2021

ÁLGEBRA II (LSI – PI)

UNIDAD Nº 3

ESTRUCTURAS ALGEBRAICAS: GRUPO - CUERPO - ÁLGEBRA DE BOOLE. SUBESTRUCTURAS ALGEBRAICAS - HOMOMORFISMOS.

Facultad de Ciencias Exactas y Tecnologías
UNIVERSIDAD NACIONAL DE SANTIAGO DEL ESTERO

UNIDAD Nº 3

ESTRUCTURAS ALGEBRAICAS: GRUPO – CUERPO –ÁLGEBRA DE BOOLE

1.- GRUPO

Definición 1

Sea G un conjunto no vacío. $*$ es una ***ley de composición interna en*** G si y sólo si $*$ es una función cuyo dominio es $G \times G$ y que toma valores en G.

En símbolos,

$*$ es una ***ley de composición interna en*** $G \Leftrightarrow *: G \times G \to G$

$$(a,b) \longmapsto * (a,b) = a * b$$

Observaciones

1.- La expresión $G \times G$ indica el producto cartesiano de G consigo mismo.

2.- Es claro que $a * b$ es la imagen del par ordenado (a,b) a través de la función $*$.

3.- Si $*$ es una ley de composición interna en un conjunto no vacío G, podemos afirmar que

$$\forall\, a,b \in G;\ a * b \in G$$

O bien,

$$a,b \in G \Rightarrow a * b \in G$$

4.- Si $*$ es una ley de composición interna en un conjunto no vacío G, se suele decir que ***G es cerrado con respecto a la operación*** $*$.

Ejemplos

a) La suma es una ley de composición interna en el conjunto $\mathbb{N}$ de los números naturales.
b) La multiplicación es una ley de composición interna en el conjunto $\mathbb{Z}$ de los números enteros.
c) La resta es una ley de composición interna en el conjunto $\mathbb{R}$ de los números reales.
d) La suma de vectores del plano es una ley de composición interna en $\mathbb{R}^2$.

En cambio,

e) La resta no es una ley de composición interna en el conjunto $\mathbb{N}$ de los números naturales.
f) La división no es una ley de composición interna en el conjunto $\mathbb{Z}$ de los números enteros.

Definición 2

Un conjunto no vacío G es un grupo si en él está definida una operación $*$ tal que se verifican los siguientes axiomas,

Ax. 1) $\forall\, a,b \in G;\ a * b \in G$ ley de composición interna (LCI)

Ax. 2) $\forall\, a,b,c \in G; (a * b) * c = a * (b * c)$ propiedad asociativa

Ax. 3) $\exists\, e \in G: \forall\, a \in G;\ a * e = e * a = a$ existencia de un único elemento neutro para *

Ax. 4) $\forall\, a \in G;\ \exists\, a' \in G: a * a' = a' * a = e$ para cada elemento de G, existe su inverso

Notas

1. La estructura algebraica de grupo ha sido definida en forma axiomática.
2. El axioma Ax. 1) indica que $*$ es una ley de composición interna en G. Es decir, el conjunto G es cerrado con respecto a la operación $*$.
3. El axioma Ax. 2) expresa que la ley de composición interna $*$ es asociativa.
4. El axioma Ax. 3) enuncia la existencia de al menos un elemento particular de G, con respecto a la operación $*$ denominado ***elemento neutro,*** al cual se simboliza con la letra e.
5. El axioma Ax. 4) afirma que cada elemento a del conjunto G admite al menos un elemento a' en G, denominado ***inverso de a***.
6. El grupo G con la operación $*$, suele denotarse con el par $(G,*)$.
7. Diremos simplemente "***sea G un grupo***" cuando la ley $*$ esté sobreentendida.

Ejemplos de grupos

- $(\mathbb{Z},+)$, es el grupo de los números enteros con la suma de números enteros.
- $(\mathbb{R},+)$, es el grupo de los números reales con la suma de números reales.
- $(\mathbb{R}-\{0\},\cdot)$, es el grupo de los números reales no nulos con la multiplicación de números reales no nulos.
- $(\mathbb{C}-\{0\},\cdot)$, es el grupo de los números complejos no nulos con la multiplicación de números complejos no nulos.

No son grupos

- El conjunto $\mathbb{N}$ de los números naturales con la suma de números naturales.
- El conjunto $\mathbb{Z}$ de los enteros con el producto usual en $\mathbb{Z}$.
- El conjunto $\mathbb{R}$ de los números reales con el producto usual en $\mathbb{R}$.
- El conjunto $\mathbb{R}^{n\times n}$ de las matrices de orden n con el producto usual de matrices.

Propiedades de los grupos 6 propiedades

Proposición 1

Sea $(G,*)$ un grupo. G admite un único elemento neutro respecto a la ley de composición interna $*$. En símbolos,

$$\exists!\, e\in G:\forall\, a\in G;\ a*e=e*a=a$$

Se lee: "existe y es único e perteneciente a G tal que para cada a perteneciente a G se verifica que, a asterisco e, es igual a e asterisco a y es igual a a".

Proposición 2

Sea $(G,*)$ un grupo. El inverso de cada elemento de G es único. En símbolos,

$$\forall\, a \in G;\ \exists!\ a' \in G:\ a * a' = a' * a = e$$

Se lee: "para cada a perteneciente a G existe y es único a' perteneciente a G tal que se verifica que, a asterisco a' es igual a a' asterisco a y es igual a e".

Proposición 3

Sea $(G,*)$ un grupo. El inverso del inverso de cada elemento a perteneciente a G es el mismo a. En símbolos,

$$(a')' = a$$

Se lee: "el inverso de inverso de a es el mismo a".

Proposición 4

Sea $(G,*)$ un grupo. Cualesquiera sean a, b pertenecientes a G se verifica que, el inverso del elemento $a * b$ es igual al elemento $b' * a'$. En símbolos,

$$\forall\, a, b \in G;\ (a * b)' = b' * a'$$

Se lee: "cualesquiera sean a y b pertenecientes a G se verifica que el inverso del resultado de la operación a asterisco b es igual al inverso de b asterisco el inverso de a".

Proposición 5

Sea $(G,*)$ un grupo. Cada elemento de G es cancelable o regular. Esto es,

$$\forall\, a, b, c \in G;\ (a * b = a * c \Rightarrow b = c) \wedge (b * a = c * a \Rightarrow b = c)$$

Proposición 6

Cualesquiera sean $a, b, c \in G$, cada una de las siguientes ecuaciones lineales en la variable x

$$a * x = b$$
$$x * a = c$$

admite solución única en G.

Notas

1. Cuando en un grupo G la ley de composición interna esté representada por el símbolo $+$, diremos que G es un ***grupo aditivo***. En esta situación, el *elemento neutro aditivo* se llama *"elemento nulo"* o simplemente *"cero"* y suele representarse con 0. Y dado $a \in G$ el *inverso aditivo de a*, denominado "*opuesto de a",* se denota con $-a$.

2. Cuando en un grupo G la ley de composición interna esté representada por el símbolo $\cdot$, diremos que G es un ***grupo multiplicativo***. En este contexto, el *elemento neutro multiplicativo* se llama "*unidad"* y suele representarse con 1. Y dado $a \in G$ el *inverso multiplicativo de a*, denominado "*recíproco de a",* se denota con a^{-1}.

3. Cuando un grupo G sea multiplicativo omitiremos el símbolo $\cdot$ de la multiplicación. Es decir, en lugar de escribir $a \cdot b$ escribiremos ab a la multiplicación de a con b.

Ejemplos de grupos aditivos

- $(\mathbb{Z}, +)$, es el grupo de los números enteros con la suma de números enteros.
- $(\mathbb{Q}, +)$, es el grupo de los números racionales con la suma de números racionales.
- $(\mathbb{R}, +)$, es el grupo de los números reales con la suma de números reales.

- $(\mathbb{C},+)$, es el grupo de los números complejos con la suma de números complejos.
- $(\mathbb{R}^2,+)$, es el grupo de los vectores del plano real (o *pares ordenados de números reales*) con la suma de vectores del plano real definida por

$$(x_1,x_2)+(y_1,y_2) \overset{def}{=} (x_1+y_1,\ x_2+y_2)$$

Donde el *cero* es el vector nulo $(0,0)$ y el *opuesto* de (x_1,x_2) es

$$-(x_1,x_2) \overset{def}{=} (-x_1,-x_2)$$

- $(\mathbb{R}^3,+)$, es el grupo de vectores del espacio real (o *ternas ordenadas de números reales*) con la suma de vectores del espacio real definida por

$$(x_1,x_2,x_3)+(y_1,y_2,y_3) \overset{def}{=} (x_1+y_1,x_2+y_2,x_3+y_3)$$

Donde, el *cero* es el vector nulo $(0,0,0)$ y el *opuesto* de (x_1,x_2,x_3) es

$$-(x_1,x_2,x_3) \overset{def}{=} (-x_1,-x_2,-x_3)$$

- $(\mathbb{R}^{m\times n},+)$, es el grupo de las matrices reales de tipo $m\times n$ con la suma de matrices definidas por

$$[a_{ij}]+[b_{ij}] \overset{def}{=} [a_{ij}+b_{ij}],\ \ \forall\ i=1,2,\dots,m\ \wedge\ \forall\ j=1,2,\dots,n$$

Donde, el *cero* es la matriz nula de tipo $m\times n$ (todos los elementos de esta matriz son iguales a 0). Y la matriz *opuesta* de $[a_{ij}]$ es

$$-[a_{ij}] \overset{def}{=} [-a_{ij}]$$

- $(\mathbb{Z}_3,+)$, con $\mathbb{Z}_3=\{\bar{0},\bar{1},\bar{2}\}$, es el grupo de las clases residuales módulo 3 con la suma definida por la siguiente tabla

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Ejemplos de grupos multiplicativos

- $(\mathbb{Q}-\{0\},\cdot)$, es el grupo de los números racionales no nulos con la multiplicación de números racionales no nulos.
- $(\mathbb{R}-\{0\},\cdot)$, es el grupo de los números reales no nulos con la multiplicación de números reales no nulos.

- $(\mathbb{C}-\{0\},\cdot)$, es el grupo de los números complejos no nulos con la multiplicación de números complejos no nulos.
- $\left(\left\{1,-\frac{1}{2}+\frac{\sqrt{3}}{2}i\,,-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right\},\ \cdot\right)$, es el grupo de las raíces cúbicas de 1 con la multiplicación de números complejos.
- $(\mathbb{Z}_3-\{\bar{0}\},\cdot)$, con $(\mathbb{Z}_3-\{\bar{0}\}=\{\bar{1},\bar{2}\}$, es el grupo de las clases residuales módulo 3 no nulas, con la multiplicación definida por la siguiente tabla

$\cdot$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

Definición 3

Sea $(G,*)$ un grupo. El grupo G es ***conmutativo*** ***(o abeliano)*** si la ley de composición interna $*$ es conmutativa. Es decir, si se verifica que

$$\forall\, a,b\in G;\ a*b=b*a$$

Ejemplos

a) Grupos aditivos conmutativos son

$(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{R}^n,+),(\mathbb{R}^{m\times n},+),(\mathbb{Z}_3,+)$.

b) Grupos multiplicativos conmutativos son

$(\mathbb{Q}-\{0\},\ \cdot),(\mathbb{R}-\{0\},\ \cdot),(\mathbb{C}-\{0\},\ \cdot),(\mathbb{Z}_3-\{\bar{0}\},\ \cdot)$.

Definición 4

Sea un grupo aditivo $(G,+)$. Cualesquiera sean a y b pertenecientes a G, se define la resta

$$a-b\ \overset{def}{=}\ a+(-b)$$

Nota

La resta de elementos de un grupo no es conmutativa.

Definición 5

Sea $(G,*)$ un grupo.

a) El ***orden*** del grupo$(G,*)$ es el número de elementos del conjunto G.

b) El grupo $(G,*)$ tiene ***orden finito*** si el conjunto G tiene un número finito de elementos.

c) El grupo $(G,*)$ tiene ***orden infinito*** si el conjunto G es un conjunto infinito.

Ejemplos

a) Grupos de orden infinito

a.i) $(\mathbb{Z}, +), (\mathbb{R}^{m\times n}, +), (\mathbb{R} - \{0\}, \cdot)$.

a.ii) $(\mathbb{Z}, *)$, donde $\mathbb{Z}$ es el conjunto de los enteros y la operación $*$ está definida por

$$\forall\, a, b \in \mathbb{Z};\ a * b = a + b - 2$$

b) Grupos de orden finito

b.i) El grupo abeliano $(\mathbb{Z}_3, +)$ tiene orden 3.

b.ii) El grupo abeliano $(\mathbb{Z}_3 - \{\bar{0}\}, \cdot)$ tiene orden 2.

b.iii) El conjunto $K = \{a, b, c, d\}$ con la ley $*$ definida en la siguiente tabla

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

forman el grupo abeliano denominado *grupo de los cuatro elementos de Klein.* El grupo $(K,*)$ tiene orden 4.

Notas

1.- Si $(G,*)$ es un grupo infinito, la ley de composición interna $*$ puede darse por una definición general como en el ejemplo a.ii), o bien por una tabla como en los tres ejemplos en b).

2.- Si $(G,*)$ es un grupo finito y la ley de composición interna $*$ está definida por medio de una tabla, ésta satisface las siguientes condiciones:

a) En la fila y en la columna del elemento neutro de G, están todos los elementos de G.

b) Cada elemento de G aparece exactamente una vez en cada fila y en cada columna. Por lo tanto, cada fila y cada columna es una permutación diferente de los elementos de G.

3.- Si $(G,*)$ es un grupo finito y la ley de composición interna $*$ se define por medio de una tabla y ésta es simétrica, entonces el grupo es conmutativo. (Como puede comprobarse, por ejemplo, en el grupo de los cuatro elementos de Klein)

1.1.- SUBGRUPO

Definición 6

Sea $(G,*)$ un grupo y sea H un subconjunto no vacío de G. El conjunto H es un ***subgrupo*** de G si y sólo si H con la operación $*$ restringida a H es un grupo.

Observación

En la definición precedente cuando se dice "*la operación $*$ restringida a H*" significa que en vez de tomar la ley $*$ con dominio en $G \times G$ debemos tomar la misma ley $*$ pero con dominio en $H \times H$.

Notación

Cuando H sea un subgrupo de G, representaremos este hecho en forma simbólica con $H \prec G$ y leeremos "H es un subgrupo de G".

Ejemplos

a) $(\mathbb{Z}, +) \prec (\mathbb{Q}, +)$

b) Sea el grupo de *los cuatro elementos de Klein* $(K, *)$, en donde $K = \{a, b, c, d\}$ y $*$ está definida por medio de la tabla

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Son subgrupos los siguientes subconjuntos no vacíos de K con la ley $*$ restringida a cada uno de ellos respectivamente,

$$\{a\}, \{a, b\}, \{a, c\}, \{a, d\}, \underbrace{\{a, b, c, d\}}_{=K}$$

En cambio el subconjunto $\{a, b, c\}$ no es subgrupo de K, ya que $*$ no es ley de composición interna en este subconjunto.

c) El conjunto de los números enteros múltiplos de dos $2\mathbb{Z}$, es un subgrupo del grupo aditivo $(\mathbb{Z}, +)$.

Definición 7

Sea $(G,*)$ un grupo y sea e el elemento neutro de G con respecto a la ley de composición interna $*$. Los subconjuntos $\{e\}$ y G de G se denominan ***subgrupos triviales*** de G.

Ejemplos

a) $\{1\}$ y $\mathbb{R} - \{0\}$ son subgrupos triviales del grupo $(\mathbb{R} - \{0\}, \cdot)$.

b) $\{0\}$ y $\mathbb{Z}$ son subgrupos triviales del grupo $(\mathbb{Z}, +)$.

Proposición 7

Sea $(G,*)$ un grupo y sea H un subconjunto no vacío de G. Condiciones necesarias y suficientes para que H con la operación $*$ restringida a H sea un subgrupo de G son,

i) $a, b \in H \Rightarrow a * b \in H$

ii) $a \in H \Rightarrow a' \in H$

Demostración

I. Probaremos que las condiciones i) y ii) son necesarias. Es decir,

Si $(H,*)$ es un subgrupo de G entonces se verifican las condiciones

i) $a,b \in H \Rightarrow a*b \in H$

ii) $a \in H \Rightarrow a' \in H$

Hipótesis

a) $(G,*)$ es un grupo

b) $H \subset G \ \wedge \ H \neq \emptyset$

c) $(H,*) \prec (G,*)$, es decir

1. $H \subset G$
2. $H \neq \emptyset$
3. $*$ es una ley de composición interna en H
4. $*$ es asociativa en H
5. $\exists\, e \in H: \forall\, a \in H; a*e = e*a = a$
6. $\forall\, a \in H; \ \exists\, a' \in H: a*a' = a'*a = e$

Tesis

i) $a,b \in H \Rightarrow a*b \in H$

ii) $a \in H \Rightarrow a' \in H$

En efecto,

i) se verifica por hipótesis 3.

ii) se verifica por hipótesis 6.

II. Probaremos ahora que las condiciones i) y ii) son suficientes. Esto es,
Si se verifican las condiciones i) y ii) entonces $(H,*)$ es un subgrupo de G.

Hipótesis

a) $(G,*)$ es un grupo

b) $H \subset G \wedge \ H \neq \emptyset$

i) $a,b \in H \Rightarrow a*b \in H$

ii) $a \in H \Rightarrow a' \in H$

Tesis

$(H,*) \prec (G,*)$, es decir

1. $H \subset G$
2. $H \neq \emptyset$
3. $*$ es una ley de composición interna en H
4. $*$ es asociativa.
5. $\exists\, e \in H: \forall\, a \in H \ a*e = e*a = a$
6. $\forall\, a \in H; \ \exists\, a' \in H: a*a' = a'*a = e$

En efecto,

1. y 2. se verifican por hipótesis b)

3. se verifica por hipótesis i)
4. se verifica por "herencia", ya que cada elemento de H es un elemento del grupo G por b) .
5. Como $H \neq \emptyset$, por hipótesis b), tiene al menos un elemento. Sea $a \in H$, entonces a admite inverso $a' \in H$, por hipótesis ii), luego

$$a \in H \wedge a' \in H \underset{\text{por hip i)}}{\Rightarrow} \underbrace{a * a'}_{=e \in G} = \underbrace{a' * a}_{=e \in G} \in H \Rightarrow e \in H$$

6. Se verifica por hipótesis ii).

Q.E.D.

Ejemplo

Sea el grupo abeliano $(\mathbb{R}^{2\times 2}, +)$ de las matrices de orden dos con la suma de matrices. El conjunto H de todas las matrices de orden dos que son antisimétricas es un subgrupo de $\mathbb{R}^{2\times 2}$.
Primero representemos simbólicamente al subconjunto H

$$H = \{A \in R^{2x2} \,/\, A = -A^t\}$$

Para mostrar que H es un subgrupo de $\mathbb{R}^{2\times 2}$ emplearemos la Proposición 7. En efecto,

1) $H \subset \mathbb{R}^{2\times 2}$, por definición de H.
2) $H \neq \emptyset$. Ya que la matriz nula de orden 2 pertenece a H , puesto que coincide con la matriz opuesta de su transpuesta.
3) Mostraremos ahora, que H es cerrado para la suma, en otras palabras mostraremos que el siguiente condicional es verdadero

$$A, B \in H \Longrightarrow A + B \in H$$

Supongamos que $A, B \in H$, entonces por definición de H es claro que

$$(\alpha) \quad \begin{cases} A = -A^t \\ B = -B^t \end{cases}$$

Luego,

$$A + B \underset{(1)}{=} -A^t + (-B^t) \underset{(2)}{=} (-1)A^t + (-1)B^t \underset{(3)}{=} (-1)(A^t + B^t) \underset{(4)}{=} (-1)(A + B)^t \underset{(2)}{=} -(A + B)^t$$

es decir la suma de matrices antisimétricas de orden 2 es otra matriz antisimétrica de orden 2. Por lo tanto $A + B \in H$.

4) Mostraremos ahora que es verdadero el siguiente condicional

$$A \in H \Longrightarrow -A \in H$$

Esto es así, pues

$$A \in H \Rightarrow A = -A^t$$

luego

$$-A \underset{(4)}{=} -(-A^t) = -(-A)^t$$

Es decir, la matriz $-A$ coincide con la matriz opuesta de su transpuesta. Por lo tanto $-A \in H$.

Luego por 1), 2), 3), 4) podemos concluir que H es un subgrupo de $\mathbb{R}^{2x2}$y expresamos en símbolos como sigue

$$(H,+) \prec (\mathbb{R}^{2x2},+)$$

Referencias

(1) Por (α).
(2) Por propiedad de matrices $(-1)C = -C$, donde C es cualquier matriz. En particular aquí $-A = (-1)A$ y $-B = (-1)B$.
(3) Por propiedad distributiva de la multiplicación de un escalar con respecto a la suma de matrices.
(4) Por propiedad de la transpuesta de la suma de matrices.

Ejemplo

Sea $(G,*)$ un *grupo abeliano*, sean S y T dos subgrupos de G. El conjunto

$$W = \{w \in G / \; w = x * y, \quad x \in S \wedge y \in T\},$$

es un subgrupo de G.

En efecto,

a) $W \subset G$, por definición de W.

b) Probaremos que $W \neq \emptyset$,
Sea e el elemento neutro de G. Ya que S y T son subgrupos de G resulta que e pertenece a S y a T por lo tanto

$$e \in S \wedge e \in T \Rightarrow e * e = e$$

y por definición de W,

$$e \in W.$$

c) Mostraremos que W es cerrado con respecto a la ley de composición $*$. Es decir, es verdadero el siguiente condicional

$$u, v \in W \Longrightarrow u * v \in W.$$

En efecto,

$$u, v \in W \implies \exists\, x,\, x' \in S \;\wedge\; y, y' \in T\colon\; u = x * y \;\wedge\; v = x' * y',$$

luego

$$u * v = (x * y) * (x' * y') \underbrace{=}_{(1)} (x * x') * (y * y')$$

y como S y T son subgrupos de G, tenemos

$$x * x' \in S \;\wedge\; y * y' \in T$$

Por lo tanto $u * v \in W$.

d) Mostraremos que es verdadero el condicional

$$u \in W \Longrightarrow u' \in W.$$

Para ello usamos el método directo de demostración

$$u \in W \Longrightarrow \exists\, x \in S \;\wedge y \in T\colon u = x * y\,,$$

luego

$$u' = (x * y)' \underset{(2)}{=} y' * x' \underset{(3)}{=} x' * y',$$

Como S y T son subgrupos de G tenemos que

$$x' \in S \ \wedge \ y' \in T \Rightarrow u' = x' * y' \in W.$$

Por lo tanto $(W,*) \prec (G,*)$.

Referencias

(1) Porque $*$ es asociativa y conmutativa ya que G es un grupo abeliano.
(2) Por Proposición 4 de Grupo.
(3) Porque $*$ es conmutativa.

2.- CUERPO

Definición 8

Sea $F \neq \emptyset$ y sean dos operaciones en F, la suma representada con $+$ y la multiplicación representada con $\cdot$. La terna $(F,+,\cdot)$ es un ***cuerpo*** si y sólo si se verifican los siguientes axiomas,

Ax.1) $(F,+)$ ***es un grupo abeliano*****.** Es decir, Grupo conmutativo

a) $+$ es una ley de composición interna en F.
$\forall\, a,\ b \in F;\ a+b \in F$

b) $+$ es asociativa en F.
$\forall\, a,b,c \in F; (a+b)+c = a+(b+c)$ 5 caracteristicas

c) Existe elemento neutro aditivo en F.
$\exists\, 0 \in F: \forall\, a \in F;\ a+0 = 0+a = a$

d) Cada elemento de F admite opuesto en F.
$\forall\, a \in F;\ \exists -a \in F:\ a+(-a) = (-a)+a = 0$

e) $+$ es conmutativa en F.
$\forall\, a,b \in F;\ a+b = b+a$

Ax.2) $(F-\{0\},\cdot)$ ***es grupo abeliano*****.** Es decir, Grupo conmutativo

f) $\cdot$ es una ley de composición interna en $F-\{0\}$**.**
$\forall\, a,\ b \in F-\{0\};\ a.b \in F-\{0\}$

g) $\cdot$ es asociativa en $F-\{0\}$.
$\forall\, a,b,c \in F-\{0\};\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$ 5 caracteristicas

h) Existe elemento neutro multiplicativo en $F-\{0\}$.
$\exists\, 1 \in F-\{0\}: \forall\, a \in F-\{0\};\ a\cdot 1 = 1\cdot a = a$

i) Cada elemento de $F-\{0\}$ admite inverso multiplicativo en $F-\{0\}$.
$\forall\, a \in F-\{0\};\ \exists a^{-1} \in F-\{0\}:\ a\cdot a^{-1} = a^{-1}\cdot a = 1$

j) $\cdot$ es conmutativa.
$\forall\, a,b \in F-\{0\};\ a\cdot b = b\cdot a$

Ax.3) La multiplicación es distributiva con respecto a la suma de izquierda a derecha y de derecha a izquierda. Es decir,

k) $\forall\, a,b,c \in F;\ a\cdot(b+c) = a\cdot b + a\cdot c$
$\forall\, a,b,c \in F;\ (a+b).c = a\cdot c + b\cdot c$

Notación

El inverso multiplicativo de un elemento $a \in F - \{0\}$ se denota con a^{-1}, o bien con $\frac{1}{a}$ y suele denominarse *el recíproco* de a.

Ejemplos de cuerpos

$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Z}_p, +, \cdot)$ con p primo.

No son cuerpos

$(\mathbb{Z}, +, \cdot), (\mathbb{R}^{n\times n}, +, \cdot), (\mathbb{Z}_4, +, \cdot)$.

Definiciones (notaciones):

Definición 9

Sea $(F, +, \cdot)$ un cuerpo. Cualesquiera sean a y b pertenecientes a F, se define la resta

$$a - b \overset{def.}{=} a + (-b)$$

Definición 10

Sea $(F, +, \cdot)$ un cuerpo. Sean a y b pertenecientes a F y $b \neq 0$, se define la ***división***

$$\frac{a}{b} \overset{def.}{=} ab^{-1}$$

Propiedades de los Cuerpos

Proposición 8

En todo cuerpo $(F, +, \cdot)$ se verifica

$$\forall\, a \in F; a\ 0 = 0\ a = 0$$

Demostración

$$\begin{aligned} a\ 0 &= a(0+0) && (1)\\ a\ 0 &= a0 + a\ 0 && (2)\\ a\ 0 + 0 &= a0 + a\ 0 && (3)\\ 0 &= a0 && (4) \end{aligned}$$

$$\begin{aligned} 0\ a &= (0+0)\ a && (1)\\ 0\ a &= 0\ a + 0\ a && (2)\\ 0\ a + 0 &= 0\ a + 0\ a && (3)\\ 0 &= 0\ a && (4) \end{aligned}$$

Luego, $a\ 0 = 0\ a = 0$

Referencias

(1) pues $0 = 0 + 0$.
(2) Por distributividad de la multiplicación respecto a la suma.
(3) 0 es elemento neutro aditivo.
(4) Por Propiedad cancelativa de grupos.

Q.E.D

Proposición 9

En todo cuerpo $(F, +, \cdot)$ se verifica

$$\forall\, a, b \in F; (-a)b = a(-b) = -(a\ b)$$

Demostración

i) Probaremos que $(-a)b$ es el opuesto de $a\ b$. En efecto

$$a\ b + (-a)b = [a + (-a)]\ b = 0\ b = 0$$

$$(-a)\ b + a\ b = [(-a) + a]\ b = 0\ b = 0$$

luego, $(-a)\ b = -(a\ b)$.

ii) Probaremos ahora que $a(-b)$ también es el opuesto de $a\ b$.

$$a\ b + a(-b) = a\ [b + (-b)] = a\ 0 = 0$$

$$a\ (-b) + ab = a\ [(-b) + b] = a\ 0 = 0$$

luego, $a(-b) = -(a\ b)$.

Q.E.D

Proposición 10

En todo cuerpo $(F, +, \cdot)$ se verifica

$$\forall\ a, b \in F;\ (-a)(-b) = a\ b$$

Demostración

Partimos del primer miembro y aplicando propiedades de cuerpo y grupo tenemos

$$(-a)(-b) = -[a(-b)] = -[-(ab)] = a\ b$$

Q.E.D

Proposición 11

En todo cuerpo $(F, +, \cdot)$ se verifica

$$\forall\ a, b, c \in F;\ a(b - c) = a\ b - a\ c$$

Demostración

Partimos del primer miembro y aplicando definiciones y propiedades de cuerpo tenemos

$$a(b - c) = a[b + (-c)] = a\ b + a(-c) = a\ b + [-(a\ c)] = \ a\ b - a\ c$$

Q.E.D

Proposición 12

En todo cuerpo $(F, +, \cdot)$ se verifica

$$\forall\ x, y \in F;\ (xy = 0 \wedge x \neq 0 \Longrightarrow y = 0).$$

Demostración

Sea entonces

$$xy = 0 \wedge x \neq 0 \qquad (*)$$

Como x es un elemento no nulo de F y $(F - \{0\}, \cdot)$ es un grupo abeliano, x admite inverso multiplicativo, luego pre-multiplicando por x^{-1} en ambos miembros de la igualdad en $(*)$, se tiene

$$x^{-1}\ x\ y = x^{-1}\ 0 \qquad (1)$$

$$(x^{-1}\ x)\ y = 0 \qquad (2)$$

$$1\,y = 0 \qquad (3)$$
$$y = 0$$

Referencias

(1) Por propiedad asociativa de la multiplicación y Proposición 8.
(2) Por Ax.2 i) de la Definición de Cuerpo.
(3) Por Ax.2 h) de la Definición de Cuerpo.

Q.E.D

Notas

1. La Proposición 12, indica que todo cuerpo carece de divisores de cero.
2. Existen conjuntos con leyes de composición interna multiplicación, en los cuales se puede encontrar elementos no nulos cuyo producto es nulo. En estas situaciones se dice que el conjunto posee divisores de cero. Como en los siguientes ejemplos.

Ejemplos

a) En el conjunto $\mathbb{R}^{2\times 2}$ de las matrices reales de orden 2, existe al menos un par de matrices no nulas cuya multiplicación da como resultado la matriz nula como vemos a continuación

$$\underbrace{\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}}_{\neq 0_{2\times 2}}\underbrace{\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix}}_{\neq 0_{2\times 2}} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

b) En el conjunto $\mathbb{Z}_4$ de las clases residuales módulo cuatro, vemos que $\bar{2}\cdot\bar{2} = \bar{0}$.

Proposición 13

En todo cuerpo $(F, +, \cdot)$ vale la ley cancelativa de la multiplicación para elementos no nulos de F. En símbolos,

$$\forall\, x, y, z \in F; (x\,z = y\,z \wedge z \neq 0 \Longrightarrow x = y).$$

Demostración

Supongamos que,

$$x\,z = y\,z \;\wedge\; z \neq 0 \qquad (*)$$ suponemos verdad

Como $(F - \{0\}, \cdot)$ es un grupo abeliano, si z es un elemento no nulo de F entonces z admite inverso multiplicativo. Post-multiplicando en ambos miembros de la igualdad en $(*)$ por z^{-1} se tiene,

$$(x\,z)\,z^{-1} = (y\,z)\,z^{-1}$$
$$x\,(z\,z^{-1}) = y\,(z\,z^{-1})$$
$$x\,1 = y\,1$$
$$x = y$$

Q.E.D

Proposición 14

En todo cuerpo $(F, +, \cdot)$, la ecuación $a\,x = b$ con $a, b \in F \wedge a \neq 0$, admite solución única en F.

Demostración

Si $a, b \in F$ y $a \neq 0$, entonces a admite inverso multiplicativo en F. Pre-multiplicamos por a^{-1} en ambos miembros de la igualdad,

$$a\,x = b$$

y tenemos,

$$a^{-1}(a\,x) = a^{-1}\,b$$

por asociatividad, escribimos

$$(a^{-1}a)\,x = a^{-1}\,b$$

por definición de inverso multiplicativo y definición de división resulta

$$1x = \frac{b}{a}$$

y por definición de neutro multiplicativo, resulta

$$x = \frac{b}{a}$$

Luego $x = \frac{b}{a}$ es solución de la ecuación dada y además es única y esto se debe a la unicidad del inverso multiplicativo.

Q.E.D

Proposición 15

En todo cuerpo $(F, +, \cdot)$, el recíproco del opuesto de todo elemento no nulo es igual al opuesto de su recíproco. En símbolos,

$$\forall\, x \in F \;\wedge\; x \neq 0;\; (-x)^{-1} = -(x^{-1}).$$

Demostración

Sea $x \in F \;\wedge\; x \neq 0$. Sabemos que

$$-x \in F \Longrightarrow (-x)^{-1} \in F$$

y que

$$(-x)(-x)^{-1} = 1 \qquad \wedge \qquad (-x)^{-1}(-x) = 1.$$

Además,

$$(-x)[-(x^{-1})] = x\,x^{-1} = 1 \qquad \wedge \qquad [-(x^{-1})](-x) = x^{-1}x = 1,$$

y como el inverso es único resulta que $(-x)^{-1} = -(x^{-1})$.

Q.E.D

Proposición 16 Operaciones con fracciones

1. $\frac{a}{b} = \frac{c}{d} \Leftrightarrow a\,d = b\,c, \quad$ con $b, d \neq 0$
2. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad$ con $b, d \neq 0$
3. $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \quad$ con $b \neq 0$
4. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad$ con $b, d \neq 0$

5. $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, con $a, b \neq 0$

2.1. SUBCUERPO

Definición 11

Sea $(F, +, \cdot)$ un cuerpo y sea $K \subset F \wedge K \neq \emptyset$. K es un ***subcuerpo*** de F si y sólo si K con las operaciones $+$ y $\cdot$ restringidas a K es un cuerpo.

Ejemplo

El cuerpo de los números racionales $(\mathbb{Q}, +, \cdot)$ es un subcuerpo del cuerpo de los números reales $(\mathbb{R}, +, \cdot)$.

Proposición 17

Sea $(F, +, \cdot)$ un cuerpo y sea $K \subset F \wedge K \neq \emptyset$. K es un ***subcuerpo*** de F si y sólo si se verifican

i). $a, b \in K \Longrightarrow a - b \in K$

ii). $a, b \in K - \{0\} \Longrightarrow \frac{a}{b} \in K - \{0\}$

Demostración

Queda para el alumno.

Ejemplo

Sea $(\mathbb{Q}, +, \cdot)$ el cuerpo de los números racionales y sea $\mathbb{Q}_{\sqrt{2}} = \{a + b\sqrt{2} \,/\, a, b \in \mathbb{Q}\}$. La terna $(\mathbb{Q}_{\sqrt{2}}, +, \cdot)$ es un subcuerpo de $(\mathbb{R}, +, \cdot)$.

Se probará que $\mathbb{Q}_{\sqrt{2}}$ es subcuerpo de $\mathbb{R}$ empleando la proposición anterior.

i) $\mathbb{Q}_{\sqrt{2}} \subset \mathbb{R}$

Sea $a + b\sqrt{2}$, con $a, b \in \mathbb{Q}$. Como $\sqrt{2}$ es un número irracional y a, b son racionales, se sigue que $a + b\sqrt{2} \in \mathbb{R}$.

ii) $\mathbb{Q}_{\sqrt{2}} \neq \emptyset$

En efecto, como $0 = 0 + 0\sqrt{2}$ con $0 \in \mathbb{Q}$ podemos concluir que $0 \in \mathbb{Q}_{\sqrt{2}}$.

iii) $x, y \in \mathbb{Q}_{\sqrt{2}} \Rightarrow x - y \in \mathbb{Q}_{\sqrt{2}}$

Para mostrar que el condicional es verdadero, partimos del antecedente,

$$x, y \in \mathbb{Q}_{\sqrt{2}} \Rightarrow x = a + b\sqrt{2} \ \wedge \ y = a' + b'\sqrt{2}$$

con a, a', b y $b' \in \mathbb{Q}$, luego

$$x - y = \left(a + b\sqrt{2}\right) - \left(a' + b'\sqrt{2}\right) = (a - a') + (b - b')\sqrt{2} \quad \in \mathbb{Q}_{\sqrt{2}}$$

iv) $\quad x, y \in \mathbb{Q}_{\sqrt{2}} - \{0\} \Rightarrow \frac{x}{y} \in \mathbb{Q}_{\sqrt{2}} - \{0\}$

Para mostrar que el condicional es verdadero, partimos del antecedente

$$x, y \in \mathbb{Q}_{\sqrt{2}} - \{0\} \Rightarrow x = a + b\sqrt{2} \ \wedge \ y = a' + b'\sqrt{2}$$

con a, a', b y $b' \in \mathbb{Q}$ **,** siendo a y b no simultáneamente nulos, y a' y b' no simultáneamente nulos. Bajo estas condiciones, calculamos

$$\frac{x}{y} = \frac{a + b\sqrt{2}}{a' + b'\sqrt{2}} = \frac{a + b\sqrt{2}}{a' + b'\sqrt{2}} \cdot \frac{a' - b'\sqrt{2}}{a' - b'\sqrt{2}} = \frac{(aa' - 2bb')}{a'^2 - 2b'^2} + \frac{(ba' - ab')}{a'^2 - 2b'^2}\sqrt{2} \in \mathbb{Q}_{\sqrt{2}} - \{0\}$$

Nota

Observemos que el denominador $a'^2 - 2b'^2$ es distinto de cero. Pues si ocurriese lo contrario tendríamos,

$$a'^2 - 2b'^2 = 0 \Rightarrow \begin{cases} a' = b' = 0, & \text{es decir a' y b' son simultaneamente nulos} \\ \text{ó} & \\ a'^2 = 2b'^2 \Rightarrow a' = \pm\sqrt{2}b', & \text{es decir a' es un número irracional} \end{cases}$$

Pero ninguna de estas dos situaciones se puede dar porque si $y = a' + b'\sqrt{2} \in \mathbb{Q}_{\sqrt{2}} - \{0\}$, entonces $a', b' \in \mathbb{Q}$ y además a' y b' son no simultáneamente nulos.

De i), ii), iii) y iv) concluimos que$(\mathbb{Q}_{\sqrt{2}}, +, \cdot)$ es un subcuerpo de $(\mathbb{R}, +, \cdot)$.

3.- HOMOMORFISMOS

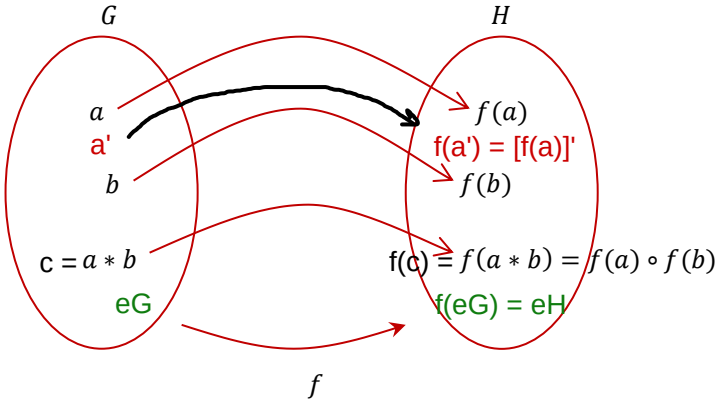
3.1 Homomorfismo de Grupos

Definición 12

Sean $(G,*)$, $(H,\circ)$ dos grupos. La función $f: G \longrightarrow H$ es un ***homomorfismo*** del grupo G en el grupo H si y sólo si

$$\forall\, a, b \in G;\ f(a * b) = f(a) \circ f(b)$$

a,b eH



Ejemplos

1) Un homomorfismo del grupo $(\mathbb{R}^+, \cdot)$ en el grupo $(\mathbb{R}, +)$ es la función logaritmo definida por

$$\begin{aligned} \log: \mathbb{R}^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto \log x \end{aligned}$$

ya que cualesquiera sean $a, b \in \mathbb{R}^+$ se verifica que

$$\log(a \cdot b) = \log a + \log b$$

2) Un homomorfismo del grupo $(\mathbb{Z}, +)$ en el grupo $(\mathbb{Z}_n, +)$ es la función definida por:

$$\begin{aligned} \phi: \mathbb{Z} &\longrightarrow \mathbb{Z}_n \\ x &\longmapsto \phi(x) = \bar{x} \end{aligned}$$

Donde $\bar{x}$ es la clase residual de los enteros módulo n.

Proposición 18

Sean $(G,*)$, $(H,\circ)$ dos grupos con elementos neutros e_G y e_H respectivamente. Si $f: G \longrightarrow H$ es un homomorfismo, entonces la imagen del elemento neutro de G es igual al elemento neutro de H. Esto es,

$$f(e_G) = e_H$$

Demostración

Como G es un grupo y por Proposición 1 de grupo, sabemos que

$$\exists!\, e_G: \forall a \in G; (a * e_G = a \wedge e_G * a = a)$$

aplicando f en ambos miembros de las dos igualdades

$$a * e_G = a \ \wedge \ e_G * a = a$$

tenemos,

$$f(a * e_G) = f(a) \quad \wedge \quad f(e_G * a) = f(a).$$

Como f es un homomorfismo, podemos escribir,

$$f(a) \circ f(e_G) = f(a) \quad \wedge \quad f(e_G) \circ f(a) = f(a).$$

Además, por ser e_H elemento neutro de H con respecto a $\circ$, podemos escribir

$$f(a) \circ f(e_G) = f(a) \circ e_H \quad \wedge \quad f(e_G) \circ f(a) = e_H \circ f(a)$$

Por hipótesis $(H,\circ)$ es un grupo, por lo tanto $f(a)$ es cancelable a izquierda y a derecha, por lo que se sigue que

$$f(e_G) = e_H.$$

Q.E.D.

Proposición 19

Sean $(G,*)$, $(H,\circ)$ dos grupos con elementos neutros e_G y e_H respectivamente. Si $f: G \longrightarrow H$ es un homomorfismo, entonces la imagen del inverso de todo elemento de G es igual al inverso de su imagen.

En símbolos,

$$\forall\, a \in G; f(a') = [f(a)]'.$$

Demostración

Por ser f una función de G en H tenemos,

$$\forall a \in G;\ f(a) \in H,$$

y como $(H,\circ)$ es un grupo podemos asegurar que, dado $f(a) \in H$ existe su inverso en H, es decir

$$\exists![f(a)]' \in H: f(a) \circ [f(a)]' = e_H \ \wedge \ [f(a)]' \circ f(a) = e_H.$$

Por otro lado,

$$\forall a \in G;\ \exists!\ a' \in G: a * a' = a' * a = e_G,$$

de aquí tenemos que $a' \in G$ por lo tanto $f(a') \in H$.

Mostraremos ahora que

$$f(a) \circ f(a') = e_H \ \wedge \ f(a') \circ f(a) = e_H$$

Partimos del primer miembro y teniendo en cuenta que f es un homomorfismo,

$$f(a) \circ f(a') = f(a * a') = f(e_G) = e_H, \text{ y}$$
$$f(a') \circ f(a) = f(a' * a) = f(e_G) = e_H$$

esto nos dice que $f(a')$ es también inverso de $f(a)$ y como en todo grupo el inverso es único se tiene

$$f(a') = [f(a)]'.$$

Q.E.D.

Núcleo de un homomorfismo de grupos

Definición 13

Sean $(G,*)$, $(H,\circ)$ dos grupos con elementos neutros e_G y e_H respectivamente y $f: G \longrightarrow H$ un homomorfismo. El ***Núcleo*** del homomorfismo f es el conjunto formado por los elementos de G cuya imagen es el elemento neutro de H.

En símbolos,

$$N_f = \{x \in G / f(x) = e_H\}.$$

De esta definición se deduce que,

$$x \in N_f \Leftrightarrow f(x) = e_H$$

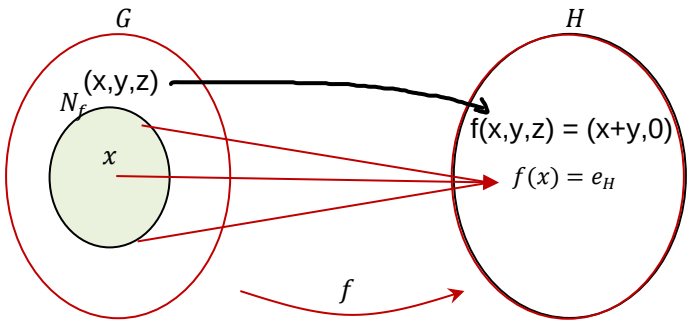


Diagrama de Venn del Núcleo del homomorfismo f

Ejemplo

El núcleo del homomorfismo $f: \mathbb{R}^3 \longrightarrow \mathbb{R}^2 / f(x,y,z) = (x+y,0)$ es

$$N_f = \{(x,y,z) \in \mathbb{R}^3 / x = -y\}.$$

En efecto,

$$N_f = \{(x,y,z) \in \mathbb{R}^3 / f(x,y,z) = (0,0)\} = \{(x,y,z) \in \mathbb{R}^3 / (x+y,0) = (0,0)\}$$

$$(x+y,0) = (0,0) \Leftrightarrow \begin{cases} x+y=0 \\ 0=0 \end{cases} \Leftrightarrow x = -y$$

De modo que

$$N_f = \{(x,y,z) \in \mathbb{R}^3 / x = -y\}.$$

Proposición 20

Sean $(G,*), (H,\circ)$ dos grupos con elementos neutros e_G y e_H respectivamente y $f: G \longrightarrow H$ un homomorfismo. El Núcleo del homomorfismo f es un subgrupo del grupo G.

Demostración

Recordemos la definición de núcleo de un homomorfismo, y luego aplicamos la Proposición 7

$$N_f = \{x \in G / f(x) = e_H\}.$$

a) $N_f \subset G$, por definición de Núcleo del homomorfismo f.

b) $N_f \neq \emptyset$.

En efecto, sabemos por Proposición 18 que $f(e_G) = e_H$, por lo tanto $e_G \in N_f$.

c) $x, y \in N_f \Rightarrow x * y \in N_f$.

$$x, y \in N_f \Rightarrow f(x) = e_H \ \wedge \ f(y) = e_H \Rightarrow f(x) \circ f(y) = e_H \circ e_H \Rightarrow f(x * y) = e_H \Rightarrow x * y \in N_f$$

d) $x \in N_f \Rightarrow x' \in N_f$.

$$x \in N_f \Rightarrow f(x) = e_H \Rightarrow [f(x)]' = e_H' \Rightarrow f(x') = e_H \Rightarrow x' \in N_f$$

Con a), b), c) y d) hemos probado que $N_f \prec G$.

Q.E.D.

Imagen de un homomorfismo de grupos

Definición 14

Sean $(G,*), (H,\circ)$ dos grupos y $f: G \longrightarrow H$ un homomorfismo. La ***Imagen*** del homomorfismo f es el conjunto formado por los elementos de H que tienen preimagen en G.

En símbolos,

$$I_f = \{y \in H / \exists\, x \in G : f(x) = y\}$$

De esta definición se deduce que,

$$y \in I_f \iff \exists\, x \in G : f(x) = y$$

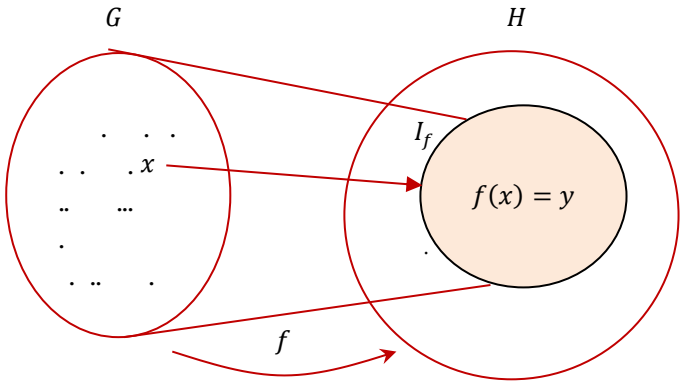


Diagrama de Venn de la Imagen del homomorfismo f

Ejemplo

La Imagen del homomorfismo $f: \mathbb{R}^3 \longrightarrow \mathbb{R}^2 / f(x,y,z) = (x+y, 0)$ es el conjunto

$$I_f = \{(a,b) \in \mathbb{R}^2 / b = 0\}$$

En efecto,

$$I_f = \{(a,b) \in \mathbb{R}^2 / \exists (x,y,z) \in \mathbb{R}^3 : f(x,y,z) = (a,b)\}$$

$$f(x,y,z) = (a,b) \Rightarrow (x+y, 0) = (a,b) \Rightarrow \begin{cases} x + y = a \\ 0 = b \end{cases}$$

Para que este sistema de ecuaciones lineales sea compatible debe ocurrir que $b = 0$, mientras que a puede asumir cualquier valor real, de modo que

$$I_f = \{(a,b) \in \mathbb{R}^2 / b = 0\}$$

Proposición 21

Sean $(G,*), (H,\circ)$ dos grupos y $f: G \longrightarrow H$ un homomorfismo. La Imagen del homomorfismo f es un subgrupo del grupo H.

Demostración

Recordemos la definición de imagen de un homomorfismo, y luego aplicamos la Proposición 7

$$I_f = \{y \in H / \exists x \in G : f(x) = y\}$$

i) $I_f \subset H$; por definición de Imagen del homomorfismo f.

ii) $I_f \neq \emptyset$.

En efecto, sabemos por Proposición 18 que $f(e_G) = e_H$, por lo tanto $e_H \in I_f$.

iii) $a, b \in I_f \Rightarrow a \circ b \in I_f$

$$a, b \in I_f \Rightarrow \exists\, x \in G: f(x) = a \ \wedge\ \exists\, y \in G: f(y) = b \Rightarrow \exists\, x, y \in G: f(x) \circ f(y) = a \circ b \Rightarrow$$

$$\Rightarrow \exists\, x * y \in G: f(x * y) = a \circ b \Rightarrow a \circ b \in I_f$$

iv) $a \in I_f \Rightarrow a' \in I_f$

$$a \in I_f \Rightarrow \exists x \in G: f(x) = a \Rightarrow \exists\, x \in G: [f(x)]' = a' \Rightarrow \exists\, x' \in G: f(x') = a' \Rightarrow a' \in I_f$$

Con i), ii), iii) y iv) llegamos a mostrar que $I_f \prec H$.

Definición 15

Sean $(G,*), (H,\circ)$ dos grupos. La función $f: G \longrightarrow H$ es un isomorfismo si y sólo si
i) f es un homomorfismo y
ii) f es biyectiva.

Nota

Si $(G,*), (H,\circ)$ son grupos y $f: G \longrightarrow H$ es un isomorfismo, se dice que "G es isomorfo a H" y se simboliza $G \cong H$.

3.2. Homomorfismo de Cuerpos

Definición 16

Sean dos cuerpos $(F, +, \cdot)$ y $(K, +, \cdot)$. La función $f: F \longrightarrow K$ es un ***homomorfismo*** del cuerpo F en el cuerpo K si y sólo si:

i). $\forall\, a, b \in F; f(a + b) = f(a) + f(b)$

ii). $\forall\, a, b \in F; f(a \cdot b) = f(a) \cdot f(b)$

Proposición 22

Sean $(F, +, \cdot)$ y $(K, +, \cdot)$ dos cuerpos, cuyas unidades son 1_F y 1_K respectivamente. Si $f: F \longrightarrow K$ es un homomorfismo, entonces $f(1_F) = 1_K$.

Demostración

Sea $a \in F$ y $a \notin N_f$. Sabemos que

$$a \cdot 1_F = a$$

Aplicando f en ambos miembros, resulta

$$f(a \cdot 1_F) = f(a)$$

Como f es un homomorfismo y 1_K es la unidad del cuerpo K, tenemos

$$f(a) \cdot f(1_F) = f(a) \cdot 1_K$$

Por ser $(K - \{0\}, \cdot)$ un grupo, vale la ley cancelativa para elementos no nulos de K de donde se sigue que,

$$f(1_F) = 1_K.$$

Q.E.D.

Definición 17

Sean $(F,+,\cdot)$ y $(K,+,\cdot)$ dos cuerpos. La función $f: F \longrightarrow K$ es un ***isomorfismo*** si y sólo si
i) f es un homomorfismo y
ii) f es biyectiva.

Nota

Si $(F,+,\cdot)$ y $(K,+,\cdot)$ son cuerpos y $f: F \longrightarrow K$ un isomorfismo, se dice que "F **es isomorfo a** K" y se simboliza $F \cong K$.

Ejemplo

El cuerpo de los números complejos con segunda componente cero es isomorfo al cuerpo de los números reales y el isomorfismo que determina esta situación es,

$$f: \mathbb{C}_0 \to \mathbb{R} / f(a,0) = a.$$

Esto indica que todo número complejo $(a,0)$ se identifica con el número real a y recíprocamente.

4.- ÁLGEBRA DE BOOLE

Definición 17

Sea un conjunto no vacío B y dos leyes denotadas con $+$ y $\cdot$, la terna $(B,+,\cdot)$ es un ***Álgebra de Boole*** si y sólo sí

1) $+$ y $\cdot$ son leyes de composición interna en B
   $\forall\, a,b \in B; a+b \in B$
   $\forall\, a,b \in B; a \cdot b \in B$

2) $+$ y $\cdot$ son asociativas
   $\forall\, a,b,c \in B; a+(b+c) = (a+b)+c$
   $\forall\, a,b,c \in B; a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) $+$ y $\cdot$ son conmutativas
   $\forall\, a,b \in B; a+b = b+a$
   $\forall\, a,b \in B; a \cdot b = b \cdot a$

4) $+$ y $\cdot$ son distributivas, cada una respecto de la otra
   $\forall\, a,b,c \in B; a+(b \cdot c) = (a+b) \cdot (a+c)$
   $\forall\, a,b,c \in B; a \cdot (b+c) = (a \cdot b)+(a \cdot c)$

5) Existen elementos neutros en B, respecto de $+$ y de $\cdot$ que se denotan con 0 y 1 respectivamente
   $\exists\, 0 \in B: \forall\, a \in B;\ a+0 = 0+a = a$
   $\exists\, 1 \in B: \forall\, a \in B;\ a \cdot 1 = 1 \cdot a = a$

6) $1 \neq 0$

7) Todo elemento $a \in B$ admite un ***complementario*** $a' \in B$, tal que
$\forall\, a \in B;\ \exists\, a' \in B: a + a' = a' + a = 1$
$\forall\, a \in B;\ \exists\, a' \in B: a \cdot a' = a' \cdot a = 0$

Notas

1.- Es frecuente que en vez de los símbolos de la suma $(+)$, la multiplicación $(\cdot)$**,** y del complementario $(')$, se empleen los símbolos de las operaciones conjuntistas de la unión $(\cup)$, la intersección $(\cap)$ y del complemento $(c$ ó $-)$, o bien las conectivas lógicas de la disjunción $(\vee)$, conjunción $(\wedge)$ y de la negación $(\sim)$ respectivamente.

2.- También suelen utilizarse términos como Y, O, NO, SI (AND, OR, NOT, IF).

3.- Se supondrá, al igual que el álgebra ordinaria, la precedencia de las operaciones, esto es, la operación multiplicación es prioritaria sobre la operación suma. Esta prioridad podrá ser alterada con el uso de paréntesis. Por ejemplo:

$a + b \cdot c = a + (b \cdot c)$, pero $a + b \cdot c \neq (a + b) \cdot c$

Modelos de la Estructura Algebraica de Álgebra de Boole

1.- Sea U un conjunto no vacío. El conjunto "***partes de*** U", denotado por $\mathcal{P}(U)$, con las operaciones de *unión*, *intersección* y *complementación* de conjuntos, es un modelo de la estructura algebraica de Álgebra de Boole. Donde el conjunto $\emptyset$ es el elemento neutro para la unión, U es elemento neutro para la intersección y $A^c = U - A$ es el complemento de cualquier subconjunto A de U**.**

2.- El conjunto de los valores de verdad de las proposiciones lógicas $\mathcal{V} = \{V,\ F\}$, con las conectivas lógicas *disjunción* $(\vee)$, *conjunción* $(\wedge)$ y *negación* $(\sim)$, definidas en las siguientes tablas

$\vee$	V	F
V	V	V
F	V	F

$\wedge$	V	F
V	V	F
F	F	F

	$\sim$
V	F
F	V

constituye un modelo del Álgebra de Boole, donde F es el elemento neutro para la disjunción**,** V es el elemento neutro para la conjunción y el valor de verdad de $\sim p$ (la negación de la proposición p) es el complementario del valor de verdad de la proposición p.

3.-El conjunto $B = \{0,1\}$ con las leyes definidas mediante las tablas

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

	$'$
0	1
1	0

constituye un modelo de la estructura algebraica de Álgebra de Boole, llamada ***Álgebra de Boole Binaria***, donde 0 es el elemento neutro para la suma, 1 es el elemento neutro para la multiplicación, el complementario de 0 es 1 $(0' = 1)$ y el complementario de 1 es 0 $(1' = 0)$.

Definición 18

Dada una proposición p, se llama proposición "***dual de*** p" a la proposición que se obtiene de p al intercambiar entre sí las operaciones de suma $(+)$ y multiplicación $(\cdot)$ y sus elementos neutros 0 y 1.

Nota
Es fácil advertir que los axiomas de la estructura de Álgebra de Boole relativo a la operación multiplicación $(\cdot)$ son los duales de los axiomas correspondientes a la operación suma $(+)$ y recíprocamente.

Propiedades del Álgebra de Boole

P1.-*Principio de dualidad*

Si una proposición p es derivable de los axiomas de Álgebra de Boole, entonces la proposición dual de p es también derivable de los axiomas de Álgebra de Boole.

Demostración

En efecto, al demostrar una proposición p empleando una sucesión de axiomas de Álgebra de Boole, la proposición dual de p se demuestra empleando la sucesión de los axiomas duales.

P2.- *Unicidad de los elementos neutros 0 y 1*

i) Existe un único elemento neutro para la suma.
ii) Existe un único elemento neutro para la multiplicación.

Demostración para el alumno

P3.-*Idempotencia*

Todos los elementos de un Álgebra de Boole son idempotentes respecto a la suma y a la multiplicación. Esto es

i) $a \in B \Longrightarrow a + a = a$
ii) $a \in B \Longrightarrow a \cdot a = a$

Demostración

i) $a \underbrace{=}_{(1)} a + 0 \underbrace{=}_{(2)} a + (a' \cdot a) \underbrace{=}_{(3)} (a + a') \cdot (a + a) \underbrace{=}_{(4)} 1 \cdot (a + a) \underbrace{=}_{(5)} a + a$

Referencias. Para ser completado por el alumno
(1) 0 es el nuetro para la suma.
(2)
(3)
(4)
(5)

ii) La propiedad dual se demuestra empleando el Principio de Dualidad.

Q.E.D.

P4.-*Identidad de los elementos 0 y 1*

i) $a \in B \Longrightarrow a + 1 = 1$
ii) $a \in B \Longrightarrow a \cdot 0 = 0$

Demostración

i) $a + 1 \underbrace{=}_{(1)} a + (a + a') \underbrace{=}_{(2)} (a + a) + a' \underbrace{=}_{(3)} a + a' \underbrace{=}_{(4)} 1$

Referencias. Para ser completado por el alumno
(1)
(2)
(3)
(4)

ii) La propiedad dual se demuestra empleando el Principio de Dualidad.

Q.E.D.

P5.- ***Absorción***

i) $a, b \in B \Longrightarrow a + (a \cdot b) = a$
ii) $a, b \in B \Longrightarrow a \cdot (a + b) = a$

Demostración

i) $a + (a \cdot b) \underbrace{=}_{(1)} (a \cdot 1) + (a \cdot b) \underbrace{=}_{(2)} a \cdot (1 + b) \underbrace{=}_{(3)} a \cdot 1 \underbrace{=}_{(4)} a$

Referencias. Para ser completado por el alumno
(1)
(2)
(3)
(4)

ii) La propiedad dual se demuestra empleando el Principio de Dualidad.

Q.E.D.

P6.- ***Unicidad del complementario***

Cada elemento a de B admite un único complementario a' *de* B**.**

Demostración

Sean a'_1 y a'_2 complementarios de a, se mostrará que $a'_1 = a'_2$. En efecto,

$$a'_2 \underbrace{=}_{(1)} a'_2 + 0 \underbrace{=}_{(2)} a'_2 + (a \cdot a'_1) \underbrace{=}_{(3)} (a'_2 + a) \cdot (a'_2 + a'_1) \underbrace{=}_{(4)} 1 \cdot (a'_2 + a'_1) \underbrace{=}_{(5)}$$

$$\underbrace{=}_{(5)} (a + a'_1) \cdot (a'_2 + a'_1) \underbrace{=}_{(6)} (a \cdot a'_2) + a'_1 \underbrace{=}_{(7)} 0 + a'_1 \underbrace{=}_{(8)} a'_1$$

Referencias. Para ser completado por el alumno

(1) ……..
(2) ……..
(3) ……..
(4) ……..
(5) ……..
(6) ……..
(7) ……..
(8) ……..

Q.E.D

P7.- ***Involución***

El complementario del complementario de un elemento $a \in B$ es a. Esto es,

$$a \in B \Longrightarrow (a')' = a$$

Demostración: queda para el alumno.

P8.- ***Leyes de De Morgan***

i) $a, b \in B \Longrightarrow (a+b)' = a' \cdot b'$

ii) $a, b \in B \Longrightarrow (a \cdot b)' = a' + b'$

Demostración

i) $(a+b)\cdot(a'\cdot b') \underbrace{=}_{(1)} a\cdot(a'\cdot b') + b\cdot(a'\cdot b') \underbrace{=}_{(2)} (a\cdot a')\cdot b' + (b\cdot b')\cdot a' \underbrace{=}_{(3)} 0$

Referencias

(1)

(2)

(3)

Análogamente se prueba que $(a' \cdot b') \cdot (a+b) = 0$, por lo tanto $(a' \cdot b')$ es el complementario de $(a+b)$ y por la unicidad del complementario $(a+b)' = (a' \cdot b')$.

ii) La propiedad dual se demuestra empleando el Principio de Dualidad.

Q.E.D

P9.- ***Complementarios de 0 y 1***

i) 0' = 1

ii) 1' = 0

P10.- ***Cancelatividad en la multiplicación***

Si a, b y c son elementos de B, entonces se verifica que

$$[a \cdot b = c \cdot b \wedge a \cdot b' = c \cdot b'] \Longrightarrow a = c$$

Demostración

$$a \underbrace{=}_{(1)} a\cdot 1 \underbrace{=}_{(2)} a\cdot(b+b') \underbrace{=}_{(3)} a\cdot b + a\cdot b' \underbrace{=}_{(4)} c\cdot b + c\cdot b' \underbrace{=}_{(5)} c\cdot(b+b') \underbrace{=}_{(6)} c\cdot 1 \underbrace{=}_{(7)} c$$

Referencias. Para ser completado por el alumno

(1) ……. (5) …….

(2) ……. (6) …….

(3) ……. (7) …….

(4) …….

Q.E.D

P11.- ***Sin nombre especial***

i) $a, b \in B \Longrightarrow a + a' \cdot b = a + b$

ii) $a, b \in B \Longrightarrow a \cdot (a' + b) = a \cdot b$

Demostración

i) $a+b \underbrace{=}_{(1)} a+1\cdot b \underbrace{=}_{(2)} a+(a+a')\cdot b \underbrace{=}_{(3)} a+a\cdot b+a'\cdot b \underbrace{=}_{(4)} a+a'\cdot b$

Referencias. Para ser completado por el alumno.

(1) …….. (3) ……..
(2) …….. (4) ……..

ii) La propiedad dual se demuestra empleando el Principio de Dualidad.

Q.E.D

4.1. Funciones Booleanas

Sea $(\boldsymbol{B}, +, \cdot)$ un Álgebra de Boole.

Definición 19

Se denomina ***constante*** a un elemento particular de $\boldsymbol{B}$, como por ejemplo el elemento neutro $\mathbf{0}$.

Definición 20

Una ***variable*** es un símbolo que representa a cualquier elemento del conjunto $\boldsymbol{B}$. Las variables se designan con las últimas letras del alfabeto castellano.

Definición 21

Una función booleana es toda expresión de un Álgebra de Boole, que consiste en combinaciones de sumas y/o productos de un número finito de variables.

Por ejemplo,

$f(x) = x + x'$
$g(x, y, z) = x + y \cdot z'$

En un Álgebra de Boole las funciones booleanas se pueden expresar en general como suma de productos distintos o como producto de sumas distintas, aplicando axiomas y propiedades. Por ejemplo,

a) $f(x,y,z) = [(x + y') \cdot (x \cdot y' \cdot z)']' \underbrace{=}_{(1)} (x + y')' + [(x \cdot y' \cdot z)']' \underbrace{=}_{(2)} (x' \cdot y) + (x \cdot y' \cdot z)$

Referencias
(1) Por leyes de De Morgan.
(2) Por leyes de De Morgan y Prop. Involutiva.

b) $f(x,y,z) = \{[(x' \cdot y')' + z] \cdot (x + z)\}' \underbrace{=}_{(1)} [(x' \cdot y')' + z]' + (x + z)' \underbrace{=}_{(2)} (x' \cdot y' \cdot z') +$

$(x' \cdot z') \underbrace{=}_{(3)} x' \cdot z'$

Referencias

(1) Por leyes de De Morgan.

(2) Por leyes de De Morgan y Prop. Involutiva.

(3) Por Prop. de absorción.

Forma Canónica de Funciones Booleanas

Definición 22

La ***forma canónica*** de una función booleana es la formada por una suma de términos, y cada uno de ellos está compuesto por un producto de todas las variables, complementadas o no, de la función.

Por ejemplo la función f siguiente se transforma a la forma canónica aplicando axiomas y propiedades de Álgebra de Boole.

$$f(x,y,z) = (x' \cdot y) + (x \cdot y' \cdot z) = (x' \cdot y \cdot 1) + (x \cdot y' \cdot z) = \big(x' \cdot y \cdot (z + z')\big) + (x \cdot y' \cdot z) =$$
$$= (x' \cdot y \cdot z) + (x' \cdot y \cdot z') + (x \cdot y' \cdot z)$$

Notas

1. La forma canónica de una función booleana en n variables contiene a lo sumo 2^n términos distintos.
2. La forma canónica de una función booleana que contiene los 2^n términos distintos se llama forma canónica completa.

   Por ejemplo, los $2^3 = 8$ términos de la forma canónica completa de una función booleana en 3 variables son:

$$f(x,y,z) = (x \cdot y \cdot z) + (x' \cdot y \cdot z) + (x \cdot y' \cdot z) + (x \cdot y \cdot z') + (x' \cdot y' \cdot z) + (x' \cdot y \cdot z') + (x \cdot y' \cdot z') + (x' \cdot y' \cdot z')$$

3. La forma canónica completa de una función booleana en n variables es igual a 1.

Definición 23

La función complementaria de una función boolena f expresada en la forma canónica, denotado con fc , es igual a la suma de todos los términos de la forma canónica completa de f que no aparecen en la forma canónica de f.

Por ejemplo, el complemento de la función booleana de la función del ejemplo precedente es

$$fc(x,y,z) = (x \cdot y \cdot z) + (x \cdot y \cdot z') + (x' \cdot y' \cdot z) + (x \cdot y' \cdot z') + (x' \cdot y' \cdot z')$$

Proposición 23

Si en la forma canónica completa de una función booleana en n variables, cada variable toma el valor 0 o el valor 1, entonces sólo un término tiene el valor 1 y todos los demás tienen el valor 0.

Proposición 24

Dos funciones booleanas son iguales si y sólo si sus formas canónicas respectivas son idénticas, es decir, sus formas canónicas tienen los mismos términos.

Forma Canónica Dual de Funciones Booleanas

Definición 24

La ***forma canónica dual*** de una función booleana es la formada por un producto de factores, y cada uno de ellos está compuesto por una suma de todas las variables, complementadas o no, de la función.

Por ejemplo la siguiente función booleana f se lleva a la forma canónica dual empleando axiomas y propiedades de Álgebra de Boole.

$$f(x,y,z) = (x+y)\cdot(y+z)\cdot(x'+z)\cdot(x'+y') = \cdots =$$
$$= (x+y+z)\cdot(x+y+z')\cdot(x'+y+z)\cdot(x'+y'+z)\cdot(x'+y'+z')$$

Notas

1. La forma canónica dual de una función booleana en n variables contiene a lo sumo 2^n factores distintos.
2. La forma canónica dual de una función booleana en n variables que contiene los 2^n términos se llama forma canónica dual completa.
3. La forma canónica dual completa de una función booleana en n variables es idénticamente 0.
4. La forma canónica dual de una función booleana en n variables, **no es** la dual de la forma canónica.

***Definición 25*:**

La función complementaria de una función boolena f expresada en la forma canónica dual, denotado con fc, es igual al producto de todos los factores de la forma canónica dual completa que no aparecen en la forma canónica dual de f.

Por ejemplo, el complemento de la función booleana del ejemplo precedente es

$$fc(x,y,z) = (x+y'+z)\cdot(x'+y+z')\cdot(x+y'+z')$$

Proposición 23'

Si en la forma canónica dual completa en n variables cada variable toma el valor 0 o el valor 1, sólo un factor tiene el valor 0 y todos los demás tienen el valor 1.

Proposición 24'

Dos funciones booleanas son iguales si y sólo sí sus formas canónicas duales respectivas son idénticas, es decir tienen los mismos factores.

Tabla de Valores de una Función Booleana del Álgebra de Boole Binaria

Si f es una función booleana en n variables del Álgebra de Boole Binaria, es posible construir una tabla de valores de la función f para todas las posibles maneras de asignar los valores 0 y 1 a las variables.

Teniendo en cuenta la Proposición 23, los términos que aparecen en la forma canónica de la función son los de la forma canónica completa en n variables que tienen valor 1 cuando f es igual a 1.

Por ejemplo si la tabla de una función booleana en tres variables viene dada por

x	y	z	$f(x,y,z)$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

$$f(x,y,z) = (x \cdot y \cdot z) + (x \cdot y' \cdot z) + (x \cdot y'.z') + (x' \cdot y' \cdot z) + (x' \cdot y' \cdot z')$$

Análogamente, los términos de la forma canónica dual de f son los de la forma canónica dual completa que tienen el valor 0 cuando f es 0.

En el ejemplo es

$$f(x,y,z) = (x' + y' + z) \cdot (x + y' + z') \cdot (x + y' + z)$$

4.2. Álgebra de Redes Eléctricas

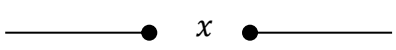
El álgebra de redes eléctricas (circuitos eléctricos) es una aplicación muy importante del Álgebra de Boole de los elementos 0 y 1. Los circuitos lógicos digitales en los que está basada la arquitectura básica de una computadora son diseñados y simplificados gracias a las funciones booleanas y a las técnicas que provee el Álgebra de Boole; esto es de mucha importancia para el especialista en informática, ya que en la construcción de computadoras electrónicas se usa la analogía de los circuitos con las relaciones lógicas para dotar a las maquinas de la capacidad de comparar y de decidir entre diversas alternativas.

Se limitará el estudio al tipo más sencillo de redes, a aquellas con sólo interruptores.

Un interruptor instalado en una red eléctrica es un mecanismo que produce dos respuestas: permite o impide el paso de la corriente eléctrica.

Se puede pensar en el conjunto de respuestas de un interruptor como en los elementos de un Álgebra de Boole binaria, $B = \{0,1\}$, asociando valor 1 a la variable que denota al interruptor cuando permite el paso de la corriente y valor 0 cuando impide el paso de la misma.

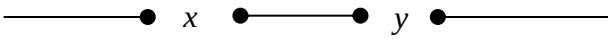
1.- La red más simple consiste en un hilo conductor con un solo interruptor x.



Al cerrar el interruptor, la corriente fluye por el hilo, se le asigna el valor 1 a x; si el interruptor está abierto y no fluye corriente, se le asigna el valor 0. Asimismo, se dará el valor 1 o 0 a toda red según la corriente fluya o no por ella.

En este caso, la red tiene valor 1 si y sólo si x tiene valor 1 y la red tiene valor 0 si y sólo si x tiene valor 0.

2.- Sea ahora una red que consiste en dos interruptores x e y conectados *en serie*

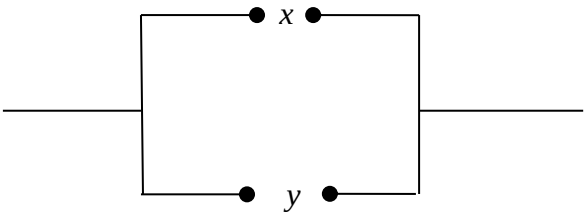


es claro que la red toma el valor 1 si y sólo si x e y tienen valor 1 pues ambos interruptores están cerrados y por lo tanto la corriente fluye por la red. En cualquier otro caso, es decir si el valor de x o el de y o el de ambos es 0, no fluye corriente y por lo tanto el valor de la red es 0. De acuerdo a lo expuesto, esta red puede ser representada por la función booleana $F(x,y)$ cuya tabla es la siguiente;

x	y	$F(x,y)$
1	1	1
1	0	0
0	1	0
0	0	0

es claro que la tabla corresponde a la función booleana $F(x,y) = x \cdot y$

3.- Sea ahora una red que consiste en dos interruptores x e y conectados *en paralelo.*

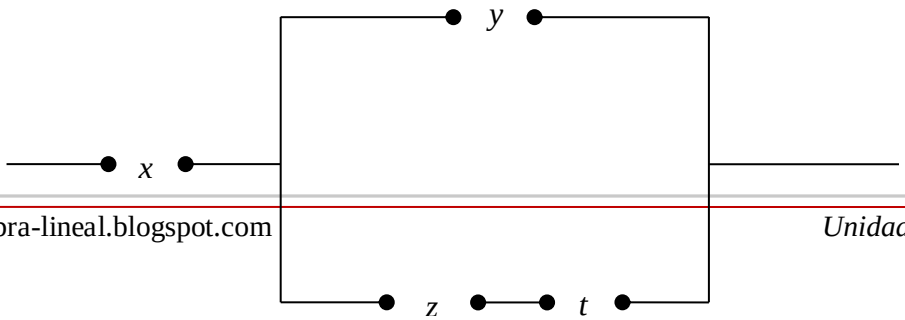


En este caso la red toma el valor 1 si y sólo si al menos uno de los interruptores x o y tiene el valor 1, y la red toma el valor 0 si y sólo si ambos interruptores x e y tienen el valor 0. Esta red puede ser representada por la función $F(x,y)$ dada en la siguiente tabla;

x	y	$F(x,y)$
1	1	1
1	0	1
0	1	1
0	0	0

Es claro que la tabla corresponde a la función booleana $F(x,y) = x + y$.

4.- Empleando más interruptores, pueden diseñarse redes más complejas, como por ejemplo



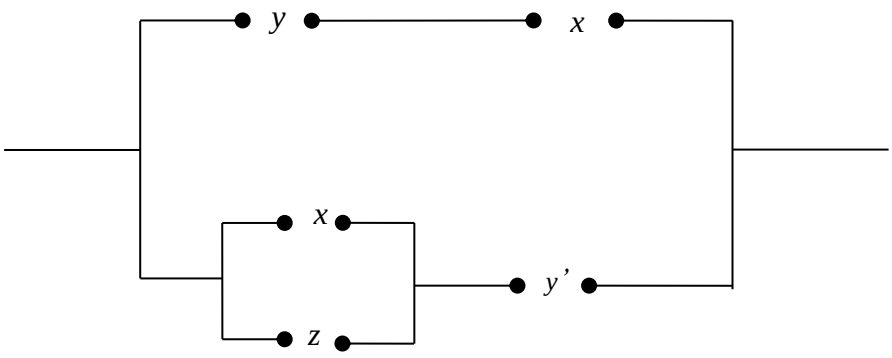
donde la función booleana asociada a esta red es $F(x,y,z,t) = x \cdot (y + z \cdot t)$.

Hasta aquí se ha supuesto que todos los interruptores de una red actúan independientemente unos de otros, sin embargo dos o más interruptores pueden estar conectados de manera tal que,

I- se abren y se cierran simultáneamente,
II- el cierre (apertura) de uno abra (cierre) otro u otros.

En el caso I se denotarán todos los interruptores por la misma letra y en el caso II se denotará a uno de los interruptores con x y los otros con x'; donde x' es el complementario de x.

Por ejemplo, la siguiente red consiste en un par de interruptores denotados por x, que se abren y cierran simultáneamente; un par de interruptores denotados por y e y' tales que, el cierre de un interruptor abre el otro y un interruptor independiente denotado por z.



la función booleana correspondiente a esta red es, $F(x,y,z) = (x \cdot y) + ((x + z) \cdot y')$.

Simplificación de redes eléctricas

En muchas ocasiones las redes resultan innecesariamente complicadas por lo que es importante disponer de técnicas que permitan obtener una red más simple equivalente a la dada; el Álgebra de Boole suministra las herramientas necesarias. Una vez que se obtiene la expresión booleana correspondiente a una red, es posible reducirla a una forma más simple aplicando axiomas y/o propiedades del Álgebra de Boole; la nueva expresión puede utilizarse para crear una nueva red, equivalente a la original, pero que contenga menos interruptores y conexiones.

Ejemplo

Sea la red del ejemplo anterior. La función booleana asociada a ella es,

$$F(x,y,z) = (y \cdot x) + ((x + z) \cdot y')$$

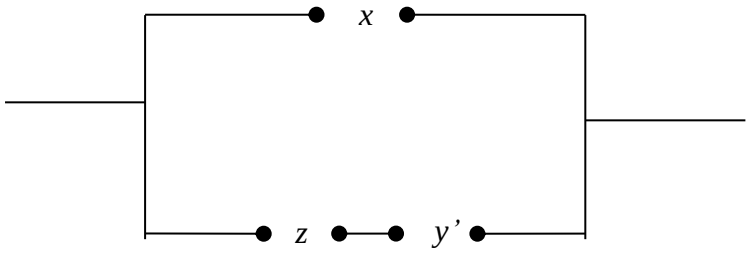
la que puede ser expresada en una forma más simple, empleando axiomas y/o propiedades del Álgebra de Boole. En efecto,

$$F(x,y,z) = (y \cdot x) + \big((x + z) \cdot y'\big) \underbrace{=}_{(1)} (y \cdot x) + [(x \cdot y') + (z \cdot y')] \underbrace{=}_{(2)}$$

$$\underset{(2)}{=} [(x \cdot y) + (x \cdot y')] + (z \cdot y') \underset{(3)}{=} [x \cdot (y + y')] + (z \cdot y') \underset{(4)}{=} x \cdot 1 + (z \cdot y') \underset{(5)}{=} x + (z \cdot y')$$

Referenicas.
(1) Por distributividad de · respecto de +.
(2) Por conmutatividad de · y asociatividad de +.
(3) Por distributividad de · respecto de +.
(4) Por suma de complementarios.
(5) Por elemento neutro respecto de ·

Luego la red correspondiente a la forma más simple de la función $F(x, y, z) = x + (z \cdot y')$ es



la cual es mucho más sencilla que la anterior ya que contiene menos interruptores. Puede observarse la equivalencia de ambas redes al confeccionar las tablas de valores de la funciones booleanas de la red original y de la red simplificada. En ambos casos se obtienen tablas equivalentes, es decir con los mismos valores.

x	y	z	y'	$y \cdot x$	$x + z$	$(x + z) \cdot y'$	$F(x, y, z) = (y \cdot x) + ((x + z) \cdot y')$
1	1	1	0	1	1	0	1
1	1	0	0	1	1	0	1
1	0	1	1	0	1	1	1
1	0	0	1	0	1	1	1
0	1	1	0	0	1	0	0
0	1	0	0	0	0	0	0
0	0	1	1	0	1	1	1
0	0	0	1	0	0	0	0

x	y	z	y'	$z \cdot y'$	$F(x, y, z) = x + (z \cdot y')$
1	1	1	0	0	1
1	1	0	0	0	1
1	0	1	1	1	1
1	0	0	1	0	1
0	1	1	0	0	0
0	1	0	0	0	0

0	0	1	1	1	1
0	0	0	1	0	0