CUADERNO III

ESTRUCTURAS ALGEBRAICAS

Miguel A. Sainz, Joan Serarols, Anna M. Pérez
Dep. de Informática y Matemática Aplicada
Universidad de Girona

RESUMEN: Veremos el concepto de estructura algebraica y las más importantes estructuras con leyes de composición internas: grupos anillos y cuerpos. Se estudiarán las cuestiones más relevantes acerca de los polinomios sobre un cuerpo, ejemplo importante de anillo. Bastante más detalle será puesto en el estudio de una cuarta estructura algebraica: el álgebra de Boole y el caso particular del algebra de circuitos eléctricos.

El Algebra, que desde su origen y durante muchos años fue la rama de las matemáticas que trataba de números y de ecuaciones, amplía su campo a finales del siglo XIX hacia nuevos objetos, como son los vectores, los polinomios, las matrices,..., etc y se separa del estudio de la solución de ecuaciones dirigiéndose hacia las estructuras abstractas. Al igual que con los números, con los vectores, polinomios, matrices,.., etc, se realizan operaciones que, en muchos casos, se denominan con los mismos nombres que las operaciones clásicas, suma, producto,.., definidas y delimitadas por propiedades análogas a las de la suma, producto,... de números, tales como la asociativa, conmutativa,.., que forman las reglas del juego con los nuevos objetos. El Algebra pasa a ser la ciencia que estudia las estructuras, es decir, conjuntos con operaciones verificando ciertas propiedades que determinan qué tipo de estructura es, recibiendo nombres como *grupo, anillo, álgebra de Boole*,.... Más aún, el Algebra estudia hoy día cualquier estructura o, mejor aún, ninguna en concreto, siendo un procedimiento lógico que en muchos casos puede adaptarse al mundo físico, de manera que es la base de muchas ciencias actuales como la inteligencia artificial o la mecánica cuántica.

III.1.- LEYES DE COMPOSICION

El concepto de operación o ley de composición es una abstración y generalización de las operaciones clásicas, suma y producto, entre números, consideradas como leyes mediante las cuales de dos elementos obtenemos otro, y así decimos que la suma de 3 y 4 es 7 o el producto 12.

Dados tres conjuntos A, B y C definimos una ***operación*** o ***ley de composición*** sobre A, B y C como una aplicación

$$\begin{aligned} f:\ A\times B &\longrightarrow C \\ (a,b) &\longrightarrow f(a,b) \end{aligned}$$

en la que a cada par de elementos de $A\times B$ le corresponde un único elemento de C que, en principio, podemos representar, mediante la notación específica para funciones, por $f(a,b)$. Pero siguiendo la notación tradicional que se ha empleado para las operaciones, es mejor representar la operación por símbolos especiales $+$, Δ, o,... y la imagen de un par, denominada compuesto de los dos elementos, escribirlo mediante las letras que designan los elementos del par separadas por el símbolo de la operación

$$\begin{aligned} \Delta : \ A\times B &\longrightarrow C \\ (a,b) &\longrightarrow a\Delta b \end{aligned}$$

Los símbolos tradicionales de suma y producto de números, $+$ y $\cdot$, también se utilizan como símbolos de operaciones entre conjuntos, cualesquiera que sea la naturaleza de sus elementos.

Según los conjuntos sobre los que se define una operación se denomina de un modo más concreto:

a) ***Ley de composición interna*** (l.c.i) sobre A, es una aplicación

$$\begin{aligned} \bullet : \ A\times A &\longrightarrow A \\ (a,b) &\longrightarrow a\bullet b \end{aligned}$$

Cuando para simbolizar una l.c.i. se usa el símbolo $+$ se denomina notación aditiva y si se usa $\cdot$ se llama notación multiplicativa; al igual que en el producto de números, es frecuente omitir del símbolo $\cdot$ para expresar el producto de dos elementos, siempre que no haya lugar a ambigüedades.

b) ***Ley de composición externa*** (l.c.e) sobre A, con dominio de operadores B, es una aplicación

$$\begin{aligned} \S : \ B\times A &\longrightarrow A \\ (\lambda,a) &\longrightarrow \lambda\S a \end{aligned}$$

donde, para evitar confusiones, suelen emplearse dos tipos de letras para distinguir los elementos de A y los de B.

No son éstos los únicos tipos de operaciones, aunque si los más frecuentes.

Una ley de composición vendrá definida cuando se conozca la imagen de cada par del conjunto inicial, lo cual puede hacerse por extensión, si se trata de conjuntos con pocos elementos, o por comprensión. Si es por extensión, las imágenes de los pares suelen disponerse en un cuadro que se denomina ***tabla de la operación*** y si es por compresión habrá que dar un predicado, que puede ser una fórmula, para averiguar la imagen de cualquier par.

Ejemplo III.1.1

Sobre **N** son leyes de composición internas la suma y el producto

$$\begin{aligned} + : \ \mathbf{N}\times\mathbf{N} &\longrightarrow \mathbf{N} \\ (a,b) &\longrightarrow a+b \end{aligned} \qquad\qquad \begin{aligned} \cdot : \ \mathbf{N}\times\mathbf{N} &\longrightarrow \mathbf{N} \\ (a,b) &\longrightarrow a\cdot b \end{aligned}$$

sin embargo no lo es la diferencia pues

$$\begin{array}{rcl} - : \mathbf{N}\times\mathbf{N} & \longrightarrow & \mathbf{N} \\ (a,b) & \longrightarrow & a-b \end{array}$$

no es una aplicación ya que si a es menor que b el par (a,b) no tiene imagen; si lo es en el caso

$$\begin{array}{rcl} - : \mathbf{Z}\times\mathbf{Z} & \longrightarrow & \mathbf{Z} \\ (a,b) & \longrightarrow & a-b \end{array}$$

Ejemplo III.1.2

Son leyes de composición internas sobre $\mathcal{P}(E)$ la unión y la intersección

$$\begin{array}{rcl} \cup : \mathcal{P}(E)\times\mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ (A,B) & \longrightarrow & A \cup B \end{array} \qquad \begin{array}{rcl} \cap : \mathcal{P}(E)\times\mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ (A,B) & \longrightarrow & A \cap B \end{array}$$

Ejemplo III.1.3

Si A es un conjunto, sobre el conjunto de aplicaciones

$$F = \{f : A \longrightarrow A\}$$

es ley de composición interna la composición de aplicaciones

$$\begin{array}{rcl} \circ : F\times F & \longrightarrow & F \\ (f,g) & \longrightarrow & f\circ g : A \longrightarrow A \\ & & x \longrightarrow (f\circ g)(x) = f(g(x)) \end{array}$$

Ejemplo III.1.4

Sobre el conjunto $A = \{a,b,c,d\}$ es ley de composición interna la definida por la tabla

$\bullet$	a	b	c	d
a	b	a	c	c
b	c	c	c	c
c	d	b	b	a
d	a	b	c	d

en la que se expresa que los elementos de la entrada vertical se componen a la izquierda con los de la entrada horizontal; p.ej.

$$c\bullet d = a \qquad d\bullet b = b \qquad b\bullet b = c$$

Ejemplo III.1.5

Es ley de composición externa en el conjunto

$$F = \{\text{funciones } f:\ \mathbf{N} \longrightarrow \mathbf{N}\}$$

con dominio de operadores **N**, la aplicación

$$\begin{aligned} \mathbf{N}\times F &\longrightarrow F \\ (a,f) &\longrightarrow af:\ \mathbf{N} \longrightarrow \mathbf{N} \\ & \qquad x \longrightarrow (af)(x) = af(x) \end{aligned}$$

Ejemplo III.1.6

Sea el conjunto de funciones reales de variable real

$$F = \{f:\ A \longrightarrow \mathbf{R} \quad \text{con } A \subseteq \mathbf{R}\}$$

En F pueden definirse la suma, diferencia y producto de funciones mediante la suma, diferencia y producto de números reales

$$\begin{aligned} \pm\cdot:\ F\times F &\longrightarrow F \\ (f,g) &\longrightarrow f\pm\cdot g:\ A \longrightarrow \mathbf{R} \\ & \qquad x \longrightarrow (f\pm\cdot g)(x) = f(x)\pm\cdot g(x) \end{aligned}$$

pues $f(x)$ y $g(x)$ son elementos de **R** y como tales pueden sumarse, restarse y multiplicarse. Sin embargo el cociente es l.c.i. únicamente para funciones que no se anulan en A, ya que si $g(x) = 0$ no existe $f(x)/g(x)$ como elemento de **R**.

Un conjunto en el que se han definido una o varias leyes de composición se denomina ***estructura algebraica***.

Es posible generalizar las propiedades de las operaciones clásicas de suma y producto de números a una ley de composición interna general.

Sea • una l.c.i. en A:

a) Si B es un subconjunto de A, diremos que B es ***estable*** para • si se verifica

$$(\forall x,y\in B)\ (x\bullet y\in B)$$

es decir, si el compuesto de dos elementos de B también pertenece a B; así, por ejemplo, para la estructura algebraica (**N**,+) el conjunto de los números pares es estable para la suma y el conjunto de los números impares no lo es.

b) Diremos que • es ***conmutativa*** si se verifica

$$(\forall x,y\in A)\ (x\bullet y = y\bullet x)$$

Dos elementos que verifiquen esta igualdad, se denominan ***conmutables***, con lo que una l.c.i será conmutativa si todos los elementos son conmutables. Así, por ejemplo, son conmutativas la suma y el producto en **N**,**Z**,**Q**,**R** y **C**, y no lo es la diferencia. Si la operación viene definida por una tabla, la conmutatividad se traduce en el hecho de que la tabla sea simétrica respecto de su diagonal; así, a la l.c.i. definida por

•	*a*	*b*	*c*	*d*
a	*b*	*c*	*c*	*a*
b	*c*	*a*	*a*	*b*
c	*c*	*a*	*b*	*b*
d	*a*	*c*	*c*	*d*

en la que los elementos de la columna se componen a la izquierda con los de la fila, los elementos *a* y *b* son conmutables pues

$$a \bullet b = c = b \bullet a$$

sin embargo la operación no es conmutativa ya que la tabla no es simétrica respecto de la diagonal, lo que se traduce en que, por ejemplo

$$d \bullet c = c \neq c \bullet d$$

c) Diremos que • es ***asociativa*** si verifica

$$(\forall x,y,z \in A)\ (x \bullet (y \bullet z) = (x \bullet y) \bullet z)$$

cuyo significado es el siguiente: la composición de tres elementos debe hacerse componiéndolos de dos en dos, pues una l.c.i. está definida sobre pares de elementos, lo cual puede hacerse de dos modos distintos; si dan el mismo resultado, para todas las ternas posibles, la l.c.i. es asociativa y en este caso el compuesto de tres elementos puede escribirse simplemente

$$x \bullet y \bullet z$$

sin necesidad de los paréntesis que señalan las asociaciones de elementos. En general, puede fácilmente demostrarse, que si la l.c.i. es asociativa, el compuesto de *n* elementos es independiente del modo como agrupemos los elementos para componerlos. Más aún, si la ley es asociativa y conmutativa se verifica

$$x_1 \bullet x_2 \bullet \ldots \bullet x_n = x_{i_1} \bullet x_{i_2} \bullet \ldots \bullet x_{i_n}$$

siendo $i_1,i_2,\ldots,i_n$ una permutación cualquiera de $1,2,\ldots,n$.

Si empleamos una notación aditiva o multiplicativa, el compuesto de un elemento consigo mismo *n* veces se representa por

$$\underbrace{x+x+\ldots+x}_{(n)} = nx \qquad\qquad \underbrace{x \ldots x}_{(n)} = x^n$$

respectivamente. Si la operación es asociativa y conmutativa se verifican entonces las igualdades

$$mx+nx = (m+n)x \qquad m(nx) = (mn)x \qquad x^m \cdot x^n = x^{m+n} \qquad (x^n)^m = x^{nm}$$

pues, por ejemplo

$$m(nx) = (\overset{(n)}{x+\ldots+x})+(\overset{(n)}{x+\ldots+x})+\overset{(m)}{\ldots}+(\overset{(n)}{x+\ldots+x}) = \overset{(mn)}{x+x+\ldots+x} = (mn)x$$

d) Si A tiene otra l.c.i., Δ, diremos que Δ es ***distributiva*** respecto a $\bullet$ si se verifica

$$(\forall x,y,z\in A)\ (x\Delta(y\bullet z) = (x\Delta y)\bullet(x\Delta z) \ \wedge\ (y\bullet z)\Delta x = (y\Delta x)\bullet(z\Delta x))$$

que en el caso de ser Δ conmutativa se reduce a una sola igualdad.

Ejemplo III.1.7

En el conjunto $\mathbf{R}$ con las l.c.i. + y $\cdot$ se verifica

$$a(b+c) = ab+ac$$

por lo que el producto de números reales es distributivo respecto de la suma y sin embargo la suma no es distributiva respecto al producto ya que, en general

$$a+(bc) \neq (a+b)(a+c)$$

como fácilmente puede comprobarse. En $\mathcal{P}(E)$ con las l.c.i. de unión e intersección tenemos que

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

una es distributiva respecto de la otra.

En una estructura con l.c.i. $(A,\bullet)$ podemos distinguir los siguientes elementos particulares:

a) $e\in A$ es ***elemento neutro*** si verifica

$$(\forall x\in A)\ (e\bullet x = x\bullet e = x)$$

igualdades que se reducen a una sola si la l.c.i. es conmutativa. El elemento neutro puede existir o no, pero si existe es único, ya que si hubiera dos e_1 y e_2 tendríamos

$$\left.\begin{array}{ll} e_1 \text{ neutro} & \Rightarrow\ e_1\bullet e_2 = e_2 \\ e_2 \text{ neutro} & \Rightarrow\ e_1\bullet e_2 = e_1 \end{array}\right| \ \Rightarrow\ e_1 = e_2$$

Si se utiliza notación aditiva, el neutro suele designarse por el símbolo 0 y en el caso de notación multiplicativa por el símbolo 1 y se denomina ***elemento unidad***. Si $e\in A$ verifica solamente

$$(\forall x\in A)\ (e\bullet x = x)$$

se denomina ***neutro por la izquierda*** y análogamente se define el ***neutro por la derecha***; obviamente, si existe elemento neutro, lo es por la derecha y por la izquierda.

b) Si $(A,\bullet)$ tiene elemento neutro e, diremos que $x,x'\in A$ son ***elementos simétricos*** si verifican

$$x\bullet x' = x'\bullet x = e$$

en cuyo caso diremos que x (y también x') es ***simetrizable***. Por ejemplo, el propio elemento neutro e es simetrizable, y su simétrico es él mismo, pues

$$e\bullet e = e$$

Cuando se utiliza notación aditiva, el simétrico de x se representa por $-x$ y se denomina ***opuesto***; en el caso de notación multiplicativa se representa por x^{-1} o $1/x$ y se denomina ***inverso***. Elemento simétrico de uno dado puede existir o no, pero si existe verifica las propiedades siguientes:

1) Si x' es simétrico de x, entonces x es simétrico de x', es decir,

$$(x')' = x$$

pues las igualdades que definen el simétrico

$$x\bullet x' = x'\bullet x = e$$

indican tanto que x' es simétrico de x, como que x es simétrico de x'.

2) Si $\bullet$ es asociativa y x' es simétrico de x, x' es único; en efecto, si x tuviera dos simétricos x' y x''

$$x'' = e\bullet x'' = (x'\bullet x)\bullet x'' = x'\bullet(x\bullet x'') = x'\bullet e = x'$$

3) Si siendo $\bullet$ asociativa, x e y tienen por simétricos x'e y', respectivamente, entonces $x\bullet y$ es simetrizable y su simétrico es

$$(x\bullet y)' = y'\bullet x'$$

ya que, en efecto

$$(x\bullet y)\bullet(y'\bullet x') = (x\bullet(y\bullet y'))\bullet x' = (x\bullet e)\bullet x' = x\bullet x' = e$$
$$(y'\bullet x')\bullet(x\bullet y) = (y'\bullet(x'\bullet x))\bullet y = (y'\bullet e)\bullet y = y'\bullet y = e$$

que indican que efectivamente $y'\bullet x'$ es el simétrico de $x\bullet y$. Esta propiedad es generalizable a un conjunto de n elementos simetrizables

$$(x_1\bullet x_2\bullet\ldots\bullet x_n)' = x_n'\bullet\ldots\bullet x_2'\bullet x_1'$$

lo que se demuestra por inducción sobre el conjunto

$$S = \{n \in \mathbf{N} \mid (x_1 \bullet x_2 \bullet \ldots \bullet x_n)' = x_n' \bullet \ldots \bullet x_2' \bullet x_1'\}$$

que verifica

$1 \in S$ pues $(x_1)' = x_1'$

$n \in S \Rightarrow (x_1 \bullet x_2 \bullet \ldots \bullet x_n)' = x_n' \bullet \ldots \bullet x_2' \bullet x_1' \Rightarrow$

$\Rightarrow ((x_1 \bullet x_2 \bullet \ldots \bullet x_n) \bullet x_{n+1})' = x_{n+1}' \bullet (x_1 \bullet x_2 \bullet \ldots \bullet x_n)' \Rightarrow$

$\Rightarrow (x_1 \bullet x_2 \bullet \ldots \bullet x_n \bullet x_{n+1})' = x_{n+1}' \bullet (x_n' \bullet \ldots \bullet x_2' \bullet x_1') = x_{n+1}' \bullet x_n' \bullet \ldots \bullet x_2' \bullet x_1' \Rightarrow$

$\Rightarrow n+1 \in S$

En el caso de notación aditiva, si $x_1 = x_2 = \ldots = x_n$ es

$$-(nx) = -(x+x+\overset{(n)}{\ldots}+x) = (-x)+(-x)+\overset{(n)}{\ldots}+(-x) = n(-x)$$

representándose por $-nx$; en notación multiplicativa

$$(x^n)^{-1} = (\overset{(n)}{xx\ldots x})^{-1} = x^{-1}\overset{(n)}{x^{-1}\ldots x^{-1}} = (x^{-1})^n$$

representándose por x^{-n}.

c) En la estructura $(A,\bullet)$ diremos que $a \in A$ es ***regular*** o ***simplificable*** si verifica

$$(\forall x,y \in A)\ ((x \bullet a = y \bullet a \Rightarrow x = y) \wedge (a \bullet x = a \bullet y \Rightarrow x = y))$$

Si únicamente es cierta una de las dos implicaciones, hablaremos de elemento regular a la derecha o a la izquierda. Se verifica que si $\bullet$ es asociativa y a tiene simétrico, a', entonces a es regular, pues

$$x \bullet a = y \bullet a \Rightarrow (x \bullet a) \bullet a' = (y \bullet a) \bullet a' \Rightarrow x \bullet (a \bullet a') = y \bullet (a \bullet a') \Rightarrow x = y$$

y análogamente se demuestra la otra implicación.

d) En $(A,\bullet)$ diremos que $a \in A$ es elemento ***idempotente*** si verifica $a \bullet a = a$.

Ejemplo III.1.8

En la estructura $(\mathbf{N},+)$ se verifica

+ es asociativa, conmutativa y 0 es elemento neutro: $(\forall x \in \mathbf{N})(x+0 = x)$.

0 es simétrico de sí mismo, por ser elemento neutro, y para cualquier otro elemento $x \in \mathbf{N}$ no existe simétrico ya que no hay ningún número natural x' tal que $x+x' = 0$.

Todo elemento es regular pues $x+a = y+a \Rightarrow x = y$

Ejemplo III.1.9

En la estructura $(A,\bullet)$ con la l.c.i. definida mediante la tabla

$\bullet$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

la asociatividad es larga de comprobar ya que habría que establecer que

$$a\bullet(b\bullet c) = (a\bullet b)\bullet c$$

para las 64 ternas posibles, p.ej.

$$\begin{array}{ccc} 3\bullet(2\bullet 3) & = & (3\bullet 2)\bullet 3 \\ 3\bullet 1 & & 1\bullet 3 \\ 0 & = & 0 \end{array}$$

Si para alguna terna salen resultados distintos, no será asociativa, pero si salen resultados iguales hay que continuar comprobando con todas las demás. Puede comprobarse que la operación es asociativa. La operación es conmutativa ya que la tabla es simétrica respecto a su diagonal. El elemento neutro es 0 pues en la fila y en la columna correspondientes a este elemento figuran los elementos de A en el mismo orden que se han escrito en las entradas de la tabla, lo que significa que, por ejemplo

$$3\bullet 0 = 3$$

$$0\bullet 2 = 2$$

El elemento 0 es simétrico de si mismo, 2 es simétrico de si mismo y 1 y 3 son simétricos. Como la operación es asociativa y todo elemento tiene simétrico, entonces todo elemento es regular.

Ejemplo III.1.10

En la estructura $(\mathbb{P}(E),\cap,\cup)$ se verifica, de acuerdo con resultados obtenidos en el Capítulo I

$\cup$, $\cap$ son asociativas y conmutativas

$\cup$ es distributiva respecto a $\cap$ y $\cap$ es distributiva respecto a $\cup$

$\emptyset$ es neutro para $\cup$, pues $(\forall X\in\mathbb{P}(E))\ (X\cup\emptyset = X)$

E es neutro para $\cap$, pues $(\forall X\in\mathbb{P}(E))\ (X\cap E = X)$

No hay inverso para $\cup$, ya que dado $X\in\mathbb{P}(E)$ no vacío, no existe ningún conjunto Y tal que

$$X\cup Y = \emptyset$$

y, de forma análoga, dado $X \in \mathcal{P}(E)$ no vacío, no tiene inverso respecto de $\cap$.

Ejercicios

III.1.- Sea $x \bullet y = \dfrac{x+y}{xy}$, razonar si es ley de composición interna en $\mathbf{R}$, $\mathbf{R^*}$, $\mathbf{R}^+$, $\mathbf{R}^-$.

III.2.- Las leyes $\bullet$ y Δ están definidas en el conjunto $\mathbf{R}^+$

$$x \bullet y = \frac{xy+1}{x+y} \qquad\qquad x \Delta y = \frac{x+y}{x+y+1}$$

estudiar si son asociativas y conmutativas.

III.3.- Consideremos dos leyes de composición interna

$$a \bullet b = 3a+2b \qquad a \Delta b = 4ab$$

ambas definidas sobre $\mathbf{Z}$. Ver si son asociativas, conmutativas y si alguna de ellas es distributiva respecto la otra.

III.4.- Averiguar las propiedades de las siguientes leyes de composición interna

a) $x \bullet y = 2^{x+y}$ sobre $\mathbf{N}$

b) $x \Delta y = \dfrac{x+y}{2}$ sobre el conjunto P de los números pares y sobre $\mathbf{Q}$

III.2.- GRUPOS

Según las propiedades que verifiquen sus leyes de composición, las estructuras algebraicas se designan de distintas formas y tienen características especiales. Vamos a estudiar las principales estructuras con leyes de composición internas.

Sea $\bullet$ una l.c.i. sobre un conjunto G; diremos que

$(G,\bullet)$ es un ***grupo*** si y sólo si
1) $\bullet$ es asociativa
2) existe elemento neutro: e
3) para todo $x \in G$ existe simétrico: x'

y si además $\bullet$ es conmutativa se denomina ***grupo abeliano***. Un grupo $(G,\bullet)$ es ***finito*** cuando el conjunto G es un conjunto finito, cuyo cardinal se denomina ***orden del grupo***.

Ejemplo III.2.1

Para las principales estructuras numéricas, tenemos

($\mathbf{N}$,+) no es grupo pues no existe opuesto para todo $x \in \mathbf{N}$.

($\mathbf{N}$,·) no es grupo pues no existe inverso para todo $x \in \mathbf{N}$.

($\mathbf{Z}$,+) es grupo abeliano, donde el neutro es 0 y el opuesto de $z \in \mathbf{Z}$ es $-z$.

($\mathbf{Z}/(n)$,+) es grupo abeliano.

($\mathbf{Z}$,−) no es grupo pues la l.c.i. no es asociativa.

($\mathbf{Z}$,·) no es grupo pues no existe inverso para todo $z \in \mathbf{Z}$.

($\mathbf{Q}$,+), ($\mathbf{R}$,+) y ($\mathbf{C}$,+) son grupos abelianos.

($\mathbf{Q}$,·) , ($\mathbf{R}$,·) y ($\mathbf{C}$,·) no son grupos pues 0 no tiene inverso.

($\mathbf{Q}^*$,·) ,($\mathbf{R}^*$,·) y ($\mathbf{C}^*$,·) son grupos abelianos.

Directamente de la definición de grupo y de las propiedades de las l.c.i., se derivan las proposiciones que se enuncian en la Tabla III.2.1.

TABLA III.2.1

Propiedades en un grupo $(G,\bullet)$

1) El elemento neutro es único

2) El simétrico x' de un elemento x es único

3) $(\forall x \in G)\ ((x')' = x)$

4) $(\forall x,y \in G)\ ((x \bullet y)' = y' \bullet x')$

5) Todo elemento de G es regular

6) La ecuación $x \bullet b = a$ tiene por única solución $x = a \bullet b'$

7) Si $x,a \in G$ son tales que $a \bullet x = a$ o $x \bullet a = a$, entonces x es el neutro de G

Demostraciones:

Teniendo en cuenta que • es asociativa, las propiedades 1), 2), 3) y 4), según vimos en la Sección III.1, se verifican en toda estructura con l.c.i. asociativa; asimismo de la asociatividad y la existencia de simétrico para todo elemento del grupo, se deduce 5). Para demostrar 6), teniendo en cuenta que cualquiera que sea b existe su simétrico b', tendremos

$$x \bullet b = a \ \Rightarrow\ (x \bullet b) \bullet b' = a \bullet b' \ \Rightarrow\ x \bullet (b \bullet b') = a \bullet b' \ \Rightarrow\ x \bullet e = a \bullet b' \ \Rightarrow\ x = a \bullet b'$$

con lo que hemos encontrado solución para la ecuación, que se obtiene simplemente "pasando" b de un miembro a otro, cambiándolo por su simétrico. Además esta solución es

única pues si

$$\left.\begin{array}{l} x_1 \text{ solución de } x\bullet b = a \;\Rightarrow\; x_1\bullet b = a \\ x_2 \text{ solución de } x\bullet b = a \;\Rightarrow\; x_2\bullet b = a \end{array}\right| \;\Rightarrow\; x_1\bullet b = x_2\bullet b \;\Rightarrow\; x_1 = x_2$$

Para demostrar 7) basta tener en cuenta que según la propiedad 6), la ecuación $x\bullet a = a$ tiene por única solución $x = a\bullet a' = e$; lo mismo para $a\bullet x = a$.

La anterior propiedad 6) tiene dos consecuencias interesantes; una ya ha sido mencionada y es la posibilidad de pasar términos de un miembro a otro de una igualdad, cambiándolos por su simétrico, y la otra es la posibilidad de definir en G una nueva l.c.i., del siguiente modo

$$\begin{array}{l} \underline{\bullet} : G\times G \longrightarrow G \\ \quad (a,b) \longrightarrow a \,\underline{\bullet}\, b = x \quad \text{siendo } x \text{ la solución de } \; x\bullet b = a \end{array}$$

con lo que todo par de $G\times G$ tiene imagen única, que es el elemento que compuesto por $\bullet$ con el segundo nos da el primero, y así $\underline{\bullet}$ es l.c.i. sobre G. Para hallarlo basta tener en cuenta la solución de la ecuación $x\bullet b = a$, con lo que

$$a \,\underline{\bullet}\, b = a\bullet b'$$

En los grupos aditivos esta ***operación inversa*** de + se denomina ***diferencia*** y se representa por −, de forma que la diferencia de dos elementos del grupo, llamados ***minuendo*** y ***sustraendo***, será el elemento que sumado con el sustraendo nos da el minuendo y es igual a la suma del minuendo con el opuesto del sustraendo. En grupos multiplicativos la operación inversa de · se denomina ***cociente***, representándose por /, siendo el cociente de dos elementos del grupo, llamados ***dividendo*** y ***divisor***, el elemento que multiplicado por el divisor nos da el dividendo y es igual al dividendo por el inverso del divisor.

Ejemplo III.2.2

Vamos a particularizar las propiedades anteriores al grupo $(\mathbf{Z},+)$. Tendremos

1) 0 es único
2) El opuesto $-x$ de un elemento x, es único
3) $(\forall x\in \mathbf{Z})\ (-(-x) = x)$
4) $(\forall x,y\in \mathbf{Z})\ (-(x+y) = (-x)+(-y))$
5) $(\forall a\in \mathbf{Z})\ (x+a = y+a \;\Rightarrow\; x = y)$
6) La ecuación $x+b = a$ tiene como única solución $x = a+(-b)$

La operación inversa, que esta propiedad permite definir, se denomina diferencia y es

$$\begin{array}{l} \mathbf{Z}\times\mathbf{Z} \longrightarrow \mathbf{Z} \\ (a,b) \longrightarrow a-b = x \quad \text{siendo } x \text{ la solución de } x+b = a \end{array}$$

es decir, la diferencia entre a y b es el número entero que sumado con b (sustraendo) nos da a (minuendo), que según lo anterior será $a-b = a+(-b)$.

Sea $(G,\bullet)$ un grupo y H un subconjunto no vacío de G; diremos que $(H,\bullet)$ es un ***subgrupo*** de $(G,\bullet)$, si y sólo si $(H,\bullet)$ es un grupo lo cual equivale a

$$(H,\bullet) \text{ es subgrupo de } (G,\bullet) \quad \text{si y sólo si} \quad \left| \begin{array}{l} 1)\ H \text{ es estable para } \bullet \\ 2)\ \bullet \text{ es asociativa en } H \\ 3)\ \text{el elemento neutro } e \in H \\ 4)\ (\forall x \in H)\ (x' \in H) \end{array} \right.$$

Si $(G,\bullet)$ es un grupo abeliano y se verifica que $\bullet$ es conmutativa en H, diremos que $(H,\bullet)$ es un subgrupo conmutativo. Cuando no haya lugar a confusión se dice, más brevemente, que H es subgrupo de G.

Como subgrupos triviales de $(G,\bullet)$ tenemos $\{e\}$ y el propio G, como subgrupo de sí mismo.

Ejemplo III.2.3

Sea $H = \{x \in \mathbf{Q}^* \mid x = (1+2a)/(1+2b) \text{ con } a,b \in \mathbf{Z}\}$ y consideremos como l.c.i. en H el producto de números racionales. Veamos si $(H,\cdot)$ es subgrupo de $(\mathbf{Q}^*,\cdot)$

1) H es estable para $\cdot$ pues para cualesquiera $x,y \in H$

$$\left| \begin{array}{l} x \in H \ \Rightarrow\ x = \dfrac{1+2a}{1+2b} \ \text{ con } a,b \in \mathbf{Z} \\ y \in H \ \Rightarrow\ y = \dfrac{1+2m}{1+2n} \ \text{ con } m,n \in \mathbf{Z} \end{array} \right. \Rightarrow\ xy = \frac{1+2(a+m+2am)}{1+2(b+n+2bn)} \in H$$

2) $\cdot$ es asociativa en H, dado que es asociativa en $\mathbf{Q}^*$, es decir, para todos los elementos de $\mathbf{Q}^*$, luego también para los elementos de H.

3) $\cdot$ es conmutativa en H por la misma razón anterior.

4) El número racional 1 es el elemento neutro para el producto de números racionales es 1, y

$$1 = \frac{1+2\cdot 0}{1+2\cdot 0} \in H$$

5) Para cualquier $x \in H$ tendremos

$$x \in H \ \Rightarrow\ x = \frac{1+2a}{1+2b} \ \Rightarrow\ x^{-1} = \frac{1+2b}{1+2a} \in H$$

Y así $(H,\cdot)$ es un subgrupo de $(\mathbf{Q}^*,\cdot)$.

De las condiciones generales para subgrupo, y de acuerdo con el razonamiento del ejemplo anterior, la asociatividad y la conmutatividad se cumplirán siempre sobre cualquier subconjunto H, pues si $\bullet$ es asociativa y conmutativa en G, lo es para todos los elementos de G, en particular para los de H. Además vamos a demostrar que las tres restantes pueden reducirse a una, es decir

$$\left.\begin{array}{l} 1)\ H \text{ es estable para } \bullet \\ 2)\ e\in H \\ 3)\ (x\in H)\ (x'\in H) \end{array}\right| \quad \text{equivalen} \quad (\forall x,y\in H)(x \underline{\bullet}\, y\in H)$$

donde $\underline{\bullet}$ es la operación inversa de $\bullet$ para la que, como hemos visto anteriormente

$$a \underline{\bullet}\, b = a\bullet b'$$

En efecto, al ser condición necesaria y suficiente tendremos que demostrar los dos teoremas que conlleva. Si se verifican 1), 2) y 3) para cualesquiera $x,y\in H$

$$\left.\begin{array}{c} x\in H \\ y\in H \ \Rightarrow\ y'\in H \end{array}\right| \ \Rightarrow\ x\bullet y'\in H \ \Rightarrow\ x \underline{\bullet}\, y\in H$$

Recíprocamente,

$2):\ x\in H \ \Rightarrow\ x \underline{\bullet}\, x\in H \ \Rightarrow\ x\bullet x'\in H \ \Rightarrow\ e\in H$

$3):\ e\in H \wedge x\in H \ \Rightarrow\ e \underline{\bullet}\, x\in H \ \Rightarrow\ e\bullet x'\in H \ \Rightarrow\ x'\in H$

$1):\ x\in H \wedge y\in H \ \Rightarrow\ x\in H \wedge y'\in H \ \Rightarrow\ x \underline{\bullet}\, y'\in H \ \Rightarrow\ x\bullet(y')'\in H \ \Rightarrow\ x\bullet y\in H$

En un grupo aditivo $(G,+)$ la condición de subgrupo será

$$(\forall x,y\in H)\ (x-y\in H)$$

y en un grupo multiplicativo $(G,\cdot)$ será

$$(\forall x,y\in G)\ (x/y\in H)$$

puesto que la diferencia y el cociente son las operaciones inversas de la suma y el producto, respectivamente.

La condición de subgrupo es muy usada cuando queremos demostrar que una estructura dada es grupo si está contenida en un grupo establecido anteriormente.

Ejemplo III.2.4

El ejemplo anterior III.2.3 puede plantearse así

$(H,\cdot)$ será grupo si $(H,\cdot)$ es subgrupo de $(\mathbf{Q}^*,\cdot)$, es decir, si

$$(\forall x,y\in H)(x/y\in H)$$

lo cual es cierto, ya que

$$\left.\begin{array}{l} x\in H \;\Rightarrow\; x=\dfrac{1+2a}{1+2b} \quad \text{con } a,b\in \mathbf{Z} \\ \\ y\in H \;\Rightarrow\; y=\dfrac{1+2m}{1+2n} \quad \text{con } m,n\in \mathbf{Z} \end{array}\right| \quad \Rightarrow \quad \frac{x}{y}=\frac{1+2(a+n+2an)}{1+2(b+m+2bm)}\in H$$

Ejercicios

III.5.- Porqué los números racionales positivos no forman grupo para la ley de composición

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

III.6.- Estudiar si el conjunto $A=\{a+b\sqrt{2} \mid a,b\in \mathbf{Z}\}$ tiene estructura de grupo abeliano con la operación suma.

III.7.- Demostrar que el conjunto $A=\{a^i \mid i\in \mathbf{Z} \wedge a>0\}$ con la operación producto tiene estructura de grupo abeliano.

III.8.- Dado el conjunto $A=\{a,b,c\}$ construir una tabla de operación de manera que con ella sea un grupo. Razonar la respuesta.

III.9.- Demostrar que un conjunto con una operación interna que verifique las propiedades asociativa, elemento neutro por la izquierda y elemento simétrico por la izquierda, tiene estructura de grupo.

III.10.- En el grupo $(\mathbf{Z},+)$ se define la relación

$$x\,R\,y \text{ si y sólo si } x-y \text{ es múltiplo de } 10$$

Demostrar que es de equivalencia y definir las clases. Demostrar que el conjunto cociente con la operación.

$$\langle x\rangle+\langle y\rangle=\langle x+y\rangle$$

es grupo. Hallar cuántos elementos tiene y todos sus subgrupos.

III.11.- Sea $A=\{\text{múltiplos de } n\}\subseteq \mathbf{Z}$. Demostrar que A es subgrupo.

III.3. ANILLOS Y CUERPOS

Estudiaremos a continuación estructuras con dos leyes de composición internas. Sea un conjunto A con dos leyes de composición interna, que designaremos por notación aditiva y

multiplicativa, $(A,+,\cdot)$. La estructura $(A,+,\cdot)$ es un ***anillo*** si verifica

1) $(A,+)$ grupo abeliano $\Leftrightarrow$ $\left|\begin{array}{l} + \text{ es asociativa} \\ + \text{ es conmutativa} \\ \text{existe elemento neutro para } + : 0 \\ \text{para todo } x\in A \text{ existe opuesto: } -x \end{array}\right.$

2) $\cdot$ es asociativa

3) $\cdot$ es distributiva respecto a $+$

Si además

4) $\cdot$ es conmutativo

se denomina ***anillo conmutativo*** y si

5) existe elemento neutro para la operación $\cdot$

se denomina anillo con elemento unidad o ***anillo unitario***. En este caso un elemento a del anillo se denomina inversible si tiene inverso, es decir, si existe $a^{-1}\in A$ tal que $aa^{-1} = a^{-1}a = e$.

Como hemos utilizado la notación aditiva para la primera operación, su elemento neutro lo designaremos por el símbolo 0, el opuesto de x por $-x$; análogamente como para la segunda l.c.i. hemos usado la notación multiplicativa, su elemento neutro, si lo tiene, lo denominaremos elemento unidad y se representa por 1.

Ejemplo III.3.1

Para los principales conjuntos numéricos, tenemos

$(\mathbf{N},+,\cdot)$ no es anillo pues $(\mathbf{N},+)$ no es grupo.

$(\mathbf{Z},+,\cdot)$, $(\mathbf{Q},+,\cdot)$, $(\mathbf{R},+,\cdot)$ y $(\mathbf{C},+,\cdot)$ son anillos conmutativos con elemento unidad.

$(\mathbf{R},\cdot,+)$ no es anillo pues $(\mathbf{R},\cdot)$ no es grupo.

$(\mathbf{R}^*,\cdot,+)$ no es anillo pues $+$ no es distributiva con respecto a $\cdot$

Ejemplo III.3.2

Sobre $\mathbf{Z}$ definimos las l.c.i.

$$a\S b = a+b-6 \qquad\qquad a\Delta b = ab-6(a+b)+42$$

Se verifica que $(\mathbf{Z},\S)$ es grupo abeliano

a) § es asociativa

$$\begin{array}{c} (a\S b)\S c \;=\; a\S(b\S c) \\ \uparrow \\ (a+b-6)\S c \;\;\big|\;\; a\S(b+c-6) \\ \big| \\ (a+b-6)+c-6 = a+(b+c-6)-6 \end{array}$$

que son iguales por las propiedades asociativa y conmutativa de + en **Z**.

b) § es conmutativa

$$\begin{array}{c} a\S b \;=\; b\S a \\ \uparrow \\ a+b-6 = b+a-6 \end{array}$$

iguales por la propiedad conmutativa de + en **Z**.

c) elemento neutro

$$a\S e = a \;\Rightarrow\; a+e-6 = a \;\Rightarrow\; e = 6$$

d) simétrico

$$a\S a' = 6 \;\Rightarrow\; a+a'-6 = 6 \;\Rightarrow\; a' = 12-a$$

luego todo elemento de **Z** tiene simétrico. Respecto de la otra operación tenemos

e) Δ es asociativa

$$(a\Delta b)\Delta c = (ab-6(a+b)+42)\Delta c = (ab-6(a+b)+42)c-6((ab-6(a+b)+42)+c)+42$$
$$a\Delta(b\Delta c) = a\Delta(bc-6(b+c)+42) = a(bc-6(b+c)+42)-6(a+(bc-6(b+c)+42))+42$$

que son iguales por asociatividad, conmutatividad y distributividad de + y $\cdot$ en **Z**.

f) Δ distributivo respecto a §

$$(a\S b)\Delta c = (a+b-6)\Delta c = (a+b-6)c-6((a+b-6)+c)+42$$
$$(a\Delta c)\S(b\Delta c) = (ac-6(a+c)+42)\S(bc-6(b+c)+42) =$$
$$= (ac-6(a+c)+42)+(bc-6(b+c)+42)-6$$

que son iguales por las mismas razones anteriores.

g) Δ es conmutativa

$$\begin{array}{c} a\Delta b \;=\; b\Delta a \\ \uparrow \\ ab-6(a+b)+42 = ba-6(b+a)+42 \end{array}$$

h) elemento unidad

$$a\Delta u = a \;\Rightarrow\; au-6(a+u)+42 = a \;\Rightarrow\; u\,(-6+a) = -42+7a = 7(-6+a)$$

es decir, 7 es el elemento unidad. Se trata pues de un anillo conmutativo unitario.

Dos elementos x e y de un anillo $(A,+,\cdot)$ diremos que son divisores de cero si siendo distintos de cero, su producto da 0, es decir

$$x \text{ e } y \ \textbf{\textit{divisores de cero}} \ \text{ si y sólo si } \quad x \neq 0 \ \wedge \ y \neq 0 \ \wedge \ xy = 0$$

En A puede que existan divisores de cero y puede que no; en este último caso diremos que $(A,+,\cdot)$ es ***anillo de integridad***.

Ejemplo III.3.3

$(\mathbf{Z},+,\cdot)$ $(\mathbf{Q},+,\cdot)$ $(\mathbf{R},+,\cdot)$ y $(\mathbf{C},+,\cdot)$ son todas ellas anillos de integridad. El anillo del Ejemplo III.3.2 es anillo de integridad pues, teniendo en cuenta que el neutro de la primera l.c.i. es 6, si

$$x\Delta y = 6 \ \Rightarrow \ \ xy-6(x+y)+42 = 6 \ \ \Rightarrow \ \ x(y-6) = -36+6y = 6(y-6) \ \ \Rightarrow \ \ x = 6 \vee y = 6$$

por lo que no existen divisores de cero.

Sea un anillo $(A,+,\cdot)$ y B un subconjunto no vacío de A; diremos que $(B,+,\cdot)$ es ***subanillo*** de $(A,+,\cdot)$ o, más brevemente, B subanillo de A, si $(B,+,\cdot)$ es un anillo; esto es equivalente a

$$(\forall x,y\in B)\ (x-y\in B \ \wedge \ xy\in B)$$

ya que entonces $(B,+)$ es subgrupo de $(A,+)$ y B es estable para $\cdot$, con lo cual se verifican las propiedades asociativa y distributiva de esta l.c.i. en B, ya que se verifican en A. Como subanillos triviales tenemos $\{0\}$ y el propio A.

Ejemplo III.3.4

$(\mathbf{R},+,\cdot)$ es un anillo conmutativo con elemento unidad, subanillo de $(\mathbf{C},+,\cdot)$ pues la diferencia y el producto son l.c.i. en $\mathbf{R}$. El anillo $(\mathbf{R},+,\cdot)$ contiene como subanillo a $(\mathbf{Q},+,\cdot)$ del cual es subanillo $(\mathbf{Z},+,\cdot)$

Sea un anillo $(A,+,\cdot)$ e I un subconjunto no vacío de A; diremos que $(I,+,\cdot)$ es un ***ideal*** de $(A,+,\cdot)$ si se verifican las condiciones

1) $(\forall x,y\in I)\ (x-y\in I)$
2) $(\forall x\in I)\ (\forall a\in A)\ (ax\in I \ \wedge \ xa\in I)$

es decir un subgrupo aditivo que verifica la condición 2), más restrictiva que la condición análoga de subanillo, por lo que todo ideal es un subanillo.

Otra estructura importante con dos l.c.i. es la estructura de cuerpo definida como sigue:

$$(K,+,\cdot) \ \textbf{\textit{cuerpo}} \text{ si y sólo si } \left| \begin{array}{l} 1)\ (K,+,\cdot) \text{ anillo unitario} \\ 2) \text{ Para todo } x\in K^* \text{ existe inverso } x^{-1} \end{array} \right.$$

siendo K^* el conjunto K excluído el 0, neutro de la primera l.c.i. Si $\cdot$ es conmutativa diremos que es un cuerpo conmutativo; en adelante cuando hablemos de un cuerpo nos referiremos a un cuerpo conmutativo, salvo que se diga lo contrario.

Ejemplo III.3.5

Son cuerpos los anillos $(\mathbf{Q},+,\cdot)$ $(\mathbf{R},+,\cdot)$ y $(\mathbf{C},+,\cdot)$ y no lo es $(\mathbf{Z},+,\cdot)$.

Si $(K,+,\cdot)$ es un cuerpo se verifican las propiedades que resumimos en la Tabla III.3.2

TABLA III.3.2

Propiedades de los cuerpos

Si $(K,+,\cdot)$ es un cuerpo

1) $(K,+,\cdot)$ es un anillo de integridad

2) $(K^*,\cdot)$ es un grupo abeliano

Demostraciones:

1) $(K,+,\cdot)$ es un anillo de integridad por no tener divisores de cero, ya que si fueran $a\cdot b = 0$ y $a \neq 0$, existe a^{-1} con lo que

$$a^{-1}(a\,b) = a^{-1}\cdot 0 \;\Rightarrow\; (a^{-1}a)b = 0 \;\Rightarrow\; 1\cdot b = 0 \;\Rightarrow\; b = 0$$

2) $(K^*,\cdot)$ es un grupo abeliano ya que por definición de cuerpo $\cdot$ es asociativo, es conmutativo, existe elemento unidad y todo elemento $x \in K^*$ tiene inverso x^{-1}.

El verificarse estas propiedades hace que, por un lado, la ecuación $a\cdot x = b$ tenga por soluciones

$$\text{si } a = 0: \quad 0\cdot x = b \;\Big|\; \begin{array}{l} \text{si } b \neq 0 \text{ no tiene solución} \\ \text{si } b = 0 \text{ todo } x \in A \text{ es solución} \end{array}$$

$$\text{si } a \neq 0: \text{ la ecuación tiene por única solución } x = ba^{-1}$$

y por otro lado que podemos definir sobre K^* la l.c.i. inversa del producto, el cociente

$$/ : K^*\times K^* \longrightarrow K^*$$
$$(b,a) \longrightarrow b/a = \text{única solución de la ecuación } ax = b$$

es decir, el cociente entre b, dividendo, y a, divisor, es el elemento de K^* que multiplicado por a es igual a b, y según el resultado anterior, será

$$b/a = ba^{-1}$$

Esta operación puede extenderse al caso de que el dividendo sea cero, ya que

$$0/a = 0 \cdot a^{-1} = 0$$

Dado un cuerpo $(K,+,\cdot)$ y un subconjunto no vacío $J \subseteq K$; diremos que $(J,+,\cdot)$ es un ***subcuerpo*** de $(K,+,\cdot)$ o, más brevemente, J subcuerpo de K, si $(J,+,\cdot)$ es cuerpo, lo que, según los resultados anteriores, equivale a

1) $(\forall x,y \in J)\ (x-y \in J)$
2) $(\forall x \in J)\ (\forall y \in J^*)\ (xy^{-1} \in J)$

Por ejemplo, **Q** es subcuerpo de **R** pues la diferencia y el cociente de dos números racionales es un número racional. De forma análoga **R** es subcuerpo de **C**.

Ejercicios

III.12.- Estudiar las siguientes estructuras algebraicas:

1) $(\mathbf{R}^+,\otimes)$ con $x \otimes y = \dfrac{x+y}{xy+1}$

2) $(\mathbf{R}^*,\oplus,\otimes)$ con $x \oplus y = 4xy$ $\quad x \otimes y = 3x+2y$

y resolver, si es posible, las ecuaciones

$$4 \otimes (x \oplus 3) = 2 \qquad \text{y} \qquad 5 \oplus (x^2 \otimes 2) = 1$$

III.13.- Sobre el conjunto $A = \{x \in \mathbf{R} \mid x > 0\}$ se definen las siguientes l.c.i.:

a) $a \bullet b = x$ tal que $1/x = 1/a + 1/b$
b) $a \Delta b = \max(a,b)$
c) $a \circ b = \min(a,b)$

Estudiar las estructuras $(A,\bullet)$, (A,Δ), $(A,\circ)$, $(A,\Delta,\circ)$, $(A,\circ,\Delta)$

III.14.- En $\mathbf{Z} \times \mathbf{Z}$ se definen las operaciones

$$(a,b)+(c,d) = (a+c,b+d)$$

$$(a,b) \cdot (c,d) = (ac-5bd,ad+bc)$$

a) Estudiar la estructura $(\mathbf{Z} \times \mathbf{Z},+,\cdot)$

b) Calcular los elementos inversibles.

c) ¿Tiene divisores de 0?.

d) El conjunto $A = \{(a,b) \in \mathbf{Z}\times\mathbf{Z} \mid a,b$ múltiplos de $2\}$. ¿Es un ideal?.

III.15.- Sea el conjunto $E \subset \mathbf{R}$ de los números reales de la forma $m+n\sqrt{3}$ con $m,n \in \mathbf{Z}$.

1) Demostrar que E es un subanillo de $(\mathbf{R},+,\cdot)$

2) Se define en E la relación

$$(m+n\sqrt{3})\ R\ (m'+n'\sqrt{3}) \iff m'-m = \dot{2} \text{ y } n'-n = \dot{2}$$

Probar que es de equivalencia y hallar el conjunto cociente $E/\mathbf{R}$.

3) Definir en $E/\mathbf{R}$ las tablas de sumar y multiplicar.

4) Averiguar si $E/\mathbf{R}$ es un cuerpo.

5) Demostrar que $E/\mathbf{R}$ contiene un ideal formado por dos elementos.

III.16.- Los conjuntos

$$\{a+b\sqrt{16} \mid a,b\in \mathbf{Q}\} \qquad \{a+b\sqrt{2} \mid a,b \in \mathbf{Q}\}$$

tienen estructura de anillo respecto a la suma y el producto ordinario de los números reales. ¿Cuál de ellos tiene estructura de cuerpo?. En caso de que algún conjunto no posea estructura de cuerpo, hallar un elemento que no tenga inverso.

III.17.- Sea $f : \mathbf{R} \longrightarrow \mathbf{R}^2$ tal que

$$(\forall a,b\in \mathbf{R})\ (f(a+b) = f(a)+f(b) \ \wedge\ f(ab) = af(a)+bf(b))$$

a) Probar que $f(1) = (0,0)$.

b) Probar que $F = \{x\in \mathbf{R} \mid f(x) = (0,0)\}$ es un subcuerpo de $\mathbf{R}$.

III.4.- POLINOMIOS SOBRE UN CUERPO

En la matemática elemental polinomio es una expresión del tipo

$$a_0+a_1x+a_2x^2+\ldots+a_nx^n$$

siendo $a_0,a_1,\ldots, a_n$ números reales y x es una indeterminada con la que se establecen sumas, productos y diferencias con los elementos $a_0, a_1,\ldots, a_n$ y consigo misma, sujetas a las reglas de cálculo, representándose por x^n el producto de x consigo misma n veces. El significado de x y, por tanto, de una expresión tal como la anterior no se establece de modo nada claro, aunque a veces x sea considerada como un elemento indeterminado de $\mathbf{R}$. Vamos a ver en esta Sección de un modo preciso que es un polinomio sobre un cuerpo.

Sea $(K,+,\cdot)$ un cuerpo. Consideremos sucesiones en K, es decir, aplicaciones

$$\begin{array}{ccc} \mathbf{N} & \longrightarrow & K \\ 0 & \longrightarrow & a_0 \\ 1 & \longrightarrow & a_1 \\ & \cdots\cdots & \\ n & \longrightarrow & a_n \\ & \cdots\cdots & \end{array}$$

que al distinguirse entre sí por las imágenes de los elementos de $\mathbf{N}$, se representan por

$$(a_0,a_1,\ldots,a_n,\ldots)$$

denominándose a a_0, $a_1,\ldots,a_n$ primero, segundo,..., n-ésimo término de la sucesión. Llamaremos ***sucesión casi-nula***, aquella cuyos términos son nulos a partir de uno en adelante, es decir, aquella sucesión $(a_0,a_1,\ldots,a_n,\ldots)$ para la cual existe un $n\in\mathbf{N}$ tal que

$$(\forall i\in\mathbf{N})\ (i > n \ \Rightarrow\ a_i = 0)$$

donde, como es habitual, 0 representa al elemento neutro de la primera l.c.i. en $(K,+,\cdot)$. Escribiremos una sucesión casi-nula mediante la notación

$$(a_0,a_1,\ldots,a_n,0,\ldots)$$

donde $a_n \neq 0$ y algún a_i puede ser nulo. Dado un cuerpo $(K,+,\cdot)$ llamaremos ***polinomio sobre K*** a una sucesión casi nula de elementos de K

$$P = (a_0,a_1,\ldots,a_n,0,\ldots)$$

Los elementos $a_0,a_1,,a_n$ se denominan ***coeficientes***, a_0 es el ***término independiente***, a_n, que es el elemento de K distinto de cero con mayor subíndice, se denomina ***coeficiente dominante*** y a su subíndice n, ***grado*** del polinomio

$$n = \mathrm{gr}(P)$$

Si $a_n = 1$ el polinomio se denomina ***polinomio mónico***. Vamos a convenir en que la sucesión nula es una sucesión casi-nula, es decir, que existe el polinomio

$$(0,0,\ldots,0,\ldots)$$

que llamaremos ***polinomio nulo***, al que atribuimos por grado $-\infty$, siendo

$$(\forall n\in\mathbf{N})\ (n > -\infty\ \wedge\ n+(-\infty) = -\infty)$$

En el conjunto de polinomios sobre K vamos a definir dos l.c.i., que denominaremos suma y producto, inducidas por las operaciones de K. Dados dos polinomios

$$P = (a_0,a_1,\ldots,a_n,0,\ldots) \qquad Q = (b_0,b_1,\ldots,b_m,0,\ldots)$$

definimos la ***suma*** de ambos, que escribiremos $P+Q$, como el polinomio

$$P+Q = (a_0+b_0, a_1+b_1, \ldots, \alpha, 0, \ldots)$$

cuyos coeficientes son la suma de coeficientes homólogos de P y Q por lo que el coeficiente dominante será

$$\alpha = \begin{cases} a_n & \text{si} \quad n > m \\ a_n+b_m & \text{si} \quad n = m \ \wedge \ a_n+b_m \neq 0 \\ b_m & \text{si} \quad n < m \end{cases}$$

siendo la relación entre los grados

$$\text{gr}(P+Q) \leq \max(\text{gr}(P), \text{gr}(Q))$$

La estructura de grupo abeliano que tiene K respecto a la suma hace que el conjunto de polinomios con la suma, así definida constituya un grupo abeliano, ya que

1) Asociativa

$$((a_0,a_1,\ldots,a_n,0,\ldots)+(b_0,b_1,\ldots,b_m,0,\ldots))+(c_0,c_1,\ldots,c_r,0,\ldots) =$$
$$= (a_0+b_0,a_1+b_1,\ldots,0,\ldots)+(c_0,c_1,\ldots,0,\ldots) = ((a_0+b_0)+c_0,(a_1+b_1)+c_1,\ldots,0,\ldots)$$

$$(a_0,a_1,\ldots,a_n,0,\ldots)+((b_0,b_1,\ldots,b_m,0,\ldots)+(c_0,c_1,\ldots,c_r,0,\ldots)) =$$
$$= (a_0,a_1,\ldots,0,\ldots)+(b_0+c_0,b_1+c_1,\ldots,0,\ldots) = (a_0+(b_0+c_0),a_1+(b_1+c_1),\ldots,0,\ldots)$$

siendo iguales ambos resultados, por la asociatividad de la suma en K.

2) Conmutativa

$$(a_0,a_1,\ldots,a_n,0,\ldots)+(b_0,b_1,\ldots,b_m,0,\ldots) = (a_0+b_0,a_1+b_1,\ldots,0,\ldots)$$

$$(b_0,b_1,\ldots,b_m,0,\ldots)+(a_0,a_1,\ldots,a_n,0,\ldots) = (b_0+a_0,b_1+a_1,\ldots,0,\ldots)$$

que son iguales, por conmutatividad de la suma en K.

3) Neutro es el polinomio nulo (0,0,...,0,...), ya que

$$(a_0,a_1,\ldots,a_n,0,\ldots)+(0,0,\ldots,0,\ldots) = (a_0+0,a_1+0,\ldots,a_n+0,0,\ldots) = (a_0,a_1,\ldots,a_n,0,\ldots)$$

4) Opuesto del polinomio $(a_0,a_1,\ldots,a_n,0,\ldots)$ es el polinomio $(-a_0,-a_1,\ldots,-a_n,0,\ldots)$, pues

$$(a_0,a_1,\ldots,a_n,0,\ldots)+(-a_0,-a_1,\ldots,-a_n,0,\ldots) = (a_0-a_0,a_1-a_1,\ldots,a_n-a_n,\ldots) = (0,0,\ldots,0,\ldots)$$

Dados dos polinomios

$$P = (a_0,a_1,\ldots,a_n,0,\ldots) \qquad Q = (b_0,b_1,\ldots,b_m,0,\ldots)$$

definimos el ***producto*** de ambos, que escribiremos $P\cdot Q$, o más brevemente PQ, como el polinomio

$$PQ = (c_0,c_1,...,c_{n+m},0,...)$$

tal que $c_0 = a_0b_0$

$c_1 = a_0b_1+a_1b_0$

$c_2 = a_0b_2+a_1b_1+a_2b_0$

. . . . . .

$$c_i = a_0b_i+a_1b_{i-1}+...+a_{i-1}b_1+a_ib_0 = \sum_{r+s=i} a_r\, b_s$$

siendo el coeficiente dominante del producto

$$c_{m+n} = a_0b_{m+n}+a_1b_{m+n-1}+...+a_{n-1}b_{m+1}+a_nb_m+a_{n+1}b_{m-1}+...+a_{m+n-1}b_1+a_{m+n}b_0=$$
$$= a_0\cdot 0+a_1\cdot 0+...+a_{n-1}\cdot 0+a_nb_m+0\cdot b_{m-1}+...+0\cdot b_1+0\cdot b_0 = a_nb_m$$

ya que

$$c_{m+n+1} = a_0b_{m+n+1}+a_1b_{m+n}+...+a_{n-1}b_{m+2}+a_nb_{m+1}+a_{n+1}b_m+...+a_{m+n}b_1+a_{m+n+1}b_0 =$$
$$= a_0\cdot 0+a_1\cdot 0+...+a_{n-1}\cdot 0+a_n\cdot 0+0\cdot b_m+...+0\cdot b_1+0\cdot b_0 = 0$$

siendo también nulos todos los coeficientes posteriores. La relación entre los grados es

$$\mathrm{gr}(PQ) = \mathrm{gr}(P)+\mathrm{gr}(Q)$$

Los polinomios para la suma anterior y el producto así definido tienen estructura de anillo conmutativo con elemento unidad y de integridad. En efecto

1) El producto es asociativo ya que dados tres polinomios

$$P = (a_0,a_1,...,a_n,0,...) \quad Q = (b_0,b_1,...,b_m,0,...) \quad R = (d_0,d_1,...,d_l,0,\ldots)$$

tenemos

$$P\cdot Q = (c_0,c_1,...,c_{m+n},0,...) \qquad \text{con } c_i = \sum_{r+s=i} a_rb_s$$

$$Q\cdot R = (c'_0,c'_1,\ldots,c'_{m+l},0,...) \qquad \text{con } c'_j = \sum_{s+u=j} b_sd_u$$

siendo, por tanto

$$P\cdot(Q\cdot R) = (p_0,p_1,...,p_{n+(m+l)},0,\ldots)$$

con $p_k = \sum_{r+j=k} a_rc'_j = \sum_{r+j=k} a_r\,(\sum_{s+u=j} b_sd_u) = \sum_{r+s+u=k} a_r(b_sd_u)$; análogamente

$$(P\cdot Q)\cdot R = (p'_0,p'_1,...,p'_{(m+n)+l},0,\ldots)$$

con $p'_k = \sum_{i+u=k} c_id_u = \sum_{i+u=k} (\sum_{r+s=i} a_rb_s)\, d_u = \sum_{r+s+u=k} a_r(b_sd_u)$

y ambos resultados son iguales por ser K un cuerpo.

2) El producto es claramente conmutativo.

3) El producto es distributivo respecto a la suma, ya que para

$$P = (a_0,a_1,\ldots,a_n,0,\ldots) \qquad Q = (b_0,b_1,\ldots,b_m,0,\ldots) \qquad R = (d_0,d_1,\ldots,d_l,0,\ldots)$$

tendremos

$$P\cdot(Q+R) = (c_0,c_1,\ldots,c_{m+n},0,\ldots) \qquad \text{con } c_i = \sum_{r+s=i} a_r(b_s+d_s)$$

$$P\cdot Q = (c'_0,c'_1,\ldots,c'_{m+n},0,\ldots) \qquad \text{con } c'_i = \sum_{r+s=i} a_r b_s$$

$$P\cdot R = (c''_0,c''_1,\ldots,c''_{n+l},0,\ldots) \qquad \text{con } c''_i = \sum_{r+s=i} a_r d_s$$

y como

$$c_i = \sum_{r+s=i} a_r(b_s+d_s) = \sum_{r+s=i} (a_r b_s+a_r d_s) = \sum_{r+s=i} a_r b_s + \sum_{r+s=i} a_r d_s$$

es $P(Q+R) = PQ+PR$

4) El elemento unidad es el polinomio (1,0,...), ya que

$$(a_0,a_1,\ldots,a_n,0,\ldots)\cdot(1,0,\ldots,0,\ldots) = (a_0\cdot 1,a_1\cdot 1,\ldots,a_n\cdot 1,0,\ldots) = (a_0,a_1,\ldots,a_n,0,\ldots)$$

5) No existen divisores de cero, puesto que si

$$P = (a_0,a_1,\ldots,a_n,0,\ldots) \neq 0 \quad \text{equivale a } \operatorname{gr}(P) = n \geq 0$$
$$Q = (b_0,b_1,\ldots,b_m,0,\ldots) \neq 0 \quad \text{equivale a } \operatorname{gr}(Q) = m \geq 0$$

por lo que

$$\operatorname{gr}(PQ) = n+m \geq 0 \quad \Rightarrow \quad PQ \neq 0$$

Los elementos del conjunto de los polinomios de grado menor que 1

$$P_0(K) = \{(a_0,0,\ldots) \mid a_0 \in K\}$$

considerar como algebraicamente idénticos los elementos de K y a los polinomios de grado 0.

Veamos cuáles son los polinomios inversibles; si P tiene por inverso a Q, será

$$P\cdot Q = (1,0,\ldots) \quad \Rightarrow \quad \operatorname{gr}(P\cdot Q) = \operatorname{gr}(P)+\operatorname{gr}(Q) = 0 \quad \Rightarrow \quad \operatorname{gr}(P) = \operatorname{gr}(Q) = 0$$

y los elementos inversibles son los polinomios de grado 0, es decir, los elementos de K^*.

Existe un polinomio especial, que indicaremos por X

$$X = (0,1,0,\ldots)$$

que, como puede comprobarse realizando el producto, verifica

$$X^2 = (0,1,0,...)\cdot(0,1,0,...) = (0,0,1,0,...)$$

y por inducción se obtiene

$$X^n = (0,0,...,0,1,0,...)\cdot(0,1,0,...) = (0,0,...,0,0,1,...)$$

lo que, junto con el isomorfismo anterior, permite escribir un polinomio dado en la forma

$$P = (a_0,a_1,...,a_n,0,...) = (a_0,0,...)+(0,a_1,0,...)+...+(0,...,0,a_n,0,...) =$$
$$= a_0\cdot(1,0,...)+a_1\cdot(0,1,0,..)+...+a_n\cdot(0,...,0,1,0,...) = a_0+a_1X+a_2X^2+...+a_nX^n$$

que puede escribirse también en orden descendente

$$P = a_nX^n+...+a_2X^2+a_1X+a_0$$

De aquí en adelante utilizaremos ambas formas de escribir un polinomio, como sucesión casi nula o en función del polinomio X. El ***anillo de los polinomios sobre un cuerpo*** K se denota por $K[X]$. Según todas las propiedades anteriores, los polinomios sobre K se pueden sumar, restar y multiplicar según los procedimientos habituales de la matemática elemental.

Ejemplo III.4.1

Dados los polinomios sobre **R**

$$P = (3,0,-1,4,0,...) = 4X^3-X^2+3$$
$$Q = (2,1,1,0,...) = X^2+X+2$$

la suma y el producto se obtienen disponiendo ambos polinomios de modo análogo a como se disponen los números naturales para sumar y multiplicar (recordemos que cualquier número natural tiene una descomposición en potencias de 10, que es análoga a la del polinomio en X)

Suma:

$$\begin{array}{r} 4X^3-X^2\quad +3 \\ X^2+X+2 \\ \hline P(X)+Q(X) = 4X^3\quad +X+5 \end{array}$$

Producto:

$$\begin{array}{r} 4X^3-X^2\quad +3 \\ X^2+X+2 \\ \hline 8X^3-2X^2\quad +6 \\ 4X^4-X^3\quad +3X \\ 4X^5-X^4\quad +3X^2 \\ \hline P(X)\cdot Q(X) = \quad 4X^5+3X^4+7X^3+X^2+3X+6 \end{array}$$

III.5.- CLASES DE RESTOS

Sea un entero n. Sobre el conjunto $\mathbf{Z}$ de los números enteros la relación binaria

$$x\ R\ y \quad \text{si y sólo si} \quad x-y = (n)$$

donde por (n) indicamos un múltiplo de n, es una relación de equivalencia por ser

$(\mathfrak{R})$: pues para todo $x\in\mathbf{Z}$ es $x\ R\ x$ ya que $x-x = 0 = (n)$

$(\mathfrak{S})$: $x\ R\ y \Rightarrow x-y = (n) \Rightarrow y-x = (n) \Rightarrow y\ R\ x$

$(\mathfrak{T})$: $(x\ R\ y \wedge y\ R\ z) \Rightarrow (x-y = (n) \wedge y-z = (n)) \Rightarrow x-z = (n) \Rightarrow x\ R\ z$

Una clase de equivalencia está definida por

$$\langle a\rangle = \{x\in\mathbf{Z} \mid x-a = (n)\} = (n)+a$$

por lo que $\langle 0\rangle = \{x\in\mathbf{Z} \mid x-0 = (n)\} = (n)$ $\quad \langle 1\rangle = \{x\in\mathbf{Z} \mid x-1 = (n)\} = (n)+1$

$\langle 2\rangle = \{x\in\mathbf{Z} \mid x-2 = (n)\} = (n)+2$ $\quad \langle 3\rangle = \{x\in\mathbf{Z} \mid x-3 = (n)\} = (n)+3$

. . . . . .

$\langle n-1\rangle = \{x\in\mathbf{Z} \mid x-(n-1) = (n)\} = (n)+(n-1)$

no existiendo más clases de equivalencia pues todo número entero al dividirlo por n da un resto menor que n, es decir, todo número entero es igual a un múltiplo de n más 0 o 1 o 2 o 3 o...o $n-1$. Por esta razón dos enteros que pertenezcan a la misma clase, dan el mismo resto al dividirlos por n , diciéndose que son ***congruentes módulo*** n, y las clases de equivalencia se denominan ***clases de restos módulo*** n. El conjunto cociente es por tanto

$$\mathbf{Z}/(n) = \{\langle 0\rangle,\langle 1\rangle,\langle 2\rangle,\langle 3\rangle,...,\langle n-1\rangle\}$$

Ejemplo III.5.1

Sobre el conjunto $\mathbf{Z}$ de los números enteros la relación binaria

$$x\ R\ y \quad \text{si y sólo si} \quad x-y = (5)$$

donde por (5) indicamos un múltiplo de 5, es una relación de equivalencia por ser

$(\mathfrak{R})$: pues para todo $x\in\mathbf{Z}$ es $x\ R\ x$ ya que $x-x = 0 = (5)$

$(\mathfrak{S})$: $x\ R\ y \Rightarrow x-y = (5) \Rightarrow y-x = (5) \Rightarrow y\ R\ x$

$(\mathfrak{T})$: $(x\ R\ y \wedge y\ R\ z) \Rightarrow (x-y = (5) \wedge y-z = (5)) \Rightarrow x-z = (5) \Rightarrow x\ R\ z$

Una clase de equivalencia está definida por

$$\langle a\rangle = \{x\in \mathbf{Z} \mid x-a = (5)\} = (5)+a$$

por lo que $\langle 0\rangle = \{x\in \mathbf{Z} \mid x-0 = (5)\} = (5)$ $\quad \langle 1\rangle = \{x\in \mathbf{Z} \mid x-1 = (5)\} = (5)+1$

$\langle 2\rangle = \{x\in \mathbf{Z} \mid x-2 = (5)\} = (5)+2$ $\quad \langle 3\rangle = \{x\in \mathbf{Z} \mid x-3 = (5)\} = (5)+3$

$\langle 4\rangle = \{x\in \mathbf{Z} \mid x-4 = (5)\} = (5)+4$

no existiendo más clases de equivalencia pues todo número entero al dividirlo por 5 da un resto igual a 0, 1, 2, 3, 4 o 5. El conjunto cociente es por tanto

$$\mathbf{Z}/(5) = \{\langle 0\rangle,\langle 1\rangle ,\langle 2\rangle ,\langle 3\rangle ,\langle 4\rangle\}$$

La suma y producto en $\mathbf{Z}$ pueden extenderse al conjunto cociente $\mathbf{Z}/(n)$ mediante

$$\langle x\rangle+\langle y\rangle = \langle x+y\rangle$$

$$\langle x\rangle\langle y\rangle = \langle xy\rangle$$

Vamos a ver que están bien definidas, es decir, que las clases resultantes, $\langle x+y\rangle$ y $\langle xy\rangle$, no dependen de los representantes elegidos para cada una de ellas:

$$\left.\begin{array}{l} x,x'\in\langle x\rangle \;\Leftrightarrow\; x'-x = (n) \\ y,y'\in\langle y\rangle \;\Leftrightarrow\; y'-y = (n) \end{array}\right| \Rightarrow \begin{array}{l} (x'+y')-(x+y) = (x'-x)+(y'-y) = (n) \;\Leftrightarrow\; x'+y',x+y\in\langle x\rangle \\ (x'y')-(xy) = y'(x'-x)+x'(y'-y) = (n) \;\Leftrightarrow\; (x'y'),(xy)\in\langle x\rangle \end{array}$$

Se demuestra fácilmente que $(\mathbf{Z}/(n),+,\cdot)$ tiene la misma estructura que $(\mathbf{Z}/(n),+,\cdot)$, es decir, es un anillo conmutativo con elemento unidad. En efecto, la asociatividad, conmutatividad y distributividad se deducen directamente de las mismas propiedades para la suma y producto en $\mathbf{Z}$. Por ejemplo,

$$\langle x\rangle(\langle y\rangle+\langle z\rangle) = \langle x\rangle\langle y+z\rangle = \langle x(y+z)\rangle = \langle xy+xz\rangle = \langle xy\rangle+\langle xz\rangle = \langle x\rangle\langle y\rangle+\langle x\rangle\langle z\rangle$$

Análogamente se prueba que el elemento neutro en la suma es la clase $\langle 0\rangle$ y elemento neutro en el producto es la clase $\langle 1\rangle$.

Este anillo $\mathbf{Z}/(n)$ es un anillo de integridad si y sólo si n es primo. En efecto, si n no es primo existe una descomposición en factores

$$n = ab \;\Rightarrow\; \langle 0\rangle = \langle n\rangle = \langle ab\rangle = \langle a\rangle\langle b\rangle$$

por lo que en $\mathbf{Z}/(n)$ existen divisores de cero; recíprocamente, si n es primo es anillo de integridad ya que

$$\langle a\rangle\langle b\rangle = \langle 0\rangle \;\Rightarrow\; \langle ab\rangle = \langle 0\rangle \;\Rightarrow\; ab = kn$$

y como n es primo, entonces es divisor de a o b, es decir, $\langle a\rangle = \langle 0\rangle$ o $\langle b\rangle = \langle 0\rangle$. Además, como $\mathbf{Z}/(n)$ es finito, entonces $(\mathbf{Z}/(n),+,\cdot)$ es un cuerpo pues para cualquier clase $\langle x\rangle\in \mathbf{Z}/(n)^*$ existe inverso: en efecto, al ser $\mathbf{Z}/(n)$ finito será $\mathbf{Z}/(n) = \{\langle x_1\rangle,...,\langle x_n\rangle\}$ y los productos

$$\langle x\rangle\langle x_1\rangle,..., \langle x\rangle\langle x_n\rangle$$

serán todos distintos, por ser K anillo de integridad, por lo que alguno será

$$\langle x\rangle\langle x_i\rangle = \langle 1\rangle \quad \Rightarrow \quad \langle x\rangle^{-1} = \langle x_i\rangle$$

Ejemplo III.5.2

En el conjunto cociente $\mathbf{Z}/(5)$ la suma y el producto tienen las siguientes tablas

$+$	$\langle 0\rangle$	$\langle 1\rangle$	$\langle 2\rangle$	$\langle 3\rangle$	$\langle 4\rangle$
$\langle 0\rangle$	$\langle 0\rangle$	$\langle 1\rangle$	$\langle 2\rangle$	$\langle 3\rangle$	$\langle 4\rangle$
$\langle 1\rangle$	$\langle 1\rangle$	$\langle 2\rangle$	$\langle 3\rangle$	$\langle 4\rangle$	$\langle 0\rangle$
$\langle 2\rangle$	$\langle 2\rangle$	$\langle 3\rangle$	$\langle 4\rangle$	$\langle 0\rangle$	$\langle 1\rangle$
$\langle 3\rangle$	$\langle 3\rangle$	$\langle 4\rangle$	$\langle 0\rangle$	$\langle 1\rangle$	$\langle 2\rangle$
$\langle 4\rangle$	$\langle 4\rangle$	$\langle 0\rangle$	$\langle 1\rangle$	$\langle 2\rangle$	$\langle 3\rangle$

$\cdot$	$\langle 0\rangle$	$\langle 1\rangle$	$\langle 2\rangle$	$\langle 3\rangle$	$\langle 4\rangle$
$\langle 0\rangle$	$\langle 0\rangle$	$\langle 0\rangle$	$\langle 0\rangle$	$\langle 0\rangle$	$\langle 0\rangle$
$\langle 1\rangle$	$\langle 0\rangle$	$\langle 1\rangle$	$\langle 2\rangle$	$\langle 3\rangle$	$\langle 4\rangle$
$\langle 2\rangle$	$\langle 0\rangle$	$\langle 2\rangle$	$\langle 4\rangle$	$\langle 1\rangle$	$\langle 3\rangle$
$\langle 3\rangle$	$\langle 0\rangle$	$\langle 3\rangle$	$\langle 1\rangle$	$\langle 4\rangle$	$\langle 2\rangle$
$\langle 4\rangle$	$\langle 0\rangle$	$\langle 4\rangle$	$\langle 3\rangle$	$\langle 2\rangle$	$\langle 1\rangle$

de modo que + es asociativa, conmutativa, existe neutro que es $\langle 0\rangle$ y todo elemento tiene opuesto, es decir, $(\mathbf{Z}/(5),+)$ es un grupo abeliano. El producto es asociativo, conmutatitvo y distributivo y tiene elemento unidad que es la clase $\langle 1\rangle$. Además como 5 es primo, $(\mathbf{Z}/(5),+,\cdot)$ es un cuerpo.

Ejercicios

III.18.- Resolver las ecuaciones

$$\langle 5\rangle\langle x\rangle = \langle 6\rangle \quad , \quad \langle 4\rangle\langle x\rangle+\langle 4\rangle = \langle 7\rangle$$

en $\mathbf{Z}/(13)$ y $\mathbf{Z}/(16)$,

III.18.- Resolver las ecuaciones

$$\langle 15\rangle\langle x\rangle = \langle 18\rangle \quad , \quad \langle 4\rangle\langle x\rangle^2+\langle 4\rangle\langle x\rangle+\langle 7\rangle = \langle 0\rangle$$

en $\mathbf{Z}/(131)$.

III.6.- ALGEBRAS DE BOOLE

Otra estructura con dos l.c.i. es la que vamos a ver en esta Sección, de gran importancia por sus aplicaciones en tecnologías como la Electrónica, Mecánica de Fluídos, y otras, y su definición viene sugerida por las propiedades que tiene la estructura de las partes de un referencial con las operaciones de unión e intersección. Si comparamos las propiedades de los conectores lógicos conjunción, disyunción y negación con las propiedades de la intersección, unión y complementario sobre el conjunto de las partes de un referencial E , vemos tal similitud que cabe preguntarse si es posible construir una estructura más general que admita a ambas como casos particulares. Tal estructura existe, recibe el nombre de Algebra de Boole y su definición axiomática es como sigue:

"Un ***álgebra de Boole*** es un conjunto A con dos l.c.i., que denotaremos por + y ·, y llamaremos ***suma*** y ***producto***, tales que verifican los axiomas

A1) Conmutatividad

$$a+b = b+a \qquad a\cdot b = b\cdot a$$

A2) Distributividad

$$a+(b\cdot c) = (a+b)\cdot(a+c) \qquad a\cdot(b+c) = (a\cdot b)+(a\cdot c)$$

A3) Existen dos elementos 0 y 1 tales que

$$a+0 = a \qquad a\cdot 1 = a$$

A4) Para todo $a \in A$, existe un $a' \in A$, llamado ***complementario*** de a, tal que

$$a+a' = 1 \qquad a\cdot a' = 0$$

Estos axiomas hacen del álgebra de Boole una estructura que contiene como casos particulares al álgebra de proposiciones y al álgebra de las partes de un referencial E, con las equivalencias de notación siguientes:

Algebra de Boole	Algebra de Proposiciones	Algebra de $\mathcal{P}(E)$
a	P	A
$+$	$\vee$	$\cup$
$\cdot$	$\wedge$	$\cap$
a'	$\neg P$	A'
1	τ	E
0	$\complement$	$\varnothing$

aunque existen otras álgebras booleanas distintas.

Ejemplo III.6.1

Si en el conjunto $B = \{0,1\}$ definimos dos l.c.i. mediante las tablas

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

el resultado $(B,+,\cdot)$ es un álgebra de Boole, por verificar los cuatro axiomas que la definen; por ejemplo, ambas son conmutativas, por ser simétricas las tablas, y

$$1' = 0 \qquad 0' = 1$$

Este álgebra de Boole se denomina ***álgebra binaria*** y es de gran importancia en las aplicaciones a la electrónica, como veremos más adelante.

De la definición del álgebra de Boole se deducen las propiedades que figuran en la siguiente Tabla III.6.1

TABLA III.6.1

Propiedades de un álgebra de Boole

P1) Principio de dualidad :

"Todo resultado verdadero deducido de los axiomas anteriores tiene un resultado dual, también verdadero, que se construye intercambiando + por · y 1 por 0"

P2) Idempotencia

$$a+a = a \qquad a\cdot a = a$$

P3) Elementos absorbentes

$$a+1 = 1 \qquad a\cdot 0 = 0$$

P4) Absorción

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

P5) Asociativa

$$a+(b+c) = (a+b)+c \qquad a\cdot(b\cdot c) = (a\cdot b)\cdot c$$

P6) Unicidad del complementario

$$(a+x = 1 \ \wedge \ a\cdot x = 0) \text{ implican } x = a'$$

P7) Involución

$$(a')' = a$$

P8) Complementarios de 0 y 1

$$0' = 1 \qquad 1' = 0$$

P9) Leyes de Morgan

$$(a+b)' = a'\cdot b' \qquad (a\cdot b)' = a'+b'$$

Demostraciones:

P1) es inmediata ya que basta darse cuenta que los axiomas que definen el álgebra de Boole son dobles, siendo una mitad dual de la otra; por ello toda propiedad de una fórmula deducida de los axiomas tiene una dual y además, la dual de la dual vuelve a ser la primitiva propiedad. Observese como todas las propiedades P2) a P9) son dobles, siendo una mitad la dual de la otra, por lo que basta demostrar una de ellas, resultando la otra por el principio de dualidad. Las demostraciones de las otras propiedades se basan en una ordenada aplicación de los axiomas y son como siguen:

P2) Idempotencia:

$$a+a \overset{A3)}{=} (a+a)\cdot 1 \overset{A4)}{=} (a+a)\cdot(a+a') \overset{A2)}{=} a+(a\cdot a') \overset{A4)}{=} a+0 \overset{A3)}{=} a$$

P3) Elementos absorbentes:

$$a+1 \overset{A3)}{=} 1\cdot(a+1) \overset{A4)}{=} (a+a')\cdot(a+1) \overset{A2)}{=} a+(a'\cdot 1) \overset{A3)}{=} a+a' \overset{A4)}{=} 1$$

P4) Ley de absorción:

$$a+a\cdot b \overset{A1)}{=} a+b\cdot a \overset{A3)}{=} 1\cdot a+b\cdot a \overset{A1)A2)}{=} (1+b)\cdot a \overset{P3)}{=} 1\cdot a \overset{A3)}{=} a$$

P5) Asociatividad: la demostración se obtiene en varias etapas

a) $a+a\cdot(b\cdot c) \overset{P4)}{=} a \overset{P4)}{=} a\cdot(a+c) \overset{P4)}{=} (a+a\cdot b)\cdot(a+c) \overset{A2)}{=} a+((a\cdot b)\cdot c)$

b) $a'+(a\cdot(b\cdot c)) \overset{A2)}{=} (a'+a)\cdot(a'+b\cdot c) \overset{A4)}{=} 1\cdot(a'+b\cdot c) \overset{A3)}{=} a'+(b\cdot c) \overset{A2)}{=} (a'+b)\cdot(a'+c) \overset{A3)}{=}$

$$= (1\cdot(a'+b))\cdot(a'+c) \overset{A4)}{=} ((a'+a)\cdot(a'+b))\cdot(a'+c) \overset{A3)}{=} (a'+(a\cdot b))\cdot(a'+c) \overset{A2)}{=} a'+((a\cdot b)\cdot c)$$

Multiplicando a) y b)

$$(a+a\cdot(b\cdot c))\cdot(a'+a\cdot(b\cdot c)) = (a+(a\cdot b)\cdot c)\cdot(a'+(a\cdot b)\cdot c)$$

y simplificando ambos miembros de esta igualdad

$$(a+a\cdot(b\cdot c))\cdot(a'+a\cdot(b\cdot c)) = (a\cdot(b\cdot c)+a)\cdot(a\cdot(b\cdot c)+a') = a\cdot(b\cdot c)+(a\cdot a') = a\cdot(b\cdot c)+0 = a\cdot(b\cdot c)$$

$$(a+(a\cdot b)\cdot c)\cdot(a'+(a\cdot b)\cdot c) = ((a\cdot b)\cdot c+a)\cdot((a\cdot b)\cdot c+a') = (a\cdot b)\cdot c+(a\cdot a') = (a\cdot b)\cdot c+0 = (a\cdot b)\cdot c$$

quedando demostrada la asociatividad del producto

P6) Unicidad del complementario:

$$x = 1\cdot x = (a'+a)\cdot x = a'\cdot x+a\cdot x = a'\cdot x+0 = a'\cdot x = x\cdot a' = 0+x\cdot a' = a\cdot a'+x\cdot a' =$$

$= (a+x)\cdot a' = 1\cdot a' = a'$

P7) Involución : como $a'+a = 1$ y $a'\cdot a = 0$, según la propiedad anterior

$$a = (a')'$$

P8) Complementarios de 1 y 0 : Según P3) $0+1 = 1$ y $1\cdot 0 = 0$, de donde, por P6)

$$0 = 1'$$

P9) Leyes de De Morgan : De los resultados

a) $(a\cdot b)\cdot(a'+b') = a\cdot b\cdot a'+a\cdot b\cdot b' = 0\cdot b+a\cdot 0 = 0+0 = 0$

b) $a\cdot b+a'+b' = a'+b'+a\cdot b = (a'+b'+a)\cdot(a'+b'+b) = (1+b')\cdot(1+a') = 1$

aplicando el resultado P6) a ambas igualdades resulta

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

Si $(A,+,\cdot)$ es un álgebra de Boole, definimos como ***función booleana*** de n variables una aplicación

$$\begin{array}{rccc} f: & A^n & \longrightarrow & A \\ & (x_1,\ldots,x_n) & \longrightarrow & f(x_1,\ldots,x_n) \end{array}$$

Sobre el conjunto $\mathbb{F}_n(A)$ de las funciones booleanas en n variables sobre A pueden definirse las operaciones de suma y producto del modo siguiente

Suma :
$$\begin{array}{rccc} f+g: & A^n & \longrightarrow & A \\ & (x_1,\ldots,x_n) & \longrightarrow & (f+g)(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)+g(x_1,\ldots,x_n) \end{array}$$

Producto :
$$\begin{array}{rccc} f\cdot g: & A^n & \longrightarrow & A \\ & (x_1,\ldots,x_n) & \longrightarrow & (f\cdot g)(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)\cdot\ g(x_1,\ldots,x_n) \end{array}$$

pudiendo verificarse fácilmente que el hecho de ser $(A,+,\cdot)$ un álgebra de Boole hace que $(\mathbb{F}_n(A),+,\cdot)$ también lo sea, siendo los elementos 0 y 1 las funciones

$$\begin{array}{rccc} 0: & A^n & \longrightarrow & A \\ & (x_1,\ldots,x_n) & \longrightarrow & 0(x_1,\ldots,x_n) = 0 \end{array}$$

$$\begin{array}{rccc} 1: & A^n & \longrightarrow & A \\ & (x_1,\ldots,x_n) & \longrightarrow & 1(x_1,\ldots,x_n) = 1 \end{array}$$

y la función complementaria de f

$$\begin{array}{rccc} f': & A^n & \longrightarrow & A \\ & (x_1,\ldots,x_n) & \longrightarrow & f'(x_1,\ldots,x_n) = (f(x_1,\ldots,x_n))' \end{array}$$

Hay dos tipos especiales de funciones booleanas que juegan un papel importante en la teoría que son los ***mintérminos*** y ***Maxtérminos***. Un mintérmino de orden n es una función

booleana del tipo

$$\begin{aligned} m: \quad & A^n \longrightarrow A \\ & (x_1,\ldots,x_n) \longrightarrow m(x_1,\ldots,x_n) = x_1^{z_1}\cdot \ldots \cdot x_n^{z_n} \end{aligned}$$

donde z es una prima (') o nada y un Maxtérmino de orden n es una función booleana del tipo

$$\begin{aligned} M: \quad & A^n \longrightarrow A \\ & (x_1,\ldots,x_n) \longrightarrow M(x_1,\ldots,x_n) = x_1^{z_1}+ \ldots + x_n^{z_n} \end{aligned}$$

Ejemplo III.6.2

Si $(A,+,\cdot)$ es un álgebra de Boole, en el álgebra booleana $(\mathbb{F}_3(A),+,\cdot)$ de las funciones de tres variables sobre A, un mintérmino es, por ejemplo

$$\begin{aligned} m: \quad & A^3 \longrightarrow A \\ & (x_1,x_2,x_3) \longrightarrow m(x_1,x_2,x_3) = x_1\cdot x_2'\cdot x_3' \end{aligned}$$

y un Maxtérmino es

$$\begin{aligned} M: \quad & A^3 \longrightarrow A \\ & (x_1,x_2,x_3) \longrightarrow M(x_1,x_2,x_3) = x_1'+x_2+x_3 \end{aligned}$$

siendo ambos complementarios pues

$$\begin{aligned} m+M: \quad & A^3 \longrightarrow A \\ & (x_1,x_2,x_3) \longrightarrow (m+M)(x_1,x_2,x_3) = (x_1\cdot x_2'\cdot x_3')+(x_1'+x_2+x_3) = 1 \end{aligned}$$

$$\begin{aligned} m\cdot M: \quad & A^3 \longrightarrow A \\ & (x_1,x_2,x_3) \longrightarrow (m\cdot M)\,(x_1,x_2,x_3) = (x_1\cdot x_2'\cdot x_3')\cdot(x_1'+x_2+x_3) = 0 \end{aligned}$$

ya que por las propiedades del álgebra de Boole

$$\begin{aligned} (x_1\cdot x_2'\cdot x_3')\cdot(x_1'+x_2+x_3) &= (x_1\cdot x_2'\cdot x_3'\cdot x_1')+(x_1\cdot x_2'\cdot x_3'\cdot x_2)+(x_1\cdot x_2'\cdot x_3'\cdot x_3) = \\ &= ((x_1\cdot x_1')\ x_3'\cdot x_2')+(x_1\cdot(x_2'\cdot x_2)\ \cdot x_3')+(x_1\cdot x_2'\cdot(x_3'\cdot x_3)) = \\ &= (0\cdot x_3'\cdot x_1')+(x_1\cdot 0\cdot x_3')+(x_1\cdot x_2'\cdot 0) = 0+0+0 = 0 \end{aligned}$$

demostrándose análogamente la otra igualdad.

Es evidente que, según su definición, hay en total 2^n posibles mintérminos y 2^n posibles Maxtérminos distintos. Todos ellos se representan por la misma letra, m para los mintérminos y M para los Maxtérminos, afectada de un subíndice construído de acuerdo con los criterios:

"dada la fórmula de un mintérmino, $x_1^{z_1}\cdot\ldots x_n^{z_n}$ escribamos un 0 si un z es ' y un 1 si no lo es; la sucesión de ceros y unos resultante representa un número en el sistema de base 2 que, pasado a base 10, es el subíndice del mintérmino"

"dada la fórmula de un Maxtérmino, $x_1^{z_1}+\ldots+x_n^{z_n}$, escribamos un 1 si un z es ' y un 0

si no lo es; la sucesión de ceros y unos resultante representa un número en el sistema de base 2 que, pasado a base 10, es el subíndice del Maxtérmino"

Ejemplo III.6.3

En el álgebra $(\mathbb{F}_3(A),+,\cdot)$ de funciones booleanas en tres variables los mintérminos son

mintérmino		Representación
$x_1'\cdot x_2'\cdot x_3'$	000	m_0
$x_1'\cdot x_2'\cdot x_3$	001	m_1
$x_1'\cdot x_2\cdot x_3'$	010	m_2
$x_1'\cdot x_2\cdot x_3$	011	m_3
$x_1\cdot x_2'\cdot x_3'$	100	m_4
$x_1\cdot x_2'\cdot x_3$	101	m_5
$x_1\cdot x_2\cdot x_3$	110	m_6
$x_1\cdot x_2\cdot x_3$	111	m_7

y los Maxtérminos

Maxtérmino		Representación
$x_1'+x_2'+x_3'$	111	M_7
$x_1'+x_2'+x_3$	110	M_6
$x_1'+x_2+x_3'$	101	M_5
$x_1'+x_2+x_3$	100	M_4
$x_1+x_2'+x_3'$	011	M_3
$x_1+x_2'+x_3$	010	M_2
$x_1+x_2+x_3'$	001	M_1
$x_1+x_2+x_3$	000	M_0

Las propiedades más importantes de mintérminos y Maxtérminos figuran en la Tabla III.6.2

TABLA III.6.2

Propiedades de los mintérminos y Maxtérminos

1) El complementario del mintérmino m_i es el Maxtérmino M_i

2) La suma de los 2^n mintérminos es igual a la función 1

2') El producto de los 2^n Maxtérminos es igual a la función 0

3) El producto de dos mintérminos diferentes es 0

3') La suma de dos Maxtérminos diferentes es 1

Demostraciones:

1) Sean

$$m_i = x_1^{z_1} \cdot \ldots \cdot x_n^{z_n} \qquad M_i = x_1^{t_1} + \ldots + x_n^{t_n}$$

de manera que cuando z_j es ' entonces t_j no lo es y viceversa, según la representación que hemos definido para mintérminos y Maxtérminos; por ello, tendremos

$$m_i \cdot M_i = x_1^{z_1} \cdot \ldots \cdot x_n^{z_n} \cdot (x_1^{t_1} + \ldots + x_n^{t_n}) = x_1^{z_1} \cdot \ldots \cdot x_n^{z_n} \cdot x_1^{t_1} + \ldots + x_1^{z_1} \cdot \ldots \cdot x_n^{z_n} \cdot x_n^{t_n} = 0 + \ldots + 0 = 0$$

demostrándose de forma análoga que

$$m_i + M_i = 1$$

2) Por inducción, definiendo para ello el conjunto

$$S = \{n \in \mathbf{N} \mid \text{la suma de todos los mintérminos en } n \text{ variables es } 1\}$$

que verifica:

a) $1 \in S$ pues $x + x' = 1$

b) $m \in S \Rightarrow m+1 \in S$ pues los 2^{m+1} mintérminos en las variables $x_1, x_2, \ldots, x_m, x_{m+1}$ son de dos tipos:

$$2^m \text{ mintérminos con } x_{m+1} \text{ y } 2^m \text{ mintérminos con } x'_{m+1}$$

por lo que la suma de todos ellos puede descomponerse en la forma

$$\begin{aligned} \sum \text{mintérminos} = {} & (\sum \text{ de los } 2^m \text{ mintérminos en } x'_{m+1}) + \\ & + (\sum \text{ de los } 2^m \text{ mintérminos en } x_{m+1}) = \\ = {} & x'_{m+1} \cdot (\sum \text{ de los } 2^m \text{ mintérminos en } x_1, \ldots, x_m) + \\ & + x_{m+1} \cdot (\sum \text{ de los } 2^m \text{ mintérminos en } x_1, \ldots, x_m) = \\ = {} & x'_{m+1} \cdot 1 + x_{m+1} \cdot 1 = x'_{m+1} + x_{m+1} = 1 \end{aligned}$$

2') Aplicando a esta igualdad anterior las fórmulas de De Morgan

$$\sum_{i=0}^{2^n-1} m_i = 1 \Rightarrow (\sum_{i=0}^{2^n-1} m_i)' = 1' \Rightarrow \prod_{i=0}^{2^n-1} (m_i)' = 0 \Rightarrow \prod_{i=0}^{2^n-1} M_i = 0$$

3) Si dos mintérminos son distintos es porque existe, por lo menos, alguna variable x_i que aparece con ' en uno y no en el otro con lo que el producto de ambos es

$$m_i \cdot m_j = (\ldots \cdot x_i \cdot \ldots) \cdot (\ldots \cdot x'_i \cdot \ldots) = x_i \cdot x'_i \cdot (\ldots) = 0 \cdot (\ldots) = 0$$

3') Aplicando de nuevo las fórmulas de De Morgan a esta igualdad

$$(m_i \cdot m_j)' = 0' \quad \Rightarrow \quad m'_i + m'_j = 1 \quad \Rightarrow \quad M_i + M_j = 1$$

Como consecuencia se obtiene que el complementario de una suma de mintérminos es la suma de los mintérminos que no aparecen en ella, es decir,

$$(\sum_{i=0}^{2^n-1} \delta_i m_i)' = \sum_{i=0}^{2^n-1} (1-\delta_i) m_i$$

siendo δ_i una variable entera tal que $\delta_i = 1$ para el caso en que el mintérmino m_i aparezca en la suma y $\delta_i = 0$ en caso contrario.

Supongamos que $f \in \mathbb{F}_n(A)$ es una función booleana que viene dada como sumas y productos en las n variables x_i y x'_i, es decir, que en su fórmula no aparecen nada más que variables; vamos a demostrar que f puede expresarse como suma de mintérminos en la forma

$$f = \sum_{i=0}^{2^n-1} \delta_i \, m_i \qquad \text{con} \quad \delta_i = 1 \text{ o } 0$$

Para ello bastará demostrar que cualquier variable x_i es expresable como suma de mintérminos en las n variables $x_1,\ldots,x_n$ y que la suma, producto o complementario de una suma de mintérminos es también una suma de mintérminos; en efecto, en primer lugar

$$x_i = x_i \cdot 1 = x_i \cdot (\sum \text{ de los } 2^{n-1} \text{ mintérminos en } x_1,\ldots,x_i,x_{i+1},\ldots,x_n) =$$

$$= \sum \text{ de los } 2^{n-1} \text{ mintérminos en } x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n$$

en segundo lugar

$$\sum \delta_i m_i + \sum \delta'_i m_i = \sum (\delta_i + \delta'_i) m_i \qquad \text{con } (\delta_i + \delta'_i) = 0 \text{ o } 1$$

ya que $m_i + m_i = m_i$

$$(\sum \delta_i m_i) \cdot (\sum \delta'_i m_i) = \sum (\delta_i \cdot \delta'_i) m_i \qquad \text{con } (\delta_i \cdot \delta'_i) = 0 \text{ o } 1$$

ya que $m_i \cdot m_i = m_i$ y $m_i \cdot m_j = 0$ y en tercer lugar si hacemos

$$S_1 = \sum_{i=0}^{2^n-1} \delta_i \, m_i \qquad \text{y} \qquad S_2 = \sum_{i=0}^{2^n-1} (1-\delta_i) \, m_i$$

el complementario de S_1 es S_2.

Asimismo se demuestra el resultado dual, según el cual f es expresable de forma única como producto de Maxtérminos

$$\sum_{i=0}^{2^n-1} \delta_i \, m_i = f = (f')' = ((\sum_{i=0}^{2^n-1} \delta_i \, m_i)')' = (\sum_{i=0}^{2^n-1} (1-\delta_i) \, m_i)' = \prod_{i=0}^{2^n-1} M_i^{(1-\delta_i)}$$

Cuando una función booleana está expresada como suma de mintérminos se dice que está expresada en ***forma normal disyuntiva*** y si lo está como producto de Maxtérminos se

denomina ***forma normal conjuntiva***.

Ejemplo III.6.4

Si A es un álgebra de Boole, para la función booleana en tres variables sobre A

$$\begin{array}{rcl} f: \quad A^3 & \longrightarrow & A \\ (x_1,x_2,x_3) & \longrightarrow & f(x_1,x_2,x_3) = x_1+x_2'\cdot x_3+x_3'\cdot x_1' \end{array}$$

la forma normal disyuntiva puede obtenerse según el proceso constructivo que se desprende de la demostración anterior, que puede abreviarse del modo siguiente

$$\begin{aligned} f(x_1,x_2,x_3) &= x_1+x_2'\cdot x_3+x_3'\cdot x_1' = x_1\cdot 1\cdot 1+1\cdot x_2'\cdot x_3+x_1'\cdot 1\cdot x_3' = \\ &= x_1\cdot(x_2+x_2')\cdot(x_3+x_3')+(x_1+x_1')\cdot x_2'\cdot x_3+x_1'\cdot(x_2+x_2')\cdot x_3' = \\ &= x_1\cdot x_2\cdot x_3+x_1\cdot x_2\cdot x_3'+x_1\cdot x_2'\cdot x_3+x_1\cdot x_2'\cdot x_3'+x_1\cdot x_2'\cdot x_3+x_1'\cdot x_2'\cdot x_3+x_1'\cdot x_2\cdot x_3'+x_1'\cdot x_2'\cdot x_3' = \\ &= x_1\cdot x_2\cdot x_3+x_1\cdot\ x_2\cdot x_3'+x_1\cdot x_2'\cdot x_3'+x_1\cdot x_2'\cdot x_3+x_1'\cdot x_2'\cdot x_3+x_1'\cdot x_2\cdot x_3'+x_1'\cdot x_2'\cdot x_3' = \\ &= m_7+m_6+m_4+m_5+m_1+m_2+m_0 \end{aligned}$$

En forma normal conjuntiva es, según lo anterior

$$f(x_1,x_2,x_3) = M_3$$

Dos mintérminos se denominan ***contiguos*** cuando tienen todos los factores iguales excepto uno de ellos que en un mintérmino está como tal y en el otro está el complementario. Análogamente se definen los maxtérminos contiguos.

La suma de dos mintérminos contiguos se pueden simplificar en la forma

$$A\cdot x+A\cdot x' = A\cdot(x+x') = A\cdot 1 = A$$

Análogamente cuatro mintérminos son contiguos si tienen todos los factores iguales excepto dos de ellos y su suma puede simplificarse en la forma

$$A\cdot x_i\cdot x_j+A\cdot x_i'\cdot x_j+A\cdot x_i\cdot x_j'+A\cdot x_i'\cdot x_j' = A\cdot x_j+A\cdot x_j' = A$$

obteniéndose el producto de las variables que son iguales en los cuatro mintérminos; este resultado puede ser generalizado a la suma de 2^r mintérminos contiguos (con $r < n$).

Ejemplo III.6.5

Los mintérminos $x_1'\cdot x_2'\cdot x_3$, $x_1\cdot x_2'\cdot x_3$, $x_1'\cdot x_2\cdot x_3$, $x_1\cdot x_2\cdot x_3$ son contiguos y su suma es

$$x_1'\cdot x_2'\cdot x_3+x_1\cdot x_2'\cdot x_3+x_1'\cdot x_2\cdot x_3+x_1\cdot x_2\cdot x_3 = x_3$$

Particularicemos todos estos resultados generales cuando usamos como álgebra de Boole de

base el álgebra binaria *B*. Una función booleana de *n* variables será una aplicación

$$\begin{array}{rccc} f: & B^n & \longrightarrow & B \\ & (x_1,\ldots,x_n) & \longrightarrow & f(x_1,\ldots,x_n) \end{array}$$

donde la imagen de cualquier *n*-pla será 0 o 1, pues éstos son los únicos elementos de *B*; la asignación de 0 o 1 a todas las *n*-plas forma la denominada ***tabla de verificación*** de la función, análoga a la tabla de verdad de una fórmula proposicional, que es un caso particular de función booleana sobre el álgebra binaria $B = \{0,1\}$. En particular, la tabla de verificación de un mintérmino m_j estará formada por todo 0 excepto un 1 en la fila correspondiente a la representación en base 2 del subíndice *j* del mintérmino; y análogamente para un Maxtérmino M_j, que tendrá una tabla de verificación formada por todo 1 excepto un 0 en la fila correspondiente a la representación en base 2 del subíndice *j*.

Ejemplo III.6.5

La tabla de verificación del mintérmino en tres variables sobre un álgebra de Boole binaria

$$m_5 = x_1 \cdot x_2' \cdot x_3$$

es la siguiente

	x_1	x_2	x_3	$(x_1 \cdot x_2') \cdot x_3$
	0	0	0	0 1 0
	0	0	1	0 1 0
	0	1	0	0 0 0
	0	1	1	0 0 0
	1	0	0	1 1 0
5 —>	1	0	1	1 1 1
	1	1	0	0 0 0
	1	1	1	0 0 0

Para el Maxtérmino

$$M_5 = x_1' + x_2 + x_3'$$

será

	x_1	x_2	x_3	$(x_1' + x_2) + x_3'$
	0	0	0	1 1 1 1
	0	0	1	1 1 1 0
	0	1	0	1 1 1 1
	0	1	1	1 1 1 0
	1	0	0	0 0 1 1
5 –>	1	0	1	0 0 0 0
	1	1	0	0 1 1 1
	1	1	1	0 1 1 0

y para la función

$$\begin{array}{rcl} f: \quad B^3 & \longrightarrow & B \\ (x_1,x_2,x_3) & \longrightarrow & f(x_1,x_2,x_3) = x_1+x_2'\cdot x_3+x_3'\cdot x_1' \end{array}$$

tendremos

x_1	x_2	x_3	$(x_1+x_2'\cdot x_3)$			$+\ x_3'\ \cdot\ x_1'$			
0	0	0	0	1	0	1	1	1	1
0	0	1	1	1	1	1	0	0	1
0	1	0	0	0	0	1	1	1	1
0	1	1	0	0	0	0	0	0	1
1	0	0	1	1	0	1	1	0	0
1	0	1	1	1	1	1	0	0	0
1	1	0	1	0	0	1	1	0	0
1	1	1	1	0	0	1	0	0	0

En el caso de una función de n variables sobre el álgebra binaria es sencillo obtener a partir de su tabla de verificación la forma normal conjuntiva o disyuntiva. Dada la función

$$\begin{array}{rcl} f: \quad B^n & \longrightarrow & B \\ (x_1,\ldots,x_n) & \longrightarrow & f(x_1,\ldots,x_n) \end{array}$$

pongamos $f(x_1,x_2,\ldots,x_n) = x_1\cdot r+x_1'\cdot s$, siendo r y s dos funciones booleanas, que podemos calcular haciendo

$$\begin{array}{l} x_1 = 1 \quad x_1' = 0 \quad \Rightarrow \quad f(1,x_2,\ldots,x_n) = 1\cdot r+0\cdot s = r \\ x_1 = 0 \quad x_1' = 1 \quad \Rightarrow \quad f(0,x_2,\ldots,x_n) = 0\cdot r+1\cdot s = s \end{array}$$

por lo cual

$$f(x_1,x_2,\ldots,x_n) = x_1\cdot f(1,x_2,\ldots,x_n)+x_1'\cdot f(0,x_2,\ldots,x_n)$$

Análogamente para $f(1,x_2,x_n) = x_2\cdot r+x_2'$s, calculando ahora r y s haciendo como antes

$$\begin{array}{l} x_2 = 1 \quad x_2' = 0 \quad \Rightarrow \quad f(1,1,\ldots,x_n) = 1\cdot r+0\cdot s = r \\ x_2 = 0 \quad x_2' = 1 \quad \Rightarrow \quad f(1,0,\ldots,x_n) = 0\cdot r+1\cdot s = s \end{array}$$

por lo cual

$$f(1,x_2,\ldots,x_n) = x_2\cdot f(1,1,\ldots,x_n)+x_2'\cdot f(1,0,\ldots,x_n)$$

y para $f(0,x_2,\ldots,x_n)$ poniendo $f(0,x_2,\ldots,x_n) = x_2\cdot r+x_2'$s, calculando ahora r y s, haciendo

$$\begin{array}{l} x_2 = 1 \quad x_2' = 0 \quad \Rightarrow \quad f(0,1,\ldots,x_n) = 1\cdot r+0\cdot s = r \\ x_2 = 0 \quad x_2' = 1 \quad \Rightarrow \quad f(0,0,\ldots,x_n) = 0\cdot r+1\cdot s = s \end{array}$$

por lo cual

$$f(0,x_2,...,x_n) = x_2 \cdot f(0,1,...,x_n) + x_2' \cdot f(0,0,...,x_n)$$

Reiterando el proceso obtendremos al final

$$\begin{aligned} f(x_1,x_2,...,x_n) = {} & x_1 \cdot x_2 \cdot x_3 \cdot \ ... \ \cdot x_n \cdot f(1,1,1,...,1) + \\ & + x_1 \cdot x_2 \cdot x_3 \cdot \ ... \ \cdot x_n' \cdot f(1,1,1,...,0) + \\ & \quad . \\ & + x_1' \cdot x_2 \cdot x_3 \cdot \ ... \ \cdot x_n' \cdot f(0,1,1,...,0) \ + \\ & \quad . \\ & \quad . \\ & + x_1' \cdot x_2' \cdot x_3' \cdot \ ... \ \cdot x_n' \cdot f(0,0,0,...,0) \end{aligned}$$

Si ponemos

$$\begin{aligned} \delta_0 &= f(0,0,...,0,0) \\ \delta_1 &= f(0,0,...,0,1) \\ \delta_2 &= f(0,0,...,1,0) \\ &. \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ \delta_{2^n-1} &= f(1,1,1,...,1) \end{aligned}$$

siendo el subíndice de cada δ la expresión decimal del número que, en base 2, forman los 0 y 1 de la *n*-pla correspondiente, tendremos

$$f(x_1,x_2,...x_n) = \sum_{i=0}^{2^n-1} \delta_i \, m_i$$

que es la forma normal disyuntiva de *f*; en ella los δ_i iguales a 1 serán los que tienen por subíndice un número en base 10 que en base 2 es la *n*-pla cuya imagen en la tabla de verificación es 1. Como producto de Maxtérminos será

$$f(x_1,x_2,...,\ x_n) = \prod_{i=0}^{2^n-1} M_i^{(1-\delta)}$$

Ejemplo III.6.6

Según lo anterior, la forma normal, conjuntiva o disyuntiva, de una función booleana se obtendrá a partir de la posición de los 0 y 1 de su tabla de verificación. Para la función de cuatro variables

$$f(x_1,x_2,x_3,x_4) = x_1' \cdot x_2 \cdot x_3' + x_4 \cdot x_1$$

construiremos su tabla de verificación

x_1	x_2	x_3	x_4	$((x_1' \cdot x_2) \cdot x_3')$		$+(x_4 \cdot x_1)$			
0	0	0	0	1	0	0	1	0	0
0	0	0	1	1	0	0	1	0	0
0	0	1	0	1	0	0	0	0	0
0	0	1	1	1	0	0	0	0	0
0	1	0	0	1	1	1	1	1	0
0	1	0	1	1	1	1	1	1	0
0	1	1	0	1	1	0	0	0	0
0	1	1	1	1	1	0	0	0	0
1	0	0	0	0	0	0	1	0	0
1	0	0	1	0	0	0	1	1	1
1	0	1	0	0	0	0	0	0	0
1	0	1	1	0	0	0	0	1	1
1	1	0	0	0	0	0	1	0	0
1	1	0	1	0	0	0	1	1	1
1	1	1	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	1	1

con lo que

$$f = m_4+m_5+m_9+m_{11}+m_{13}+m_{15}$$

y en Maxtérminos

$$f = M_0 \cdot M_1 \cdot M_2 \cdot M_3 \cdot M_6 \cdot M_7 \cdot M_8 \cdot M_{10} \cdot M_{12} \cdot M_{14}$$

Del concepto de igualdad de funciones se deduce que dos funciones booleanas de n variables sobre $\{0,1\}$ serán iguales cuando coincidan las imágenes de cada elemento, es decir, cuando tengan iguales sus tablas de verificación. Al proceso de partiendo de una función booleana, obtener otra igual de expresión más sencilla recibe el nombre de ***simplificación*** y se realiza en dos etapas:

1) expresar la función en forma normal disyuntiva como suma de mintérminos (o conjuntiva como producto de maxtérminos)

2) simplificar las sumas de mintérminos contiguos (o los productos de maxtérminos contiguos).

Un proceso tan poco preciso como éste es natural que no dé un resultado único, es decir, que la expresión simplificada de una función booleana no será única. Veámoslo sobre la función

$$\begin{aligned} f:\ \{0,1\}^3 &\longrightarrow \{0,1\} \\ (x_1,x_2,x_3) &\longrightarrow f(x_1,x_2,x_3) = x_1 \cdot x_2 \cdot x_3' + x_2 \cdot x_3' + x_1 \cdot x_2' \end{aligned}$$

1) Expresar la función en forma normal disyuntiva, como suma de mintérminos, se consigue fácilmente construyendo su tabla de verificación, que es

x_1	x_2	x_3	$((x_1 \cdot x_2) \cdot x_3' + x_2 \cdot x_3') + x_1 \cdot x_2'$									
0	0	0	0	0	1	0	0	1	0	0	1	
0	0	1	0	0	0	0	0	0	0	0	1	
0	1	0	0	0	1	1	1	1	1	0	0	
0	1	1	0	0	0	0	0	0	0	0	0	
1	0	0	0	0	1	0	0	1	1	1	1	
1	0	1	0	0	0	0	0	0	1	1	1	
1	1	0	1	1	1	1	1	1	1	0	0	
1	1	1	1	0	0	0	0	0	0	0	0	

que nos permite escribir, fijándonos en las posiciones de los 1 en la columna final

$$f(x_1,x_2,x_3) = m_2+m_4+m_5+m_6 = x_1'\cdot x_2\cdot x_3'+x_1\cdot x_2'\cdot x_3'+x_1\cdot x_2'\cdot x_3+x_1\cdot x_2\cdot x_3'$$

2) Aplicamos el esquema de simplicación de mintérminos contiguosque nos permite obtener

$$f(x_1,x_2,x_3) = x_2\cdot x_3'\cdot(x_1+x_1')+x_1\cdot x_2'\cdot(x_3+x_3') = x_2\cdot x_3'+x_1\cdot x_2'$$

Esta expresión simplificada no es mucho más simple que la fórmula de *f*, por lo que este procedimiento de simplificación es, para este caso, poco eficiente pero tiene la ventaja de poder ser desarrollado de forma automática mediante unos esquemas generales denominados ***diagramas de Karnaugh*** consistentes en colocar los mintérminos de la forma normal disyuntiva de *f* en un casillero de 2^n celdas de forma apropiada para poder aplicar a las casillas contiguas la fórmula de simplificación anterior.

En el caso $n = 3$ los mintérminos se colocan según indica el diagrama

x_1x_2 / x_3	00	01	11	10
0	m_0	m_2	m_6	m_4
1	m_1	m_3	m_7	m_5

en el que en dos casillas contiguas aparecen mintérminos contiguos que se diferencian sólamente en una variable, que en uno aparece complementada y en el otro sin complementar. Así, cada casilla posee tres contiguas, siendo las que directamente aparecen en el diagrama, que se supone enrrollado en forma de cilindro de manera que, por ejemplo, m_4 y m_0 son contiguas, al igual que m_1 y m_5. De este modo conseguimos que dos casillas contiguas se simplifiquen dando lugar al producto de los factores que son iguales en ambas, con ' si son 0 y, de forma análoga, si existen cuatro casillas contiguas dan lugar a la única variable común, con ' si es 0

Ejemplo III.6.7

Dada la función booleana de tres variables

$$f = m_2+m_6+m_7 = x_1'\cdot x_2\cdot x_3'+x_1\cdot x_2\cdot x_3'+x_1\cdot x_2\cdot x_3$$

la representamos en el casillero poniendo un 1 en cada casilla correspondiente a los

mintérminos que contiene la expresión de *f* y agrupando los contiguos, teniendo en cuenta que un 1 determinado puede estar en varias agrupaciones, según justifica la propiedad idempotente.

x_3 \ x_1x_2	00	01	11	10
0		1	1	
1			1	

Los dos contiguos que están en la 1ª fila determinan la simplificación

$$x_1'\cdot x_2\cdot x_3'+x_1\cdot x_2\cdot x_3' = (x_1'+x_1)\cdot x_2\cdot x_3' = x_2\cdot x_3'$$

y los contiguos de la 3ª columna

$$x_1\cdot x_2\cdot x_3'+x_1\cdot x_2\cdot x_3 = x_1\cdot x_2\cdot(x_3'+x_3) = x_1\cdot x_2$$

En definitiva, hemos hecho

$$f = x_1'\cdot x_2\cdot x_3'+x_1\cdot x_2\cdot x_3'+x_1\cdot x_2\cdot x_3 = x_2\cdot x_3'+x_1\cdot x_2$$

El diagrama de Karnaugh de los mintérminos para cuatro variables es el que sigue:

x_3x_4 \ x_1x_2	00	01	11	10
0 0	m_0	m_4	m_{12}	m_8
0 1	m_1	m_5	m_{13}	m_9
1 1	m_3	m_7	m_{15}	m_{11}
1 0	m_2	m_6	m_{14}	m_{10}

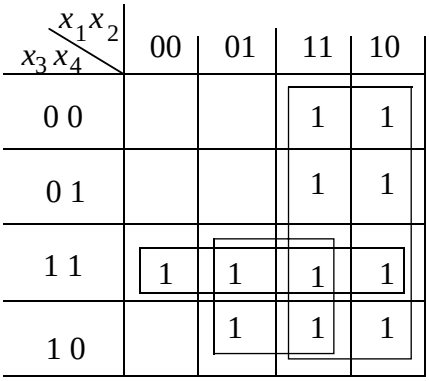
teniendo cada casilla cuatro contiguas; para las casillas interiores lo son las que directamente aparecen en el diagrama y para las casillas de las líneas de los bordes se considera el diagrama arrollado en doble cilindro, de modo que, por ejemplo, son contiguos los mintérminos m_4 y m_6 y también m_2 y m_{10}. Cuatro mintérminos que sean contiguos es porque tienen dos factores iguales difiriendo en los otros dos , que figuran con y sin ' ; la simplificación de los cuatro da por resultado el producto de los dos factores comunes, con ' si son 0; análogamente para ocho casillas contiguas que dan lugar al único factor común, con ' si es 0.

Ejemplo III.6.8

La función booleana de cuatro variables cuya forma normal disyuntiva es

$$f = m_3+m_6+m_7+m_8+m_9+m_{10}+m_{11}+m_{12}+m_{13}+m_{14}+m_{15}$$

tiene por representación en diagrama de Karnaugh



por lo que la función simplificada es $f = x_1 + x_2 \cdot x_3 + x_3 \cdot x_4$

El método de Karnaugh es de aplicación práctica para simplificar funciones de un máximo de 4 variables, pero, cuando dicho número es mayor es necesario recurrir a otros métodos, de los cuales el de Quine-McCluskey es el de uso más corriente.

Este metodo sirve para simplificar funciones booleanas en *n* variable supuestas expresadas previamente como suma de mintérminos. Se basa en el convenio que hemos establecido de asignar un número decimal a cada mintérmino; sabemos que si dos mintérminos son contiguos, sus subíndices correspondientes difieren en una potencia de 2; en efecto, si los mintérminos se diferencian en la variable x_i serán de la forma

$$A_1 x_i A_2 \qquad\qquad A_1 x_i' A_2$$

cuyos subíndices serán

$$B_1 1 B_2 \qquad\qquad B_1 0 B_2$$

que en base 10 tienen por diferencia

$$(p_1 + 1 \cdot 2^{n-i} + p_2) - (p_1 + 0 \cdot 2^{n-i} + p_2) = 2^{n-i}$$

por lo que se hace corresponder a cada variable x_i la potencia 2^{n-i}. Por ello, pueden agruparse en un solo sumando al cual le falta la variable correspondiente a dicha potencia. A su vez, si dos sumandos a los cuales les falte la misma variable, considerados como mintérminos en $n-1$ variables, difieren en una potencia de dos, pueden ser agrupados en un nuevo término el cual le falte la variable correspondiente a dicha potencia. Repitiendo este proceso se logra obtener todos los sumandos primos, que son aquellos que contienen el máximo número de mintérminos de la función y no existe ningún mintérmino de menor complejidad que los contenga.

Aunque el proceso que vamos a describir es general, para una mejor comprensión vamos a ilustrarlo sobre la función booleana en cuatro variables *a*, *b*, *c* y *d*, dada por

$$f(a,b,c,d) = m_0 + m_1 + m_3 + m_4 + m_7 + m_8 + m_{11} + m_{12} + m_{13} + m_{15}$$

Asignemos a cada variable la correspondiente potencia de 2: $a \to 2^3$, $b \to 2^2$, $c \to 2^1$, $d \to 2^0$ y

actuemos en la forma que indican las siguientes fases:

Fase 1) Se forma una tabla en la que los mintérminos se ordenan en grupos según tengan 0, 1, 2, 3 o 4 variables sin complementar.

Fase 2) Partiendo de esta primera tabla, se forma una segunda comparando los mintérminos que pertenecen a grupos adyacentes, grupo 0 con grupo 1, grupo 1 con grupo 2,..., etc, y agrupando en un solo mintérmino aquellos cuya diferencia del perteneciente al grupo i+1 con el del grupo i sea una potencia de dos positiva; cada variable eliminada se sustituye por un *. Todos los términos de la primera tabla que han sido utilizados para realizar la segunda se marcan con una cruz. En esta segunda tabla se crea una columna en la cual se indica la diferencia entre los mintérminos que forman parte de cada elemento de la misma.

Fase 3) A partir de esta segunda tabla se forma una tercera agrupando los mintérminos pertenecientes a grupos adyacentes cuya diferencia es igual y que además difieren entre sí en una potencia de dos. Por ejemplo, los mintérminos 4−0 y 12−8 de la fase 2 se pueden agrupar entre sí porque su diferencia es la misma, 4, lo que indica que les falta la misma variable, y ademas difieren en una potencia de dos positiva, pues 8−0 = 12−4 = 8, lo que indica que difieren en la situación de complementación de la variable a . En esta tercera tabla se indican en una segunda columna ambas diferencias, la interna de cada grupo y la que existe entre grupos que unen. Por ejemplo, la diferencia del grupo 12−8−4−0 es (4,8) que indica que le faltan las variables b y a.

El proceso se continúa realizando tablas sucesivas hasta que realizar todas las agrupaciones.

Fase 1

mint.	número	
$a'b'c'd'$	0	×
$a'b'c'd$	1	×
$a'b\ c'd'$	4	×
$a\ b'c'd'$	8	×
$a'b'c\ d$	3	×
$a\ b\ c'd'$	12	×
$a'b\ c\ d$	7	×
$a\ b'c\ d$	11	×
$a\ b\ c'd$	13	×
$a\ b\ c\ d$	15	×

Fase 2

mint.	número	dif.	
$a'b'c'*$	1–0	1	
$a'*c'd'$	4–0	4	×
$*b'c'd'$	8–0	8	×
$a'b'*d$	3–1	2	
$*b\ c'd'$	12–4	8	×
$a\ *c'd'$	12–8	4	×
$a'*c\ d$	7–3	4	×
$*b'c\ d$	11–3	8	×
$a\ b\ c'*$	13–12	1	
$*b\ c\ d$	15–7	8	×
$a\ *c\ d$	15–11	4	×
$a\ b\ *d$	15–13	2	

Fase 3

mint.	número	dif.
$*\ *c'd'$	12–8–4–0	(4,8)
$*\ *c'd'$	12–4–8–0	(8,4)
no hay		
$*\ *c\ d$	15–11–7–3	(4,8)
$*\ *c\ d$	15–7–11–3	(8,4)

Debido a que una expresión formada por el agrupamiento de cuatro mintérminos contiguos puede obtenerse de dos formas distintas, se obtienen en la tercera tabla todos los mintérminos por duplicado con diferente ordenación. De ellos solamente es necesario considerar uno, por ejemplo, aquel en que los mintérminos estan ordenados en orden decreciente.

Una vez obtenidas todas las tablas, consideramos todos los términos primos que no han sido marcados con una cruz; se denominan ***implicantes primos*** y son los que sumados van a formar parte de la fórmula simplificada de la función. En nuestro caso son

1–0, 3–1, 13–12, 15–13, 12–8–4–0, 15–11–7–3

Ahora es necesario elegir la mínima combinación de estos implicantes primos. Para ello seguiremos los siguientes pasos:

1) Construiremos una tabla con una columna para cada mintérmino de la forma normal original de la función y una fila por cada implicante primo.

implicantes primos		m_0	m_1	m_3	m_4	m_7	m_8	m_{11}	m_{12}	m_{13}	m_{15}
$a'\,b'\,c'$	1–0	×	×								
$a'\,b'\,d$	3–1		×	×							
$a\,b\,c'$	13–12								×	×	
$b\,c\,d$	15–13									×	×
$c'\,d'$	12–8–4–0	×			⊗		⊗		×		
$c\,d$	15–11–7–3			×		⊗		⊗			×

2) En la fila correspondiente a un determinado implicante primo, marcaremos la columna cuyo número de mintérmino está contenido en el del implicante.

3) Señalaremos las columnas que contengan una sola marca, ya que el implicante primo correspondiente será esencial, es decir, ha de formar parte de la función. Por tanto, todos los mintérminos incluídos en ese implicante primo esencial quedan realizados por este. En el ejemplo, los términos 12–8–4–0 y 15–11–7–3 son esenciales y por tanto, al formar parte de la expresión final, quedan realizados los mintérminos 0, 3, 4, 7, 8, 11, 12 y 15.

4) Elegiremos la combinación más sencilla de los implicantes primos restantes que realiza el resto de los mintérminos. Para ello realizaremos una tabla reducida, cuyas columnas son los mintérminos que todavía no han sido realizados y cuyas filas corresponden a los mintérminos primos no esenciales.

Como puede observarse, existen cuatro formas de combinar los mintérminos primos

1–0 y 13–12 1–0 y 15–13 3–1 y 13–12 3–1 y 15–13

y las expresiones más reducidas de la función son en nuestro caso

f = (12–8–4–0)+(15–11–7–3)+(1–0)+(13–12)

f = (12–8–4–0)+(15–11–7–3)+(1–0)+(15–13)

f = (12–8–4–0)+(15–11–7–3)+(3–1)+(13–12)

f = (12–8–4–0)+(15–11–7–3)+(3–1)+(15–13)

Finalmente obtendremos la fórmula de la función partiendo de las expresiones numéricas anteriores. Por tanto las fórmulas mínimas de la función son

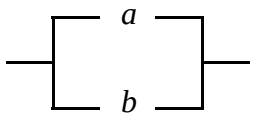
$$f(a,b,c,d) = c'd'+c\ d+a'b'c'+a\ b\ c'$$

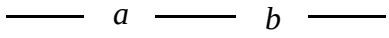
$$f(a,b,c,d) = c'd'+c\ d+a'b'c'+b\ c\ d$$

$$f(a,b,c,d) = c'd'+c\ d+a'b'd+a\ b\ c'$$

$$f(a,b,c,d) = c'd'+c\ d+a'b'd+b\ c\ d$$

Un caso particular de algebra de Boole binaria es la denominada ***algebra de circuitos***, base de toda la electrónica y de la cual vamos a ver sus primeros conceptos. Llamaremos ***interruptor*** a un dispositivo susceptible de dos estados: abierto, cuando no deja pasar una corriente eléctrica, que representaremos por 0, o cerrado, si deja pasar la corriente, que representaremos por 1. Dos interruptores *a* y *b* pueden conectarse de dos maneras:

en ***paralelo***, que representaremos por $a+b$: 

en ***serie***, que representaremos por $a\cdot b$: 

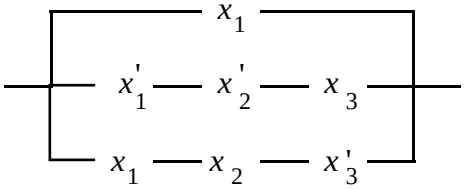
Según pase corriente a través de *a* o *b*, tenemos las siguientes situaciones

+	0	1
0	0	1
1	1	1

.	0	1
0	0	0
1	0	1

es decir, estamos en un álgebra de Boole binaria en la que el elemento 0 es el estado del interruptor que está siempre abierto, el 1 es el estado del interruptor que está siempre cerrado y para un interruptor x el complementario x' es aquel que está cerrado si x está abierto y viceversa. Una función booleana de n variables sobre esta álgebra es un conjunto de n interruptores, conectados en serie o en paralelo, formando lo que denominaremos un ***circuito eléctrico***, que deja pasar o no corriente según el estado de cada interruptor y de como han sido conectados. Recíprocamente, un circuito de n interruptores da lugar a una función booleana de n variables, denominada ***función de encendido***, que toma valores 0 o 1, para cada estado de sus interruptores, según pase corriente o no a través de él.

Ejemplo III.6.9

El circuito con tres interruptores 

tiene por función booleana asociada

$$f(x_1,x_2,x_3) = x_1+x_1'\cdot x_2'\cdot x_3+x_1\cdot x_2\cdot x_3'$$

cuya tabla de verificación es

x_1	x_2	x_3	$x_1 +$	$(((x_1' \cdot x_2') \cdot x_3) + ((x_1 \cdot x_2) \cdot x_3'))$								
0	0	0	0	1	1	1	0	0	0	0	0	1
0	0	1	1	1	1	1	1	1	1	0	0	0
0	1	0	0	1	0	0	0	0	0	0	0	1
0	1	1	0	1	0	0	0	1	0	0	0	0
1	0	0	1	0	0	1	0	0	0	0	0	1
1	0	1	1	0	0	1	0	1	0	0	0	0
1	1	0	1	0	0	0	0	0	1	1	1	1
1	1	1	1	0	0	0	0	1	0	1	0	0

que indica que pasar corriente a través del circuito en los casos

x_1	x_2	x_3
ab	ab	ce
ce	ab	ab
ce	ab	ce
ce	ce	ab
ce	ce	ce

donde ab significa abierto y ce cerrado

Dos circuitos son ***equivalentes*** si ambos dejan pasar o no corriente para los mismos estados de sus interruptores, por lo que tendrán la misma función de encendido. Simplificar un circuito es hallar otro equivalente a él más sencillo, para lo cual basta simplificar su función de encendido, como función booleana; para ello se sigue el proceso siguiente: 1) hallar la función de encendido, 2) simplificar esta función y 3) construir el circuito que represente la función simplificada

Ejemplo III.6.10

Una máquina indicadora de mayoría de votos se instala en una determinada compañía en la que existen un presidente y tres vicepresidentes; las decisiones se toman por mayoría simple, teniendo cada uno de ellos un voto y en caso de empate decide el voto del presidente. Se trata de diseñar un circuito eléctrico para tal máquina. Representando por x_1 el interruptor accionado por el presidente y por x_2,x_3,x_4 los correspondientes a los vicepresidentes, la función de encendido tendrá por tabla de verificación

x_1	x_2	x_3	x_4	f
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	0	0

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

y su expresión en mintérminos será

$$f = m_7+m_9+m_{10}+m_{11}+m_{12}+m_{13}+m_{14}+m_{15}$$

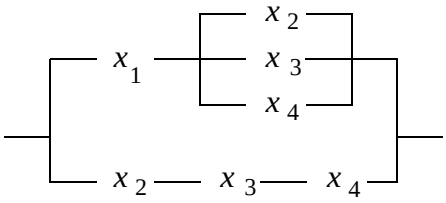
y el correspondiente diagrama de Karnaugh es

$x_3\,x_4$ \ $x_1\,x_2$	00	01	11	10
0 0			1	
0 1			1	1
1 1		1	1	1
1 0			1	1

la expresión simplificada

$$f = x_1\cdot x_3+x_1\cdot x_4+x_1\cdot x_2+x_2\cdot x_3\cdot x_4 = x_1\cdot(x_2+x_3+x_4)+x_2\cdot x_3\cdot x_4$$

y el circuito



Ejercicios

III.20.- Demostrar que el conjunto $S = \{a,b,c,d\}$ con las operaciones definidas por

$\cup$	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

$\cap$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

es un álgebra booleana.

III.21.- Simplificar, utilizando las propiedades del álgebra de Boole, las expresiones

a) $x_1+x_1'(x_2'x_3x_4+x_3'+x_4)+x_2x_4'$

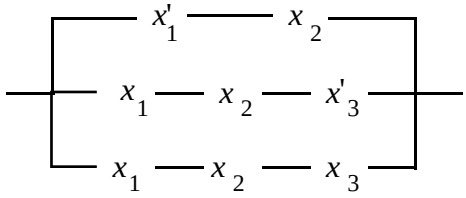
b) $x_1x_3'+x_2x_4+x_1x_3x_4'+x_2'x_4$

c) $(x_1x_1'+x_1x_2'+x_1'x_2'+x_2'x_2')(x_1'+x_2)$

Suponiendo que estas funciones pertenezcan al álgebra booleana de los circuitos, representar los circuitos simplificados.

III.22.- Un tribunal de exámenes está formado por tres miembros. El alumno aprueba por mayoria simple de votos. Si cada miembro del tribunal tiene ante sí un interruptor que lo aprieta si considera que el alumno debe aprobar, diseñar un circuito de modo que se encienda una lámpara si el alumno es aprobado. Escribir la tabla de verdad y el esquema lo más simplificado posible del circuito, razonándolo.

III.23.- Simplificar el siguiente circuito :



III.24.- Unos conmutadores *x* e *y* independientemente controlan una bomba inyectora de aceite para horno. Un tercer conmutador *z* está controlado por un par termoeléctrico de tal manera que se cierra automáticamente cuando el piloto se apaga. Diseñar un circuito para que con los conmutadores *x* o *y* se pueda conectar o desconectar la bomba, excepto que cuando el piloto esté apagado no pueda ser conectada.

EJERCICIOS DE RECAPITULACION

III.25.- La ley de composición de resistencias en paralelo es

$$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2}$$

averiguar que propiedades cumple.

III.26.- En la teoría de la relatividad restringida, la ley de composición de velocidades v_1, v_2 en la misma dirección viene dada por

$$v_1 \bullet v_2 = \frac{v_1 + v_2}{1 + \dfrac{v_1 v_2}{c^2}}$$

donde c es la velocidad de la luz. Estudiar sus propiedades.

III.27.- Probar que el conjunto $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ cuyos elementos son las aplicaciones

$$f_1(x) = x \qquad f_2(x) = 1 - x \qquad f_3(x) = \frac{x-1}{x}$$

$$f_4(x) = \frac{1}{x} \qquad f_5(x) = \frac{1}{1-x} \qquad f_6(x) = \frac{x}{x-1}$$

con f_i de $\mathbf{R} - \{0,1\}$ en $\mathbf{R}$, tiene estructura de grupo respecto la composición de aplicaciones.

III.28.- Estudiar la estructura $(\mathbf{R}, \bullet)$ con $x \bullet y = x + y - xy$. Para qué valores de a tiene solución la ecuación $x \bullet x = a$. Resolverla cuando sea posible.

III.29.- Demostrar que si en un grupo $(G, \bullet)$ se verifica

$$(\forall x \in G)\ (x \bullet x = e)$$

entonces G es abeliano.

III.30.- En el conjunto $\mathbf{Z}$ se define la siguiente operación:

$$a \bullet b = a + b - 3$$

Estudiar la estructura $(\mathbf{Z}, \bullet)$.

III.31.- Probar que $G =]-1,1[\subset \mathbf{R}$ es grupo respecto a la operación

$$x \bullet y = \frac{x + y}{1 + xy}$$

Estudiar las soluciones de la ecuación $x^2 = a$, con $a \in G$.

III.32.- Sea $(G,\cdot)$ un grupo. Definimos en G la relación binaria

$$a\ R\ b \text{ si y sólo si } (\exists x \in G)\ (a = x \cdot b \cdot x^{-1})$$

a) Demostrar que R es de equivalencia.

b) Estudiar si hay alguna clase de equivalencia que sea subgrupo.

c) ¿A qué se reduce R si el grupo es abeliano?.

III.33.- Demostrar que todo grupo con 4 elementos es conmutativo.

III.34.- Demostrar que si G es un grupo de n elementos, entonces $(\forall x \in G)\ (x^n = e)$.

III.35.- En el conjunto C de aplicaciones de **R** en **R** de la forma

$$F_a^{\,b}(x) = ax+b \quad \text{con } a \in \mathbf{R}^*$$

se define la operación

$$(F_c^{\,d} \circ F_a^{\,b})(x) = F_c^{\,d}\,(F_a^{\,b}(x))$$

Ver en qué casos forma grupo respecto de dicha operación

a) Si $a,b,c,d \in \mathbf{N}$.

b) Si $a,b,c,d \in \mathbf{Z}$.

c) Si $a,b,c,d \in \mathbf{Q}$.

Demostrar que las aplicaciones de la forma $F_1^{\,b}(x)$ forman un subgrupo de C.

III.36.- En **Z** definimos dos operaciones

$$a \bullet b = a+b-6 \qquad a \Delta b = ab+\alpha a+\alpha b+42$$

a) Encontrar el valor de α para que $(\mathbf{Z},\bullet,\Delta)$ sea anillo.

b) Averiguar si hay divisores de cero.

III.37.- Construir las tablas de sumar y multiplicar de los anillos **Z**/(5), **Z**/(6), **Z**/(8). Buscar los divisores de 0 y los elementos inversibles.

III.38.- Sea $\Omega = \{1,2\}$; sobre el conjunto $\mathcal{P}(\Omega)$ de las partes de Ω definimos las siguientes operaciones :

$$A \oplus B = (A \cup B) \cap (A \cap B)'$$
$$A \otimes B = A \cap B$$

a) Construir las tablas de sumar y multiplicar.

b) Estudiar la estructura $(\mathbb{P}(\Omega),\oplus,\otimes)$.

c) En el caso de ser anillo, buscar los ideales.

III.39.- Sea $(A,+,\cdot)$ un anillo conmutativo. En el conjunto $A\times A$ se definen las siguientes operaciones :

$$(a,b)\oplus(m,n) = (a+m,b+n)$$
$$(a,b)\otimes(m,n) = (am,0)$$

La estructura $(A\times A,\oplus,\otimes)$ ¿es un anillo?.

III.40.- En el conjunto $\mathbf{Q}\times\mathbf{Q}$ definimos las operaciones

$$(a,b)\oplus(c,d) = (a+c,b+d)$$
$$(a,b)\otimes(c,d) = (ac,bd)$$

a) Demostrar que $(\mathbf{Q}\times\mathbf{Q},\oplus,\otimes)$ es un anillo conmutativo con divisores de cero.

b) Demostrar que el conjunto $I = \{(a,0) \mid a\in\mathbf{Q}\}$ es un ideal.

III.41.- Sea $(A,+,\cdot)$ un anillo.

1) Si A no es conmutativo, averiguar el tipo de estructura que es $(\mathbf{Z}\times A,+,\cdot)$ con las operaciones

$$(m,a)+(n,b) = (m+n,a+b)$$
$$(m,a)\cdot(m,b) = (mn,mb+na+ab)$$

2) Si A es conmutativo, dado el elemento fijo $a\in A$, demostrar que el conjunto de elementos $I = \{x\in A \mid x\cdot a = 0\}$ es un ideal de A.

III.42.- Sea el anillo $\mathbf{Z}/(15)$ y los subconjuntos

$$A = \{\langle 0\rangle,\langle 5\rangle,\langle 10\rangle\} \qquad B = \{\langle 0\rangle,\langle 3\rangle,\langle 6\rangle,\langle 9\rangle,\langle 12\rangle\}$$

a) Averiguar si A y B son subanillos. ¿Son cuerpos?.

b) Siendo D el conjunto de los divisores de cero de $\mathbf{Z}/(15)$ y G el conjunto de los elementos de $\mathbf{Z}/(15)$ que son suma de dos elementos de D averiguar si $(G,\cdot)$ es grupo.

III.43.- Sea el conjunto $\mathbf{Z}\times\mathbf{Z}$ con las leyes

$$(x,y)\oplus(x',y') = (x+x',y+y')$$
$$(x,y)\otimes(x',y') = (xx',xy'+yx')$$

a) ¿Es anillo?. En caso afirmativo ¿qué tipo de anillo es?,¿tiene divisores de cero?,¿es cuerpo?.

b) El conjunto $A = \{(0,b) \mid b\in\mathbf{Z}\}$ ¿es un ideal?.

III.44.- Demostrar que si I_1 y I_2 son ideales de un anillo $(A,+,\cdot)$, su intersección $I_1\cap I_2$

también es un ideal.

III.45.- Sea $\mathbf{Z}(\sqrt{3}) = \{a+b\sqrt{3} \mid a,b \in \mathbf{Z}\} \subset \mathbf{R}$. Dar una condición suficiente para que un elemento de $\mathbf{Z}(\sqrt{3})$ sea inversible y la expresión del inverso, supuesta verificada la condición. Escribir algunos elementos inversibles distintos del 1.

III.46.- Sea el conjunto $\mathbf{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbf{Q}\}$

a) Demostrar que $\mathbf{Q}(\sqrt{2})$ es un cuerpo.

b) En $\mathbf{Q}(\sqrt{2})$ resolver la ecuación $z^2 = 22-12\sqrt{2}$.

III.47.- En un álgebra de Boole definimos la relación binaria

$$a \; R \; b \quad \text{si y solo si} \quad a+b = b$$

a) Demostrar que es de orden y hallar el primer y el último elemento.

b) Comprobar que

$$ab \; R \; a \quad \text{y} \quad bc \; R \; (ab+a'c)$$

c) Demostrar que

$$a \; R \; b \iff ab = a$$
$$a \; R \; b \iff a'+b = 1$$

d) En el caso del álgebra de Boole de $(\mathfrak{P}(E),\cup,\cap)$ la relación binaria definida anteriormente, ¿es alguna relación conocida?.

III.48.- Demostrar que si a,b,c son elementos de un álgebra de Boole que verifican

$$ab = ac \quad \text{y} \quad a+b = a+c \quad \text{entonces} \quad b = c$$

III.49.- En una habitación de tres estudiantes se desea instalar un circuito de interruptores que controle la luz del techo de la habitación, de tal forma que se encienda cuando lo decide la mayoría, es decir, cuando como mínimo dos estudiantes lo quieran. Diseñar el circuito.

III.50.- Un viajero desea atravesar un río con un lobo, una cabra y una col. En el bote caben él y uno de las otros tres, no pudiendo dejar sólos en una misma orilla ni a la cabra con la col ni al lobo con la cabra. Construir un circuito con cuatro interruptores de forma que se encienda una bombilla cuando se dé una situación no permitida. Extender el problema a tres hombres con sus tres mujeres que deben atravesar un río en una barca para dos personas, de forma que ninguna mujer esté sin su marido en compañía de otro hombre.

BIBLIOGRAFIA

Condamine M. (1971). *Algèbre*. Delagrave. París.

de Burgos J. (1988). *Curso de Algebra y Geometría*. Alhambra. Madrid.

Dixmier J. (1974). *Matemáticas Generales.* Editorial Aguilar. Madrid.

Godement R. (1974). *Algebra*. Tecnos. Madrid.

Hoffmann R., Kunze R. (1974). *Algebra Lineal*. Prentice. Madrid.

Lentin A., Rivaud J. (1973). *Algebra Moderna*. Aguilar. Madrid.

Noble B., Daniel J.W. (1988). *Applied Linear Algebra*. Prentice Hall. London.

Puerta F. (1986). *Algebra lineal*. Marcombo. Barcelona.

Queysanne M. (1985) *Algebra*. Vicens-Vives. Barcelona.

Rorres A., Anton H. (1979). *Aplicaciones del Algebra Lineal*. Limusa. Méjico.

Sainz M.A., Serarols J.L. Pérez A.M. (1994). *Álgebra*. Escuela Politécnica Superior. Gerona.

Strang G. (1982). *Algebra Lineal y sus aplicaciones.* Fondo Educativo Interamericano. Méjico.

Torregrosa J.R., Jordan C. (1987). *Algebra Lineal y sus aplicaciones*. McGraw-Hill. Madrid.

Whitsitt J.E.. (1975). *Algebra booleana y sus aplicaciones*. CECSA. Méjico.