquad \text{según (4).}\end{aligned}$$

Para contar los elementos de $A \cup B$ podemos usar la regla generalizada de la suma en la ecuación (6), pues los conjuntos del lado izquierdo son ajenos:

$$\begin{aligned}(A \cap B^c) \cap (A^c \cap B) &= \varnothing \\ (A \cap B^c) \cap (A \cap B) &= \varnothing \\ (A \cap B^c) \cap (A \cap B) &= \varnothing;\end{aligned}$$

y obtenemos

$$|A \cup B| = |A \cap B^c| + |A^c \cap B| + |A \cap B|$$

pero de (4) $|A \cup B| = |A \cap B^c| + |B|$, de donde $|A \cap B^c| = |A \cup B| - |B|$; y de la ecuación (5), de forma similar, obtenemos $|A \cup B| = |A^c \cap B| - |A|$. Por lo que

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

despejando y cancelando:

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

□

El teorema de inclusión-exclusión puede redactarse de la forma siguiente:

Principio de inclusión-exclusión: si una tarea T_2 se puede realizar de n_1 formas y una tarea T_2 se puede realizar de n_2 formas entonces, las formas de realizar la tarea T_1 ó T_2 es $n_1 + n_2$ menos las formas de realizar simuláneamente las tareas T_1 y T_2.

Ejemplo 143. ¿Cuántas cadenas de bits hay que tengan longitud 8 y que comiencen con 1 o bien que terminen en 00?

Sol. El número de cadenas de longitud 8 que comienzan en 1 es 2^7, mientras que el número de cadenas de longitud 8 que terminan en 00 es $2^6 = 64$. A su vez, el número de cadenas que comienzan con 1 y terminan en 00 es $2^5 = 32$. Luego el total pedido es

$$128 + 64 - 32 = 60.$$

□

Ejemplo 144. En la versión 4 del protocolo de Internet (IPv4) a cada máquina conectada se le asigna una cadena de caracteres de 32 bits (dirección IP). La cadena tiene un *netid* (número de red) y un *hostid* (número de servidor).

Se usan tres formas de direcciones con una cantidad diferente de bits para el netid y el hostid:

- Clase A (direcciones de redes grandes): la dirección IP empieza con un 0 y luego un netid de 7 bits. El hostid usa los restantes 24 bits.
- Calse B (direcciones de redes medianas): empiezan con 10 y lluego el netid usa 14 bits y el hostid los restantes 16 bits.

- Clase C (dirección de redes pequeñas): empiezan con 110 seguido por un netid de 21 bits y un hostid de 8 bits.

Existen resticciones:

- Clase A: ningún netid es 1111111; ningún hostid está compuesto de sĺo 0's y 1's.
- Clase B: ningún hostid está compuesto de sĺo 0's o sólo 1's.
- Clase C: las mismas que en la clase B.

¿Cuántas direcciones disponibles IP hay según el sistema IPv4?

Sol. Sean P_A el conjunto de cadenas de clase A, P_B las de clase B y P_C las de clase C. Notemos que tales conjuntos son ajenos. Luego el numńero total pedido es

$$|P_A| + |P_B| + |P_C|.$$

Contemos los elementos de P_A, P_B, P_C.

Para P_A: el netid se puede elegir de $2^7 - 1$ formas (recordar que sólo unos no está permitido) y el hostid de $2^24 - 2$ (hay dos exepciones). Luego

$$|P_A| = (2^7 - 1)(2^24 - 2) = 2,130,706,178.$$

Para P_B: el netid se puede elegir de 2^{14} formas y el hostid de $2^{16} - 2$ formas:

$$|P_B| = 2^{14}(2^{16} - 2) = 1,073,709,056$$

Similarmente

$$|P_C| = 2^{21}(2^8 - 2) = 532,676,608.$$

Luego es número de direcciones según IPv4 es

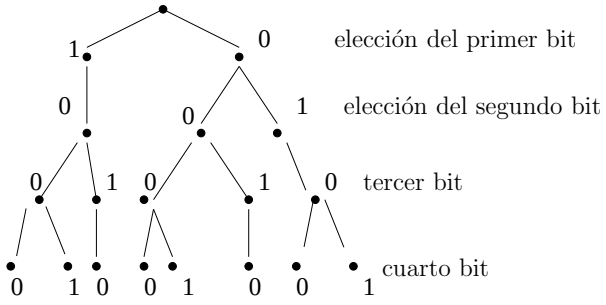
$$2,130,706,18 + 1,073,709,056 + 532,576,608 = 3,737,091,842.$$

□

2.1. Diagramas de árbol.

Ejemplo 145. ¿Cuántas cadenas de bits de longitud cuatro no tienen dos unos consecutivos?

Sol. La eleción del primer bit se puede hace de dos formas. La elección del segundo bit, debido a nuestras restricciones se puede hacer de una forma si el primer bit fué 1 o bien de dos formas si el primer bit fué 0. La elección del tercer bit va a depender de como se eligió el segundo, etc. tales dependencias las podemos visualizar en un diagrama



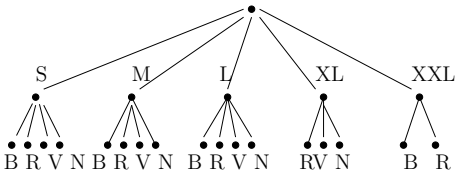
Los caminos (de arriba hacia abajo) dan las cadenas posibles:

$$000, 1001, 1010, 0000, 0001, 0010, 0100, 0101$$

luego hay 8 cadenas. □

EJEMPLO 146. Supongamos que un modelo de camiseta se fabrica en cinco tallas: S,M,L,XL,XXL. Supóngase además que cada talla se fabrica en colores blanco, negro, rojo y verde exepto la talla XXL que se fabrica en verde y negro y la XL en rojo, verde y negro. ¿Cuántas camisetas diferentes debe haber en el almacén de una tienda si se quiere tener disponible una de cada modelo?

SOL. El diagrama de árbol es:



Luego, el número total de modelos es $4 * 3 + 3 + 2 = 17$. □

3. Principio del palomar

Supóngase un grupo de palomas dispuestas a anidar. Si hay más palomas que nidos entonces debe haber algún nido con más de una paloma.

TEOREMA 18. *Si $f : A \to B$ función y $|A| > |B|$ con A, B finitos, entonces existen $a \neq a'$ en A tales que $f(a) = f(a')$.*

DEMOSTRACIÓN. Como $|A| > |B|$ entonces f no puede ser inyectiva, esto es existen $a, a' \in A$ con $f(a) = f(a')$ pero $a \neq a'$. □

COROLARIO 3. *Si se colocan $K+1$ objetos en K cajas diferentes existe al menos una caja que contiene dos o más objetos.*

DEMOSTRACIÓN. Sea A el conjunto de objetos y B el conjunto de cajas. Si $A = \{a_1, a_2, \ldots, a_{K+1}\}$ y $B = \{c_1, c_2, \ldots, c_k\}$ definimos una función $f : A \to B$ como $f(a_i) = c_j$ si c_j contiene a a_i (es decir, $a_i f c_j$ si c_j contiene a a_i).

Como $|A| > |B|$ entonces existen $a_i \neq a_\ell$ tales que $f(a_i) = f(a_\ell)$, es decir a_i y a_ℓ están en la misma caja. □

EJEMPLO 147. En un grupo de 367 personas debe haber dos personas que cumplan años el mismo día, pues sólo hay 366 posibles fechas de cumpleaños.

EJEMPLO 148. En un grupo de 28 palabras debe haber al menos dos que comiencen con la misma letra ya que sólo hay 27 letras en el alfabeto español.

EJEMPLO 149. *Demostrar que todo número entero n tiene un múltiplo cuya expresión decimal está compuesta sólo de 0's y 1's.*

DEMOSTRACIÓN. Consideremos los números

$$1, 11, 111, \ldots, \underbrace{111\cdots1}_{(n+1)-\text{unos}}$$

y pongamos sus residuos al dividir por n:

$$r_1, \quad r_2, \quad \ldots, r_{n+1}$$

como los residuos cumplen $0 \leq r_i < n$ entonces tales residuos deben de repetirse, es decir, existen $j \neq i$ tales que $r_j = r_i$. Luego, como

$$\underbrace{11\cdots1}_{j\text{-unos}} = nq_j + r_j$$

y

$$\underbrace{11\cdots1}_{i\text{-unos}} = nq_i + r_i$$

restando lado a lado estas ecuaciones

$$\underbrace{11\cdots1}_{j\text{-unos}} - \underbrace{11\cdots1}_{i\text{-unos}} = n(q_j - q_i)$$

siendo el lado derecho un número con sólo ceros y unos. □

TAREA 55. (1) *En un cajón hay una docena de calcetines marrones y una docena de calcetines negros sin marcar. Un hombre elige los calcetines al azar.*
   (a) *¿Cuántos calcetines debe elegir para asegurar que al menos dos deben de ser del mismo color?*
   (b) *¿Cuántos calcetines debe elegir para asegurar que al menos dos son negros?*

(2) *Supongamos que en una clase hay 9 estudiantes.*
   (a) *Demuestra que en la clase hay al menos cinco chicos o al menos cinco chicas.*
   (b) *Demuestra que en la case hay al menos tres chicos o al menos siete chicas.*

(3) *Supongamos que en una clase de veinticinco estudiantes todos tienen entre dieciocho y veinte años.*
   (a) *Demuestra que hay al menos nueve estudiantes que tienen la misma edad.*
   (b) *Demuestra que hay bien al menos tres estudiantes de deciocho años, bien al menos 19 estudiantes de diecinueve años o bien cinco estudiantes de veinte años en la clase.*

4. Permutaciones

DEFINICIÓN 150. *Sea A un conjunto finito. Una* **permutación (sin repetición)** *de A es una lista ordenada de elementos distintos de A. Si tal lista tiene r elementos se llama r-***permutación**.

EJEMPLO 151. Sea $A = \{a, b, c\}$. Entonces (a, b, c) es una permutación de A. También (b, c, a) es una permutación de A diferente a la anterior. Mientras que (a, c) es una 2-permutación de A, (b, c) es 2-permutación de A, (c, b) es otra permutación de A.

DEFINICIÓN 152. *Con $P(n, r)$ se denota el número de r-permutaciones de un conjunto con n elementos.*

EJEMPLO 153. Sea $A = \{a, b, c\}$, entonces las 2-permutaciones de A son

$$(a, b), (b, a), (c, a), (a, c), (b, c), (c, b)$$

luego $P(3, 2) = 6$. Las 1-permutaciones de A son

$$(1), (2), (3)$$

por lo que $P(3, 1) = 3$. Mientras que las 3-permutaciones (=permutaciones) de A son

$$(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)$$

de donde $P(3, 3) = 6$.

Pudimos haber usado *Maxima* para hacer el ejemplo anterior: primero declaramos el conjunto A:

Maxima

```
A:{a,b,c};
```

$$\{a, b, c\}$$

enseguida calculamos el conjunto de permutaciones de A (=3-permutaciones) con la instrucción `permutations`:

Maxima

```
permutations(A);
```

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

El cálculo de las 2-permutaciones requiere un poco más de código. Con la instrucción `powerset` se calcula el conjunto potencia: esto es `powerset(A)` es 2^A:

Maxima

```
powerset(A);
```

$$\{\{\}, \{a\}, \{a, b\}, \{a, b, c\}, \{a, c\}, \{b\}, \{b, c\}, \{c\}\}$$

Con `cardinality` se calcula la cardinalidad de un conjunto:

Maxima

```
cardinality(powerset(A));
```

$$8$$

Con `powerset(A,n)` se calcula los subconjuntos de A de cardinalidad 2:

Maxima

```
powerset(A,2);
```

$$\{\{a,b\},\{a,c\},\{b,c\}\}$$

Ahora, como queremos las 2-permutaciones necesitamos calcular las permutaciones de cada uno de los elementos de esta última salida.

Para aplicar una instrucción `f` a los elementos de un conjunto o una lista se puede usar la instrucción `map`. Por ejemplo

Maxima

```
map(f,[a,1,2,3,7]);
```

$$[f(a), f(1), f(2), f(3), f(7)]$$

Probamos con `f` como `permutations`:

Maxima

```
P:map(permutations,powerset(A,2));
```

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

Estas aún no forman el conjunto de 2-permutaciones, pues cuando calculamos su cardinalidad da:

Maxima

```
cardinality(P);
```

$$3$$

lo cual es evidentemente incorrecto. El problema son las llaves anidadas. Podemos quitar llaves con la instrucción `flatten`.

Maxima

```
P:flatten(P);
```

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

Luego este es el conjunto de las 2-permutaciones de $A=\{a,b,c\}$:

Maxima

```
cardinality(P);
```

$$6$$

Podemos resumir nuestra serie de instrucciones como una composición de funciones:

Maxima

```
permutaciones(A,r):=flatten(map(permutations,powerset(A,r)));
```

$$\text{permutaciones}\,(A,r) := \text{flatten}\,(\text{map}\,(\text{permutations}, \text{powerset}\,(A,r)))$$

Esto es, hemos creado un procedimiento general llamado `permutaciones` que calcula de un conjunto A el conjunto de r-permutaciones. Por ejemplo; las 3-permutaciones de $\{0,1,2,3,7,8\}$ son

Maxima

```
permutaciones({0,1,2,3,7,8},3);
```

$$\{[0,1,2],[0,1,3],[0,1,7],[0,1,8],[0,2,1],[0,2,3],[0,2,7],[0,2,8],[0,3,1],[0,3,2],$$
$$[0,3,7],[0,3,8],[0,7,1],[0,7,2],[0,7,3],[0,7,8],[0,8,1],[0,8,2],[0,8,3],[0,8,7],$$
$$[1,0,2],[1,0,3],[1,0,7],[1,0,8],[1,2,0],[1,2,3],[1,2,7],[1,2,8],[1,3,0],[1,3,2],$$
$$[1,3,7],[1,3,8],[1,7,0],[1,7,2],[1,7,3],[1,7,8],[1,8,0],[1,8,2],[1,8,3],[1,8,7],$$
$$[2,0,1],[2,0,3],[2,0,7],[2,0,8],[2,1,0],[2,1,3],[2,1,7],[2,1,8],[2,3,0],[2,3,1],$$
$$[2,3,7],[2,3,8],[2,7,0],[2,7,1],[2,7,3],[2,7,8],[2,8,0],[2,8,1],[2,8,3],[2,8,7],$$
$$[3,0,1],[3,0,2],[3,0,7],[3,0,8],[3,1,0],[3,1,2],[3,1,7],[3,1,8],[3,2,0],[3,2,1],$$
$$[3,2,7],[3,2,8],[3,7,0],[3,7,1],[3,7,2],[3,7,8],[3,8,0],[3,8,1],[3,8,2],[3,8,7],$$
$$[7,0,1],[7,0,2],[7,0,3],[7,0,8],[7,1,0],[7,1,2],[7,1,3],[7,1,8],[7,2,0],[7,2,1],$$
$$[7,2,3],[7,2,8],[7,3,0],[7,3,1],[7,3,2],[7,3,8],[7,8,0],[7,8,1],[7,8,2],[7,8,3],$$
$$[8,0,1],[8,0,2],[8,0,3],[8,0,7],[8,1,0],[8,1,2],[8,1,3],[8,1,7],[8,2,0],[8,2,1],$$
$$[8,2,3],[8,2,7],[8,3,0],[8,3,1],[8,3,2],[8,3,7],[8,7,0],[8,7,1],[8,7,2],[8,7,3]\}$$

Podemos calcular su cardinalidad;

Maxima

```
cardinality(permutaciones({0,1,2,3,7,8},3));
```

$$120$$

Si se quiere calcular $P(n,r)$ siguiendo el procedimiento anterior, este no resulta muy eficiente. Es mejor usar

TEOREMA 19. *Si* $n \geq r$

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$$

DEM. Sea $A = \{a_1, \ldots, a_n\}$ un conjunto con n elementos. Luego para formar una r-permutación se tiene que elegir un primer elemento de A lo cual se puede hacer de n formas. La elección del segundo elemento se puede hacer de $n-1$ formas pues no se debe de repetir el primero, similarmente el tercer elemento se puede elegir de $n-2$ formas, etc. El último elemento de la lista, es decir, el r-ésimo se puede elegir de $n-r+1$ formas. Luego, segun la regla del producto generalizada, tenemos que

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1).$$

□

EJEMPLO 154. ¿Cuántas formas existen de escoger el primer, segundo y tercer clasificado de un concurso, si hay un total de 100 concursantes?

SOL. Los primeros tres lugares forman listas de 3 elementos, i.e., 3-permutaciones de un conjunto de 100 concursantes. Luego, el número pedido es

$$P(100,3) = 100 * 99 * 98 = 970,200$$

□

EJEMPLO 155. Supongamos na carrera con 8 participantes. El ganador recibe oro, el segundo lugar plata y el tercer bronce ¿de cuántas formas distintas se pueden distribuir las medallas si no hay empates?

SOL. Los medallistas formas listas de 3 elementos, esto es 3-permutaciones de 8 elementos. El número pedido es

$$P(8,3) = 8 * 7 * \underbrace{6}_{8-3+1} = 336.$$

□

EJEMPLO 156. Supongamos que un agente viajero debe visitar 8 ciudades diferentes. Debe de comenzar su trabajo en una ciudad prefijada, pero tiene libertad de elegir las restantes ¿De cuántas formas distintas puede organizar su viaje?

SOL. Las restantes 7 ciudades forman listas de 7 elementos de un total de 7. Por lo que la respuesta es

$$P(7,7) = 7 * 6 * 5 * 4 * 3 * 2 * \underbrace{1}_{7-7+1} = 7! = 5040$$

□

EJEMPLO 157. ¿Cuántas permutaciones de las letras ABCDEFGH contienen la cadena ABC?

SOL. En tales permutaciones la cadena ABC se comporta como una sola letra. Luego, el número pedido es

$$P(6,6) = 6! = 720.$$

□

5. Combinaciones

DEFINICIÓN 158. *Una* r**-combinación** *de elementos de un conjunto es un subconjunto de* r *elementos, es decir, una colección de* r *elementos sin ordenar.*

EJEMPLO 159. Sea $A = \{1, 2, 3, 4\}$. Entonces $\{1, 4, 3\} = 1, 3, 4$ es una 3-combinación de A. Todas las 2-combinaciones de A son

$$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$$

En general, las r-combinaciones de un conjunto A se pueden calcular en *Maxima* con la instrucción `powerset(A,r)`. Por ejemplo

Maxima

```
A:{1,2,3,4}
```

es el conjunto de nuestro ejemplo. Y todas las 2-combinaciones de tal conjunto resultan de

Maxima

```
powerset(A,2);
```

$$\{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$$

DEFINICIÓN 160. *Con* $C(n, r)$ *se denota al número de* r*-combinaciones de un conjunto de* n *elementos.*

EJEMPLO 161. Sea $A = \{a, b, c, d\}$.

Maxima

```
A:{a,c,b,d};
```

$$\{a, b, c, d\}$$

Consideremos las 2-combinaciones de A:

Maxima

```
powerset(A,2);
```

$$\{\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\},\{c,d\}\}$$

cuyo número es 6. Por lo tanto

$$C(4,2)=6$$

También $C(4,1)=4$ pues

Maxima

```
powerset(A,1);
```

$$\{\{a\},\{b\},\{c\},\{d\}\}$$

mientras que $C(4,0)=1$ pues

Maxima

```
powerset(A,0);
```

$$\{\{\}\}$$

el cual tiene un elemento. También $C(4,4)=1$ porque

Maxima

```
powerset(A,4);
```

$$\{\{a,b,c,d\}\}$$

TEOREMA 20. *Sea $n \geq r \geq 0$, entonces*

$$C(n,r)=\frac{n!}{r!\,(n-r)!}$$

DEMOSTRACIÓN. Las r-permutaciones de un conjunto de n elementos se forman de las r-combinaciones por permutación de éstas. Es decir, para obtener las r-permutaciones podemos hacer lo siguiente:

(1) poner una r-combinación (de $C(n,r)$ formas);
(2) se permutan los elementos de éstas (de $P(r,r)=r!$ formas)

por lo que

$$P(n,r) = C(n,r)r!$$

y despejando

$$C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{(n-r)!\,r!}$$

□

Nótese que

$$C(n,r) = \binom{n}{r}$$

La instrucción en *Maxima* para calcular el binomial, y en consecuencia en número de r-combinaciones de un conjunto de n elementos es `binomial(n,r)`.

Ejemplo 162. ¿De cuántas formas se pueden seleccionar cinco jugadores de un grupo de diez para formar un equipo?

Sol. Tenemos que contar los subconjuntos de 5 elementos de un total de 10. Este es $C(10,5)$:

Maxima

```
binomial(10,5);
```

252

$$C(10,5) = \frac{10!}{5!\,5!} = 252.$$

□

Ejemplo 163. Un grupo de 38 personas han sido entrenadas para ir a Marte. La tripulación contará sólo de seis miembros. ¿De cuántas formas se puede seleccionar la tripulación?

Sol.

$$C(30,6) = \frac{30!}{24!\,6!} = 593,775$$

Maxima

```
binomial(30,6);
```

593775

□

EJEMPLO 164. ¿Cuántas cadenas de n bits contienen exactamente r unos?

SOL. Para formar tales cadenas se tienen que elegir las posiciones de los unos de los números $1, 2, 3, \ldots, n$, es decir, se tiene que elegir r números de $\{1, 2, 3, \ldots, n\}$, lo cual se puede hacer de

$$C(n, r) = \frac{n!}{(n-r)!\, r!}$$

formas. □

EJEMPLO 165. De cuántas formas se puede seleccionar una comisión integrada de 3 hombre y 4 mujeres si hay disponibles 9 hombres y 11 mujeres?

SOL. Primero se pueden elegir los hombre; de $C(9, 3) = \frac{9!}{6!3!} = 84$ formas, y enseguida las mujeres, de $C(11, 4) = \frac{11!}{7!4!} = 330$ formas. Luego, la comisión se puede elegir de

$$84 * 330 = 27,720$$

formas. □

TAREA 56.
(1) *Escribir todas las permutaciones de* $\{a, b, c\}$.
(2) *¿Cuántas permutaciones tiene el conjunto* $\{a, b, c, d, e, f, g\}$*?*
(3) *¿Cuántas permutaciones del conjunto* $\{a, b, c, d, e, f, g\}$ *terminan en* a*?*
(4) *Sea* $S = \{1, 2, 3, 4, 5\}$.
   (a) *Enumera todas las 3-permutaciones de* S.
   (b) *Enumera todas las 3-combinaciones de* S.
(5) *Calcular*
   (a) $P(6, 3), P(6, 5), P(8, 8), P(10, 9)$
   (b) $C(5, 1), C(5, 3), C(8, 0), C(12, 6)$.
(6) *¿De cuántas formas diferentes pueden terminar una carrera de cinco corredores, si no hay empates?*
(7) *¿Cuántas posibilidades hay para las tres primeras posiciones de una carrera de caballos con doce participantes si son posibles todos los ordenes de llegada y no hay empates?*
(8) *Hay cuatro candidatos en las eleciones para presidente municipal. ¿De cuántas formas distintas se pueden imprimir los nombres en la papeleta electoral?*
(9) *¿Cuántas cadenas de diez bits contienen*
   (a) *exactamente cuatro unos?*
   (b) *como mucho cuatro unos?*
   (c) *al menos cuatro unos?*
   (d) *una cantidad igual de unos y ceros?*
(10) *En un grupo hay n hombres y n mujeres. ¿De cuántas formas se pueden ordenar estas personas en una fila si los hombres y las mujeres se deben alternar?*
(11) *¿De cuántas formas se pueden escoger un par de números enteros positivos menores que 100?*
(12) *¿Cuántos subconjuntos con un número imoar de elementos tiene un conjunto con diez elementos?*
(13) *¿Cuántos subconjuntos de más de dos elementos tiene un conjunto con 100 elementos?*

(14) *Se tira una moneda al aire diez veces y los resultados posibles son águila o sol. ¿Cuántos resultados*
   (a) *hay en total?*
   (b) *tiene exactamente dos soles?*
   (c) *tiene al menos tres soles?*
   (d) *tiene el mismo número de soles que de águilas?*

(15) *¿Cuántas cadenas de diez bits tienen*
   (a) *exactamente tres ceros?*
   (b) *más ceros que unos?*
   (c) *al menos siete ceros?*
   (d) *al menos tres unos?*

(16) *¿Cuántas permutaciones de las letras ABCDEFGH contienen*
   (a) *la cadena ED?*
   (b) *la cadena CDE?*
   (c) *las cadenas BA y FGH?*
   (d) *las cadenas AB, DE y GH?*
   (e) *las cadenas CAB y BED?*
   (f) *las cadenas BCA y ABF?*

(17) *Un conjunto de cien papeletas, numeradas del 1 al 100, se venden a cien personas diferentes para una lotería. Hay cuatro premios distintos, el primero de los cuales es un viaje a Cancún. ¿De cuántas formas se pueden repartir los premios si*
   (a) *no hay ninguna restricción?*
   (b) *la persona con la papeleta número 47 gana el primer premio?*
   (c) *la persona con la papeleta gana uno de los premios?*
   (d) *la persona con la papeleta número 47 no gana ningún premio?*
   (e) *las personas con las papeletas 19 y 47 ganas ambas algún premio.*

6. Permutaciones y combinaciones con repetición

6.1. Permutaciones con repetición. Hasta ahora hemos contado objetos que no se repiten. Veamos el caso contrario.

Ejemplo 166. ¿Cuántas cadenas de longitud n se pueden formar con las 27 letras del alfabeto español?

Sol. Tenemos que formar listas de longitud n; la primera letra se puede elegir de 27 formas, la segunda letra de 27 formas, etc. En total 27^n. □

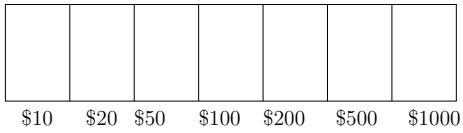
Estas listas se llaman **permutaciones con repetición**.

Teorema 21. *El número de r-permutaciones con repetición de un conjunto con n elementos es n^r.*

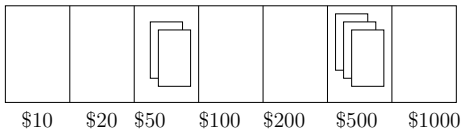
6.2. Combinaciones con repetición.

Ejemplo 167. ¿De cuántas formas se pueden seleccionar cinco biletes de una caja registradora que contiene billetes de 10, 20, 50, 100, 200, 500 y 1000?

Sol. Cuando seleccionamos los billetes los colocamos en nuestra propia caja que tiene etiquetas:



Por ejemplo, si tomamos 2 de 50 y 3 de 500:



Tal elección la podemos simbolizar con |'s y ∗'s:

$$||**|||***||$$

Por ejemplo, tomar 1 de 10, 1 de 20, 2 de 100 y 1 de 500 es:

$$*|*|**|||*$$

Así, una selección es de 11 lugares disponibles, poner |'s y ∗'s. de hecho sólo importan los ∗'s, pues una vez elegidos éstos, se puede deducir donde están los |'s o bien sólo importan los |'s. Luego, el número pedido es $C(11,5)$ ó $C(11,6)$:

$$C(11,5) = C(11,6) = 462.$$

□

TEOREMA 22. *En un conjunto con n elementos hay* $C(n+r-1,r)$ *r-combinaciones con repetición de n elementos.*

SOL. Cada r-combinación con repetición se puede representar como una lista de $n-1$ barras y r asteriscos. Por ejemplo

$$**|*||***$$

es una 6-combinación de 4 elementos, con 2 del primer tipo, 1 del segundo tipo y 3 del cuarto tipo.

El número de estas es

$$C(\underbrace{n-1}_{\text{número de barras}} + \underbrace{r}_{\text{número de asteriscos}}, r) = C(n-1+r, n-1)$$

□

EJEMPLO 168. Supongamos que una tienda de galletas tiene cuatro diferentes tipos de galletas; ¿de cuántas formas se pueden seleccionar 6 galletas?

SOL. Tenemos 4 tipos. Y una seleción la podemos indicar con barras y asteriscos. Por ejemplo,

$$***|*|*|**$$

indica una selección con 3 del primer tipo de galleta, 1 del segundo tipo, 1 del tercer y 2 del cuarto tipo; estas son 6-combinaciones con repetición de un conjunto de 4, cuyo número total es

$$C(4-1+6,6) = C(9,6) = 84.$$

□

EJEMPLO 169. ¿Cuántas soluciones enteras x_1, x_2, x_3 no negativas tiene la ecuación

$$x_1 + x_2 + x_3 = 11?$$

SOL. Tenemos que

$$1+1+1+1+1+1+1+1+1+1+1 = 11 \tag{7}$$

y entonces una solución en x_1, x_2, x_3 corresponde a poner un par de barras para separar los unos de la ecuación (7):

$$\underbrace{1+\cdots+1}_{x_1}+|\underbrace{1+\cdots+1}_{x_2}+|\underbrace{1+\cdots+1}_{x_3} = 11$$

por lo que las soluciones forman 11-combinaciones con repetición de un conjunto de 3 elementos. El número de ellas es

$$C(11+3-1,11) = C(13,11) = \frac{11!}{2!\,7!} = 78$$

Maxima

```
binomial(13,11);
```

78

□

EJEMPLO 170. ¿Cuántas soluciones tiene la ecuación

$$x_+x_2 + x_3 = 11$$

si x_1, x_2, x_3 son enteros tales que $x_1 \geq 1$, $x_2 \geq 2$ y $x_3 \geq 3$?

SOL. Definimos nuevas variables:

$$x_1' = x_1 - 1, x_2' = x_2 - 2, x_3' = x_3 - 3$$

luego

$$x_1' \geq 0, x_2' \geq 0, x_3' \geq 0$$

y tenemos que resolver

$$x_1 - 1 + x_2 - 2 + x_3 - 3 = 11 - 6$$

i.e,

$$x_1' + x_2' + x_3' = 5$$

cuyas soluciones corresponden a 5-combinaciones con repetición de 3 objetos: en total hay

$$C(3+5-1,5) = C(7,5) = 21$$

□

EJEMPLO 171. ¿De cuántas formas se pueden colocar diez bolas iguales en 8 cajas distintas?

Sol. Las bolas se pueden representar con $*$ y las cajas con $|$. Por ejemplo

$$***||**|**||*||**$$

corresponde a una 10-combinación con repetición de 8 elementos. En total hay

$$C(8+10-1,10) = C(17,10) = 19,448.$$

□

Ejemplo 172. ¿Cuányas cadenas distintas se pueden formar reordenando las letras de la palabra PAPAYA?

Sol. Un reordenamiento corresponde a una selecci'on de

(1) las posiciones de las letras A's
(2) las posiciones de las letras P's

entonces la letra Y queda completamente determinada:

(1) de $C(6,3) = 20$ formas
(2) $C(3,2) = 3$ formas

luego el total es $C(6,3) * C(3,2) = 60$. □

Teorema 23. *El número de n-permutaciones con repetición donde hay n_1 objetos indistinguibles de tipo 1, n_2 objetos indistinguibles de tipo 2,..., n_k objetos indistinguibles de tipo k es*

$$\frac{n!}{n_1!\,n_2!\cdots n_k!}$$

Demostración. Para formar una n-permutación, primero colocamosl los del tipo 1 de $C(n,n_1)$ formas, luego los del tipo 2, de $C(n-n_1,n_2)$ formas, del tipo 3 de $C(n-n_1-n_2,n_3)$ formas,..., los del tipo n_k de $C(n-n_1-\cdots-n_{k-1},n_k)$ formas. Luego hay en total

$$\begin{aligned} &C(n,n_1)C(n-n_1,n_2)C(n-n_1-n_2,n_3)\cdots C(n-n_1-\cdots-n_{k-1},n_k) \\ &\quad = \frac{n!}{(n-n_1)!\,n_1!}\frac{(n-n_1)!}{(n-n_1-n_2)!\,n_2!}\cdots\frac{(n-n_1-\cdots n_{k-1})!}{0!\,n_k!} \\ &\quad = \frac{n!}{n_1!\,n_2!\cdots n_k!} \end{aligned}$$

□

Ejemplo 173. ¿De cuántas formas se pueden distribuir a cuatro jugadores manos de 5 cartas usando una baraja de 52 cartas?

Sol. Al primer jugador se le distribuyen sus cartas de $C(52,5)$ formas, al segundo de $C(47,5)$ formas, al tercer de $C(42,5)$ formas y al cuarto de $C(37,5)$. En total

$$C(52,5)C(47,5)C(42,5)C(37,5) = \frac{52!}{5!\,5!\,5!\,5!} =$$

Maxima

```
52!/(5!)^4;
```

388976539211727809469814028049786684873116827936358400000000

□

TAREA 57. (1) *¿De cuántas formas se pueden asignar tres trabajos a cinco empleados si a cada empleado se le le puede asignar más de un trabajo?*

(2) *Todos lis días un estudiante elige al azar un bocadillo de una bandeja de bocadillos preparados. Si hay seis tipos de bocadillos ¿de cuántas formas puede el estudiante elegir los bocadillos para los siete días de la semana si tenemos en cuenta el orden en que los escoge?*

(3) *¿De cuántas formas se pueden seleccionar cinco elementos sin ordenar de un conjunto de tres elementos si se permite la repetición?*

(4) *¿De cuántas formas se pueden seleccionar tres elementos sin ordenar de un conjunto de cinco elementos si se permite la repetición?*

(5) *De cuántas formas se pueden escoger una docena de donas de entre las 21 variedades de una tienda?*

(6) *En un bar de tapas tiene patatas bravas, calamares, aceitunas, boqueones, jamón, queso tortilla y gambas. ¿De cuántas formas se pueden escoger*
   (a) *seis tapas?*
   (b) *una docena de tapas?*
   (c) *una docena de tapas con al menos uan de cada tipo?*
   (d) *una docena de tapas con al menos tres tapas de boquerones y no más de dos tapas de tortilla?*

(7) *Una tienda de cruasanes tiene cruasanes sin relleno, cruasanes con chocolte, cruasanes con crema, cruasanes con nata, cruasanes vegetales y crasanes con salmón. ¿De cuántas formas se pueden escoger*
   (a) *una docena de cruasanes?*
   (b) *tres docenas de cruasanes?*
   (c) *dos docenas de cruasanes con al menos dos de cad clase? dos docenas de cruasanes con no más de dos cruasanes con nata?*
   (d) *dos docenas de cruasanes con al menos cinco cruasanes de chocolate y al menos tres de crema?*
   (e) *dos docenas de curasanes con al menos un cruasán sin relleno, al menos dos de nata, al menos tres de chocolate, al menos uno de crema, al menos dos vegetales y no más de tres de salmón?*

(8) *¿De cuántas formas se puede elegir ocho monedas de un bolso que contiene 100 monedas de un euro y 80 monedas de dos euros?*

(9) *¿Cuántas soluciones tiene la ecuación*

$$x_1 + x_2 + x_3 + x_4 = 17$$

donde x_1, x_2, x_3, x_4 son enteros no negativos?

(10) *¿Cuántas soluciones tiene la ecuación*

$$x_1 + x_2 + x_3 + x_4 + x_5 = 21$$

donde x_i, $i = 1, 2, 3, 4, 5$ *son enteros no negativos tales que*
(a) $x_1 \geq 1$*?*
(b) $x_i \geq 2, i = 1, 2, 3, 4, 5$*?*
(c) $0 \leq xi \leq 10, i = 1, 2, 3, 4, 5$*?*
(d) $0 \leq xi \leq 3, 1 \leq x2 < 4, x3 \geq 15$*?*

(11) *¿Cuántas soluciones tiene la ecuación*

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 29$$

donde $x_1, x_2, x_3, x_4, x_5, x_6$ *son enteros no negativos tales que*
(a) $x_i > 1$ *para* $i = 1, 2, 3, 4, 5, 6$*?*
(b) $x_i \geq i$, $i = 1, 2, 3, 4, 5, 6$*?*
(c) $x_1 \leq 5$*?*
(d) $x1 < 8$ *y* $x_2 > 8$*?*

(12) *¿De cuántas formas se pueden distribuir seis bolas indistinguibles en nueve cajas distintas?*

(13) *¿De cuántas formas se pueden distribuir 12 bolas indistinguibles en seis cajas distintas?*

(14) *¿De cuántas formas se pueden distinguir 12 objetos distinguibles en seis cajas distinguibles, de forma que se coloquen dos objetos en cada caja?*

(15) *¿De cuántas formas se pueden distribuir 15 objetos distinguibles entre cinco cajas distintas de forma que las cajas contengan uno, dos, tres cuatro y cinco objetos respetivamente?*

(16) *¿Cuántas cadenas distintas se pueden formar con asl letras de las palabra MISSISSIPPI si hay que utilizarlas todas?*

(17) *17) ¿Curítas cadenas distintas se pueden formar con las letras de la palabra ABRACADABRA si hay que utilizar todas las letras?*

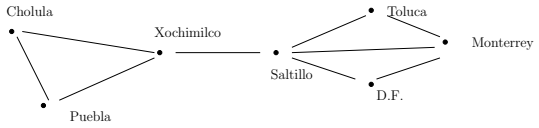
(18) *¿Cuántas cadenas distintas se pueden formar con las letras de AARDVARK si hay que utilizar todas las letrasy las tres letras A deben de aparecer de forma consecutiva?*

(19) *¿Cuántas cadenas distintas se pueden formar con las letras de ORONO si se pueden utilizar todas o una parte de las letras?*

CAPíTULO 6

Grafos

Supóngase varias comptadoras en diferentes ciudades conectadas por una red telefónica:



Tal dibujo representa un *grafo simple.*

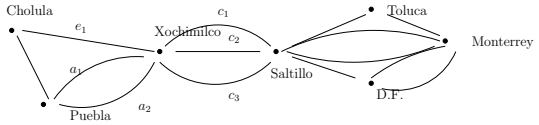
DEFINICIÓN 174. *Un* **grafo simple** G *es un par* (V, E) *donde* V *es un conjunto no vacío de vértices y* E *es un conjunto formado por parejas no ordenadas de vértices distintos.*

EJEMPLO 175. En el dibujo anterior:

$$V = \{Cholula, Puebla, Xochimilco, Saltillo, Toluca, D.F., Monterrey\}$$

$$E = \{\{Cholula, Puebla\}, \{Cholula, Xochimilco\}, \{Puebla, Xochimilco\},$$
$$\{Xochimilco, Saltillo\}, \{Saltillo, Toluca\}, \{Saltillo, Monterrey\}, \{Saltillo, D.F.\},$$
$$\{Toluca, Monterrey\}, \{D.F., Monterrey\}\}$$

Si en ejemplo anterior se tienen varias lineas telefónicas entre computadoras:



se tiene entonces un *multigrafo.*

DEFINICIÓN 176. *Un* **multigrafo** G *es un par* (V, E) *donde* V *es un conjunto de vértices y* E *es un conjunto de aristas; además de una función*

$$f : E \to \{\, \{u, v\} \,|\, u, v \in V \text{ con } u \neq v\}$$

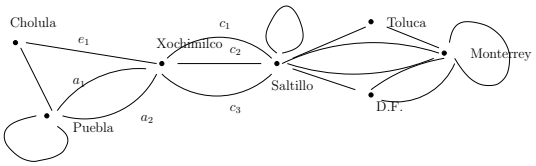
Se dice que las aristas e_1, e_2 *son* **paralelas** *o* **múltiples** *si* $f(e_1) = f(e_2)$.

La función f dice los vértices que son unidos por una arista.

EJEMPLO 177. El el diagrama anterior:

$$f(e_1) = \{Cholula, Xochimilco\}, \quad f(a_1) = \{Puebla, Xochimilco\},$$
$$f(a_2) = \{Puebla, Xochimilco\}$$

Ni en los grafos simples, ni en los multigrafos se admiten bucles: para eso están los **pseudografos**:

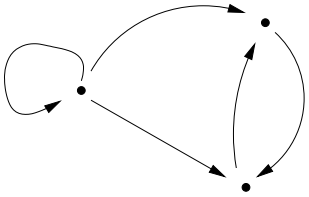


DEFINICIÓN 178. *Un* **pseudografo** G *es un par* (V, E) *donde* V *es un conjunto de vértices y* E *de aristas; además de una función*

$$f : E \to \{\{u, v\} \mid u, v \in V\}$$

Una arista e *es un* **bucle** *o* **lazo** *si* $f(e) = \{u, u\} = \{u\}$ *para algún* $u \in V$.

Un *grafo dirigido* o *digrafo* es algo como:



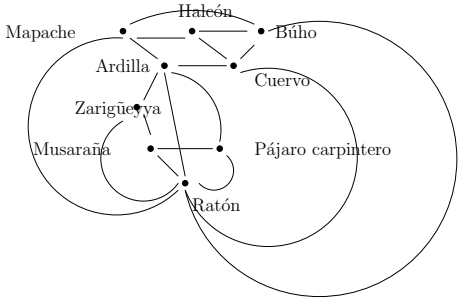
DEFINICIÓN 179. *Un* **grafo dirigido** G *es un par* (V, E) *donde* V *es un conjunto de vértices y* E *es un conjunto de pares ordenados de vértices llamados aristas.*

Similarmente a los anterior existen grafos dirigidos simples, multigrafos y pseudografos.

EJEMPLO 180 (Grafos de solapamiento en Ecología).

- Vértices: especies animales
- Aristas: se conecta dos vertices a y b si la especia a compite con la especie b, es decir si tienen la misma fuente de alimento.

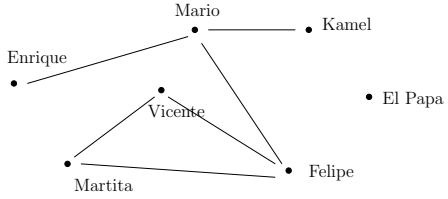
Por ejemplo:



Significa que los ratones compiten con casi todos.

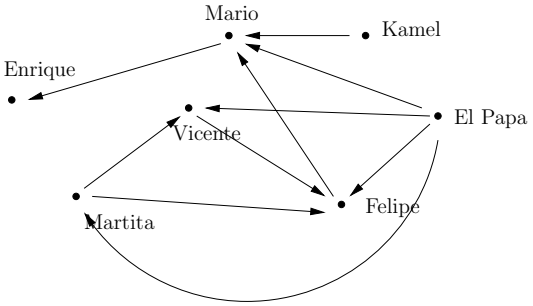
EJEMPLO 181 (Grafos de conocidos).

- Vértices: personas.
- Aristas: se conecta la persona a con la b si son amigos.



Ejemplo 182 (Grafo de influencia).

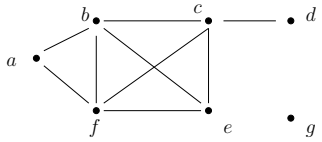
- Vértices: personas.
- Aristas: $a \to b$ si a influye sobre b.



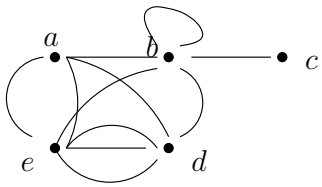
Definición 183. *Sea G un grafo no dirigido. Dos vértices u, v se dicen* **adyacentes** *o* **vecinos** *si $\{u, v\}$ es arista de G. Si $e = \{u, v\}$ es arista de G entonces e es* **incidente** *con u y v y se dice que e* **conecta** *u con v; también se dice que u, v son* **extremos** *de e.*

Definición 184. *Si v es un vértice de un grafo no dirigido, el* **grado** *de v es $\delta(v)$ que es el número de aristas que inciden en v exepto los bucles que contribuyen con dos a tal grado.*

Ejemplo 185.



$$\delta(a) = 2, \delta(b) = 4 = \delta(c) = \delta(f), \delta(d) = 1, \delta(d) = 1, \delta(e) = 3, \delta(g) = 0.$$



$$\delta(a) = 4, \delta(b) = 6, \delta(c) = 1, \delta(d) = 5, \delta(e) = 6.$$

Teorema 24 (Apretones de mano). *Sea $G = (V, E)$ un grafo no dirigido con $e = |V|$. Entonces*

$$\sum_{v \in V} \delta(v) = 2e.$$

Ejemplo 186. ¿Cuántas aristas hay en un grafo con diez vértices si cada una de las cuales stiene grado 6?

Sol. Por el teorema de apretones de manos:

$$2e = \sum_{v \in V} \delta(v) = 10 * 6$$

de donde $e = 30$. □

COROLARIO 4. *Todo grfo no dirigido $G = (V, E)$ tiene un número par de vértices de grado impar.*

DEMOSTRACIÓN. Sea V_1 el conjunto de vértices de grado par y V_2 el de grado impar. Entonces

$$2|E| = \sum_{v \in V} \delta(v) = \sum_{v \in V_1} \delta(v) + \sum_{v \in V_2} \delta(v)$$

lo que implica que

$$\underbrace{2|E| - \underbrace{\sum_{v \in V_1} \delta(v)}_{\text{par}}}_{\text{par}} = \sum_{v \in V_2} \underbrace{\delta(v)}_{\text{impar}}$$

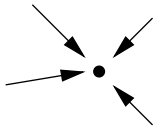
Como la única forma que la suma de impares sea par es que con un número de sumandos par, se sique que $|V_2|$ es par. □

DEFINICIÓN 187. *Si $e = (u, v)$ es una arista de un grafo dirigido G entonces*

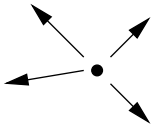
(1) *u es* **adyacente** *a v;*
(2) *v es* **adyacente** *desde u;*
(3) *u es* **vértice inicial**, **vértice final** *de e.*

DEFINICIÓN 188. *Sea v vértice de un grafo G dirigido:*

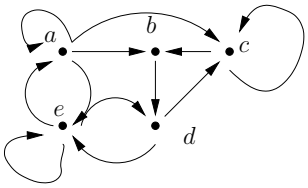
(1) *$\delta^-(v)$ es el* **grado de entrada** *de v y este es el número de aristas que tiene a v como vértice final.*



(2) *$\delta^+(v)$ el el* **grado de salida** *de v y el número de aristas que tiene a v como vértice inicial.*



EJEMPLO 189.



$$\delta^-(a) = 2 \qquad \delta^+(a) = 4$$
$$\delta^-(b) = 2 \qquad \delta^+(b) = 1$$
$$\delta^-(c) = 3 \qquad \delta^+(c) = 2$$
$$\delta^-(d) = 2 \qquad \delta^+(d) = 2$$
$$\delta^-(e) = 3 \qquad \delta^+(e) = 3$$

TEOREMA 25. *Sea $G = (V, E)$ un grafo dirigido. Entonces*

$$\sum_{v \in V} \delta^-(v) = |E| = \sum_{v \in V} \delta^+(v).$$

DEMOSTRACIÓN. Sea $V = \{v_1, \ldots, v_n\}$. Para cada $v_i \in V$ ponemos

$$V^-(v_i) = \{(u, v_i) \in E \,|\, u \in V\}.$$

Luego $\delta^-(v_i) = |V^-(v_i)|$; además

$$E = V^-(v_1) \cup V^-(v_2) \cup \ldots V^-(v_n)$$

pues si $e \in E$ entonces $e = (v_i, v_j) \in V(v_i)$. También si $i \neq j$ entonces $V^-(v_i) \cap V(v_j) = \varnothing$ pues en otro caso $\exists e \in V^-(v_i) \cap V^-(v_j)$ lo que implica que e tiene vértice final v_i y v_j, esto es $v_i = v_j$: absurdo.

Luego por la regla de la suma

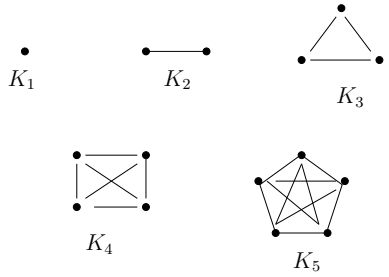
$$|E| = |V^-(v_1)| + |V^-(v_2)| + \cdots + |V^-(v_n)|$$
$$= \delta^-(v_1) + \delta^-(v_2) + \cdots + \delta^-(v_n).$$

Similarmente para δ^+. □

Hay grafos especiales:

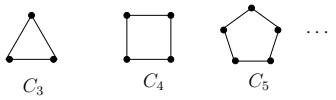
EJEMPLO 190 (Grafos completos). Sea $n \geq 1$, $n \geq 1$.
K_n:

- Vértices: n vértices.
- Aristas: exactamente una arista entre dos vértices.

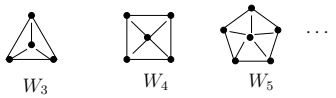


EJEMPLO 191 (Ciclos). Sea $n \in \mathbb{N}$, $n \geq 3$. Luego

- Vértices: $v_1, v_2, \ldots, v_n$;
- Aristas: $\{v_1, v_2\}, \{v_2, v_n\}, \ldots, \{v_n, v_1\}$.



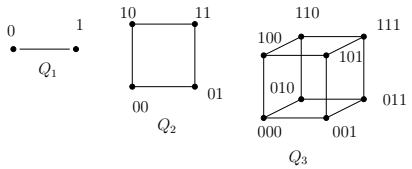
EJEMPLO 192 (Ruedas). $n \in \mathbb{N}$, $n \geq 3$.



EJEMPLO 193 (Cubos). *Sea $n \in \mathbb{N}$, $n \geq 1$.*
Q_n:

- *Vértices: cadenas de bits de longitud n.*

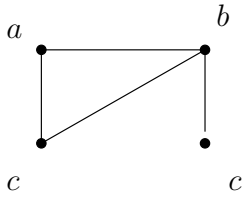
- *Aristas: dos cadenas son adyacentes si y sólo si difieren exactamente por un bit.*



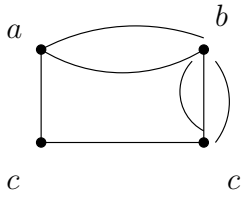
TAREA 58. (1) *¿Qué clase de grafo puede ser usado para modelar un sistema de carreteras entre ciudades donde*
   (a) *hay una arista entre los vértices representando ciudades si hay una carretera interestatal entre ellos?*
   (b) *hay una arista entre los vértices representando ciudades para cada carretera interestatal entre ellas?*
   (c) *hay una arista entre vértices representando ciudades para cada carretera interestatal entre ellas y hay un lazo en cada vértice representando una ciudad si hay una carretera interestatal que rodea la ciudad?*

(2) *Determine la clase de grafo que se muestra (simple, multigrafo, etc):*

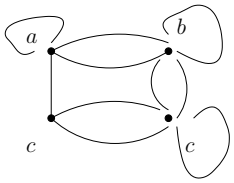
(a)



(b)



(c)



El grafo de intersección de una colección de conjuntos $A_1, A_2, \ldots, A_n$ es el grafo con vértices : $A_1, A_2, \ldots, A_n$ aristas : el vértice i se une con el j si $A_i \cap A_j \neq \varnothing$ Construir el grafo de intersección de las siguientes colecciones de conjuntos:

(a) $A_1 = \{0, 2, 4, 6, 8\}, A_2 = \{0, 1, 2, 3, 4\}, A_3 = \{1, 3, 5, 7, 9\}, A_4 = \{5, 6, 7, 8, 9\}, A_5 = \{0, 1, 8, 9\}$

(b)

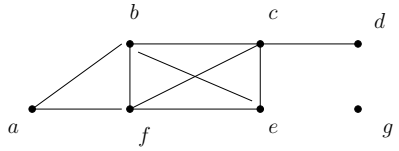
$$A_1 = \{\ldots, -4, -3, -2, -1, 0, \ldots\}$$
$$A_2 = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
$$A_3 = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$
$$A_4 = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$$
$$A_5 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

(c)

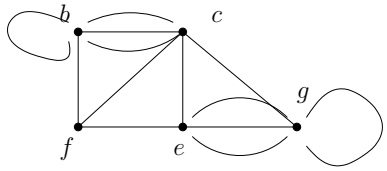
$$A_1 = \{x \,|\, x < 0\}$$
$$A_2 = \{x \,|\, 1 < x < 0\}$$
$$A_3 = \{x \,|\, 1 < x < 1\}$$
$$A_4 = \{x \,|\, 0 < x < 1\}$$
$$A_5 = \{x \,|\, x > 1\}$$

(3) *Hallar el número de vértices, el número de aristas y el grado de cada vértice:*

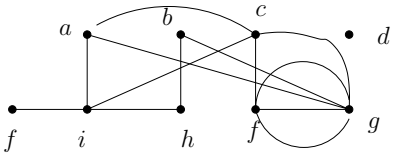
(a)



(b)



(c)



(4) *Hallar la suma de los grados de los vértices para cada grafo del problema anterior y comprobar que es el doble del número de aristas.*

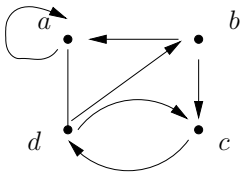
(5) *¿Puede existir un grafo con 15 vértices, cada uno de ellos de grado 5?*

(6) *Para cada una de las personas que asisten a una fiesta se considera el número de personas a las que ha saludado dándoles la mano. Demuestrar que la suma de todos esos números es un número par. Se supone que nadie se da la mano a sí mismo.*

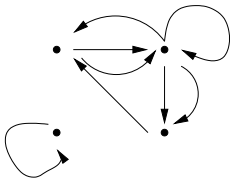
(7) *Determinar el número de vértices y de aristas, hallar los grados de entrada y de salida de cada uno de los vértices del multigrafo correspondiente.*

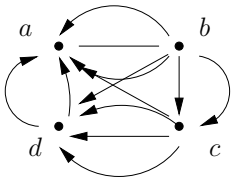
(a)

(b)



(c)





(8) *Para cada uno de los anteriores determinar la suma de los grados de entrada y la suma de los grados de salida. Comprobar que ambos son iguales al número de aristas que hay en el grafo.*
(9) *¿Cuántas aristas tiene un grafo si los grados de sus vértices son 4,3,3,2,2? Dibujarlo.*
(10) *¿Cuántas aristas tiene un grafo si los grados de sus vértices son 5,2,2,2,2,1? Dibujarlo.*
(11) *¿Existe algún grafo simple de seis vértices con los grados siguientes?. Si es así, dibuja un grafo con esta propiedad.*
   (a) *0,1,2,3,4,5*
   (b) *1,2,3,4,5,6*
   (c) *2,2,2,2,2,2*
   (d) *3,2,3,2,3,2*
   (e) *3,2,2,2,2,3*
   (f) *3,3,3,3,3,5*
   (g) *1,1,1,1,1,1*
   (h) *1,2,3,4,5,5*
(12) *Sea G un grafo con v vértices y e aristas. Sea M el máximo grado entre los vértices de G y sea m el mínimo grado de entre los vértices de G. Demostrar que*
   (a) $\frac{2e}{v} \geq m$
   (b) $\frac{2e}{v} \leq M$

1. Grafos y matrices

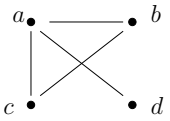
DEFINICIÓN 194. *Sea $G = (V, E)$ grafo no dirigido simple con $n = |V|$ y $V = \{v_1, \ldots, v_n\}$. Se define la* **matriz de adyacencia** *de G como*

$$A_G = (a_{ij})$$

donde

$$a_{ij} = \begin{cases} 1 & si\ \{v_i, v_j\} \in E \\ 0 & otro\ caso. \end{cases}$$

EJEMPLO 195. Sea G el grafo



Calcular su matriz de adyacencia

SOL.

$$A_G = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

□

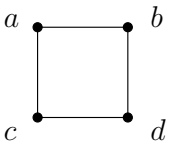
EJEMPLO 196. Dibujar el grafo con matriz de adyacencia

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

SOL. Numeramos los vértices: a, b, c, d. Luego

$$A_G = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

De donde obtenemos que el grafo G es



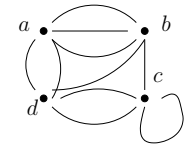
□

DEFINICIÓN 197. *Sea $G = (V, E)$ un pseudografo no dirigido (con bucles y/o aristas múltiples posiblemente). Se define la* **matriz de adyacencia** *de G como*

$$A_G = (a_{ij})$$

donde a_ij es el número aristas (múltiples) entre los vértices v_i y v_j.

EJEMPLO 198. *Sea*

$G:$ 

$$A_G = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 \end{pmatrix} \end{array}$$

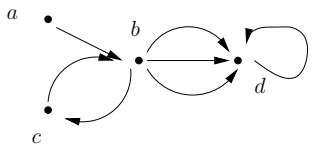
Nótese que A_G es simétrica para G grafo no dirigido.

DEFINICIÓN 199. *Sea $G = (V, E)$ multigrafo dirigido con $V = \{v_1, \ldots, v_n\}$. Se define la* **matriz de adyacencia** *de G como*

$$A_G = (a_{ij})$$

donde a_ij es el número de aristas que inician en el vértice v_i y finalizan en v_j.

EJEMPLO 200.

$G:$ 

$$A_G = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Com puede notarse del ejemplo anterior, la matriz de adyacencia A_G no es necesariamente siétrica cuando G es grafo dirigido.

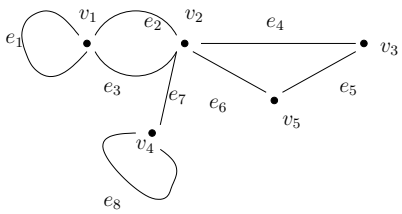
DEFINICIÓN 201. *Sea $G = (V, E)$ grafo no dirigido con $V = \{v_1, \ldots, v_n\}$, $n = |V|$ y $E = \{e_1, \ldots, e_m\}$ con $m = |E|$. La* **matriz de incidencia** *de G es*

$$M = (m_{ij})$$

donde

$$m_{ij} = \begin{cases} 1 & \text{si } e_j \text{ incide con } v_i \\ 0 & \text{otro caso.} \end{cases}$$

EJEMPLO 202. Sea



$$M_G = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

Tarea 59.

(1) *Representar los siguientes grafos mediante su matriz de adyacencia*
   (a) K_5
   (b) C_4
   (c) W_4
   (d) Q_3

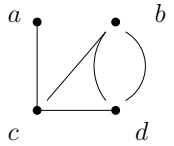
(2) *Dibujar el grafo cuya matriz de adyacencia es:*

(3) $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

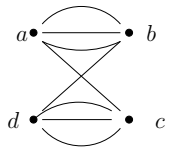
(4) $\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

(5) $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

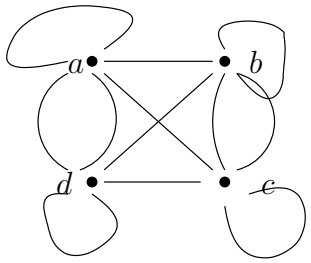
(6) *Representar el grafo correspondiente mediante su matriz de adyacencia*
   (a)



   (b)



   (c)



(7) *Dibujar el grafo dirigido representado por la matriz correspondiente.*

(a) $\begin{pmatrix} 1 & 3 & 2 \\ 3 & 0 & 4 \\ 2 & 4 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

(c) $\begin{pmatrix} 0 & 1 & 3 & 0 & 4 \\ 1 & 2 & 1 & 3 & 0 \\ 3 & 1 & 1 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix}$

(8) *Hallar la matriz de adyacencia de los grafos*
   (a) K_n
   (b) C_n
   (c) W_n

2. Isomorfismo de grafos

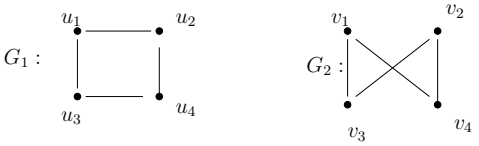
La información esencial de un grafo no está dada exactamente por su diagrama, sino por la conecciones marcadas por las aristas.

DEFINICIÓN 203. *Sea $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ grafos simples. Se dice que G_1 es* **isomorfo** *a G_2 si existe $f : V_1 \to V_2$ función biyectiva tal que*

$$e = \{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2.$$

En tal caso f se dice **isomorfismo** *entre G_1 y G_2.*

EJEMPLO 204. Sean



entonces G_1 es isomorfo a G_2 pues existe $f : V_1 \to V_2$ dada por

$$f(u_1) = v_1, f(u_2) = v_4, f(u_4) = v_2, f(u_3) = v_3.$$

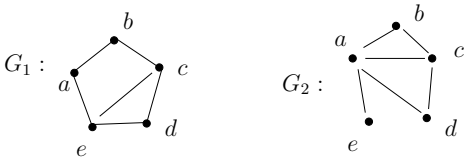
f es isomorfismo pues las aristas de G_1 mediante f corresponden a aristas de G_2:

E_1	E_2
$\{u_1, u_2\}$	$\{f(u_1), f(u_2)\} = \{v_1, v_4\}$
$\{u_2, u_4\}$	$\{f(u_2), f(u_4)\} = \{v_4, v_2\}$
$\{u_4, u_3\}$	$\{f(u_4), f(u_3)\} = \{v_2, v_3\}$
$\{u_3, u_1\}$	$\{f(u_3), f(u_1)\} = \{v_3, v_1\}$

Si $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ son isomorfos entonces
(1) $|V_1| = |V_2|$
(2) $|E_1| = |E_2|$
(3) Si $v \in V_1$ entonces $\delta(v) = \delta(f(v))$

donde $f : V_1 \to V_2$ es isomorfismo. En general dos grafos son isomorfos si tienen exactamente las mismas propiedades. Luego si encontramos un par de grafos que no comparten las mismas propiedes, entonces no son isomorfos.

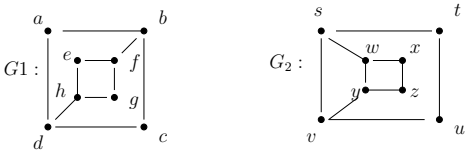
Ejemplo 205. Sean



Demostrar que G_1 no es isomorfo a G_2.

Sol. El grafo G_2 tiene un vértice de grado uno: $\delta(e) = 1$, pero todos los grados de los vértices de G_1 son de grado diferente a uno. Por lo tanto, no pueden ser isomorfos. □

Ejemplo 206. Sean



Determinar si G_1 es isomorfo a G_2.

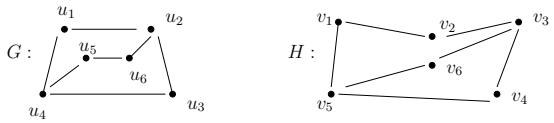
Sol. Supongamos que sí son isomorfos y que f es un isomorfismo entre G_1 y G_2. Como $\delta(a) = 2$ entonces $\delta(f(a)) = 2$. Como los elementos de grado 2 de G_2 son

$$x, z, t, u$$

entonces $f(a) = x$ o $f(a) = z$ o $f(t) = 2$ o $f(a) = u$. Pero todos éstos se conectan con vértices de grado 2, lo cual no ocurre con a (los vecinos de a tienen grado 3). □

Si G, H son grafos tales que *para alguna numeración de sus vértices* $A_G = A_H$ entonces G es isomorfo a H.

Ejemplo 207. Determinar si los grafos siguientes son isomorfos:



Sol. Tenemos la matrices de adyacencia:

$$A_G = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{array} \begin{array}{c} \begin{array}{cccccc} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

y

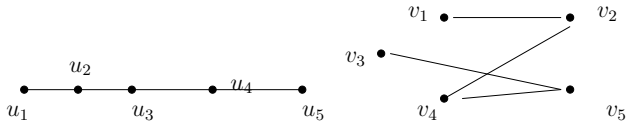
$$A_H = \begin{array}{c} \\ v_6 \\ v_3 \\ v_4 \\ v_5 \\ v_1 \\ v_2 \end{array} \begin{array}{c} \begin{array}{cccccc} v_6 & v_3 & v_4 & v_5 & v_1 & v_2 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Esto es, $A_G = A_H$ de donde se sigue que H y G son isomorfos.

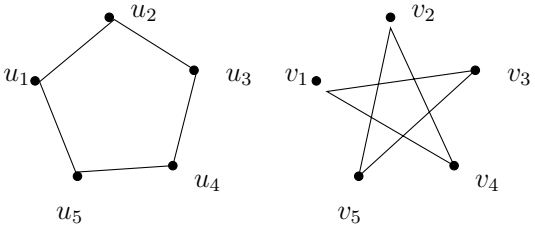
□

TAREA 60. (1) *Determinar si el par de grafos dados es isomorfo o no. Construir un isomorfismo o proporcionar un argumento riguroso que demuestre que no son isomorfos.*

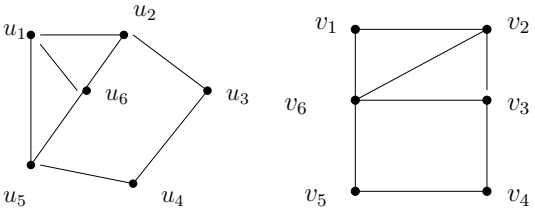
(a)



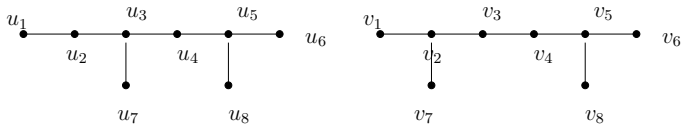
(b)



(c)



(d)



CAPíTULO 7

Álgebras

1. Álgebras de Boole y bits

El álgebra de Boole proporciona leyes y operaciones sobre el conjunto de bits $\{0, 1\}$. Las más básicas definiciones son:

(1) Complemento (NOT): $\bar{0} = 1$, $\bar{1} = 0$.
(2) Suma booleana (OR):

$$0 + 0 = 1 \qquad 0 + 1 = 1$$
$$1 + 0 = 1 \qquad 1 + 1 = 1$$

(3) Producto booleano (AND):

$$0 \cdot 0 = 0 \qquad 0 * 1 = 0$$
$$1 \cdot 0 = 0 \qquad 1 \cdot 1 = 1$$

Ante ausencia de paréntesis, las regla de precedencia entre las operaciones son

(1) complementos;
(2) productos;
(3) sumas.

EJEMPLO 208. Evaluar:

$$1 \cdot 0 + \bar{1}$$

SOL.

$$\begin{aligned} 1 \cdot 0 + \bar{1} &= 1 \cdot 0 + 0 \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

□

(1) Si $B = \{0, 1\}$ y $n \in \mathbb{N}$, entonces $B^n = \{(x_1, \ldots, x_n) \,|\, 1 \leq i \leq n, x_i \in B\}$
(2) Si x es una variable tal que toma valores en B , entonces x se llama **variable booleana**.
(3) Una función $F : B^n \to B$ se llama **función booleana de grado** n.

EJEMPLO 209. Sea $F : B^2 \to B$, $F(x, y) = \bar{x}y$ es función booleana de grado 2. Sus valores veien dados por la tabla:

x	y	$F(x, y)$
1	1	0
1	0	1
0	1	0
0	0	0

DEFINICIÓN 210. *Sean F, G funciones booleanas de grado n. Se definen:*

(1) $F = G \Leftrightarrow (\forall b_1, \ldots, b_n \in B),\ F(b_1, \ldots, b_n) = G(b_1, \ldots, b_n)$
(2) (a) $(F+G)(x_1, \ldots, x_n) = F(x_1, \ldots, x_n) + G(x_1, \ldots, x_n)$ *(suma booleana).*
    (b) $(FG)(x_1, \ldots, x_n) = F(x_1, \ldots, _n)G(x_1, \ldots, x_n)$ *(producto booelano)*
    (c) $\bar{F}(x_1, \ldots, x_n) = \overline{F(x_1, \ldots, x_n)}$

PROPIEDAD 12. *Si x, y, z son variables booleanas,*

$$x(y + z) = xy + xz.$$

DEMOSTRACIÓN. Sean $F(x, y, z) = x(y + z)$ y $G(x, y, z) = xy + xz$. Demostraremos que $F = G$, esto es, que $F(b_1, b_2, b_3) = G(b_1, b_2, b_3)\ \forall b_i,\ i = 1, 2, 3$. Para esto basta con calcular sus valores de verdad en una tabla:

x	y	z	$y+z$	xy	xz	$x(y+z)$	$xy+xz$
1	1	1	1	1	1	1	1
1	1	0	1	1	0	1	1
1	0	1	1	0	1	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

y como las dos últimas columnas son iguales, se concluye que

$$x(y + z) = xy + xz.$$

□

La propiedad anterior se llama *distributiva del producto con respecto la suma*. También existe la *propiedad distributiva de la suma con respecto al producto*:

PROPIEDAD 13. *Si x, y, z son variables booleanas entonces*

$$x + yz = (x + y)(x + z).$$

DEMOSTRACIÓN. Calcularemos las tablas de verdad:

x	y	z	$x+yz$	$(x+y)(x+z)$
1	1	1	1	1
1	1	0	1	1
1	0	1	1	1
1	0	0	1	1
0	1	1	1	1
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

$$\therefore x + yz = (x + y)(x + z).$$

□

Otra forma de demostrar igualdades es utilizando únicamente propiedades algebraicas.

EJEMPLO 211. Demostrar la *propiedad de absorción*:

$$x(x+y) = x.$$

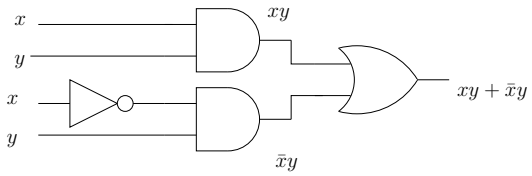
DEMOSTRACIÓN. Tenemos que

$$\begin{aligned} x(x+y) &= (x+0)(x+y), && \text{neutro} \\ &= x + 0 \cdot y, && \text{Propiedad 13} \\ &= x + y \cdot 0, && \text{conmutativa} \\ &= x + 0 \\ &= x && \text{neutro} \end{aligned}$$

□

DEFINICIÓN 212. *El* **dual** *de una expresión booleana se obtiene al intercambiar las sumas con productos y los 0's por 1's.*

EJEMPLO 213. El dual de $x(y+0)$ es $x + y \cdot 1$; el dual de $\bar{x} \cdot 1 + (\bar{y} + z)$ es $(x+0)\bar{y}z$.



El *principio de dualidad* en álgebras de Boole asegura que si dos expresiones son iguales entonces son iguales sus duales.

EJEMPLO 214. Sabemos que

$$x(x+y) = x$$

entonces, por el principio de dualidad, obtenemos que

$$x + (xy) = x.$$

TAREA 61.

(1) *Calcular las tablas de verdad de las siguientes funciones booleanas*
   (a) $F(x,y,z) = \bar{z}$.
   (b) $F(x,y,z) = \bar{x}y + \bar{y}z$
   (c) $F(x,y,z) = x\bar{y}z + \overline{xyz}$
   (d) $F(x,y,z) = \bar{y}(xz + \overline{\bar{x}\bar{z}})$
(2) *¿Qué valores de las variables boolenas x, y satisfacen la ecuación $xy = x + y$?*
(3) *¿Cuántas funciones boolenas de grado 7 hay?*
(4) *Demostrar que $x + xy = x$ para cualesquiera variables booleanas x, y.*
(5) *Sean x, y, z variables booelanas. Demostrar que*

$$x\bar{y} + y\bar{z} + \bar{x}z = \bar{x}y + \bar{y}z + x\bar{z}$$

(6) *El operador booleano $\oplus$ llamado XOR, se define mediante $1 \oplus 1 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 0 \oplus 0 = 0$. Sean x, y variables boolenas. Demostrar que*
   (a) $x \oplus y = (x+y)\overline{(xy)}$
   (b) $x \oplus y = x\bar{y} + \bar{x}y$
(7) *Calcular los duales de las siguientes expresiones booleanas.*

(a) $x + y$
(b) $\bar{x}\bar{y}$
(c) $xyz + \bar{x}\bar{y}\bar{z}$
(d) $x\bar{z} + x \cdot 0 + \bar{x_1} \cdot 1$

2. Álgebras de Boole en Abstracto

Definición 215. *Un* **álgebra de Boole** B *es un conjunto* B *junto con dos operaciones* $\wedge : B \times B \to B$, $\vee : B \times B \to B$ *y los elementos* 0 *y* 1 *en* B *junto con una operación unaria* $\_\_ : B \to B$ *tales que* $\forall x, y, z \in B$ *se cumplen,*

(1) $x \vee 0 = x$ *y* $x \wedge 1 = x$ *(neutro)*
(2) $x \vee \bar{x} = 1$ *y* $x \wedge \bar{x} = 0$ *(complemento)*
(3) $(x \vee y) \vee z = x \vee (y \vee z)$ *y* $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ *(asociativa)*
(4) $x \vee y = y \vee x$ *y* $x \wedge y = y \wedge x$ *(conmutativa)*
(5) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ *y* $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ *(distributiva)*

Ejemplo 216. El conjunto $B = \{0, 1\}$ junto con $\wedge$ =AND y $\vee$ =OR, $\_\_$ =NOT y $0, 1$ forman un álgebra de Boole.

Ejemplo 217. Sea E un conjunto. El conjunto potencia $B = 2^E$ junto con $\wedge = \cap$, $\vee = \cup$, $\_\_ = \tilde{}$, y $0 = \varnothing$, $1 = E$ es un álgebra de Boole.

Propiedad 14 (involutiva). *Sea* B *un álgebra de Boole. Entonces, para* $x \in B$ *arbitrario se cumplen*

(1) $x \vee x = x$
(2) $x \wedge x = x$.

Demostración.

(1) Tarea
(2)

$$\begin{aligned} x &= x \wedge 1 && \text{neutro} \\ &= x \wedge (x \vee \bar{x}), && \text{complemento} \\ &= (x \wedge x) \vee (x \wedge \bar{x}) && \text{distributiva} \\ &= (x \wedge x) \vee 0 && \text{complemento} \\ &= x \wedge x && \text{neutro} \end{aligned}$$

□

Teorema 26. *Sea* B *un álgebra de Boole y* $x \in B$*, entonces existe un único* $\bar{x} \in B$ *tal que*

(1) $x \vee \bar{x} = 1$
(2) $x \wedge \bar{x} = 0$

Demostración. Supongamos que existe otro x^* tal que cumple

$$x \vee x^* = 1 \tag{8}$$

$$x \wedge x^* = 0 \tag{9}$$

Tenemos entonces que

$$x \vee x^* = x \vee \bar{x}$$

lo que implica

$$x^* \wedge (x \vee x^*) = x^* \wedge (x \vee \bar{x})$$

y distribuyendo lado a lado:

$$\underbrace{(x^* \wedge x)}_{0} \vee \underbrace{(x^* \wedge x^*)}_{x^*} = \underbrace{(x^* \wedge x)}_{0} \vee (x^* \wedge \bar{x})$$

usando conmutativa, neutro y complemento para obtener

$$x^* = x^* \vee \bar{x}$$

Ahora, notemos que el papel de x^* y $\bar{x}$ es simétrico; por lo que podemos obtener

$$\bar{x} = \bar{x} \vee x^*$$

y entonces usando conmutativa:

$$x^* = x^* x \vee \bar{x} = \bar{x}$$

□

Ejemplo 218. Probar que, en un álgebra de Boole, $\bar{0} = 1$.

Demostración. Tenemos, por complemento que

$$0 \vee \bar{0} = 1, \quad 0 \wedge \bar{0} = 0$$

y

$$0 \vee 1 = 1, \quad 0 \wedge 1 = 0$$

por neutro. Es decir 1 satisface las mismas ecuaciones que el complemento $\bar{0}$, luego, por unicidad del complemento $\bar{0} = 1$. □

Tarea 62.

(1) *Demostrar que en un álgebra de Boole que el complemento de 1 es 0.*
(2) *Sea B un álgebra de Boole. Demostrar*
(3)
$$\forall x, y \in B, \bar{\bar{x}} = x$$
(4)
$$\forall x, yy \in B, \overline{(x \vee y)} = \bar{x} \wedge \bar{y}$$
(5)
$$\forall x, y \in B, \overline{(x \wedge y)} = \bar{x} \vee \bar{y}$$
(6) *Sea B un algebra de Boole. Sean $x, y \in B$. Demostrar*
   (a) *$x \vee y = 0$ implica que $x = 0$ y $y = 0$.*
   (b) *$x \wedge y = 1$ implica que $x = 1$ y $y = 1$.*

3. Forma Normal Disyuntiva

Si $F(x_1, \ldots, x_n)$ es una función booleana entonces F se puede escribir como una combinación de $+, \cdot$ y $\bar{}$.

EJEMPLO 219. Sean $F(x, y, z)$, $G(x, y, z)$ funciones booleanas dadas por las tablas:

x	y	z	F	G
1	1	1	0	0
1	1	0	0	1
1	0	1	1	0
1	0	0	0	0
0	1	1	0	0
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

entonces

$$F(x, y, z) = x\bar{y}z$$

pues

$$x\bar{y}z = 1 \Leftrightarrow x = \bar{y} = z = 1 \Leftrightarrow x = 1, y = 0 \text{ y } z = 1$$

es decir,

$$x\bar{y}z = \begin{cases} 1 & \text{si } x = 1, y = 0 \text{ y } z = 1 \\ 0 & \text{otro caso} \end{cases}$$
$$= F(x, y, z).$$

Además,

$$G(x, y, z) = xy\bar{z} + \bar{x}y\bar{z}$$

TAREA 63. (1) *Calcular el producto booleano de las variables x, y, z o de sus complementos, que valga 1 si y sólo si*
   (a) $x = y = 0, z = 1$
   (b) $x = 0, y = 1, z = 0$
   (c) $x = 0, y = z = 1$
   (d) $x = y = z = 0$

(2) *Hallar la forma normal disyuntiva de las funciones booleans siguientes:*
   (a) $F(x, y, z) = x + y + z$
   (b) $F(x, y, z) = (x + z)y$
   (c) $F(x, y, z) = x$
   (d) $F(x, y, z) = x\bar{y}$

(3) *Hallar la forma normal disyuntiva de la función booleana $F(x_1, x_2, x_3, x_4, x_5)$ que vale 1 si y sólo tres o más de las variables x_1, x_2, x_3, x_4 y x_5 toman el valor 1..*

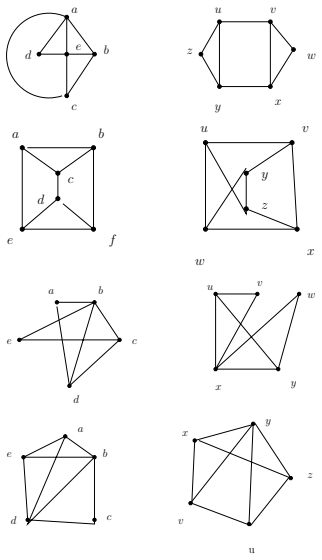
(4) *Expresar las siguientes funciones booleanas usando sólo los operadores $\cdot$ y $\bar{}$.*
   (a) $x + y + z$
   (b) $\overline{x + \bar{y}(\bar{x} + z)}$
   (c) $\overline{(x + \bar{y}}$
   (d) $\bar{x}(x + \bar{y} + z)$

(5) *Expresar las funciones booleanas del ejercicio anterior usando sólo los operadores* $+$ *y* $^-$ *.*
(6) *Demostrar que*
   (a) $\bar{x} = x|x$
   (b) $xy = (x|y)|(x|y)$
   (c) $x + y = (x|x)|(y|y)$
   (d) $\bar{x} = x \downarrow x$
   (e) $xy = (x \downarrow x) \downarrow (y \downarrow y)$
   (f) $x + y = (x \downarrow y) \downarrow (x \downarrow y)$

TAREA 64. (1) *Para cada operación* $*$ *definida en el conjunto señalado dígase cuándo* $*$ *dota al conjunto de una estructura de grupo. En caso contrario diga que axioma falla.*
   (a) $\mathbb{Q}$ *con* $a * b = ab$
   (b) $\mathbb{R}^+$ *con* $a * b = a/b$
   (c) $\mathbb{C}$ *con* $a * b = a + b$
   (d) $\mathbb{R}\backslash\{-1\}$ *con* $a * b = a + b + ab$
   (e) $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ *con* $a * b = |a|\, b$.
(2) *Sea* $(G, *)$ *un grupo y* a, b *elementos arbitrarios de* G*. Demostrar que*

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

(3) *Un elemento* x *en un grupo* G *se llama idempotente si* $x * x = x$*. Muestre que un grupo tiene exactamente un elemento idempotente.*
(4) *Muéstrese que si* G *es un grupo finito con identidad* e *y con un número par de elementos, entonces existe* $a \neq e$ *tal que* $a * a = e$*.*



Bibliografía

[1] K.H. Rosen, Matemática discreta y sus aplicaciones, 5a ed., McGraw-Hill, Madrid 2004.

[2] A. Abian, The Theory of Sets and Transfinite Arithmetic, W.B. Saunders Co. E.E. U.U, 1965.

[3] E. Mendelson, Introduction to Mathematical Logic, 4th ed. Chapman & Hall, E.E.U.U, 1997.