ESTRUCTURAS ALGEBRAICAS

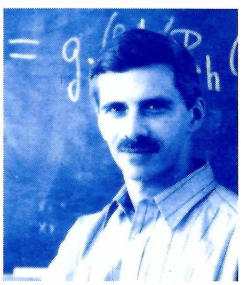
LIA OUBIÑA

Ejercicios

RUBEN ZUCCHELLO

Editorial Exacta

Lía Oubiña es Doctora en Matemática y ProfesoraTitular con dedicación exclusiva de la Facultad de Ciencias Exactas de la Universidad Nacional de La Plata, donde tiene a su cargo la cátedra de Estructuras Algebraicas para alumnos de la Licenciatura en Informática. Entre los años 1987 y 1990 fué Profesora de Algebra y Matemática Discreta en la Escuela Superior Latinoamericana de Informática.
Es autora del libro, Introducción a la Teoría de Conjuntos y de varios trabajos de investigación científica en Teoría de Grafos.

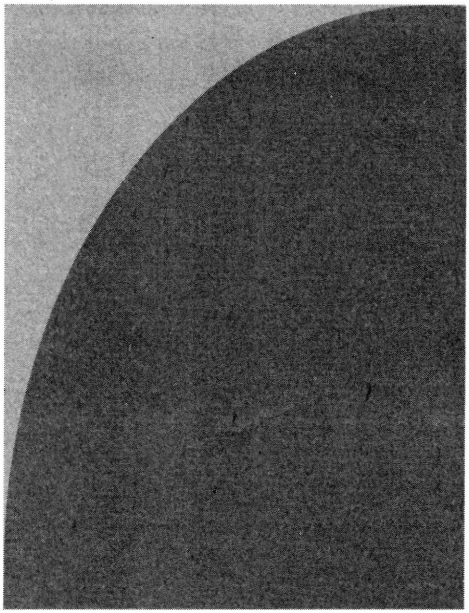


Rubén Zucchello es Licenciado en Matemática y Profesor Adjunto de la Facultad de Ciencias Exactas de la Universidad Nacional de La Plata, donde dicta un curso de Algebra para alumnos de la Licenciatura en Informática.
Durante cuatro años fué instructor de la Escuela Superior Latinoamericana de Informática. Es autor de varios trabajos de investigación científica en Teoría de Grafos.

ESTRUCTURAS ALGEBRAICAS

LIA OUBIÑA
Ejercicios
RUBEN ZUCCHELLO

Departamento de Matemática
Facultad de Ciencias Exactas
Universidad Nacional de La Plata



ESTRUCTURAS ALGEBRAICAS

LIA OUBIÑA

Ejercicios

RUBEN ZUCCHELLO

Primera edición, Marzo de 1994
I.S.B.N. 987-99858-1-8
Depósito que marca la ley 11.723
La Plata - República Argentina

Prólogo

El propósito de este libro es cubrir los tópicos algebraicos que, según los especialistas, son básicos en el actual desarrollo de la ciencia de la computación.

Tiene su origen en la experiencia adquirida por los autores durante el dictado del curso de Algebra en la Escuela Superior Latinoamericana de Informática, desde 1987 a 1990, y por la adquirida por L. Oubiña en el curso de Estructuras Algebraicas para alumnos de la Licenciatura en Informática de la Facultad de Ciencias Exactas de la Universidad Nacional de La Plata. Lía Oubiña es responsable del texto teórico y Rubén Zucchello de los ejercicios.

Puede ser utilizado en parte o en su totalidad por estudiantes de informática y también, como texto complementario, por estudiantes de matemática y de otras disciplinas que requieran el conocimiento de nociones algebraicas básicas.

Se suponen conocimientos previos de Teoría de Conjuntos en forma intuitiva, y los dados usualmente en un primer curso universitario de Algebra; se requiere además familiaridad con el razonamiento matemático.

Teniendo en cuenta las necesidades de los estudiantes y profesionales de informática se han introducido las estructuras algebraicas desde el punto de vista del Algebra Universal, lo que distingue a este texto de los clásicos sobre estructuras algebraicas. Partiendo del enfoque universal se estudian en particular los semigrupos, monoides, grupos y anillos.

Los apartados de cada capítulo, en su mayoría, están acompañados por varios ejemplos cuya lectura cuidadosa se recomienda ya que permiten comprender el significado de los conceptos abstractos. Incluyen además varios ejercicios que se consideran una parte importante del texto.

El capítulo 1 se refiere a las relaciones sobre conjuntos, especialmente a las binarias, sus representaciones por medio de digrafos y matrices booleanas, composición y propiedades.

El capítulo 2 trata las relaciones de orden, sus representaciones mediante diagramas de Haase, los conceptos básicos ligados a ellas (cadenas, elementos minimales y maximales, primero y último, supremo e ínfimo, etc.) que se usarán a menudo en capítulos subsiguientes. Se definen además los morfismos de conjuntos ordenados o aplicaciones crecientes.

El capítulo 3 introduce las relaciones de equivalencia en un conjunto explicitando su vínculo con las particiones; los "enteros módulo p" constituyen uno de los ejemplos más importantes ente los presentados. Se da la noción de función compatible con dos relaciones de equivalencia; situación que aparece reiteradamente en distintas estructuras algebraicas.

Los capítulos 4 y 5 contienen, respectivamente, las definiciones de reticulados y álgebras de Boole como conjuntos ordenados y luego sus presentaciones algebraicas, las subestructuras, productos y morfismos. Además el capítulo 4 contiene los semirreticulados y las propiedades básicas de los reticulados distributivos y complementados. El capítulo 5 incluye también la representación de las álgebras de Boole finitas.

El capítulo 6 introduce la noción de álgebra desde el punto de vista del Algebra Universal. Comienza aquí el estudio de los semigrupos, monoides, grupos, anillos y semianillos como álgebras especiales, estudio que continúa en los capítulos siguientes.

El capítulo 7 trata de las subálgebras y morfismos en general. Especial énfasis se da a las subálgebras generadas por un conjunto, en particular, se tratan los semigrupos, monoides y grupos cíclicos. Se dan además los teoremas tipo Cayley de representación de semigrupos, monoides y grupos.

El capítulo 8 se refiere a las álgebras cocientes y productos en general. Comienza con el estudio general de congruencias en un álgebra y continúa con el estudio de las congruencias en semigrupos, grupos, anillos y álgebras de Boole.

El capítulo 9 introduce las álgebras libres, se estudian en particular los semigrupos, monoides y grupos libres. Se definen los términos y el álgebra de los términos y se prueba que esta última es un álgebra libre.

Los autores expresan su agradecimiento a las autoridades y al personal de la Escuela Superior Latinoamericana de Informática quienes contribuyeron a que en un ámbito agradable y propicio fuera posible realizar la mayor parte del trabajo que dio origen al presente texto. Agradecen a la Fundación Ciencias Exactas la oportunidad que ha brindado para su publicación.

Lía Oubiña

Rubén Zucchello

Contenidos

Capítulo 1

Relaciones

En este capítulo se definen las relaciones n-arias y se tratan especialmente las binarias. Se muestra como se representa una relación binaria sobre un conjunto finito por medio de una matriz de ceros y unos y por medio de un grafo dirigido. Se definen la relación producto y la composición de relaciones binarias. Se muestra el vínculo entre la composición y el producto booleano de matrices. Se definen las propiedades de las relaciones y la clausura transitiva.

1.1. Producto cartesiano y relaciones.

1.1.1. **Definición.** Sean $A_1,\ldots, A_n$ conjuntos. El *producto cartesiano* de $A_1,\ldots,A_n$, denotado $A_1x\ldots xA_n$, es el conjunto de las n-uplas $(a_1,\ldots,a_n)$ tales que ai $\in$Ai, para todo i, i=1,...,n.
El elemento ai $\in$ Ai se denomina la *i-ésima coordenada* de $(a_1\ldots, a_n)$. Cuando Ai=A para todo i, entonces $A_1x\ldots xA_n$ se denota A^n.

1.1.2. **Definición.** Una *relación n-aria* sobre $A_1,\ldots,A_n$ es un subconjunto del producto cartesiano $A_1 x \ldots x A_n$.

Si R es una relación n-aria sobre $A_1,\ldots,A_n$ se llama *i-ésima* proyección p_i a la aplicación de R en Ai que a cada n-upla de R le asigna su i-ésima coordenada.

Las relaciones 2-arias se llaman también binarias. Si R es una relación binaria sobre A, B, se dirá también que R es una relación de A en B y si A=B se dirá que R es una relación en A o sobre A.

Si R es una relación binaria de A en B y el par $(a,b) \in R$ se dice que a está R relacionado con b y se escribe también aRb. El *dominio* de R es el conjunto de los elementos a de A tales que a está R relacionado con b, para algún b de B. Si X es un subconjunto de A, la *imagen de* X *por* R, denotada R(X), es el conjunto de los elementos b de B tales que, para algún a de X, a está relacionado con b. En particular, la imagen de A por R, o R(A), se llama simplemente *imagen de* R. Si X es un conjunto unitario, X= {x}, escribiremos R(x) en lugar de R({x}). El conjunto formado por los pares (b,a) tales que $(a,b) \in R$, denotado R^{-1}, es una relación binaria de B en A, llamada relación *inversa* de R.

Ejemplos

1.1.3. La relación identidad sobre A, denotada I_A, es el conjunto de los pares (a,a) para todo a $\in$A.

1.1.4. Sean A= { 2,3,4,5 }, B= { 2,6,7,8,12 } y R la relación de A en B dada por aRb si y sólo si a divide a b. El dominio de R es { 2,3,4 } y la imagen R(A) es { 2,6,8,12 }.

1.1.5. Sean A el conjunto de los alumnos de un curso, B el intervalo racional [0,10] y R la relación de A en B dada por : aRb si y sólo si a tiene promedio b. El dominio de R es A y un número b pertenece a R(A) si y sólo si algún alumno del curso obtuvo promedio b.

1.1.6. Sean A el personal de una empresa, B el conjunto de los cargos que existen en ella, C el conjunto de los números racionales positivos y R la relación 3-aria sobre A,B,C dada por: (a,b,c) $\in$ R si y sólo si a tiene el cargo b y percibe el sueldo c.

En lo sucesivo nos ocuparemos de relaciones binarias. La palabra relación indicará una relación binaria.

Las relaciones sobre conjuntos finitos se representan por medio de matrices de ceros y unos y también por medio de grafos dirigidos. Sea R una relación

de A en B, se toman los elementos de A y de B en un orden determinado: $a_1,...a_n$ y $b_1,...,b_m$ respectivamente, se construye la matriz r de n filas y m columnas en la siguiente forma: $r_{ij} = 1$ si a_i R b_j y $r_{ij} = 0$ en caso contrario. Se dirá que r es una matriz de la relación R.

Un *grafo dirigido o digrafo* G es un par ordenado G = (V,E) donde V es un conjunto y E es un subconjunto de VxV, o sea una relación en V. Los elementos de V se llaman vértices y los de E se llaman *arcos*. Si e = (a,b)∈E, se dice que a es el *extremo inicial* u *origen* de e y b el *extremo final*. Usualmente se representan los elementos de V por puntos del plano y un arco (a,b) por una flecha de a hacia b.

Si R es una relación de A en B se le asocia el digrafo G = (AUB , R).

Ejemplo

1.1.7. En el ejemplo 1.1.4 la matriz r asociada con la relación R es la siguiente matriz de 4 x 5.

	2	**6**	**7**	**8**	**12**
2	1	1	0	1	1
3	0	1	0	0	1
4	0	0	0	1	1
5	0	0	0	0	0

y el digrafo de la relación R es el de la figura 1.

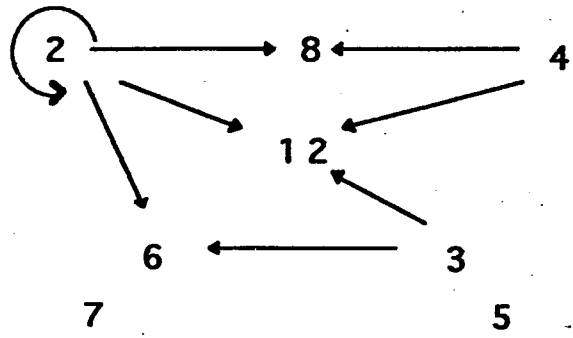


Fig. 1

Sea, para i=1,..., n, R_i una relación de A_i en B_i. La relación *producto*, denotada $R_1x \ldots xR_n$, es la relación de $A_1x \ldots xA_n$ en $B_1x \ldots xB_n$ dada por: $(a_1,\ldots a_n)\ R_1x \ldots xR_n\ (b_1,\ldots,b_n)$ si y sólo si, para todo i, i=1,...,n, $a_i\ R_i\ b_i$.

Ejercicios

1.1.8. Sea A = {1,2,3,4,5,6}, dada la relación R sobre A, en cada uno de los siguientes casos encontrar la imagen R(A), una matriz de la relación y el digrafo de la misma.

a) aRb si y sólo si a=b,

b) aRb si y sólo si a | b,

c) aRb si y sólo si a < b,

d) aRb si y sólo si a,b son coprimos.

1.1.9. En los siguientes casos encontrar la imagen de la relación R, una matriz de R y el digrafo de R.

a) Sean A={0,1,2}, B={0,2,4} y la relación R de A en B dada por aRb si y sólo si a.b $\in A \cap B$.

b) Sean A=$P(\{0,1\})$, B= $P(\{0,1,2\})$-$P(\{0\})$ y R la relación de A en B dada por aRb si y sólo si a-b=$\emptyset$.

1.1.10. Sea R una relación de A en B y sean E,F dos subconjuntos de A tales que $E \subseteq F$. Demostrar que $R(E) \subseteq R(F)$.

1.2. Composición de relaciones

1.2.1. **Definición**. Sean R una relación de A en B y S una relación de B en C. La *composición* de R y S, denotada RS, es la relación de A en C definida por

aRSc si y sólo si existe $b \in B$ tal que aRb y bSc.

Se comprueba inmediatamente que si R,S y T son relaciones de A en B, de B en C y de C en D, respectivamente, entonces (RS)T = R (ST) (ejercicio 1.2.6),

con lo cual escribiremos simplemente RST. Si R es una relación en A, pondremos R^2 = RR, y en general, R^n = R...R (n veces). De la definición resulta, por inducción sobre n, que aR^nb si y sólo si existen $x_1,...,x_{n-1}$, en A tales que $aR\,x_1R..Rx_{n-1}\,Rb$.

Ejemplos.

1.2.2. Sean A un conjunto de alumnos, B un conjunto de preguntas y C el intervalo [1,10]. Sea R la relación de A en B dada por: aRb si y sólo si a contestó correctamente la pregunta b y sea S la relación de B en C: bSc si y sólo si c es el puntaje asignado a la pregunta b. Entonces aRSc si y sólo si a contestó correctamente una pregunta de c puntos.

1.2.3. Sea A un conjunto y sean R y S las siguientes relaciones en el conjunto $P(A)$, de todas las partes de A: XRY si y sólo si $X\cap Y = \emptyset$, XSY si y sólo si $X\cup Y = A$. Entonces RS coincide con la relación de inclusión; en efecto, si X RS Z existe Y tal que $X\cap Y = \emptyset$ y $Y\cup Z = A$, con lo cual $Y\supseteq A-Z$, de donde, $X\subseteq Z$. Recíprocamente, si $X\subseteq Z$, tomando como Y a A-Z se obtiene que X RS Z.

1.2.4. Sea R la relación < en el conjunto Z de los números enteros (es decir, aRb si y sólo si a<b). Entonces aR^2c si y sólo si a < c-1.

La suma *booleana* en el conjunto {0,1} difiere de la suma ordinaria sólo en que 1+1=1. El producto *booleano* en el mismo conjunto coincide con el producto ordinario.

Si r y s son matrices de ceros y unos, r de m filas y n columnas y s de n filas y p columnas, el producto *booleano* de r por s es la matriz rs, nxp, dada por

$$(rs)_{ij} = \sum_{k=1}^{n} r_{ik} s_{kj}$$

donde los signos de suma y producto representan la suma y el producto booleanos respectivamente.

1.2.5. **Teorema**. *Sean* A, B *y* C *conjuntos finitos,* R, S *relaciones de* A *en* B *y de* B *en* C, *respectivamente, y r, s matrices correspondientes. Entonces, el producto booleano rs es una matriz de la composición* RS.

Demostración. Sean $A=\{a_1,\ldots,a_m\}$, $B=\{b_1,\ldots,b_n\}$, $C=\{c_1,\ldots,c_p\}$ y T=RS. Entonces, las siguientes proposiciones son equivalentes, lo que prueba el enunciado.

$a_i \, T c_j$

$(\exists k)$ ($a_i \, R b_k$ y $b_k \, S c_j$)

$(\exists k)$ ($r_{ik} = 1$ y $s_{kj} = 1$)

$(\exists k)\,(r_{ik}\, s_{kj} = 1)$

$$\sum_{h=1}^{n} r_{ih} s_{hj} = 1$$

$rs)_{ij} = 1$ ∎

Ejercicios

1.2.6. a) Probar que la composición de relaciones es asociativa, pero no es en general conmutativa.
b) Establecer si en general la composición de una relación $R \subseteq AxB$, con R^{-1} es la identidad en A.

1.2.7. Dadas las siguientes relaciones en A= { 0,1,2,3 },
R_1 = { (i,j); j=i+1 ó 2j=i }
R_2 = { (i,j) ; i=j+2 },
hallar las composiciones $R_1R_2, R_2R_1, R_1R_2R_1$.
Construir matrices de R_1, de R_2 y de las composiciones citadas.

1.2.8. Sean R,S,T relaciones en un conjunto A. Probar que si $R \subseteq S$, entonces $RT \subseteq ST$ y $TR \subseteq TS$.

1.2.9. a) Dadas R= {(0,1),(1,2),(3,4)} , RS= {(1,3),(1,4),(3,3)} encontrar una relación S de mínimo cardinal,
b) Establecer si, en general, dadas R y RS, la relación S queda determinada de manera única. Establecer si lo está cuando tiene cardinal mínimo.

1.3. Propiedades de las relaciones.

1.3.1. **Definición.** Sea R una relación en un conjunto A. Entonces
R es *reflexiva* en A si, para todo a $\in$ A, aRa.
R es *simétrica* en A si, para todo par a,b de elementos de A, aRb implica bRa.
R es *antisimétrica* en A si, para todo par a,b de elementos de A, aRb y bRa implica a=b.
R es *transitiva* en A si para toda terna a,b,c de elementos de A, aRb y bRc implica aRc.

Ejemplos

1.3.2. La relación < entre números naturales no es reflexiva, no es simétrica, es antisimétrica y es transitiva.

1.3.3. La relación " divide a" entre números naturales es reflexiva, no es simétrica, es antisimétrica y es transitiva.

1.3.4. La relación " es padre de" en un conjunto de personas tiene, en general, solamente la propiedad antisimétrica.

1.3.5. La relación de inclusión, entre las partes de un conjunto, es reflexiva, antisimétrica y transitiva.

1.3.6. La relación XRY si y sólo si $X \cap Y = \varnothing$, entre las partes de un conjunto dado, tiene, en general, solamente la propiedad simétrica.

1.3.7. La identidad, en un conjunto dado, tiene todas las propiedades definidas en 1.3.1.

Sea R una relación en un conjunto A. Entonces queda definida la sucesión de las potencias de R (1.2): $R=R^1, R^2,\ldots, R^n,\ldots$ y consecuentemente, la unión de todas esas potencias, que es también una relación en A. Pondremos:

$$[R] = U^{\infty}_{n=1} R^n,$$

1.3.8. **Teorema.** *Sea* R *una relación en un conjunto* A. *Entonces,* [R] *es una relación en* A, *transitiva, que contiene a* R. *Además, si* S *es una relación en* A, transitiva, que contiene a R,' *se tiene que* $[R] \subseteq S$.

Demostración. Sean a y b elementos de A tales que a[R]b y b[R]c. Luego, existen enteros m y n tales que $aR^m b$ y $bR^n c$, con lo cual, existen $x_1,\ldots,x_{m-1}$, $y_1,\ldots,y_{n-1}$, en A, tales que

$aRx_1R\ldots Rx_{m-1}Rb$ y $bRy_1R\ldots Ry_{n-1}Rc$,

con lo cual $aR^{m+n}c$. Entonces a[R]c.

Sea ahora S una relación transitiva tal que $R \subseteq S$ y sea a[R]b.

Entonces, existen $x_1,\ldots,x_n$ en A tales que $aRx_1R\ldots Rx_nRb$, con lo cual, también $aSx_1S\ldots Sx_nSb$. Por ser S transitiva, resulta aSb.

Luego $[R] \subseteq S$. ∎

En vista del resultado precedente, la relación [R] recibe el nombre de *clausura transitiva de* R.

Ejercicios

1.3.9. Sea X un conjunto no vacio, definir en $P(X)$ una relación:

a) reflexiva y no-transitiva,

b) no-reflexiva, simétrica y transitiva.

1.3.10. Establecer qué propiedades tienen las siguientes relaciones:

a) En el conjunto de los números naturales, nRm si y sólo si n.m >8.

b) En el conjunto P(S) de partes de un conjunto S, X R Y si y sólo si X∩Y es no vacío.

c) En el conjunto de los números reales, rTs si y sólo si r≤s.

d) En el conjunto de los números complejos, zRw si y sólo si $|z| < |w|$.

e) En el conjunto P(E) de partes de un conjunto E, A R B si y sólo si A y B se cortan propiamente (es decir si A∩B, A-B y B-A son no vacios).

1.3.11. Demostrar que una relación simétrica no es antisimétrica si y sólo si existen por lo menos un par de elementos distintos relacionados.

1.3.12. Sea p la propiedad: "aRb y cRb implica aRc" (dos elementos relacionados con un tercero están relacionados entre sí). Demostrar:

a) Si una relación es simétrica y transitiva, entonces tiene la propiedad p .

b) Si una relación es simétrica y tiene la propiedad p , entonces es transitiva.

1.3.13. Demostrar que si las relaciones R_i , para todo i=1,...,n, son todas reflexivas (respectivamente simétricas, antisimétricas, transitivas) entonces la relación producto $R_1 x ... x R_n$ también es reflexiva (respectivamente simétrica, antisimétrica, transitiva).

1.3.14. Sea R una relación en un conjunto A y sea B un subconjunto de A. Se dice que B es un conjunto *R-independiente* si para todo a,b ∈B, (a,b) no pertenece a R.

a) Probar que todo subconjunto de un conjunto R-independiente es también R-independiente.

b) Establecer si la intersección o la unión de conjuntos R-independientes es también R-independiente.

c) Sea R una relación en A tal que para todo a ∈ A , (a,a) no pertenece a R. Sea B un subconjunto R-independiente de A tal que no existe ningún subconjunto R-independiente de A que contenga propiamente a B.

Probar que para todo a ∈ A-B se cumple que (a,b) ∈ R o (b,a) ∈ R, para algún b ∈ B.

Capítulo 2

Relaciones de orden

En este capítulo se definen las relaciones de orden y de preorden, se muestra como se representa una relación de orden sobre un conjunto finito por medio de un diagrama de Hasse, se definen el orden producto y el orden lexicográfico, se da el vocabulario de las relaciones de orden y se definen los morfismos e isomorfismos de conjuntos ordenados.

2.1. Preorden y orden

2.1.1. **Definición.** Una relación binaria sobre un conjunto A es un *preorden* en A si es reflexiva y transitiva, y es un *orden* en A si es reflexiva, antisimétrica y transitiva.

Ejemplos

2.1.2. Sea A un conjunto de personas y R la relación en A dada por aRa´ si y sólo si la estatura de a es menor o igual que la estatura de a´, entonces R es un

preorden en A. Si en A hay un par de personas con la misma estatura, R no es un orden.

2.1.3. La relación $\leq$ usual entre los números naturales, enteros, racionales, reales, es un orden.

2.1.4. Si F es un conjunto de conjuntos, la inclusión es una relación de orden en F.

2.1.5. En un conjunto N de los números naturales la relación R dada por aRb si y sólo si a divide a b, que se denotará a | b, es un orden.

Una relación de orden se denotará generalmente con el símbolo $\leq$; si $a \leq b$ y $a \neq b$, se escribirá $a < b$.
Sea A un conjunto ordenado por $\leq$. Para $a, b \in A$ se dice que a *cubre a* b si $a > b$ y no existe c tal que $a > c > b$.
Si A es finito se representa el conjunto ordenado $(A,\leq)$ con el llamado *diagrama de Hasse*, construido en la siguiente forma: si $a > b$ se representan a y b mediante puntos del plano, el representante de a por encima del representante de b. Si a cubre a b se traza un segmento uniendo a y b.

Ejemplo

2.1.6. Sea A = { 1,2,3,4,5,6,8,9,10 } con la relación " divide a". El diagrama de Hasse de (A, |) se muestra en la fig. 2.

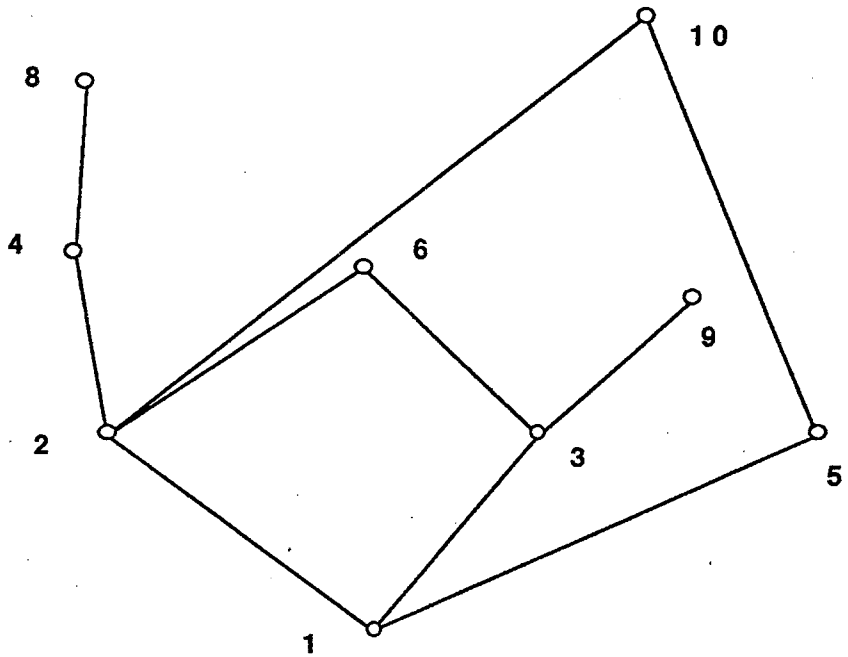


fig. 2

Si R_i es una relación de orden en un conjunto A_i , i=1,...,n, la relación producto $R_1 x... R_n$ es un orden en $A_1 x... A_n$ (ver 1.3.13.) que se llama *orden producto*..

Sea ahora L la relación sobre $A_1 x... xA_n$ definida por :

$(a_1,...,a_n)$ L $(b_1,...,b_n)$ si y sólo si $a_i = b_i$ para todo i, i=1,...,n ó $a_i R_i b_i$, siendo i el primer índice tal que $a_i \neq b_i$.

La relación L es un orden sobre $A_1 x...xA_n$ que se llama *producto lexicográfico* de $R_1,...,R_n$.

Ejercicio

2.1.7. Sea R una relación en un conjunto A y sea Δ_A la diagonal del producto cartesiano AxA. Demostrar que R es una relación de orden en A si y sólo si se verifican las siguientes condiciones:

(i) $R R = R$,

(ii) $R \cap R^{-1} = \Delta_A$.

2.2 Vocabulario de las relaciones de orden.

Si R es una relación de preorden (respectivamente de orden) la relación R^{-1} es un preorden (respectivamente un orden) y se llama *preorden opuesto* (respectivamente *orden opuesto*) a R.

Un *conjunto ordenado* es un par (A,≤) tal que ≤ es una relación de orden sobre A. Muchas veces se dirá que A es un conjunto ordenado sin mencionar la relación de orden.

Un *subconjunto ordenado* del conjunto ordenado (A,R) es un par (A´,R´) donde $A' \subseteq A$ y $R' = R \cap (A' \times A')$ (restricción de R a A´), se dice que A´ está ordenado por el orden *inducido* por el de A.

Dos elementos x e y de un conjunto ordenado (A,≤) se dicen *comparables* si se verifica $x \leq y$ o $y \leq x$, en caso contrario se dicen *incomparables*. Si todos los elementos de A son dos a dos comparables entonces se dice que A está *totalmente ordenado* y que ≤ es un *orden total* en A.

Sea (A,≤) un conjunto ordenado. Si a y b son elementos de A, el conjunto $\{x \in A ;\ a \leq x \leq b\}$ se llama *intervalo cerrado* de extremos a y b y se denota [a,b], el conjunto $\{ x \in A;\ a < x \leq b\}$ se llama *intervalo semiabierto a izquierda* y se denota (a,b] (en forma análoga se definen los intervalos

semiabiertos a derecha), y el conjunto $\{ x \in A; a < x < b \}$ se llama *intervalo abierto* y se denota (a,b).

Un subconjunto C de A es una *cadena* en A si C, con el orden inducido por el de A, está totalmente ordenado.

Un elemento $a \in A$ es *primer elemento* de A si para todo $x \in A$, $a \leq x$, y un elemento u de A es *último elemento* de A si para todo $x \in A$, $u \geq x$.

Un elemento m de A es *maximal* (respectivamente *minimal*) de A si no existe x en A tal que $x > m$ (resp. si no existe x en A tal que $x < m$).

Sea X un subconjunto de A. Un elemento k de A es *cota superior* (resp. *cota inferior*) de X en A si $k \geq x$ (resp. si $k \leq x$) para todo $x \in X$. El *supremo* de X (si es que existe) es el primer elemento del conjunto de las cotas superiores de X en A y el *ínfimo* de X (si es que existe) es el último elemento del conjunto de las cotas inferiores de X en A.

Ejemplos

2.2.1. Sea E un conjunto, $(P(E),\subseteq)$ no es totalmente ordenado, el conjunto vacío es el primer elemento y E es el último. En el subconjunto ordenado $(P(E) - \{\varnothing\},\subseteq)$ los elementos minimales son los conjuntos unitarios. En $(P(E) - \{E\},\subseteq)$ los elementos maximales son los conjuntos de la forma $E - \{x\}$, con $x \in E$.

2.2.2. Sea (N, |) el conjunto de los números naturales con el orden "divide a" y sea A = { 0,2,3,4,6,8,12 }. Tomando sobre A el orden inducido por el de (N, |), resulta que A no tiene primer elemento, su último elemento es 0, 2 y 3 son elementos minimales,
{ 2,4,8,0 } es una cadena contenida en A, 1 es el ínfimo de A en N.

2.2.3. Sea R el conjunto de los números reales. La relación de orden usual ≤ es un orden total, (R, ≤) no tiene ni primer ni último elementos.
La relación producto en RxR no es un orden total, por ejemplo los pares (2,3) y (4,1) son incomparables. El conjunto C = { (2,3) , (2,5), (3,6), (4,6) } es una cadena en RxR.
En la Fig. 3 se muestra un subconjunto X de RxR y los conjuntos de sus cotas superiores e inferiores. Los elementos de X son todos dos a dos incomparables, X no tiene ni primer ni último elemento y X tiene supremo s e ínfimo i.

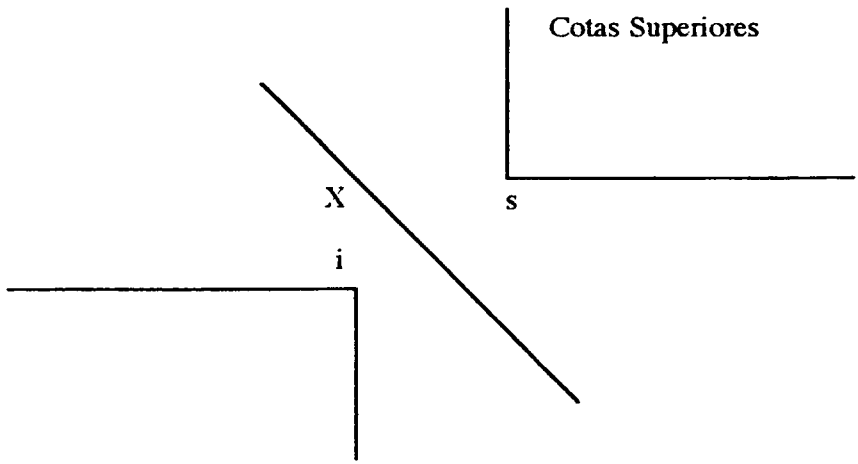


Fig. 3

Ejercicios

2.2.4. Sea A = { 1,2,3,4,5,6,7,8 } ordenado por la relación "divide a",

a) construir su diagrama de Hasse,

b) determinar los elementos maximales y los minimales de este conjunto ordenado,

c) Determinar las cotas superiores y las cotas inferiores del subconjunto C = { 2,3,5,6 }.

2.2.5. Sea (P , ≤) un conjunto ordenado y sea S un conjunto cualquiera.

Se define la relación & en el conjunto F de todas las funciones de S en P, por : f & g si y sólo si $f(s) \leq g(s)$, para todo $s \in S$.
Probar que $(F,\&)$ es un conjunto ordenado.

2.2.6. Sea (E,R) un conjunto ordenado y sean m un elemento maximal de E y k una cota superior de un subconjunto B de E. Demostrar que si E se ordena con la relación opuesta a R, entonces m es minimal y k es una cota inferior de B.

2.2.7. Sean E_1 , E_2 , E_3 subconjuntos de cardinal tres de un conjunto X tales que $E_i \cap E_j = \{x_0\}$ para todo i, j distintos, $1 \leq i , j \leq 3$, sean $E_4 = \{ x_0, x_1, x_2, x_3 \}$, donde $x_i \in E_i$, para i=1,2,3, y $X = E_1 \cup E_2 \cup E_3 \cup E_4$.
Demostrar que no existe ningún orden $\leq$ sobre X tal que cada E_i , i = 1,2,3,4, sea un intervalo cerrado de (X , $\leq$).

2.2.8. Sean a, b elementos de un conjunto ordenado (X , $\leq$), b cubre a a si $a< b$ y no existe $c \in X$ tal que $a < c < b$.
En un conjunto ordenado finito sea $a< b$. Demostrar que existe una sucesión $a = x_0 < x_1 \ldots < x_n = b$ tal que x_i cubre a x_{i-1} , para todo i, i = 1,... , n.
(**Indicación**: inducción sobre el cardinal de $\{ x; a< x < b\}$.)

2.2.9. Sea (E,≤) un conjunto ordenado y sea $X \subseteq E$. Demostrar que si un elemento de X es cota superior de X, éste es un elemento maximal de X con el orden inducido por el de E.
Establecer si vale el enunciado recíproco.

2.2.10. Sea R_i una relación de orden en A_i para i = 1,...,n.
a) Probar que la relación producto $R_1 x \dots x R_n$ es un orden en $A_1 x \dots x A_n$.
b) Recíprocamente, probar que si para todo i, i = 1,...,n A_i no es vacío, y la relación producto es un orden en $A_1 x \dots x A_n$, entonces R_i es un orden en A_i , para todo i.
c) Sea L el producto lexicográfico de $R_1,\dots,R_n$. Probar que si para todo i,R_i es un orden total, entonces L es un orden total.

2.2.11.Sea H_i, i = 1,2, el diagrama de Hasse de un conjunto ordenado (A_i, R_i) y sea L el producto lexicográfico de R_1, R_2. Probar que el diagrama de Hasse de L se obtiene de la siguiente forma:
1) Reemplazar cada vértice j de H_1 por una copia H^j_2 de H_2 , obtenida cambiando cada vértice x de H_2 por el par (j,x),
2) Si k cubre a j en el orden R_1 unir por un segmento todo par de vértices de la forma (j,x), (k,y), donde x, y pertenecen a A_2.

2.2.12. Sea E un conjunto finito y sea F un subconjunto del conjunto de partes de E. El par (E,F) es un *antimatroide* si F satisface las propiedades siguientes:

(i) $\varnothing$ pertenece a F ,

(ii) Si X es no vacío y X pertenece a F , entonces existe $x \in X$ tal que X-{x} pertenece a F

(iii) La unión de elementos de F pertenece a F .

Sea (E, $\leq$) un conjunto ordenado, $X \subseteq E$ es un *ideal superior* de $(E,\subseteq)$ si para todo $x \in X$, para todo y $\in E$, $y \geq x$ implica $y \in X$.

Sea $(E,\subseteq)$ ordenado y finito , sea F el conjunto de ideales superiores de $(E,\subseteq)$, probar que (E,F) es un antimatroide.

2.3. Morfismos de conjuntos ordenados.

2.3.1. **Definición.** Sean A y B conjuntos ordenados, las relaciones de orden se denotan ambas con $\leq$ aunque pueden ser distintas. Un *morfismo de orden* de A en B es una aplicación f de A en B tal que para todo par a,a´ de elementos de A, $a \leq a'$ implica $f(a) \leq f(a')$. Los morfismos de conjuntos ordenados se llaman también aplicaciones crecientes o monótonas crecientes.

Un *isomorfismo de orden* f de A en B es una aplicación biyectiva f de A en B tal que para todo par a, a´ de elementos de A, se verifica que $a \leq a'$ si y solamente si $f(a) \leq f(a')$.

Se prueba fácilmente que si f es un isomorfismo de orden, entonces f^{-1} también lo es, (ejercicio (2.3.3.)).

Los conjuntos ordenados A y B son *isomorfos* si existe un isomorfismo (de orden) de A en B. Se escribirá $A \approx B$.

Sean A un conjunto, (B, $\leq$) un conjunto ordenado y f una biyección de A en B. Se define en A la relación R dada por : aRa´ si y sólo si $f(a) \leq f(a')$. Resulta que R es un orden en A, llamado orden *inducido* por $\leq$ f(a´). Resulta que R es un orden en A, llamado orden *inducido* por $\leq$ a través de f, y que f es un isomorfismo de orden de (A,R) en (B,$\leq$). La demostración queda propuesta como ejercicio (2.3.4.)

Ejemplo

2.3.2. La aplicación f (n) = n´ entre los conjuntos ordenados representados por los siguientes diagramas de Hasse es creciente y biyectiva pero no es un isomorfismo:

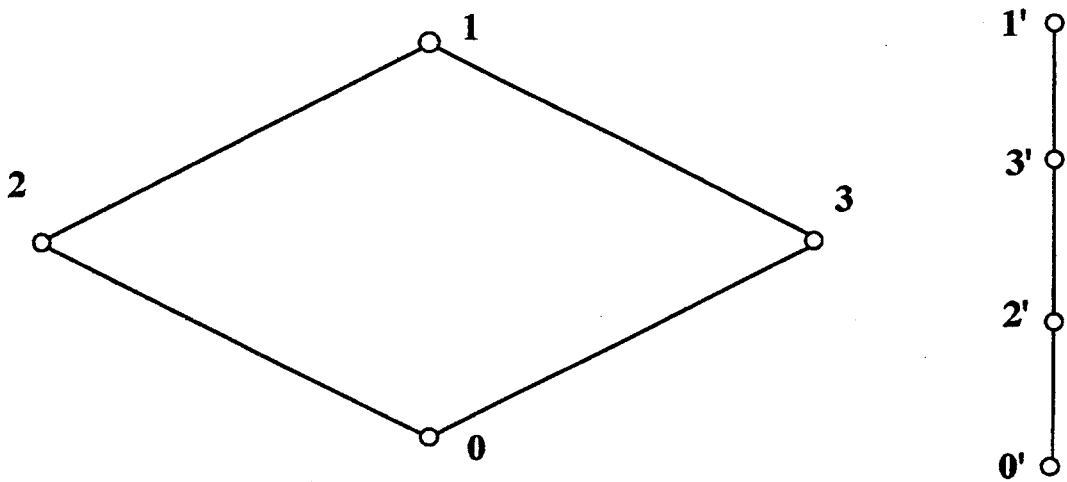


Fig. 4

En cambio si f es una aplicación de A en B creciente, biyectiva y ambos conjuntos están totalmente ordenados, entonces f es un isomorfismo (ejercicio (2.3.5.)).

Ejercicios

2.3.3. Sea f un isomorfismo de orden de A en B, probar que f^{-1} también es un isomorfismo de orden.

2.3.4. Sean A un conjunto, (B,≤) un conjunto ordenado, f una biyección de A en B y R la relación en A dada por aRa´ si y sólo si f(a) ≤ f(a´). Demostrar que R es un orden en A y que f es un isomorfismo de orden de (A,R) en (B,≤).

2.3.5. Sean A y B dos conjuntos totalmente ordenados y sea f de A en B una biyección creciente. Demostrar que f es un isomorfismo de orden entre A y B.

2.3.6. Sean A y B conjuntos ordenados, isomorfos entre si.
Demostrar:
a) A está totalmente ordenado si y sólo si B lo está.
b) *a* es primer elemento (resp. último elemento) de A si y sólo si f (*a*) es primer (resp. último) elemento de B.
c) *m* es un elemento maximal (resp. minimal) en A si y sólo si f(m) es maximal (resp. minimal) en B.

d) k es cota superior (resp. inferior) de $X \subseteq A$ si y sólo si $f(k)$ es cota superior (resp. inferior) de B.

Capítulo 3

Relaciones de equivalencia y particiones

El concepto de relación de equivalencia es de suma importancia para la matemática y sus aplicaciones. En este capítulo se definen las relaciones de equivalencia y se da la noción de conjunto cociente explicitando su vínculo con las particiones. Se introducen las relaciones de equivalencia que permiten definir los enteros módulos p y caracterizar las relaciones de preorden. Se da finalmente la noción de función compatible con dos relaciones de equivalencia, una en su dominio y otra en su codominio, lo que permite introducir una función por el llamado " pasaje al cociente".

3.1. Relaciones de equivalencia

3.1.1. **Definición.** Una relación binaria sobre un conjunto A es de *equivalencia* en A si es reflexiva, simétrica y transitiva.

En lo sucesivo designaremos frecuentemente a una relación de equivalencia con el signo ~.

Ejemplos

3.1.2. La relación de paralelismo en el conjunto de las rectas del plano es de equivalencia.

3.1.3. Se dice que un conjunto X es *coordinable* con un conjunto Y si existe una biyección de X sobre Y. La relación de coordinabilidad es de equivalencia en cualquier conjunto de conjuntos.

3.1.4. Sea p un número entero. Se dice que un entero x es *congruente módulo p* con un entero y si x-y es un múltiplo de p. La congruencia módulo p es de equivalencia en el conjunto Z de los números enteros.

3.1.5. Sea f una función de A en B. La relación en A: aRa´ si y sólo si f(a) = f(a´), llamada *asociada a f*, es de equivalencia.

3.1.6. Sea S un preorden en un conjunto A (2.1.1.). La relación en A: aRa´ si y sólo si aSa´ y a´Sa es de equivalencia. La llamaremos *asociada al preorden S*.

Ejercicios

3.1.7. Establecer si alguna de las relaciones binarias definidas en (1.1.8.) es una equivalencia.

3.1.8. Sea R una relación reflexiva. Probar que R es una equivalencia si y sólo si RR=R y $R=R^{-1}$.

3.1.9. Sea R una relación reflexiva y transitiva, probar que $R \cap R^{-1}$ es una equivalencia.

3.1.10. Sean R y S equivalencias sobre un conjunto E, probar que $R \cap S$ es una equivalencia sobre E.

3.1.11. Sean K un cuerpo, K^{mxn} el conjunto de matrices de m filas y n columnas a coeficientes en K y R la relación en K^{mxn} dada por A R B si y sólo si B se obtiene aplicando un número finito de operaciones elementales sobre las filas de A. Probar que R es una equivalencia.

3.2. Conjunto cociente y particiones.

3.2.1. **Definición.** Sean R una relación de equivalencia en un conjunto A y $a \in A$. El conjunto $R(a) = \{b \in A; aRb\}$ se llama la *clase de equivalencia de a por* R; cualquier elemento de R(a) se llama *representante* de esa clase. El conjunto $\{ R(a) ; a \in A \}$, denotado A/R, es el *conjunto cociente* de A por R. La función ρ de A en A/R que asigna a cada elemento de A su clase de equivalencia es la *aplicación canónica* de A en A/R.
Denotaremos, cuando resulte conveniente, $[a]_R$, o simplemente [a], si R está sobrentendida, a la clase de equivalencia, R(a), de a por R.
La aplicación canónica de A en A/R es evidentemente suryectiva.

3.2.2. **Definición.** Una partición de un conjunto A es un conjunto de partes no vacías de A, disjuntas dos a dos y tales que su unión coincide con A.

Sea π una partición de A. Definimos sobre A la siguiente relación R: aRb si y sólo si existe $X \in \pi$ tal que $a,b \in X$. Es inmediato que R es reflexiva y simétrica. Para comprobar la transitividad, sean aRb y bRc. Entonces existen $X,Y \in \pi$ tales que $a,b \in X$ y $b,c \in Y$. Luego $b \in X \cap Y$, con lo cual debe cumplirse $X = Y$.
Por lo tanto aRc. La relación R es entonces de equivalencia ; la llamaremos *asociada a la partición* π.

3.2.3. **Lema.** *Sea R una relación de equivalencia en un conjunto* A. *Entonces para todo par a , b de elementos de A, R(a) = R(b) si y sólo si aRb.*
Demostración. Supongamos R(a) = R(b) . Por ser R reflexiva b $\in$ R(b), luego b $\in$ R(a), de donde aRb.
Recíprocamente, supongamos aRb y sea z un elemento de R(a), es decir aRz. Por la simetría y la transitividad de R se tiene zRb, con lo cual bRz y, por lo tanto, z $\in$ R(b). Entonces $R(a) \subseteq R(b)$.
En la misma forma se prueba la inclusión inversa. ∎

3.2.4. **Teorema.** *Si R es una relación de equivalencia sobre un conjunto A, entonces el conjunto cociente, A/R, es una partición de A.*
Demostración. Cada clase R(a) es no vacía puesto que a $\in$ R(a).
Si z $\in$ R(a) $\cap$ R(b), resulta aRz y bRz, de donde se obtiene aRb.
Entonces, por el lema precedente, R(a) = R(b). Puesto que cada elemento de A pertenece a su clase de equivalencia, la unión de todas las clases es el conjunto A. ∎

En el teorema siguiente E_A designa el conjunto de todas las relaciones de equivalencia sobre un conjunto A y Π_A el conjunto de todas las particiones de A.

3.2.5. **Teorema** *La aplicación, que a cada relación de equivalencia, R, sobre un conjunto A le asigna el cociente A/R es una biyección de* E_A *sobre* Π_A .

Demostración. Llamemos φ a la aplicación del enunciado, es decir, para toda relación $R \in E_A$, $\varphi(R) = A/R$.

Supongamos que R y R´ son relaciones de equivalencia en A tales que φ(R) = φ(R´). Sean a y b elementos de A tales que aRb.

Puesto que $R(a) \in A/R = A/R'$, existe z en A tal que R(a) = R´(z).

Como $a \in R(a)$, $a \in R'(z)$, es decir, aR´z. Teniendo en cuenta que R(a) = R(b), se obtiene también bR´z, de donde, aR´b. En forma análoga se demuestra que aR´b implica aRb, con lo cual, R = R´. La aplicación φ es entonces inyectiva.

Resulta inmediatamente que φ es suryectiva, considerando, para una partición π de A la relación de equivalencia asociada. ∎

Ejemplos

3.2.6. Si *F* es un conjunto de conjuntos finitos cada clase de equivalencia por la relación de coordinabilidad de 3.1.3. se compone de los conjuntos de *F* que tienen el mismo número de elementos.

3.2.7. **Enteros módulos p**. Como se mencionó en 3.1.4. la relación en Z, a ≡ b (mód p) si y sólo si a-b es un múltiplo de p, es de equivalencia, para todo entero p. Cada clase de equivalencia es un *entero módulo p* . El conjunto cociente será denotado Zp.

Puesto que evidentemente, la congruencia módulo p coincide con la congruencia módulo -p, es suficiente considerar p ≥0. La congruencia módulo 0 es la igualdad en Z. Para p≥1, Z_p tiene exactamente p elementos: las clases de 0,...,p-1. En efecto, si a,b ∈ { 0,..., p-1}, | a-b | <p, de donde, a y b no son equivalentes. Dado z no perteneciente a { 0,...,p-1}, efectuando el cociente de z por p, se encuentran q y r enteros, 0 ≤ r ≤ p-1, tales que z = p. q+r. Entonces z-r = p.q, con lo cual z ≡ r (mód p).

3.2.8. Sean f una función de A en B y ~ la relación de equivalencia asociada a f (3.1.5). Queda determinada una función f´ de A/ ~ en B que asigna a la clase [a] el elemento f(a), puesto que, si a´~ a, f(a) = f(a´). La función f´ es evidentemente inyectiva.

3.2.9. Sean S un preorden en un conjunto A y ~ la relación de equivalencia asociada a S. Se tiene que si aSb, a ~ a´ y b ~ b´, entonces a´Sb´. Esto permite definir una relación ≤ en A/ ~ poniendo: [a]≤[b] si y sólo si aSb. Es fácil comprobar que ≤ es un orden, y que el preorden S queda caracterizado en la forma siguiente: aSb si y sólo si ρ(a) ≤ ρ(b). Recíprocamente, si f es una

función de un conjunto A en un conjunto B, ordenado por $\leq$, la relación S en A dada por aSa´ si y sólo si f(a)$\leq$ f(a´) es un preorden en A. Puede decirse entonces que una relación S en un conjunto A es un preorden, si y sólo si existe un conjunto ordenado (B,$\leq$) y una función f: A $\rightarrow$ B tales que aSb si y sólo si f(a) $\leq$ f(b).

Sean π y π' particiones de un conjunto A. Se dice que π *refina* a π' si, para todo conjunto X perteneciente a π existe X´, perteneciente a π' tal que $X \subseteq X'$. Es evidente que esta relación es reflexiva y transitiva. Veamos que es también antisimétrica: Supongamos que π refina a π' y que π' refina a π. Si $X \in \pi$, existe $X' \in \pi'$ tal que $X \subseteq X'$, y también, existe $Y \in \pi$ tal que $X' \subseteq Y$. Luego $X \subseteq Y$, de donde X=Y. Luego la relación "refina a" es un orden en el conjunto Π_A de todas las particiones de A.

3.2.10. **Teorema.** *La aplicación que a cada clase de equivalencia R sobre un conjunto A le asigna el cociente A/R es un isomorfismo de* E_A. *ordenado por inclusión,* sobre Π_A, *ordenado por refinamiento* (ver 3.2.5).

Demostración. Sean R y R´ relaciones de equivalencia tales que $R \subseteq R'$. Si b $\in$ R(a) entonces b $\in$ R´ (a), de donde, A/R refina a A/R´.
Recíprocamente, si A/R refina a A/R´y (a,b) $\in$ R, resulta que existe z $\in$ A tal que R(a) = R(b) $\subseteq$ R´(z), con lo cual, aR´z y bR´z, de donde, (a,b) $\in$ R´.

Entonces $R \subseteq R'$. ∎

Ejercicios

3.2.11. Sean R la relación en ZxZ dada por (a,b) R(c,d) si y sólo si a.d = b.c. Probar que R es una equivalencia.
Por definición se llama número racional a cada clase de equivalencia según R de los elementos de ZxZ.

3.2.12. Sean **R** el conjunto de los números reales y f la función de **R** en **R** definida por:

$$f(x) = \begin{cases} 3x, \text{si } x \leq -1 \\ 9, \text{si } -1 < x \leq 2 \\ x, \text{si } x > 2 \end{cases}$$

y sea S la equivalencia asociada con f. Encontrar las clases de equivalencia.

3.2.13. Sea f una función y A su dominio. Probar que para todo $x \in A$, la clase de equivalencia de x según la relación de equivalencia asociada con f es $f^{-1}(f(x))$.

3.2.14. Sean R una equivalencia en un conjunto X y S una equivalencia en el conjunto cociente X/R. Se define T en X por : xTy si y sólo si R(x) S R(y).
a) Demostrar que T es una equivalencia en X, que contiene a S.
b) Expresar la clase de equivalencia por T de x $\in$X en función de R y S.

3.3 Aplicaciones compatibles con relaciones de equivalencia.

3.3.1. **Definición**. Sean f una aplicación de A en B, R una relación de equivalencia sobre A y S una relación de equivalencia sobre B.
Se dice que f es *compatible* con R y S si, para todo par a,a´ de elementos de A, aRa´ implica f(a) S f(a´).

3.3.2. **Teorema.** *Sean f una función de A en B, R una relación de equivalencia sobre A y S una relación de equivalencia sobre B.*
Entonces, f es compatible con R y S si y sólo si existe una aplicación g de A/R en B/S tal que $\rho_B \circ f = g \circ \rho_A$, *donde* ρ_A y ρ_B *designan las aplicaciones canónicas de A en A/R y de B en B/S respectivamente.*

Demostración. Si f es compatible con R y S queda bien definida la aplicación g de A/R en B/S que asigna a la clase R(a) la clase S(f(a)). Es evidente que g cumple con las condiciones pedidas en el enunciado.
Recíprocamente, supongamos que existe g en esas condiciones. Si aRa´, $\rho_A(a) = \rho_A(a')$ y puesto que $g(\rho_A(a)) = \rho_B(f(a))$ y $g(\rho_A((a')) = \rho_B(f(a'))$, resulta f (a) S f (a´). ∎

Si f es compatible con R y S , la aplicación g del teorema precedente es evidentemente única; la denotaremos f´. La igualdad $f' \circ \rho_A = \rho_B \circ f$ se expresa también diciendo que el diagrama siguiente es conmutativo.

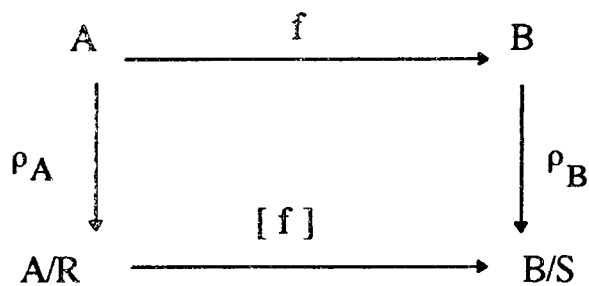


Fig. 5

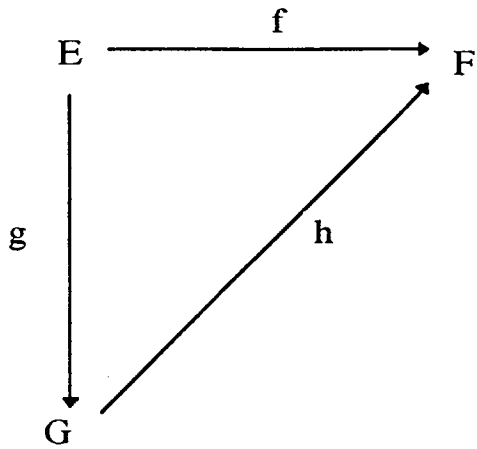
3.3.3. **Corolario.** *Sean f una función de A en B y R una relación de equivalencia sobre A. Entonces R es la relación de equivalencia asociada a f (3.1.5) si y sólo si existe una aplicación g de A/R en B tal que* $f = g\rho_A$.

Demostración. El enunciado resulta del teorema precedente teniendo en cuenta que R es la relación de equivalencia asociada a f si y sólo si f es compatible con R y con la identidad sobre B. ∎

Ejercicios.

3.3.4. Sean E un conjunto , A una parte de E, f la aplicación de $P(E)$ en $P(E)$ dada por $f(X) = X \cap A$ y R la equivalencia asociada con f.
Probar que existe una biyección de $P(A)$ en $P(E)/R$.

3.3.5. Sean E y F dos conjuntos y f una función de E en F. Hallar un tercer conjunto G, una suryección g de E en G y una inyección h de G en F tales que el siguiente diagrama conmute:



3.3.6. Sean E y F dos conjuntos y R la equivalencia en ExF asociada a la proyección p_1 de ExF en E. Encontrar las clases de equivalencia según R y una biyección de E en (ExF)/R.

3.3.7. Sean R, S equivalencias en los conjuntos E,F respectivamente.

a) Probar que RxS es una equivalencia en ExF. (ver (1.3.13)).

b) Demostrar que (RxS) (x,y) = R(x) x S(y).

c) Si u y v son las aplicaciones canónicas de E en E/R y de F en F/S respectivamente, demostrar que la extensión canónica uxv a los conjuntos productos es compatible con RxS.

d) Demostrar que la aplicación inducida por uxv por pasaje al cociente es una biyección de (ExF)/RxS en (E/R)x(F/S).

Capítulo 4

Reticulados

En este capítulo se introducen los conceptos y resultados de la teoría de reticulados que desempeñan un rol importante en los capítulos siguientes. Se introducen los reticulados como conjuntos ordenados, y luego se los presenta desde el punto de vista algebraico. Se tratan someramente los reticulados distributivos y los distributivos y complementados. Se dan definiciones y ejemplos relativos a los reticulados atómicos y supatómicos.

4.1. Definición y propiedades generales.

Sean (A,≤) un conjunto ordenado y a,b elementos de A. El conjunto de las cotas superiores de {a,b} en (A,≤) puede ser o no vacío; si no es vacío puede suceder que tenga o no primer elemento; si lo tiene, entonces es único y se lo llama *supremo* en (A,≤) del conjunto {a,b}. En forma análoga se define el *ínfimo* en (A,≤) de {a,b}, si es que existe.

4.1.1. **Definición.** Un *reticulado* es un conjunto ordenado (L,≤) tal que, para todo par a,b, de elementos de L existen el supremo y el ínfimo de {a,b} en (L,≤).

Denotaremos sup(L,≤) {a,b} e inf(L,≤) {a,b} al supremo y al ínfimo, respectivamente, de {a,b} en (L,≤). Si (L,≤) está sobreentendido se los designará con avb y a∧b respectivamente.

Entonces a v b queda caracterizado por las propiedades siguientes:

$$a \leq avb \text{ y } b \leq avb$$

para todo s tal que a≤s y b≤s, se cumple avb≤s.

Similarmente, las propiedades que caracterizan a∧b son:

$$a \wedge b \leq a \text{ y } a \wedge b \leq b$$

para todo i tal que i≤a y i≤b, se cumple i≤a∧b.

En particular, resulta que si a≤b entonces avb = b y a∧b = a.

Ejemplos

4.1.1. Todo conjunto totalmente ordenado es un reticulado, siendo avb el máximo entre a y b , y a∧b el mínimo entre a y b.

4.1.2. Si E es un conjunto entonces el conjunto $P(E)$ de las partes de E, ordenado por inclusión, es un reticulado, siendo AvB = A∪B y A∧B = A∩B.

4.1.3. Como caso particular del ejemplo precedente se tiene que el conjunto $R_A = P(AxA)$ de las relaciones binarias sobre un conjunto A, ordenado por inclusión, es un reticulado.

4.1.4. El conjunto E_A de las relaciones de equivalencia sobre A, ordenado por inclusión, es también un reticulado, con la diferencia de que, para las relaciones de equivalencia R y R´, RvR´ es la clausura transitiva de R∪R´ (1.3.8) ya que, en general, R∪R´ no es transitiva. Puesto que la intersección de relaciones de equivalencia es de equivalencia, R∧R´ = R∩R´.

4.1.5. Si f es un isomorfismo de un conjunto ordenado (A,≤) sobre (B,≤) y si (A,≤) es un reticulado, es fácil verificar que (B,≤) también es un reticulado y que, para a,a´∈A, f(ava´) = f(a) v f(a´) y f(a∧a´) = f (a) ∧ f(a´). Teniendo en cuenta que (E_A,⊆)es isomorfo a Π_A, ordenado por refinamiento (3.2.10), resulta que Π_A es un reticulado tal que, si π y π' son particiones correspondientes a las relaciones de equivalencia R y R´, respectivamente, entonces $\pi v \pi' = A/[R \cup R']$ y $\pi \wedge \pi' = A/R \cap R'$.

4.1.6. El conjunto (N,|), de los números naturales ordenado por la relación "divide a" (2.1.5) es un reticulado, siendo avb el mínimo común múltiplo de a y b, y a∧b el máximo común divisor de a y b.

4.1.7. El conjunto ordenado definido por el diagrama de Hasse de la figura siguiente no es un reticulado. En efecto, el conjunto de las cotas superiores de {2,3} es {4,5,1} pero este conjunto no tiene primer elemento.

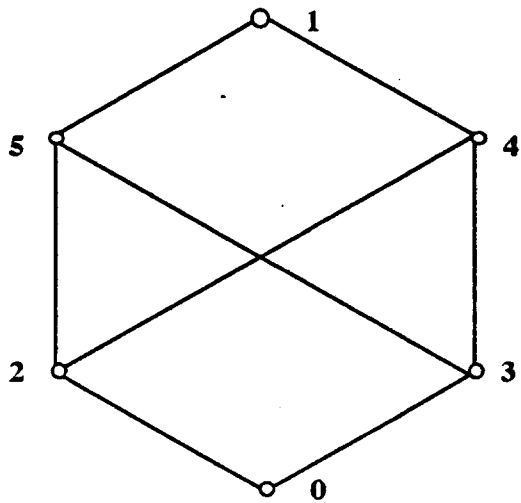


Fig. 6

4.1.8. Una *n-anticadena*, para un número natural $n \geq 1$, es un conjunto ordenado formado por n elementos incomparables dos a dos, un primer elemento y un último elemento. Entonces, toda anticadena es un reticulado. Denotaremos M_n a una n-anticadena. La figura siguiente muestra el diagrama de Hasse de M_3.

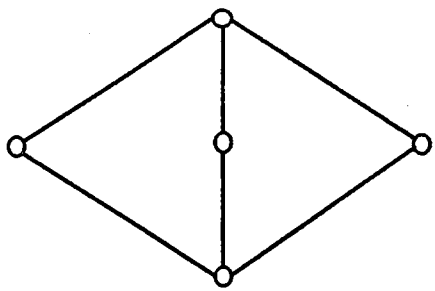


Fig . 7

4.1.9. Una *n-grilla* , para un número natural n≥1, denotada G_n, es un conjunto ordenado isomorfo al conjunto, ordenado por inclusión, de todos los intervalos de {1,...,n} con el orden usual. Es inmediato comprobar que G_n es un reticulado con primero y último elemento. El ínfimo de los intervalos A y B es A∩B; el supremo es A∪B, siempre que A∩B sea no vacío. La figura siguiente muestra el diagrama de Hasse de G_3.

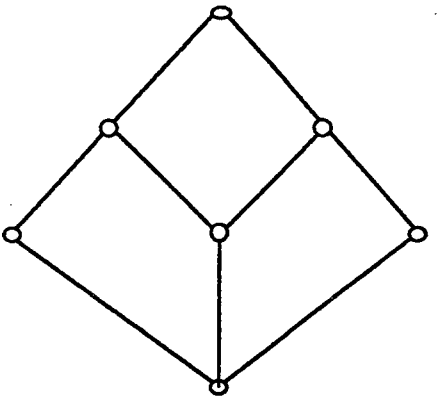


Fig. 8

4.1.10. Un *booleano* de orden n, para un número natural $n \geq 1$, denotado B_n, es un reticulado isomorfo al conjunto de las partes de {1,...,n}, ordenado por inclusión.

Sea $(L,\leq)$ un reticulado. Es inmediato comprobar que si $\geq$ denota el orden opuesto de $\leq$, $(L, \geq)$ es también un reticulado tal que $\sup_{(L,\geq)} \{a,b\} = \inf_{(L,\leq)}\{a,b\}$ e $\inf_{(L,\geq)} \{a,b\} = \sup_{(L,\leq)} \{a,b\}$.

Resulta entonces que de una propiedad válida, en general, para todo reticulado se obtiene una propiedad también válida en general cambiando $\vee$ por $\wedge$, $\wedge$ por $\vee$ y $\leq$ por $\geq$. Esta regla recibe el nombre de *principio de dualidad para reticulados.*

4.1.11. **Teorema.** *Sea (L.≤) un reticulado. Para toda terna a,b,c, de elementos de L, se cumplen las siguientes propiedades*

1) Idempotencia : $ava = a$ *y* $a \wedge a = a$

2) Conmutatividad : $avb = b \vee a$ *y* $a \wedge b = b \wedge a$

3) Asociatividad : $av(bvc) = (avb)vc$ *y* $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

4) Absorción : $av(a \wedge b) = a$ *y* $a \wedge (avb) = a.$

Demostración. Por el principio de dualidad basta probar las propiedades relativas al signo v.

Las propiedades de idempotencia y conmutatividad se deducen inmediatamente de la definición de supremo. Para comprobar la asociatividad veremos que av(bvc) y (avb)vc coinciden con sup{a,b,c}. En efecto, si z = av(bvc), entonces a≤z y bvc≤z.

Puesto que b≤bvc y c≤bvc, resulta que z es cota superior de {a,b,c}. Si z´ es cota superior de {a,b,c} entonces a≤z´ y bvc≤z´. Consecuentemente, z≤z´. Luego z= sup{a,b,c}. Puesto que (avb)vc = cv(avb), resulta de lo que antecede, (avb)vc = sup{a'b'c}.

Ya que a≤a y a∧b≤a, de la definición de supremo se obtiene, av(a∧b)≤a y consecuentemente 4).

∎

Sean $a_1 \ldots a_n$ elementos de un reticulado. Teniendo en cuenta la propiedad asociativa de v y ∧, denotaremos $a_1 v \ldots v a_n$ (resp.$a_1 \wedge \ldots \wedge a_n$) al elemento

$(\ldots((a_1 \vee a_2) \vee a_3) \vee \ldots) \vee a_n)$ (resp.$(\ldots((a_1 \wedge a_2) \wedge a_3) \wedge \ldots) \wedge a_n$). Es fácil probar, por inducción sobre n, que $a_1 \vee \ldots \vee a_n$ y $a_1 \wedge \ldots \wedge a_n$ son el supremo y el ínfimo, respectivamente, de $\{a_1, \ldots a_n\}$. Luego, todo reticulado finito tiene primero y último elemento. De estas consideraciones surge también que en todo reticulado existen el supremo y el ínfimo de todo subconjunto finito; no está asegurada en cambio la existencia de supremo e ínfimo para subconjuntos infinitos.

4.1.12 **Definición.** Un reticulado L es *completo* si, para todo subconjunto A de L, existen el supremo y el ínfimo de A en L.
De la definición surge que un reticulado completo debe tener primer y último elemento, y que ellos coinciden con el supremo y el ínfimo, respectivamente, del conjunto vacío.

4.1.13. **Teorema.** *Si L es un conjunto ordenado con último elemento tal que, para todo subconjunto A de L, no vacío, existe el ínfimo de A en L, entonces para todo subconjunto A no vacío existe el supremo de A en L.*
Demostración. Sea A un subconjunto no vacío de L. Puesto que L tiene último elemento, no es vacío el conjunto K de las cotas superiores de A. Entonces existe $k = \inf_L A$. Si a es un elemento de A, $a \leq x$, para todo $x \in K$, con lo cual a es una cota inferior de K.

Luego, a≤k, de donde k∈K. Puesto que k es la menor de las cotas superiores de K, resulta k=sup$_L$A. ∎

Dualmente, si un conjunto ordenado L tiene primer elemento y existe, para todo subconjunto no vacío A de L, el supremo de A en L, entonces, para todo subconjunto no vacío A de L, existe el ínfimo de A en L.

Ejemplos.

4.1.14 Para todo conjunto E, $(P(E),\subseteq)$ es un reticulado completo, siendo el supremo y el ínfimo de un subconjunto A, no vacío, de $P(E)$, la unión y la intersección, respectivamente, de los conjuntos de A.s

4.1.15. El conjunto $P_f(N)$, de las partes finitas de N, ordenado por inclusión, no es un reticulado completo. Por ejemplo, el conjunto $\{ \{n\}; n\in N \}$ no está acotado en $P_f(N)$, con lo cual no admite supremo.

4.1.16 Para un conjunto A, el reticulado $(E_A,\subseteq)$, de las relaciones de equivalencia sobre A, es un reticulado completo. En efecto, es fácil ver que la intersección de un conjunto no vacío cualquiera de relaciones de equivalencia es de equivalencia. Luego $(E_A,\subseteq)$ está en las condiciones del Teor. 4.1.13. El supremo de un subconjunto X de E_A es la clausura transitiva de la unión de

los elementos de X. Utilizando el isomorfismo de orden entre este reticulado y el de las particiones de A, ordenado por refinamiento, resulta (como en 4.1.4.) que este último reticulado también es completo.

Veremos ahora que las propiedades 1),...,4) de 4.1.11 permiten dar una definición algebraica de un reticulado, interpretando $\vee$ y $\wedge$ como operaciones binarias sobre un conjunto.

4.1.17, **Teorema**. *Sean L un conjunto y* $\vee$, $\wedge$ *operaciones binarias sobre L (aplicaciones de LxL en L) que satisfacen las propiedades de idempotencia, conmutatividad, asociatividad y absorción del Teor. 4..1.11. Definiendo en L la relación* $a \leq b$ *por "*$a \vee b = b$*", resulta que* $a \leq b$ *si y sólo si* $a \wedge b = a$ *y que* $(L, \leq)$ *es un reticulado tal que* $\sup_{(L,\leq)} \{a, b\} = a \vee b$ *y* $\inf_{(L,\leq)} \{a,b\} = a \wedge b$.

Demostración. Si $a \vee b = b$, entonces $a \wedge b = a \wedge (a \vee b)$. Por la propiedad de absorción, resulta $a \wedge b = a$. Similarmente de $a \wedge b = a$ se deduce $a \vee b = b$.

Puesto que $a \vee a = a$, es $a \leq a$. Si $a \leq b$ y $b \leq a$ se tiene $a \vee b = b$ y $b \vee a = a$, y por la propiedad conmutativa, $a = b$. Si $a \leq b$ y $b \leq c$ se tiene $a \vee b = b$ y $b \vee c = c$, entonces $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$, de donde $a \leq c$. Luego, $\leq$ es una relación de orden.

Por las propiedades asociativa y de idempotencia $a \vee (a \vee b) = a \vee b$, de donde $a \leq a \vee b$. Utilizando también la conmutatividad resulta $b \leq a \vee b$. Si c es una cota

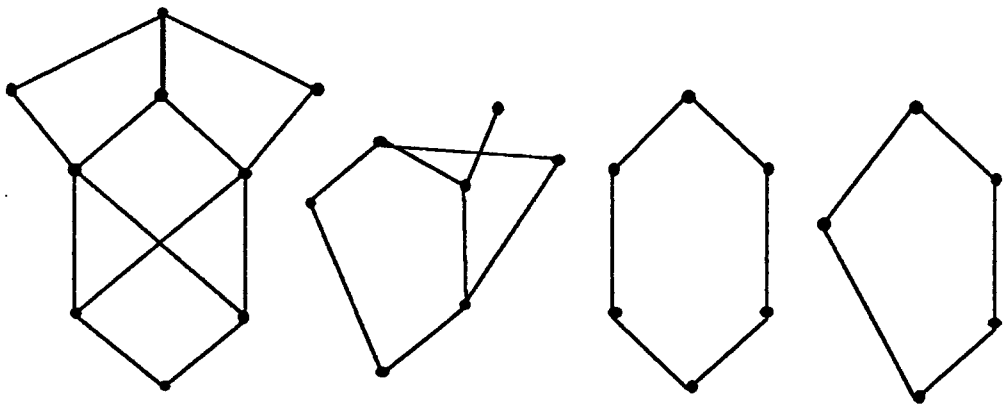
superior de {a,b} se tiene cv(avb)=(cva)vb=cvb=c, de donde, avb≤c. Entonces avb= $\sup_{(L,\leq)}$ {a,b}.

Teniendo en cuenta que, como se demostró más arriba, a≤b si y sólo si a∧b=a, se obtiene similarmente que a∧b= $\inf_{(L,\leq)}$ {a,b}. ∎

El teorema precedente permite definir un reticulado como una terna (L,v,∧), donde L es un conjunto y v, ∧ son operaciones binarias sobre L cumpliendo las propiedades 1),..., 4) del Teorema 4.1.11. En lo sucesivo nos referiremos a un reticulado L, sobreentendiendo que L es el conjunto subyacente, ≤ la relación de orden y v,∧ las dos operaciones binarias.

Ejercicios

4.1.18. Establecer si los siguientes diagramas de Hasse representan reticulados.



4.1.19. Sea $\{A_1,A_2\}$ una bipartición de un conjunto ordenado A, tal que existen ínf A, ínf A_1, ínf A_2 e ínf { ínf A_1, ínf A_2}. Demostrar que ínf A = inf{ínf A_1, ínf A_2}.

4.1.20. Probar que en un reticulado L existen el ínfimo y el supremo de todo subconjunto finito C.
(**Indicación**: Para la existencia del ínfimo, inducción sobre el cardinal de C y usar (4.1.19)). Análogamente se prueba la existencia del supremo).

4.1.21. a) Demostrar que el conjunto de todas las particiones de un conjunto X con la relación de refinamiento es un reticulado.

b) Construir el reticulado de las particiones de un conjunto con cuatro elementos.

4.1.22. Un *grafo* (simple, finito, no-dirigido) es un par ordenado G=(V,E) de dos conjuntos: un conjunto finito V de elementos llamados vértices y un conjunto $E \subseteq P_2(V)$, cuyos elementos se llaman *aristas*.

Un grafo G´= (V´,E´) es un *subgrafo* de G si V´,E´ están incluídos en V y en E respectivamente.

Un *camino* en G es una sucesión alternada $v_0\ e_1\ v_1\ e_2 \ldots v_{k-1}\ e_k\ v_k$ de vértices $v_0,\ldots,v_k$ todos distintos y aristas $e_1,\ldots,e_k$ tales que $e_i = \{v_{i-1}, v_i\}$ para i=1,..., k. Cada arista e se denota simplemente e=uv, en lugar de {u,v}.

Un subgrafo G´ de G es una *componente conexa* de G si para todo par de vértices en G´, existe un camino en G´que los une.

Un grafo G es *bipartido* si existe una bipartición {A,B} del conjunto V de vértices tal que toda arista de E consta de un elemento de A y uno de B.

a) Sea X un conjunto y P = { X_i ; i ∈I }, Q={ Yj ; j ∈J } dos particiones de X. Se define el grafo bipartido G = (AUB , E) donde A = { a_i ; i ∈ I}, B = { b_j; j ∈J} y $a_i b_j$ es una arista de E si y sólo si $X_i \cap Y_j$ es no vacío.

Probar que cada elemento de PvQ es unión de los X_i y los Y_j correspondientes a los vértices de una componente conexa de G.

b) Dado {a,b,c,d,e,f,g,h,i} y las particiones P= { {a,b},{c,d},{e,f},{g,h,i} } y Q = { {a,f},{b,c},{d,e},{g,h},{i} }, encontrar PvQ y P∧Q.

4.1.23. a) Sea V un espacio vectorial y sea S el conjunto de los subespacios de V. Si S, T $\in S$, sean S$\vee$T = S+T y S$\wedge$T = S$\cap$T. Demostrar que (S,$\vee$,$\wedge$) es un reticulado.
b) Describa el reticulado que se obtiene cuando V = R^2.

4.1.24. Sean A = {2,3,4,6,9,12,18,36} y las operaciones $\vee$ y $\wedge$ definidas por a$\vee$b = mcm {a,b} y a$\wedge$b = mín{a,b} respecto al orden usual.
Mostrar que (A, $\vee$, $\wedge$) no es un reticulado.

4.2. Subreticulados y productos.

4.2.1. **Definición**. Sean L un reticulado y S un subconjunto no vacío de L, tal que, para todo par a,b de elementos de S, a$\vee$b y a$\wedge$b pertenecen a S. Entonces, se dice que S, con las operaciones $\vee$ y $\wedge$ restringidas a S, es un *subreticulado* de L.

4.2.2. **Teorema.** *Un subreticulado S de un reticulado L es un reticulado, considerando sobre S el orden inducido por el de L.*
Demostración. Las operaciones $\vee$ y $\wedge$ de L, restringidas a S satisfacen evidentemente las propiedades 1),...,4) del Teor. 4.1.11. Entonces, S es un

reticulado con el orden definido por $a \leq b$ si y sólo si $a \vee b = b$, que es el orden inducido por el de L. ∎

4.2.3. **Teorema** *La intersección de una familia de subreticulados de un reticulado L es un subreticulado de L.*

Demostración. Sea S una familia de subreticulados de L. Si a y b pertenecen a la intersección de los elementos de S, para todo $S \in S$, $a,b \in S$, de donde $a \vee b, a \wedge b \in S$. Luego $a \vee b$ y $a \wedge b$ están en la intersección de los elementos de S. ∎

El teorema precedente permite formular la siguiente

4.2.4. **Definición**. Sea E un subconjunto de un reticulado L. El subreticulado de L *engendrado* , o *generado*, por E es la intersección de todos los subreticulados de L que contienen al conjunto E.

Denotaremos $[E]_L$ o simplemente [E], si L está sobreentendido, al subreticulado de L engendrado por E. Es evidente que [E] es el menor subreticulado de L, en el sentido de la inclusión, que contiene a E.

Ejemplos.

4.2.5. Si $a \leq b$ en un reticulado L, entonces el intervalo [a,b] es un subreticulado de L.

4.2.6. La figura 9 a) muestra el diagrama de Hasse del reticulado de los divisores de 12, con el orden "divide a". La figura 9 b) muestra el subreticulado engendrado por {3,4}.

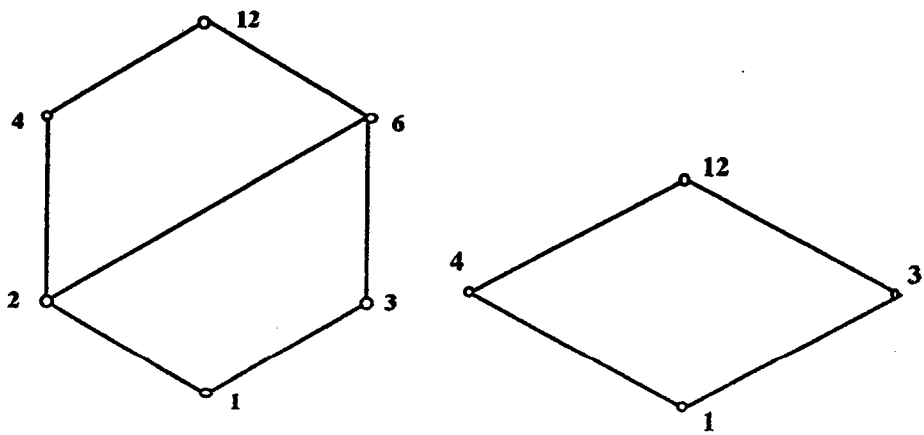


Fig. 9

Sean L y L´ reticulados. (Las operaciones binarias se denotan en L y en L´ con los signos v y ∧, aunque puedan ser distintas). Definimos sobre LxL´ las siguientes operaciones binarias: (a,a´) v (b,b´) = (avb, a´vb´) y (a,a´) ∧ (b,b´) = (a∧b,a´∧b´). Es fácil probar que estas dos operaciones satisfacen las propiedades de 4.1.11, con lo cual, (LxL´, v,∧) es un reticulado llamado *producto* de L y L´.

4.2.7. **Teorema.** *El reticulado producto, LxL´, está ordenado con el orden producto del orden de L y del orden de L´.*

Demostración. (a,a´) ≤ (b,b´) en LxL´ si y sólo si (a,a´) v (b,b´) = (b,b´), lo que equivale a "avb = b y a´ vb´ = b´", que es equivalente a "a≤b y a´≤b´". ∎

Ejercicios

4.2.8. Sea A un conjunto no vacío. Mostrar que el conjunto Q_A de todos los preórdenes sobre A, ordenado por inclusión, es un reticulado que tiene primer y último elementos.

4.2.9. a) Probar que la intersección de dos intervalos cerrados de un reticulado es un intervalo cerrado o es el conjunto vacío.

b) Probar que en un reticulado todo intervalo cerrado es un subreticulado.

4.2.10. Sean A, B conjuntos y f una función de A en B. Demostrar que el conjunto de imágenes f(S) de subconjuntos $S \subseteq A$ es un subreticulado de $(P(A), \cup, \cap)$.

4.2.11. a) Demostrar que el conjunto I de ideales superiores de un conjunto ordenado y finito $(E,\leq)$, es un subreticulado del reticulado $(P(E), \cup, \cap)$.
b) Demostrar que si $I \in I$, I es no vacío, entonces existe un elemento $x \in I$ tal que $I\{x\}$ también pertenece a I.

4.3. Morfismos de reticulados.

4.3.1. **Definición.** Sean L y L´ reticulados. Un *morfismo* de *reticulados* de L en L´ es una función f: L→L´ tal que, para todo par a,b de elementos de L, $f(a \vee b) = f(a) \vee f(b)$ y $f(a \wedge b) = f(a) \wedge f(b)$.
Un *monomorfismo* es un morfismo inyectivo, un *epimorfismo* es un morfismo suryectivo, y un *isomorfismo* es un morfismo biyectivo.

4.3.2. **Teorema.** *Si f es un isomorfismo de L en L´ entonces la aplicación inversa f^{-1} es un isomorfismo de L´ en L.*
Demostración. Sean a´, b´∈ L´. Entonces $f(f^{-1}(a' \vee b')) = a' \vee b'$. Por otra parte, puesto que f es un morfismo, se tiene,

$f(f^{-1}(a') \vee f^{-1}(b')) = f(f^{-1}(a')) \vee f(f^{-1}(b')) = a' \vee b'$. Comparando esta igualdad con la precedente y teniendo en cuenta que f es inyectiva, resulta, $f^{-1}(a' \vee b') = f^{-1}(a') \vee f^{-1}(b')$. En la misma forma se demuestra que $f^{-1}(a' \wedge b') = f^{-1}(a') \wedge f^{-1}(b')$. ∎

Observación. Si f es un morfismo de reticulados de L en L' resulta que f es un morfismo de orden. En efecto, si $a,b \in L$ y $a \leq b$, se tiene $b = a \vee b$, de donde, $f(b) = f(a \vee b) = f(a) \vee f(b)$, con lo cual $f(a) \leq f(b)$. El ejemplo siguiente muestra que la recíproca no es cierta en general: Sean L y L' los reticulados que muestran las figuras 10 a) y 10b) respectivamente y f la aplicación de L en L' dada por $f(x) = x'$. Es claro que f es un morfismo de orden pero no lo es de reticulados ya que $f(b \vee c) = f(d) = d'$ y $f(b) \vee f(c) = c'$.

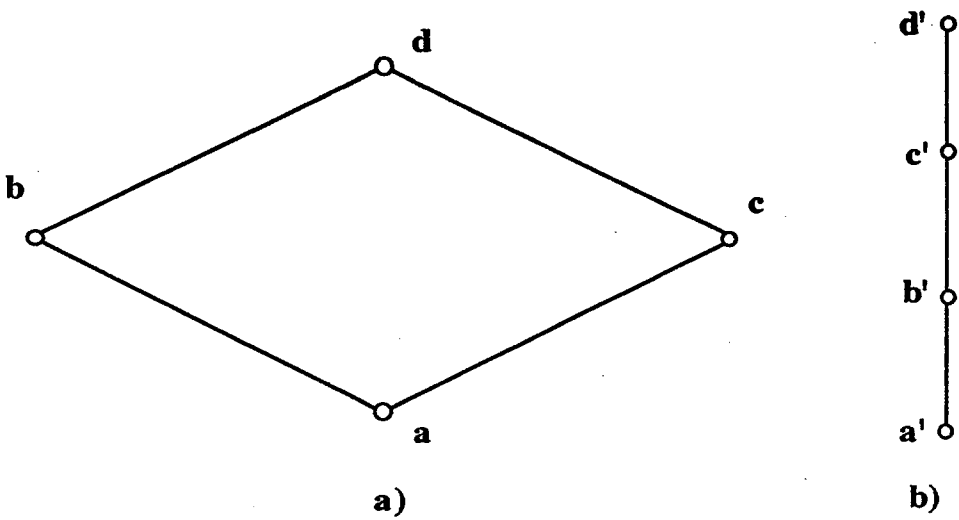


Fig. 10

Ejemplos.

4.3.3. $M_1 x M_1$ es isomorfo al reticulado de los divisores de 36 con el orden "divide a".

4.3.4. B_n es isomorfo a $(B_1)^n = B_1 x \ldots x B_1$, n veces, por medio de la función que asigna al conjunto $A \in P(\{1,\ldots,n\})$ la n-upla $(a_1,\ldots a_n)$, , definida por " $a_i = 1$ si $i \in A$, y $a_i = 0$ en caso contrario".

4.3.5. Sean U y V conjuntos disjuntos. Entonces la aplicación de $P(U \cup V)$ en $P(U) \times P(V)$ que asigna a Z el par $(Z \cap U, Z \cap V)$ es un isomorfismo del primer conjunto, ordenado por inclusión, en el segundo, ordenado con el orden producto de la inclusión por la inclusión.

Ejercicios.

4.3.6. Encontrar todos los reticulados no isomorfos de cuatro elementos.

4.3.7. Probar que si L_1 y L_2 son cadenas entonces todo morfismo de orden de L_1 en L_2 es un morfismo de reticulados.

4.3.8. Sean L_1 y L_2 reticulados Y $M(L_1, L_2)$ el conjunto de los morfismos de orden de L_1 en L_2.

Sean f,g $\in$ $M(L_1,L_2)$, se definen las funciones fvg y f$\wedge$g por las siguientes igualdades:

(fvg)(x) = f(x) v g(x)

(f$\wedge$g)(x) = f(x) $\wedge$ g(x), para todo x $\in L_1$.

a) Probar que fvg y f$\wedge$g pertenecen a $M(L_1, L_2)$,

b) Probar que $M(L_1, L_2)$ con las operaciones definidas arriba es un reticulado.

4.3.9. Sea n un número natural, n≥1, sea $n = p_1^{r1} \ldots p_k^{rk}$ su descomposición en factores primos.

Sea Cr+1 el intervalo natural [0 , r] con el orden usual, donde

$r = máx\{r_1,\ldots,r_k\}$. Sea L el reticulado $(Cr+1)^k$.

Probar que existe un monomorfismo de reticulados del reticulado (D,|) de los divisores de n en el reticulado L.

4.3.10. Sea L un reticulado. Para todo a $\in$ L se define el conjunto X_a ={x$\in$ L; x≤a}. Sea L el conjunto de los X_a , con el $a \in$ L.

a) Mostrar que $X_a \cup X_b$, con $a,b \in$ L, no pertenece en general a L .

b) Probar que L ordenado por inclusión, es un reticulado.

c) Probar que L y L son reticulados isomorfos.

4.4. Semirreticulados.

4.4.1. **Definición.** Un *semirreticulado* superior (resp. inferior) es un conjunto ordenado (L,≤) tal que, para todo par a,b, de elementos de L existe el supremo (resp. el ínfimo) de {a,b} en L.

Ejemplos

4.4.2. El diagrama de Hasse de la figura 11 muestra un semireticulado superior.

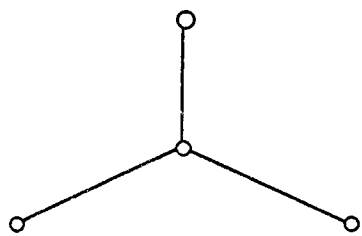


Fig. 11

4.4.3. El conjunto O_A de las relaciones de orden sobre un conjunto A, ordenado por inclusión, es un semirreticulado inferior, puesto que la intersección de relaciones de orden es de orden. En cambio no es, en general, un semirreticulado superior.
Por ejemplo, si R es una relación de orden que tiene un par (a,b) con $a \neq b$, $\{R,R^{-1}\}$ no tiene supremo en O_A.

Según se vio en el Teor. 4.1.11 las operaciones $\vee$ en un semirreticulado superior y $\wedge$ en un semirreticulado inferior son idempotentes, conmutativas y asociativas y la relación de orden queda expresada por $a \vee b = b$, en el primer caso, y por $a \wedge b = a$ en el segundo. De la demostración del Teor. 4.1.11 resulta el siguiente.

4.4.4. **Teorema.** *Sean L un conjunto y . una operación binaria en L idempotente, conmutativa y asociativa. Entonces las relaciones $a \leq b$ si y sólo si $a.b = b$ y $a \propto b$ si y sólo si $a.b = a$ son relaciones de orden opuestas. Además, $(L,\leq)$ es un semirreticulado superior tal que $a.b = \sup_{(L,\leq)} \{a,b\}$ y consecuentemente $(L,\propto)$ es un semirreticulado inferior tal que $a.b = \inf_{(L,\propto)} \{a,b\}$.*

En vista del resultado precedente puede definirse un semirreticulado como un par (L,.), donde L es un conjunto y . es una operación binaria en L idempotente, conmutativa y asociativa.
El semirreticulado será superior si se define el orden por la relación a.b = b y será inferior si se lo define por medio de a.b = a.

Ejercicios

4.4.5. Establecer cuáles de los diagramas del ejercicio (4.1.18) son semirreticulados.

4.4.6. Encontrar todos los semirreticulados inferiores no isomorfos con cuatro elementos.

4.4.7. Sea R una relación sobre un conjunto A y sea I el conjunto formado por los subconjuntos de A que son R-independientes.
Establecer si $(I,\subseteq)$ es un reticulado, en caso que no sea establecer si es un semirreticulado inferior o superior.

4.4.8. Probar que si L es un semirreticulado inferior finito y con último elemento, entonces L es un reticulado.

4.4.9. Probar que en un reticulado finito, los intervalos cerrados juntamente con el conjunto vacío, forman un reticulado con la relación de inclusión.

(**Indicación :** Usar (4.2.9) y (4.4.8)).

4.5. Reticulados distributivos.

4.5.1. **Definición.** Un reticulado L es distributivo si, para toda terna a,b,c de elementos de L, valen las dos propiedades siguientes.
1) distributividad de v con respecto a $\wedge$: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$,
2) distributividad de $\wedge$ con respecto a v: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Observaciones. 1) Una de las propiedades 1) o 2), de la definición precedente, implica la otra. En efecto, supongamos que vale 1), entonces $(a \wedge b) \vee (a \wedge c) = (a \vee (a \wedge c)) \wedge (b \vee (a \wedge c))$ que es igual, por absorción y 1), a $a \wedge ((b \vee a) \wedge (b \vee c))$. Por asociatividad, conmutatividad y absorción, se obtiene finalmente $a \wedge (b \vee c)$. En forma análoga se prueba que 2) implica 1).
2) En todo reticulado vale la "distributividad débil" siguiente

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c).$$

En efecto, $a \leq a \vee b$ y $a \leq a \vee c$. Luego $a \leq (a \vee b) \wedge (a \vee c)$. También $b \wedge c \leq b \leq a \vee b$ y $b \wedge c \leq c \leq a \vee c$, con lo cual $b \wedge c \leq (a \vee b) \wedge (a \wedge c)$. Por ser el supremo la menor de las cotas superiores, resulta lo afirmado.
Aplicando el principio de dualidad, resulta válida, para todo reticulado, la propiedad siguiente

$$(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c).$$

Ejemplos.

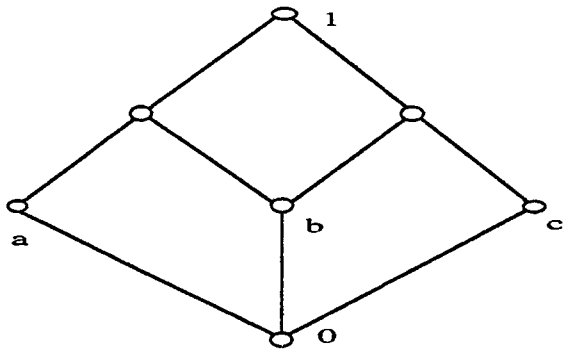
4.5.2. Los reticulados de la forma $(P(A), \subseteq)$ son distributivos.

4.5.3. Por las propiedades del mínimo común múltiplo y del máximo común divisor entre dos números naturales resulta que el conjunto de números naturales, ordenado por la relación "divide a" es un reticulado distributivo.

4.5.4. Los conjuntos totalmente ordenados son reticulados distributivos.

4.5.5. Las anticadenas M_n (4.1.8.), para $n \geq 3$, no son distributivas. En efecto, si a,b,c son elementos incomparables dos a dos, 0 es el primer elemento y 1 el último, se tiene $a \vee (b \wedge c) = a \vee 0 = a$, mientras que $(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1$.

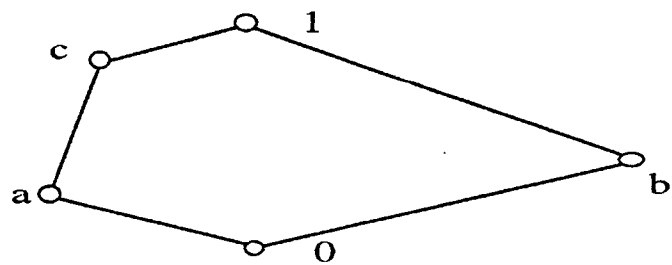
4.5.6. Las grillas G_n, para $n \geq 3$, no son distributivas. La figura siguiente lo muestra para G_3



$b \wedge (a \vee c) = b \wedge 1 = b$, mientras que $(b \wedge a) \vee (b \wedge c) = 0 \vee 0 = 0$.

Fig . 12

4.5.7. El reticulado que muestra la figura siguiente no es distributivo



$c \wedge (a \vee b) = c \wedge 1 = c$, mientras que $(c \wedge a) \vee (c \wedge b) = a \vee 0 = a$

Fig 13

Es inmediato que el reticulado opuesto de un reticulado distributivo es también distributivo y que todo subreticulado de un reticulado distributivo es distributivo. También, el producto de reticulados distributivos es distributivo.

4.5.8. **Teorema.** *Sea L un reticulado distributivo. Entonces, para toda terna a,b,c, de elementos de L, las igualdades "avc = bvc" y "a∧c = b∧c" implican "a = b".*

Demostración. Por la propiedad de absorción, a= av(a∧c): empleando una de las igualdades de enunciado, av(a∧c) = av(b∧c), que es igual, por la propiedad distributiva, a (avb)∧(avc).
Empleando las igualdades del enunciado, distributividad y absorción, resulta (avb)∧(avc) = (avb)∧(bvc) = (a∧c)vb = (b∧c)vb = b. ∎

4.5.9. **Definición.** Un reticulado *con cero* es un reticulado que tiene primer elemento, denotado habitualmente 0. Un reticulado *con uno* es un reticulado que tiene último elemento, denotado habitualmente 1.

4.5.10. **Definición.** Sean L un reticulado con 0 y 1 y a un elemento de L. Un elemento b de L es un *complemento*, o es *complementario*, de a si avb = 1 y

$a \wedge b = 0$. Se dice que L es *complementado* si todo elemento de L tiene complemento.

Es claro que si b es complementario de a, entonces a es complementario de b: diremos simplemente que a y b son complementarios, luego 0 y 1 son complementarios. Entonces, si a y b son complementarios en L, también lo son en el dual de L. Luego si L es complementado, su reticulado dual es complementado.

También resulta inmediatamente que el producto de dos reticulados complementados es complementado.

Ejemplos.

4.5.11. En M_n, con $n \geq 3$, todo elemento distinto de 0 y 1 tiene más de un complemento.

4.5.12. En $P(A)$, ordenado por inclusión, cada elemento X tiene un único complemento, a saber, A-X.

4.5.13. En la grilla G_3 de la figura 12, a y c son complementarios y b no tiene complemento.

4.5.14. **Teorema.** *En un reticulado distributivo con 0 y 1 cada elemento tiene a lo sumo un complemento.*

Demostración. Si b y c son complementarios de a, se tiene, $a \vee b = a \vee c = 1$ y $a \wedge b = a \wedge c = 0$. Por aplicación del Teor. 4.5.8 resulta $b = c$. ∎

Ejercicios

4.5.15. Probar que en un reticulado distributivo L el conjunto de elementos que tienen complemento es un subreticulado de L.

4.5.16. Sean L un reticulado distributivo, M (L,L) el conjunto de morfismos de orden de L en L y a un elemento de L,
a) Probar que la función f_a de L en L, definida por $f_a(x)=a \wedge x$ es un morfismo de reticulados,
b) Demostrar que el conjunto $M= \{f_a \; ; \; a \in L\}$ es un reticulado distributivo, subreticulado de M (L,L).

4.5.17. Sea f un epimorfismo de reticulados del reticulado L en el reticulado L´. Demostrar que si L tiene 0 y 1, entonces f(0) y f(1) son primer y último elemento respectivamente de L´.

4.5.18. Mostrar que un subreticulado de un reticulado complementado no es necesariamente complementado.

4.5.19. Sea f un epimorfismo de reticulados del reticulado L en el reticulado L´. Demostrar que si L es complementado entonces L´ también lo es.

4.5.20. Un reticulado L se llama *modular* si para todo x,y,z $\in$ L se verifica que $x \geq z$ implica $x \wedge (y \vee z) = (x \wedge y) \vee z$.
Probar que si L es un reticulado modular y b, c son elementos comparables de L, entonces:
$a \wedge b = a \wedge c$ y $a \vee b = a \vee c$ implica $b = c$.

4.5.21. Sean a y b dos elementos de un reticulado L, se dice que dos elementos x, y $\in$ L son *complementarios relativos* respecto del intervalo [a,b] de L, si $x \vee y = b$ y $x \wedge y = a$.
Probar que si L es un reticulado modular, x e y son complementarios en L y $a \leq x \leq b$, entonces el complemento relativo de x respecto de [a,b] es el elemento
$z = b \wedge (y \vee a)$

4.6. Reticulados distributivos y complementados.

En el siguiente teorema se designa con a´ al complemento del elemento a de un reticulado distributivo, con 0 y 1 y complementado (el complemento es único por el
Teor. 4.5.14.)

4.6.1. **Teorema.** *Sean a y b elementos de un reticulado distributivo, con 0 y 1 y complementado. Entonces se cumplen las siguientes propiedades:*
a) <u>*Ley de involución*</u> *:* $(a')' = a$
b) <u>*Leyes de De Morgan*</u> *:* $(avb)' = a' \wedge b'$ *y* $(a \wedge b)' = a' \vee b'$.
c) $a \leq b$ *si y sólo si* $a \wedge b' = 0$ *(o equivalentemente,* $avb' = 1$ *).*

Demostración. La ley de involución es inmediata por la definición de complemento. En cuanto a las leyes de De Morgan, se tiene, por aplicación de las propiedades distributivas y conmutativas y asociativas,
$(avb) \vee (a' \wedge b') = (avbva') \wedge (avbvb') = (bv1) \wedge (av1) = 1,$
$(avb) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (0 \wedge b') \vee (0 \wedge a') = 0,$

lo que demuestra la primera igualdad. En cuanto a la segunda, aplicando la primera igualdad y la ley de involución, resulta $(a' \vee b')' = a \wedge b$, de donde, por la ley de involución, $a' \vee b' = (a \wedge b)'$.

En cuanto a c) si $a \leq b$, $a \wedge b = a$, de donde se obtiene,

$a \wedge b' = (a \wedge b) \wedge b' = a \wedge (b \wedge b') = a \wedge 0 = 0$.

Recíprocamente, si $a \wedge b' = 0$, resulta $a \vee b = (a \vee b) \wedge (b \vee b') = (a \wedge b') \vee b = b$ con lo cual $a \leq b$.

∎

4.7. Atomos y coátomos

4.7.1. **Definición.** Sea L un reticulado con 0 y 1. Un átomo de L, si es que existe, es un elemento minimal de L-{0} y un coátomo de L, si es que existe, es un elemento maximal de L-{1},

Es evidente que todo reticulado finito tiene átomo y coátomos.

Ejemplos

4.7.2. En $(P(E), \subseteq)$ los átomos son los conjuntos unitarios y los coátomos son de la forma E-{x}, con $x \in E$. En particular, si E es un conjunto unitario, el reticulado tiene a 0 y 1 como únicos elementos y 0 es un coátomo y 1 es un átomo.

4.7.3. El intervalo real [0,1], con el orden usual, no tiene átomos ni coátomos.

4.7.4. En M_1 el único elemento distinto de 0 y de 1 es a la vez átomo y coátomo.

4.7.5. El reticulado (N, |) no tiene coátomos (dado $n \in N$, $n \mid 2n$) y los átomos son los números primos.

4.7.6. **Definición.** Un reticulado L es *atómico* si, para todo elemento x de L, existe un átomo a de L tal que $a \leq x$.

4.7.7. **Teorema.** *Todo reticulado finito es atómico.*

Demostración. Sea x un elemento de un reticulado finito L.
Si x es un átomo ponemos a = x. Si no lo es, definimos una sucesión $x_1,\ldots,x_n,\ldots$ de elementos de L como sigue: $x_1 = x$, supuesto definido x_n, para $n \geq 1$, si x_n no es un átomo, tomamos como x_{n+1} un elemento de L menor estrictamente que x_n. Puesto que L es finito se obtendrá un átomo a en la sucesión que, evidentemente, es menor que x.

∎

4.7.8. **Definición.** Un reticulado L es *supatómico* si cada elemento x de L es el supremo del conjunto de los átomos a de L tales que a≤x.
Para cada elemento x de L denotaremos A(x) al conjunto de los átomos a de L tales que a≤x. Entonces, L es supatómico si y sólo si, para todo $x \in L$, $x = \sup_L A(x)$.
Puesto que $A(0) = \emptyset$, se verifica que $0 = \sup_L A(0)$.

Ejemplos

4.7.9. Para todo conjunto E, $(P(E), \subseteq)$ es supatómico. También son supatómicos las anticadenas Mk y las grillas Gk, para todo k≥2.

4.7.10. Las cadenas finitas con más de dos elementos no son supatómicas. En efecto, si 0≤ a ≤1 es una cadena con tres elementos, A(1)= {a}, con lo cual sup A(1) es distinto de 1.

4.7.11. El reticulado (N, |) no es supatómico. Por ejemplo, A (12) = {2,3}, con lo cual sup A (12) = 6

4.7.12. El reticulado cuyo diagrama de Hasse muestra la figura siguiente no es supatómico. En efecto, la condición pedida no se cumple para los elementos d,e y 1.

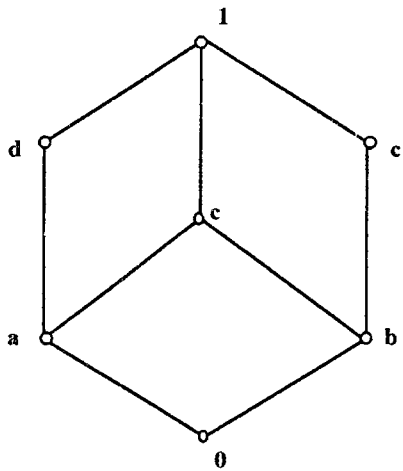


Fig. 14

Ejercicios.

4.7.13. Sea L un reticulado atómico y tal que todo elemento de L posee un único complemento. Sean x, y $\in$ L tales que x > y. Probar que existe en L un átomo a tal que $a \leq x$, $a \wedge y = 0$.

4.7.14. Sea L un reticulado atómico, tal que todo elemento de L tiene un único complemento.
Probar que el complemento de un átomo es un coátomo.

Capítulo 5

Algebras de Boole

En este capítulo se introducen las álgebras de Boole como reticulados distributivos, complementados, con primer y último elemento (ambos distintos). Se las examina desde el punto de vista algebraico y se dan las nociones de subálgebra, producto y morfismo. Finalmente se demuestra que toda álgebra de Boole finita es isomorfa al álgebra de un conjunto de partes.

5.1. Definición y propiedades elementales.

5.1.1. **Definición.** Un álgebra de Boole es un reticulado con 0 y 1, tal que 0 es distinto de 1, distributivo y complementado.

Si B es un álgebra de Boole, cada elemento b de B tiene un único complemento b′ (ver 4.5.14). Luego la asignación b → b′ define una

función de B en B, u operación unaria sobre B. Como corolario del Teor. 4.1.17 y de la definición 5.1.1, se obtiene el siguiente resultado.

Teorema. *Sean B un conjunto, v y ∧ operaciones binarias sobre B, una operación unaria sobre B y 0, 1 elementos distintos de B.*
Si las dos operaciones binarias satisfacen las propiedades de 4.1.11 y las leyes distributivas de 4.5.1 y, además, se cumplen las propiedades siguientes, para todo a ∈ B.
$av0 = a$ y $av1 = a$
$ava' = 1$ y $a \wedge a' = 0$,
entonces B ordenado por la relación $a \leq b$ si y sólo si $avb = b$ (o equivalentemente, $a \wedge b = a$) es un álgebra de Boole tal que $avb = sup\{a,b\}$, $a \wedge b = inf\{a,b\}$, a' es el complementario de a y 0 y 1 son el primero y último elemento respectivamente de B.
De acuerdo con este teorema un álgebra de Boole puede darse como un séxtuple
$B = (B, v, \wedge, ', 0, 1)$ donde B es un conjunto, v y ∧ son operaciones binarias sobre B, ' es una operación unaria sobre B y 0, 1 son elementos distintos de B cumpliendo las propiedades del enunciado.

Ejemplos

5.1.2. Para todo conjunto E, no vacío, $(P(E),\subseteq)$ es un álgebra de Boole. En particular, el conjunto de todas las relaciones binarias sobre un conjunto A, ordenado por inclusión, es un álgebra de Boole. Para todo $x \in E$, {x} es un átomo de $(P(E),\subseteq)$.

5.1.3. Sea E un conjunto no vacío. Se dice que un subconjunto X de E es cofinito si E-X es finito. El subconjunto de P (E) formado por las partes finitas y cofinitas de E, ordenado por inclusión, es un álgebra de Boole. Como en el ejemplo precedente, para todo $x \in E$, {x} es un átomo. Tomando E = N, se obtiene un álgebra de Boole que no es completa; por ejemplo, el conjunto $\{\{2n+1\}, n \in N\}$, no admite supremo.

5.1.4. Sean Dn el conjunto de los divisores de un número natural n mayor que 1. Entonces Dn, ordenado por la relación "divide a", es un reticulado distributivo con 0 y 1 (los números 1 y n respectivamente). Puede suceder que Dn no sea complementado, como es el caso de D_4, pero si n cumple la propiedad: " para todo k mayor que 1, k^2 no divide a n", resulta que, para todo $a \in$ Dn, n / a es complementario de a. Luego , en este caso, (Dn, |) es un álgebra de Boole. Todo divisor primo de n es un átomo.

5.1.5. Sea [0,1) el intervalo real semiabierto a derecha de extremos 0 y 1, es decir, el conjunto de los números reales x tales que $0 \leq x < 1$. Sea B el conjunto de todas las uniones finitas de intervalos reales, semiabiertos a derecha contenidos en [0,1).

Entonces, $(B, \subseteq)$ es un álgebra de Boole. En efecto, es evidente que la unión de dos elementos de B pertenece a B. Si $u = [a_1,b_1) \cup ... \cup [a_n,b_n)$ y $v = [c_1,d_1) \cup ... \cup [c_m,d_m)$ son elementos de B, se tiene que $u \cap v = \cup [a_i,b_i) \cap [cj,dj)$, donde la unión se toma sobre todos los pares (i,j) , tales que $1 \leq i \leq n$ y $1 \leq j \leq m$. Puesto que la intersección de dos intervalos semiabiertos a derecha es un intervalo semiabierto a derecha, resulta que $u \cap v \in B$. Para cada elemento u de B, sea $u' = [0,1) - u$. Si u es la unión de los intervalos dada más arriba, se tiene que $u' = [a_1,b_1)' \cap ... \cap [a_n,b_n)'$, y puesto que, para cada i, [ai,bi)' es una unión finita de intervalos semiabiertos a derecha, resulta que $u' \in B$. El primero y el último elemento son, respectivamente,

$\varnothing$ y [0,1).

Este álgebra de Boole no tiene átomos, puesto que si u es un elemento de B no vacío, existe un intervalo [a,b), no vacío, contenido en u. Entonces, existe un número real c tal que $a<c<b$, de donde $[a,c) \subseteq u$. Esta álgebra de Boole no es completa.

5.1.6. El reticulado opuesto de un álgebra de Boole B es también un álgebra de Boole, llamada opuesta o dual de B. El álgebra dual de $(B,\vee,\wedge,',0,1)$ es $(B,\wedge,\vee,',1,0)$. Nótese que ambas álgebras tienen la misma operación unaria.

Ejercicios

5.1.7. Sea B el conjunto de las partes finitas y las partes cofinitas de un conjunto no vacío E, tal como se define en (5.1.3). Demostrar que $(B, \cup, \cap, C_E, \varnothing, E)$ es un álgebra de Boole.

5.1.8. Sea B un álgebra de Boole y sean a, b, c $\in$ B. Usando únicamente las leyes de conmutatividad, de distributividad, de que 0 y 1 son neutros, la existencia de complemento y el hecho de que 0 y 1 son distintos, probar:

a) Si $a\wedge c = b\wedge c$ y $a\wedge c' = b\wedge c'$, entonces a = b.

(**Indicación:** Escribir $a = a\wedge 1 = a\wedge(c\vee c')$).

b) las leyes de idempotencia (**Indicación:** escribir $a = a\vee 0 = a\vee(a\wedge a')$).

c) las leyes de absorción. (**Indicación:** Probar primero que para cualquier a, $a\wedge 0=0$, escribiendo $a\wedge 0 = (a\wedge 0)\vee 0 = (a\wedge 0)\vee(a\wedge a')$, luego escribir $a\wedge(a\vee b)=(a\vee 0)\wedge(a\vee b)$ para probar absorción).

d) la asociatividad de $\vee$ (la de $\wedge$ se prueba en forma análoga)

(**Indicación:** Usar las partes anteriores de este ejercicio).

5.1.9. Sea **N** el conjunto de los números naturales, se define en $P(\mathbf{N})$ la relación $\propto$ dada por $A \propto B$ si y sólo si A-B es finito.

a) Demostrar que $\propto$ es un preorden,

b) Explicitar la relación de equivalencia R en $P(\mathbf{N})$ asociada con el preorden, y el orden $\leq$ que se obtiene en el cociente,

c) Demostrar que si $A \subseteq B$, entonces $[A] \leq [B]$, siendo $[A], [B] \in P(\mathbf{N})/R$. Describa las clases $[\varnothing]$ y $[\mathbf{N}]$.

d) Demostrar que $(P(\mathbf{N})/R, \leq)$ es un álgebra de Boole.

e) Demostrar que este álgebra de Boole no tiene átomos.

5.1.10. Sea Δ la diferencia simétrica o suma booleana de los elementos a y b, de un álgebra de Boole, definida por $a\Delta b = (a \wedge b') \vee (a' \wedge b)$.

Demostrar las siguientes igualdades: $a\Delta b' = a'\Delta b$, $a\Delta b = a'\Delta b'$, $(a\Delta b)\Delta c = a\Delta(b\Delta c)$.

5.2. Subálgebras y productos.

5.2.1. **Definición.** Sean B = (B,v,∧, ´, 0,1) un álgebra de Boole y S un subconjunto de B. Se dice que S es cerrado para todas las operaciones de B si se cumplen las condiciones siguientes

1) para todo par a,b de elementos de S, avb, a∧b, a´, ∈ S,

2) 0,1, ∈ S.

Una *subálgebra* de B es un álgebra de Boole (S,v,∧, ´, 0, 1) tal que S es un subconjunto de B, cerrado para todas las operaciones de B y v,∧,´ son las restricciones a S de las operaciones de B.

Ejemplos

5.2.2. Sea X un subconjunto propio de un conjunto Y. Entonces $(P(X),\subseteq)$ es un subreticulado de $(P(Y),\subseteq)$ pero no es una subálgebra puesto que el último elemento de
$(P(Y),\subseteq)$ no pertenece a $P(X)$.

5.2.3. Como generalización del ejemplo precedente, sea x un elemento, distinto de 0, de un álgebra de Boole (B,v,∧, ´,0,1).

Entonces el intervalo [0,x] = {b∈B; 0≤b≤x} es un álgebra de Boole con las operaciones binarias restringidas de las de B, la operación unaria dada por

$b \rightarrow b' \wedge x$, el primer elemento igual a 0 y el último igual a x. Pero entonces este álgebra no es una subálgebra de B.

5.2.4. El álgebra B definida en 5.1.5. es una subálgebra del álgebra de las partes del intervalo [0,1), sin embargo un subconjunto infinito de B tiene siempre supremo (o ínfimo) en $P([0,1))$ y puede no tenerlo en B, más aún, puede suceder que ambos supremos existan pero que sean distintos. Tal es el caso del conjunto $A = \{[1/n,1) ; n \in N- \{0\}\}$, puesto que $\sup_B A = [0,1)$ y $\sup_{P[0,1)} A = (0,1)$.

Sean B_1 y B_2 álgebras de Boole (las operaciones y los primeros y últimos elementos se denotan con los mismos símbolos aunque pueden ser distintos). Se comprueba inmediatamente que el reticulado producto (4.2) es un álgebra de Boole donde, la operación unaria está dada por: $(b_1,b_2)' = (b_1', b_2')$, (0,0) es el primer elemento y (1,1) el último.
Se denomina el *álgebra producto* de B_1 por B_2.

Ejercicios

5.2.5. Sea B un álgebra de Boole. Demostrar que si un conjunto $A \subseteq B$ es cerrado con respecto al par de operaciones v, ´ o con respecto al par de operaciones $\wedge$, ´ entonces es cerrado con respecto a las tres operaciones v, $\wedge$,´.

5.2.6. Determinar en qué condiciones el reticulado del ejercicio (4.2.10) es una subálgebra de Boole de $(P(A), \cup, \cap, C_A, \varnothing, A)$.

5.2.7. Mostrar que el reticulado I del ejercicio (4.2.11) no es una subálgebra de Boole de $(P(E), \cup, \cap, C_E, \varnothing, E)$.

5.2.8. a) Hacer el diagrama de Hasse de los siguientes conjuntos ordenados: $B_1 \times B_2$ con el orden producto y $B_1 \times B_2$ con el orden lexicográfico L. Decir si $(B_1 \times B_2, L)$ es un reticulado; en caso que sea decir si es o no complementado.

b) Sean $A_1, \ldots, A_n$ reticulados con 0 y 1. Sean $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ dos elementos no comparables de $(A_1 \times \ldots \times A_n, L)$. Sea i el primer índice tal que a_i es distinto de b_i. Probar que $(a_1, \ldots, a_{i-1}, a_i \wedge b_i, 1, 1, \ldots, 1)$ es el ínfimo de a y b.

5.2.9. a) Sean B un álgebra de Boole y S_B el conjunto de las subálgebras de B. Probar que $S_B\subseteq$ es un reticulado. (**Indicación:** Usar el concepto de subálgebra engendrada por un conjunto).
b) Sea X un conjunto no vacío y finito y sea S una subálgebra de $(P(X),\subseteq)$. Demostrar que el conjunto de los átomos de S es una partición de X.

5.2.10. Sea B un álgebra de Boole sin átomos. Establecer si el álgebra de Boole producto B_1xB tiene átomos y, en caso afirmativo, establecer si para todo elemento no nulo (x,y) de B_1xB, existe un átomo (a,b) tal que $(a,b) \leq (x,y)$.

5.3 Morfismos de álgebras de Boole.

5.3.1. **Definición.** Sean B_1 y B_2 álgebras de Boole. (Las operaciones y el primer y último elemento se denotan en ambas con los mismos símbolos $\vee,\wedge,',0,1$, aunque pueden ser distintos). Un morfismo de B_1 en B_2 es una aplicación $f: B_1\to B_2$ tal que, para todo par a,b, de elementos de B_1 se cumplen las siguientes propiedades.

1) $f(a\vee b) = f(a)\vee f(b)$ 3) $f(a') = (f(a))'$
2) $f(a\wedge b) = f(a)\wedge f(b)$ 4) $f(0) = 0$ y $f(1) = 1$.

Es decir, un morfismo de álgebras de Boole es un morfismo de los reticulados subyacentes que, además , conserva la complementación, 0 y 1.
Como en el caso de los reticulados, un morfismo inyectivo, (resp. suryectivo, biyectivo) recibe el nombre de monomorfismo (resp. epimorfismo, isomorfismo). Se demuestra sin dificultad (ejerc 5.3.3), que la aplicación inversa de un isomorfismo es también un isomorfismo.
Las condiciones dadas en 5.3.1 no son independientes, en efecto 1) y 2) implican que 3) es equivalente a 4): Si valen 1), 2) y 3) se tiene, para un elemento $a \in B_1$, $f(0) = f(a \wedge a') = f(a) \wedge f(a') = f(a) \wedge (f(a))' = 0$ y $f(1) = f(a \vee a') = f(a) \vee (f(a))' = 1$.
Si valen 1), 2) y 4) resulta $f(a) \wedge f(a') = f(a \wedge a') = f(0) = 0$ y $f(a) \vee f(a') = f(a \vee a') = f(1) = 1$, de donde se verifica 3).

5.3.2. **Teorema.** *Si B es un álgebra de Boole la complementación, como operación de B en B, es un isomorfismo de B en el álgebra dual.*
Demostración. Teniendo en cuenta que, para todo $a \in B$, $(a')' = a$, resulta que la complementación es una aplicación biyectiva que cumple, además, la propiedad 3) de 5.3.1. Las propiedades 1) y 2) se satisfacen en virtud de las leyes de De Morgan. ∎

Ejercicios

5.3.3. Sea f un isomorfismo del álgebra de Boole A en el álgebra de Boole B. Probar que la aplicación inversa de f es también un isomorfismo de álgebras de Boole.

5.3.4. Sean A y B álgebras de Boole y f un morfismo booleano de A en B. Demostrar que:

a) si S es una subálgebra de A, entonces $f(S) = \{f(s) ; s \in S\}$ es una subálgebra de B.

b) Si T es una subálgebra de B, entonces $f^{-1}(T) = \{x \in A ; f(x) \in T\}$ es una subálgebra de A.

5.3.5. Sean A y B álgebras de Boole y f un morfismo booleano de A en B.

a) Probar que el elemento 0 de A pertenece a la imagen inversa por f del elemento 0 de B.

b) Probar que para todo $a \in A$, si $a \in f^{-1}(0_B)$, entonces $f^{-1}(0_B)$ contiene al intervalo $[0_A,a]$.

c) Sean a_1, a_2 elementos de A. Probar que si $a_1, a_2 \in f^{-1}(0_B)$, entonces también $a_1 \vee a_2 \in f^{-1}(0_B)$.

d) Establecer si $f^{-1}(0_B)$ es una subálgebra de Boole de A.

5.3.6. Sea B un álgebra de Boole, la diferencia entre dos elementos a y b de B es

$a-b = a \wedge b'$.

a) Probar que $(a-b) \wedge b = 0$ y que, si $b \leq a$, entonces $(a-b) \vee b = a$.

b) Sea a un elemento no nulo de B. Probar que el intervalo I=[0,a], con el orden inducido por el de B, es un álgebra de Boole.

Establecer si I es una subálgebra de B.

c) Demostrar que la aplicación f_a de B en I, dada por $f_a(x) = a \wedge x$ es un epimorfismo de álgebras de Boole.

d) Demostrar que la aplicación F de B en [0,a] x [0,a´], dada por $F(x) = (f_a(x), f_{a'}(x))$ es un isomorfismo de álgebras de Boole.

5.4 Representación de las álgebras de Boole finitas.

Toda álgebra de Boole no es necesariamente atómica (ver 4.7.6), por ejemplo, las álgebras de Boole que no tienen átomos como la del ejemplo 5.1.5. Existen álgebras que tienen átomos pero que no son atómicas, por ejemplo, si B es un álgebra de Boole sin átomos y B´ es el producto cartesiano B_1 xB resulta que (1,0) es el único átomo de B´ y que (1,0) no es

menor o igual que ninguno de los elementos de la forman (0,x), con $x \neq 0$. Según 4.7.7 las álgebras de Boole finitas son atómicas. Con respecto a la propiedad de ser supatómica (ver 4.7.8), se tiene el siguiente resultado.

5.4.1. **Teorema.** *Toda álgebra de Boole atómica es supatómica.*

Demostración. Sean B un álgebra de Boole atómica y $x \neq 0$ un elemento de B. Entonces, A(x) (ver 4.7.8) es no vacío y x es cota superior de A(x).
Sea z una cota superior de A(x) y supongamos que x no es menor o igual que z. Entonces, por 4.6.1, $x \wedge z' \neq 0$. Siendo B atómica, existe un átomo a de B tal que $a \leq x \wedge z'$. Luego $a \leq x$, de donde $a \in A(x)$ y por lo tanto $a \leq z$. Como también $a \leq z'$, resulta $a \leq z \wedge z' = 0$, lo que es absurdo. Entonces $x \leq z$, de donde, $x = \sup A(x)$. ■

5.4.2. **Corolario.** *Toda álgebra de Boole finita es supatómica.*

Sean B un álgebra de Boole finita y T el conjunto de sus átomos. La asignación $x \to A(x)$ define una aplicación A, de B en $P(T)$. Por otra parte, asignando a cada $X \in P(T)$ el elemento sup X de B se obtiene una aplicación S, de $P(T)$ en B. Según el Teor. 5.4.1, para todo $x \in B$, $x = S(A(x))$, o equivalentemente, $SoA = id_B$. El teorema siguiente muestra el valor de AoS.

5.4.3. **Teorema.** *Si B es un álgebra de Boole finita, entonces* $AoS = id_{P(T)}$.

Demostración. Sea $X \in P(T)$; compararemos los conjuntos A(S(X)) y X. Si $a \in X$, entonces $a \leq S(X)$, de donde, por la definición de A, $a \in A(S(X))$. Luego $X \subseteq A(S(X))$.

Recíprocamente, si $a \in A(S(X))$, $a \leq S(X)$, con lo cual $a \wedge S(X) = a$. Por ser B finito, X es un conjunto finito, pongamos $X = \{a_1,\ldots,a_n\}$. Entonces $S(X) = a_1 \vee \ldots \vee a_n$, de donde,

$a = a \wedge S(X) = (a \wedge a_1) \vee \ldots \vee (a \wedge a_n)$. Puesto que $a \neq 0$, existe i, $1 \leq i \leq n$, tal que $a \wedge a_i \neq 0$. Pero entonces, siendo a y a_i átomos, debe cumplirse $a = a_i$. Luego $a \in X$, con lo cual $A(S(X)) \subseteq X$.

∎

5.4.4. **Teorema.** *Sean B un álgebra de Boole finita y T el conjunto de los átomos de B. Entonces la aplicación A de B en* $P(T)$. *definida mas arriba, es un isomorfismo de B sobre el álgebra* $(P(T), \cup, \cap, ', \varnothing, T)$.

Demostración. Puesto que $SoA = id_B$ y $AoS = id_{P(T)}$, resulta que A es una biyección y S la aplicación inversa.

Sean ahora $x,z \in B$. Si $x = 0$, $A(x \vee z) = A(z)$ y $A(x) = \varnothing$.

Luego, $A(x \vee z) = A(x) \cup A(z)$. Por otra parte, $A(x \wedge z) = A(0) = \varnothing$, de donde, $A(x \wedge z) = A(x) \cap A(z)$.

Supongamos ahora que x y z son ambos distintos de 0 y pongamos

$A(x)=\{a_1,\ldots,a_n\}$ y $A(z) = \{b_1,\ldots,b_m\}$. Entonces $x = a_1 \vee \ldots a_n$ y $z = b_1 \vee \ldots \vee b_m$.

Luego,

$A(x \vee z) = A(S(\{a_1,\ldots,a_n,b_1,\ldots,b_m\}) = \{a_1,\ldots,a_n,b_1,\ldots,b_m\} = \{a_1,\ldots,a_n\} \cup \{b_1,\ldots,b_m\} = A(x) \cup A(z)$.

Por la propiedad distributiva $A(x \wedge z) = A(S(\{a_i \wedge b_j \; ; \; 1 \leq i \leq n \; , \; 1 \leq j \leq m\}))$, que es igual a $A(S(A(x) \cap A(z)))$, puesto que para $a_i \neq b_j$, $a_i \wedge b_j = 0$. Entonces, $A(x \wedge z) = A(x) \cap A(z)$.

Ya que $A(0) = \varnothing$ y $A(1) = T$, resulta que A es un isomorfismo de álgebras de Boole. ∎

5.4.5. **Corolario.** *El número de elementos de un álgebra de Boole finita es una potencia de dos. Si dos álgebras de Boole finitas tienen el mismo número de elementos, entonces son isomorfas*

Demostración. Si B es una álgebra de Boole finita y T es el conjunto de sus átomos, por el teorema precedente se tiene que $|B| = |P(T)| = 2^{|T|}$.

Si B_1 y B_2 son álgebras de Boole finitas tales que $|B_1| = |B_2|$ y T_i, i=1,2, es el conjunto de los átomos de B*i*, se tiene que $|T_1| = |T_2|$, con lo cual las álgebras de Boole sobre $P(T_1)$ y $P(T_2)$ son isomorfas. Por el teorema precedente B_1 y B_2 son isomorfas. ∎

5.4.6. **Corolario.** *Toda álgebra de Boole finita con n átomos es isomorfa a* $(B_1)^n$.

Demostración. Si B es un álgebra de Boole finita con n átomos, entonces $|B| = 2^n$. Puesto que $|(B_1)^n| = 2^n$, el resultado se deduce por aplicación de 5.4.5. ∎

Ejercicio.

5.4.7. a) Sea B un álgebra de Boole finita con n átomos $a_1,\ldots,a_n$.
Probar que para todo k, k=1,...,n, a_k es el ínfimo de los complementos de los elementos a_j, para todo j distinto de k, j=1,...,n.
b) Demostrar que si S es una subálgebra de Bn engendrada por n-1 átomos, entonces $S=B_n$.

Capítulo 6

Definición de álgebras

En este capítulo se definen las álgebras desde el punto de vista del álgebra universal. Esta óptica prepara el camino para el estudio de las álgebras heterogéneas, de especial importancia en informática. Se definen los semigrupos, monoides, grupos, anillos y semianillos como álgebras especiales y se dan los ejemplos mas relevantes.

6.1 Nociones fundamentales.

Sea A un conjunto. Para un número natural $n \geq 1$, se denota A^n al producto cartesiano de n veces el conjunto A, es decir al conjunto de todas las n-uplas $(a_1,...,a_n)$ con $a_1,...,a_n \in A$. Convendremos, además, en que $A^0 = \{\varnothing\}$. Denotaremos, cuando convenga, $\bar{a}$ a un elemento de A^n ; entonces, si $n = 0$, $\bar{a} = \varnothing$, y si $n>0$, $\bar{a}$ designará una n-upla $(a_1,...,a_n)$ de elementos de A.

6.1.1. **Definición.** Sean A un conjunto y n un número natural. Una operación *n-aria* sobre A es una aplicación de A^n en A. Una operación de *aridad finita* es una operación n-aria, para algún n natural.

Si f es una operación n-aria sobre A se dice que n es el *rango* o la *aridad* de f. Si n= 0 se denotará f por f (∅), entonces, una operación 0-aria será considerada como un elemento de A.

6.1.2. **Definición**. Un *álgebra* es un par ordenado **A**=(A,F), donde A es un conjunto no vacío y F = $(f_i)_{i \in I}$ es una familia de operaciones sobre A de aridad finita.

El conjunto A es el *universo* o el *conjunto subyacente* del álgebra A. Muchas veces en lo sucesivo se utilizará el mismo símbolo para designar al álgebra y a su conjunto subyacente. En caso de que convenga remarcar la distinción, se designará al álgebra con la letra, en negrita, que se utiliza para designar a su conjunto subyacente. Un álgebra es *finita* si su universo A es finito, y es *trivial* si $|A| = 1$.

Los elementos de la familia F son las *operaciones fundamentales o básicas* del álgebra; el conjunto de índices I de la familia F es el conjunto de *símbolos operacionales* del álgebra. La función ρ de I en N, que asigna a un símbolo operacional $i \in I$ el rango de la operación f_i, es la *función rango* del álgebra.

Si el número k, de índices de la familia F es pequeño, se acostumbra ordenar los elementos de I en la forma $i_1,...,i_k$, de modo que, para todo j, j=1,...,k-1, $\rho(i_j) \geq \rho(i_{j+1})$ y , en ese caso, el álgebra **A** se denota por la k+1 upla $(A, f_{i1},..., f_{ik})$.

La función rango de un álgebra **A** se llama también el tipo de **A**.
Un álgebra **A** es *similar* a un álgebra **B** si la función rango de **A** es igual a la función rango de **B**, ó sea si **A** y **B** tienen el mismo tipo.
La relación de similaridad entre álgebras es una relación de equivalencia.

Un álgebra $\mathbf{A} = (A,(f_i)_{i \in I})$ es una *reducción* de un álgebra $\mathbf{B} = (B, (g_j)_{j \in J})$, o **B** es una *expansión de* **A**, si $A = B$, la función rango de **A** es una restricción de la función rango de **B** y, para todo $i \in I$, $f_i = g_i$. Es decir, **B** se obtiene de **A** agregando otras operaciones básicas.

Ejemplos

6.1.3. Si sg (o siguiente) denota la función de N en N, dada por, sg (n) = n+1, (N,sg) es un álgebra que tiene como única operación a una operación unaria.

6.1.4. Un reticulado es un álgebra $(L,\vee,\wedge)$ con dos operaciones binarias.

6.1.5. Un álgebra de Boole es un álgebra $\mathbf{B} = (B,\vee,\wedge, ' ,0,1)$ con dos operaciones binarias, una unaria y dos cero arias. El reticulado $(B,\vee,\wedge)$ es una *reducción* del álgebra de Boole **B**.

Ejercicios

6.1.6. Sea (A,f) un álgebra con una única operación unaria f. Sean x, y ∈A, se define la relación R en A dada por xRy si y sólo si existen enteros m, n ≥ 0 tales que

$f^m(x) = f^n(y)$ (se conviene en que $f^0(x)$ es x).

Probar que R es una equivalencia en A.

Las clases de equivalencia según R se llaman *componentes conexas* de (A,f). ([11]).

6.2. Semigrupos, monoides y grupos.

6.2.1. **Definición.** Un *semigrupo* es un álgebra (S,.) tal que . es una operación binaria asociativa (es decir, para toda terna a,b,c de elementos de S, (a.b).c = a.(b.c)). Si además, la operación . es conmutativa, se dice que (S,.) es un semigrupo conmutativo.

6.2.2. **Definición.** Un *monoide* es un álgebra (M, . , 1) tal que (M,.) es un semigrupo y 1 ∈M, denota una operación 0-aria cumpliendo, para todo a ∈ M, a.1 = 1.a = a. El monoide es conmutativo si el semigrupo (M , .) es conmutativo. El elemento 1 es la unidad de M.

6.2.3. **Definición** Un *grupo* es una álgebra $(G, . ,^{-1},1)$ tal que $(G,.,1)$ es un monoide y $^{-1}$ es una operación unaria cumpliendo, para todo $a \in G$, $a.a^{-1} = a^{-1}.a = 1$. Si el semigrupo $(G , .)$ es conmutativo se dice que el grupo es conmutativo o *abeliano* .

Ejemplos

6.2.4. Si R_A denota el conjunto de todas las relaciones binarias sobre un conjunto A, entonces $(R_A,.,I_A)$ es un monoide, donde . denota la composición de relaciones (ver 1.2) e I_A la relación identidad. En general, es un monoide no conmutativo que no puede expandirse a un grupo.

6.2.5. Un semireticulado (S,.) (ver 4.4) es un semigrupo conmutativo. Se dice que es idempotente porque, para todo $a \in S$, a.a=a.

6.2.6. Si + denota la suma usual entre números naturales, se tiene que (N,+) es un semigrupo conmutativo que puede expandirse al monoide (N,+,0), pero no a un grupo.

6.2.7. Si + denota la suma usual entre enteros y - la aplicación de Z en Z que a cada entero le asigna su opuesto, se tiene que (Z,+,-,0) es un grupo abeliano que será llamado el *grupo de los enteros* .

6.2.8. Sean p un número entero mayor que 1, R la relación congruencia módulo p en Z (3.1.4) y Zp el conjunto de los enteros módulo p (3.2.7). Si a,b,c,d son enteros tales que aRb, y cRd, entonces (a+c) R (b+d). Luego puede definirse una operación binaria, también denotada +, en Zp, por : R(a)+R(c)=R(a+c). Como también de aRb se deduce (-a) R (-b), puede definirse la operación unaria, denotada -, sobre Zp, por -R(a)=R (-a). Se demuestra fácilmente que el álgebra (Zp,+,-,R(0)) es un grupo abeliano, llamado el *grupo de los enteros módulo p* .

6.2.9. Si P es el conjunto de los números enteros pares y . la multiplicación usual, (P,.) es un semigrupo conmutativo que no puede expandirse a un monoide.

6.2.10. Sea A un conjunto. Denotaremos A^A al conjunto de todas las aplicaciones de A en A, e id_A a la aplicación idéntica sobre A.
Sean o y ¤ las operaciones binarias sobre A^A, dadas por : fog(a)=f(g(a)) y f ¤g(a) = g(f(a)), respectivamente, para todo a de A. Entonces (A^A,o, id_A) y $(A^A,¤,id_A)$ son monoides, en general, no conmutativos.
Si S(A) designa al subconjunto de A^A formado por todas las biyecciones de A en A, o permutaciones de A, se tiene que $id_A \in S(A)$, y que para todo $f \in S(A)$, existe una única aplicación $f^{-1} \in S(A)$ tal que $fo f^{-1} = f^{-1} of=id_A$. Se tiene entonces que $(S(A),o,^{-1}, id_A)$ y $(S(A),¤,^{-1},id_A)$ son grupos, el primero

de los cuales se llama el *grupo de las permutaciones de* A, y *grupo simétrico de orden n,* en el caso A = {1,...,n}.

6.2.11. Sean A un conjunto no vacío y . la operación binaria sobre A definida por: a.b = b. Entonces (A,.) es un semigrupo denotado A^d, que no puede expandirse, en general a un monoide. En forma análoga se define a^i=(A,.), poniendo a.b=a.

6.2.12. **Definición.** Sea *S* = (S,.) un semigrupo. Un elemento u∈S es *neutro* en *S* , o es una *unidad* de *S* , si para todo a∈S, a.u = u.a=a.
Si u es una unidad de *S* , el semigrupo se expande al monoide (S,.,u). Si u y u´ son unidades de *S* , se tiene que u.u´ = u y u .u´ = u´ , con lo cual *S* tiene a lo sumo una unidad.
A partir de *S* se define un monoide S^1 como sigue: si *S* tiene una unidad u. S^1 = (S,.,u). En caso contrario, sea 1 un elemento no perteneciente a S. Ponemos S^1 = SU{1} y definimos una operación binaria * en S^1 por : a *b= a.b, para a, b ∈ S y a*1 = 1* a = a, para a ∈S^1. Es fácil verificar que (S^1,*,1) es un monoide. Se dice que S^1 ha sido obtenido de S por *adjunción de una unidad.*

6.2.13. **Definición.** Sea **M** = (M,.,1) un monoide. Un elemento a de M es *invertible* si existe b. en M, tal que a.b = b.a = 1.

Si tal elemento b existe, entonces es único, ya que si un elemento b´ tiene la misma propiedad, resulta (b.a).b´ = 1.b´= b´y b.(a.b´) = b.1 = b, de donde b = b´ . Se dice que b es el *inverso* de a y se escribe $b=a^{-1}$. De la definición resulta claramente que $(a^{-1})^{-1}= a$.
Si todo elemento de M es invertible, queda definida sobre M una operación unaria $^{-1}$ y resulta que **M** se expande al grupo (M, . , $^{-1}$, 1).

6.2.14. **Teorema.** *En un grupo (G, . , $^{-1}$, 1) vale la propiedad, llamada cancelativa, siguiente: para toda terna a,b,c de elementos de G, a.c = b.c o c.a = c.b implica a=b.*
Demostración. Si a.c = b.c, entonces $(a.c).c^{-1} = (b.c).c^{-1}$.
Aplicando la propiedad asociativa y puesto que $c.c^{-1} = 1$, resulta a= b. Si c.a = c.b, se multiplica a la izquierda por c^{-1}. ∎

6.2.15 **Definición.** Un elemento a de un álgebra **A** es *idempotente,* con respecto a una operación binaria, fundamental ., de **A** si a.a = a.

6.2.16. **Teorema.** *En un grupo, el único elemento idempotente es la unidad.*
Demostración. Si a es un elemento idempotente de un grupo $(G,.,^{-1},1)$, se tiene, a.a = a = 1.a . Aplicando la propiedad cancelativa, resulta a = 1. ∎

Ejercicios

6.2.17. Un elemento z de un semigrupo S se llama *cero* a *izquierda* (respectivamente *cero* a *derecha)* si z.s=z (respectivamente si s.z=z) para todo s en S. Se llama *cero* si es a la vez cero a izquierda y cero a derecha.

a) Probar que si z es un cero a izquierda de un semigrupo S, entonces todos sus múltiplos a izquierda xz ($x \in S$) son también ceros a izquierda.

b) Encontrar un semigrupo que tenga identidad a izquierda y cero a derecha y que no sea monoide.

c) Sea S un semigrupo con un cero a izquierda y un cero a derecha. Probar que son iguales y que éste es el único cero del semigrupo.

d) Mostrar que un grupo con dos o más elementos no puede tener ningún cero.

e) Sea B un conjunto con más de un elemento. Probar que el monoide de todas las transformaciones de B tiene más de un cero a izquierda y ningún cero a derecha.

6.2.18. Sea X un conjunto. Probar que (P(X),$\cup$) y (P(X), $\cap$) son monoides conmutativos.

6.2.19. Demostrar que si todo elemento de un grupo es su propio inverso entonces el grupo es abeliano.

6.2.20. Sean a,b números reales y f_{ab} una función de **R** en **R** definida por $f_{ab}(x)=ax+b$. Sea $G=\{f_{ab}; a, b \in \mathbf{R}, a \text{ distinto de } 0\}$, probar que $(G,o,^{-1}, id)$ es un grupo.

6.2.21. Sean (M,.,1) un monoide y $A \subseteq M$. Para todo $a \in A$ se define la aplicación f_a de M en M definida por $f_a(x) = a.x$.
Mostrar que en el álgebra $(M, (f_a)_{a\in A})$ se verifica que $f_{a_1} \ldots f_{a_n}(x) = f_{b_1}\ldots f_{b_k}(x)$ si y sólo si $a_1 \ldots a_n = b_1 \ldots b_k$.

6.3 Anillos

6.3.1. **Definición.** Un anillo es un álgebra (A,+,.,-.0) tal que (A,+,-,0) es un grupo abeliano, (A,.) es un semigrupo y se cumple la propiedad siguiente, llamada *distributiva* de . con respecto a +,: para toda terna a,b,c de elementos de A, a.(b+c) = a.b+a.c y (b+c).a = b.a+ c.a.
Si (A,.) es un semigrupo conmutativo, se dice que el anillo **A** es conmutativo. Se acostumbra llamar *suma* a la primera operación y *producto* a la segunda.
Un anillo *con unidad* es un álgebra **A** = (A,+,.,-,0,1) tal que (A,+,.,-,0) es un anillo y (A,.,1) es un monoide. El anillo con unidad **A** es un *cuerpo* si todo elemento de A, distinto de 0, es invertible en el monoide (A,.,1).

Ejemplos

6.3.2. A partir del grupo *de los enteros* (Z,+,-,0) se obtiene el anillo con unidad de los enteros (Z,+,.,-,0,1) tomando como segunda operación binaria a la multiplicación usual. Este anillo no es un cuerpo, en cambio, los conjuntos : K, de los números racionales, R de los números reales y C, de los números complejos, son cuerpos, con las operaciones usuales, 0 y 1.

6.3.3. A partir del grupo de los enteros módulo p (6.2.8) se obtiene el anillo con unidad de *los enteros módulo p*

$$(Zp,+,.,-,R(0),R(1)),$$

donde . es la operación binaria definida por : R(a) . R(b) = R(a .b) (se demuestra fácilmente que si aRa´ y bRb´ entonces (a .b)R (a´. b´)).

6.3.4. Si m es un número entero distinto de 1, el conjunto de los múltiplos enteros de m, con la suma y el producto usual entre enteros y 0 como operación cero aria, es un anillo conmutativo que no puede extenderse a un anillo con unidad.

6.3.5. Sea **A** = (A,+,.,-,0) un anillo y $A^{n\times n}$, con n entero mayor o igual que 1, el conjunto de las matrices con coeficientes en A, de n filas y n columnas. Definiendo la suma de las matrices a y b por

$(a+b)_{ij} = a_{ij}+b_{ij}$

y el producto por

$$(a.b)_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj}$$

se obtiene un anillo $(A^{nxn}, +,.,-,o)$, donde $(-a)_{ij} = -a_{ij}$ y $o_{ij}=0$, para todo i,j, en general, no conmutativo. Si (A,.) tiene unidad 1, la matriz u dada por $u_{ij}=1$, si i=j y $u_{ij}=0$, si $i\neq j$, es unidad de $(A^{nxn},.)$.

6.3.6. Sea C el cuerpo de los números complejos (las operaciones son las usuales) y sea K el subconjunto de C^{2x2} dado por las matrices de la forma

$$\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix}$$

Se comprueba inmediatamente que K, con las operaciones de C^{2x2}, la matriz nula y la matriz unidad, constituye un cuerpo no conmutativo.

6.3.7. Sea R[x] el conjunto de los polinomios en la indeterminada x a coeficientes reales. Designando con + y . a la suma y al producto, respectivamente, usuales entre polinomios, con -p al polinomio opuesto del polinomio p y con o al polinomio nulo, se obtiene que (R[x], +,.,-,o) es un anillo conmutativo.

6.3.8, Sea $(B,v,\wedge,',0,1)$ un álgebra de Boole. Sea Δ la operación binaria sobre B definida por

$$a\Delta b = (a\wedge b') \vee (a' \wedge b),$$

Resulta fácilmente que Δ es una operación asociativa (ver (5.1.10)) y conmutativa, y que, para todo $a\in B$, $a\Delta a = 0$. Luego, $(B,\Delta,id_B,0)$ es un grupo abeliano. Como además $\wedge$ es distributiva con respecto a Δ, se tiene que $(B,\Delta,\wedge,id_B,0,1)$ es un anillo conmutativo con unidad.

6.3.9. Sea X un conjunto y $(A,+,.,-,0)$ un anillo. Definimos sobre el conjunto A^X,
de las aplicaciones de X en A, las siguientes operaciones binarias, denotadas también con + y .,
$(f+g)(x) = f(x) + g(x)$ y $(f.g)(x) = f(x).g(x)$, para todo $x\in X$, y la operación unaria - , dada por
$(-f)(x) = -f(x)$, para todo $x\in X$.
Resulta que $(A^X,+,.,-,o)$ es un anillo, donde o denota la aplicación constantemente igual a 0. Este anillo es conmutativo si lo es A y se puede expandir a un anillo con unidad si (A,.) tiene unidad.

6.3.10. **Teorema.** *Si $(A,+,.,-,0)$ es un anillo, entonces, para todo par a,b de elementos de A. valen las siguientes propiedades*
1) $a.0 = 0.a = 0$,

2) (-a) . b = a.(-b) = -(a.b),

3) (-a).(-b) = a.b.

Demostración. Por la propiedad distributiva, a.0 = a(0+0) = a.0+a.0. Luego 0+a.0 = a.0+a.0. Por la propiedad cancelativa del grupo (A,+,-,0), resulta 0 = a.0. En la misma forma resulta 0.a=0.

Por la propiedad distributiva, a.b + (-a).b = (a-a).b = 0.b = 0. Luego, (-a).b = - (a.b). Análogamente resulta a. (-b) = - (a.b).

Por lo recién demostrado, (-a).(-b) = -(a.(-b)) = -(-(a.b)) =a.b. ∎

Ejercicios

6.3.11. Sea $Z(2^{1/2})$ el conjunto de los números reales de la forma $m+n.2^{1/2}$, donde m,n son enteros. Mostrar que $(Z(2^{1/2}),+,.,-,0,1)$, siendo las operaciones indicadas las habituales de los números reales, es un anillo.

6.3.12. Sean a,b,c elementos de un anillo A. Probar que:

a) Si a.b=b.a y si existe b^{-1}, entonces $a.b^{-1} = b^{-1}.a$

b) Si a.b=b.a y a.c=c.a , entonces a.(b.c) = (b.c).a

6.3.13. Sea A=(A+,.,-,0,1) un anillo con unidad. Sea U el subconjunto de A formado por los elementos a de A para los que existe en A el elemento a^{-1} tal que $a.a^{-1} = a^{-1}.a = 1$.
Probar que $U=(U,.,^{-1},1)$ es un grupo.

6.3.14. Sea **A**= (A+,.,-,0,1) un álgebra que satisface todos los axiomas de los anillos con unidad con la posible excepción de a+b=b+a, para todo a, b ∈ A. Probar que esta propiedad debe verificarse en **A**. (**Indicación:** Desarrollar (a+b)(1+1) en dos formas).

6.3.15. Los *cuaternios reales* son los símbolos de la forma $\propto o + \propto_1 i + \propto_2 j + \propto_3 k$, donde $\propto t$ es un número real para t=0,...,3.
Dos cuaternios $X= \propto o + \propto_1 i + \propto_2 j + \propto_3 k$, $Y = \beta o + \beta_1 i + \beta_2 j + \beta_3 k$,
son iguales si $\propto t = \beta t$, para t=0,...,3.
Sea Q el conjunto de todos los cuaternios reales, para X,Y ∈ Q se definen las operaciones siguientes:
$X+Y = (\propto o+\beta o) + (\propto_1+\beta_1) i + (\propto_2+\beta_2) j + (\propto_3+ \beta_3) k$
$X.Y = (\propto o\beta o - \propto_1\beta_1 - \propto_2\beta_2 - \propto_3\beta_3) + (\propto o\beta_1 + \propto_1\beta o + \propto_2\beta_3 - \propto_3\beta_2) i +$
$(\propto o\beta_2 + \propto_2\beta o + \propto_3\beta_1 - \propto_1\beta_3) j + (\propto o\beta_3 + \propto_3\beta o + \propto_1\beta_2 - \propto_2\beta_1)k$
$0 = 0+0i+0j+0k$, $1 = 1+0i+0j+0k$.
Definir la operación - de Q en Q y probar que (Q,+,.,-,0,1) es un anillo no conmutativo con unidad.

Encontrar el grupo U formado por los elementos invertibles de Q.

6.3.16 Un *dominio de integridad (o dominio entero)* es un anillo conmutativo y sin divisores de cero, esto es, tal que a.b =0 implica a=0 o b=0, para todo par a,b de elementos del anillo.
Sea A un anillo con unidad tal que para todo a∈ A, a^2 = a. Probar que:
a) Para todo a∈ A, a+a = 0,
b) A es conmutativo.
c) Si A tiene más de dos elementos, entonces A no es un dominio de integridad.

6.3.17. Sea D un dominio de integridad finito. Probar que D es un cuerpo.
6.3.18. Probar que todo cuerpo conmutativo es un dominio de integridad.

6.4 Semianillos

6.4.1. **Definición.** Un semianillo es un álgebra S = (S.+,.,0,1) tal que
1) (S,+,0) es un monoide conmutativo.
2) (S,.,1) es un monoide,
3) la operación . es distributiva con respecto a la operación +,
4) para todo a∈ S, a.0 = 0.a = 0.

Se dirá que 0 es el elemento *nulo* de S y 1 la *unidad* de S.

Ejemplos.

6.4.2. Si $(A,+,.,-,0,1)$ es un anillo con unidad, entonces, de acuerdo con 6.3.1, $(A,+,.,0,1)$ es un semianillo.

6.4.3. Si $(B,\vee,\wedge,',0,1)$ es un álgebra de Boole, $(B,\vee,\wedge,0,1)$ es un semianillo.

6.4.4. $(N,+,.,0,1)$ es un semianillo, donde + y . designan, respectivamente, a la suma y al producto usual en el conjunto N de los números naturales.

6.4.5 Siendo R el conjunto de los números reales, $(R\cup\{\infty\},\min,+,\infty,0)$ es un semianillo, donde min(a,b) = mínimo {a,b}, para $a,b \in R$,+ es la suma usual en R y $0 \in R$.

6.4.6. Siendo R^+ el conjunto de los números reales mayores o iguales que 0, $(R^+ \cup\{\infty\},\max,\min,0,\infty)$ es un semianillo, donde max (a,b) = máximo {a,b}, para $a,b \in R^+$, min está definido como en 6.4.5. y $0\in R$.

6.4.7. Si [0,1] es el intervalo real de extremos 0 y 1, $([0,1], \max,.,0,1)$ es un semianillo, donde max está definido como en 6.4.6 y $0,1 \in R$.

Capítulo 7

Subálgebras y morfismos

Los conceptos de subreticulado y subálgebra de Boole, así como los de homomorfismos de reticulados y álgebras de Boole, son ahora generalizados presentando los subuniversos y subálgebras de un álgebra y los homomorfismos de álgebras de un mismo tipo. Se estudian las subálgebras generadas por un conjunto, y en particular, los semigrupos, monoides y grupos generados por un elemento, que se llaman *cíclicos.*
Según un teorema de Cayley, todo grupo es isomorfo a un grupo de permutaciones de su conjunto subyacente. Se expone este teorema y los del mismo tipo para semigrupos y monoides.

7.1 Subuniversos y subálgebras

7.1.1. **Definición.** Sean **A** un álgebra y f una operación n-aria fundamental de **A**. Un subconjunto B de A es *cerrado* con respecto a f si, para todo $\bar{b} \in$

B^n , $f(\bar{b}) \in B$. El conjunto B es un *subuniverso* de **A** si es cerrado para todas las operaciones fundamentales de **A**.

En particular, si B es un subuniverso de **A** y f es una operación 0-aria de **A**, la definición precedente implica que $f(\varnothing) \in B$, con lo cual, un subuniverso de un álgebra que tiene operaciones 0-arias no es vacío.

7.1.2. **Definición.** Una subálgebra de un álgebra **A** es un álgebra **B** = (B,G) tal que B es un subuniverso no vacío de **A** y G es la familia de operaciones fundamentales de **A** restringidas a **B**.

Ejemplos

7.1.3. Las subálgebras de un reticulado **L** son los subreticulados de **L**, según 4.2.1, y las subálgebras de un álgebra de Boole **B** son las subálgebras de **B**, según la definición 5.2.1.

7.1.4. Un subuniverso de un semigrupo S = (S,.) es un subconjunto S´de S tal que, para todo par a,b de elementos de S´, a .b $\in$ S´.
Puesto que la operación de S restringida a un subuniverso sigue siendo asociativa, resulta que una subálgebra de un semigrupo es también un

semigrupo, llamado *subsemigrupo* de S. Resulta también inmediatamente que una subálgebra de un monoide $\mathbf{M}=(M,.,1)$ es un monoide, llamado *submonoide* de **M**. La unidad del submonoide es 1.

7.1.5. Un subuniverso de un grupo $\mathbf{G}=(G,.,^{-1},1)$ es un subconjunto G' de G tal que $1 \in G'$ y para todo par a,b de elementos de G', $a.b \in G'$ y $a^{-1} \in G'$. Una subálgebra de G es también un grupo, cuya unidad coincide con la de G. Se dice que es un *subgrupo* de G.
Los subuniversos de G quedan también caracterizados en la forma siguiente (ejercicio 7.1.7): un subconjunto G' de G es un subuniverso de G si y sólo si $G' \neq \emptyset$ y, para todo par a,b de elementos de G', $a.b^{-1} \in G'$.

7.1.6. **Teorema .** *Todo subuniverso del grupo* $\mathbf{Z} = (Z,+,-,0)$ *de los enteros es de la forma* $\{km; k \in Z\}$, *para algún número entero m (es decir, igual al conjunto de los múltiplos de un entero m).*
Demostración. Para un entero m, pongamos $[m] = \{km; k \in Z\}$.
Puesto que $0 \in [m]$, $km+k'm = (k+k')m$ y $-(km) = (-k)m$ resulta que [m] es un subuniverso de **Z**.
Recíprocamente, sea S un subuniverso de **Z**. Entonces $0 \in S$. Si $S = \{0\}$, $S = [0]$, en caso contrario, sea m el primer entero estrictamente positivo perteneciente a S. Puesto que para un entero k, km es igual a la suma de k

veces el entero m, se tiene que $[m] \subseteq S$. Sea ahora $s \in S$. Existen enteros q y r tales que
$s=qm+r$ y $0 \leq r < m$.
Puesto que $r= s-qm$ y S es un subuniverso, resulta $r \in S$, de donde por la hipótesis efectuada sobre m, $r = 0$. Entonces $s \in [m]$, con lo cual $S \subseteq [m]$. ∎

Ejercicios

7.1.7. Sea $G=(G,.,^{-1},1)$ un grupo. Probar que un subconjunto G' de G es un subuniverso de G si y sólo si G' es no vacío y, para todo par a,b de elementos de G', $a.b^{1} \in G'$

7.1.8. El *centro* de un semigrupo S es el conjunto c(S) de elementos que conmutan con todo elemento de S.
Probar que, si es no vacío, el centro c (S) del semigrupo S, es un subsemigrupo de S.

7.1.9. Sea M un monoide. Probar que el conjunto de los elementos invertibles a izquierda (respectivamente a derecha) de M es un submonoide de M.
Probar que si M es conmutativo el conjunto de los elementos idempotentes de M, es un submonoide de M.

7.1.10. Sea S=(S,.) un semigrupo, si A, B$\subseteq$ S, A .B denota el conjunto {a .b ; a$\in$ A, b$\in$ B}. Si s$\in$ S y A$\subseteq$S, se denota con s.A al conjunto { s.a ; a$\in$ A}. Un subsemigrupo I de un semigrupo S=(S,.) se llama *ideal a izquierda* (respectivamente *ideal a derecha*) de S si S.I$\subseteq$I (respectivamente I.S$\subseteq$ I). Se dice que I es un ideal de S si I es a la vez ideal a izquierda y a derecha de S (ver (8.2.1)).

En cada caso si I es un subconjunto propio, no vacío de S, I es un ideal propio a izquierda, ideal propio a derecha o ideal propio, según corresponda.

a) Sea n un entero, probar que el conjunto de los múltiplos de n es un ideal del semigrupo (**Z**,.) y que no es ideal del semigrupo (Q,.), siendo Q el conjunto de los números racionales.

b) Probar que {$\varnothing$} es un ideal de (P (X),$\cap$), para un conjunto cualquiera X.

c) Sean S un semigrupo con algún cero a izquierda e I={ z$\in$ S; z es cero a izquierda de S}. Probar que todo subconjunto no vacío de I es un ideal a derecha de S.

7.1.11. Probar que si un semigrupo S no tiene ningún ideal propio a izquierda entonces S.s=S, para todo s $\in$ S.

(Vale la propiedad análoga para un semigrupo sin ideales propios a derecha y la igualdad s.S=S).

7.1.12. Probar que un semigrupo que no tiene ideales propios a izquierda ni a derecha es un grupo.
(Indicaciones: Usar (7.1.11) para encontrar una identidad a izquierda, análogamente buscar una identidad a derecha, probar que son iguales y que esa identidad es la única. Usar de nuevo (7.1.11) y la existencia de esa identidad para encontrar un inverso a izquierda y uno a derecha de un elemento cualquiera, luego probar que éstos son iguales.).

7.1.13. Mostrar que un grupo no tiene ideales propios de ninguna clase Reunir este resultado con el de (7.1.12) y enunciar la conclusión.

7.1.14. Sea S un semigrupo finito y sea I el conjunto de los ideales de S.
a) Sean $I_1, I_2 \in I$. Probar que $I_1.I_2 \subseteq I_1 \cap I_2$ y que $I_1.I_2$, $I_1 \cap I_2$ e $I_1 \cup I_2$ pertenecen a I.
b) Probar que $(I, \subseteq)$ es un reticulado.
c) Sean $I_1,...,I_n$ **todos** los elementos de I probar que $I_1 .....I_n = \cap_{i=1,...,n} I_i$.
d) Probar que si z es un cero de S, entonces $\cap_{i=1,...,n} I_i = \{z\}$, siendo I_i si=1,...,n, todos los elementos de I.

7.1.15. Determinar los subgrupos (subsemigrupos que además son grupos) maximales de los semigrupos A^i, $(P(E), \cap)$ y (X^X, o).

Determinar los elementos idempotentes de A^i y de $(P(E),\cap)$.

7.2 Subálgebras generadas por un conjunto.

7.2.1. **Teorema.** *La intersección de una familia de subuniversos de un álgebra A es un subuniverso de A.*

Demostración. Sea $(U_i)_{i\in I}$ una familia de subuniversos de un álgebra **A**. Si f es una operación fundamental n-aria y $\bar{a}\in(\cap U_i)^n$, resulta que $\bar{a}\in(U_i)^n$, para todo $i \in I$,

con lo cual $f(\bar{a}) \in U_i$, para todo $i\in I$, y entonces $f(\bar{a})$ pertenece a la intersección de la familia dada. ∎

El teorema precedente justifica la definición siguiente

7.2.2. **Definición.** Sean **A** un álgebra y X un subconjunto de A. El *subuniverso de* **A** *generado por* X (o *engendrado* por X) es la intersección de la familia de los subuniversos de **A** que contienen a X.

Se designará con $Sg^{\mathbf{A}}[X]$, o simplemente con [X] , si **A** está sobrentendida, al subuniverso de **A** generado por X. Si A = [X] se dice que X genera **A** o que **A** está generada por X. Si además X es finito, se dice que **A** está finitamente generada. Más generalmente, si [X] no es vacío, la subálgebra de **A** generada por X es la subálgebra de **A** cuyo universo es [X]. Es evidente que [A] = A.

Designaremos con $U(\mathbf{A})$ al conjunto de todos los subuniversos del álgebra **A**.

7.2.3. **Teorema.** *El conjunto U(A) de todos los subuniversos de un álgebra A, ordenado por inclusión, es un reticulado completo. Si S es un subconjunto de U(A), entonces el ínfimo y el supremo de S en $(U(A),\subseteq)$ están dados respectivamente por*

$$\inf S = \bigcap_{S\in\mathcal{S}} S \quad \text{y} \quad \sup S = \left[\bigcup_{S\in\mathcal{S}} S\right]$$

Demostración. Puesto que $\bigcap_{S\in\mathcal{S}} S$ es claramente el ínfimo de S en $(U(\mathbf{A}),\subseteq)$ y que A es el último elemento de este conjunto ordenado, resulta de 4.1.13 que $(U(\mathbf{A}),\subseteq)$ es un reticulado completo. En general, [X] es el primer elemento del conjunto de los subuniversos de **A** que contienen a X. Luego sup S tiene el valor del enunciado. ■

El próximo teorema muestra la construcción de [X] paso a paso: si X no es un subuniverso, se agregan a X los resultados de todas las operaciones fundamentales de **A** aplicadas a elementos de X; a este nuevo conjunto se vuelven a aplicar todas las operaciones de **A** y se agregan los resultados; continuando en la misma forma se obtiene una sucesión de subconjuntos de A, $X \subseteq X_1 \subseteq \ldots \subseteq X_r \subseteq \ldots$; se demostrará que la unión de los mismos es [X].

7.2.4. **Teorema.** *Sean* **A** *un álgebra y* X *un subconjunto de* A . *Si* Xo,...,Xr,Xr+1... *es la sucesión de subconjuntos de* A *definida por inducción en la forma siguiente*

$$Xo = X,$$

supuesto definido Xr, $Xr+1 = X_r \cup \{f(\bar{a}) \; ; f$ *es una operación fundamental de* **A** y $\bar{a} \in (Xr)^{\rho(f)}\}$, *entonces* $Sg^{\mathbf{A}}[X] = \bigcup_{r \in N} X_r$.

Demostración. Sea B la unión de los Xr, con $r \in N$.

Demostraremos primero que B es un subuniverso de **A**. En efecto, sean f una operación fundamental de **A**, n-aria, y $\bar{a} \in B^n$. Puesto que n es finito y $X_r \subseteq Xr+1$, para todo $r \in N$, existe $m \in N$ tal que $\bar{a} \in (Xm)^n$. Entonces $f(\bar{a}) \in Xm+1$ y, por lo tanto, $f(\bar{a}) \in B$.

Como $X \subseteq B$ y $Sg^{\mathbf{A}}[X]$ es la intersección de todos los subuniversos de **A** que contienen a X, resulta $Sg^{\mathbf{A}}[X] \subseteq B$.

Sea ahora U un subuniverso de **A** que contiene a X. Probaremos, por inducción sobre r, que, para todo $r \in N, X_r \subseteq U$.

Por hipótesis, $X_o = X \subseteq U$. Supongamos que $X_r \subseteq U$, para un $r \geq 0$ y sea f una operación fundamental de **A** de aridad n. Si $\bar{a} \in (Xr)^n$, entonces $\bar{a} \in U^n$, con lo cual, siendo U un subuniverso, $f(\bar{a}) \in U$. Entonces $Xr+1 \subseteq U$.

Se tiene entonces que $B \subseteq U$ y como $S_g{}^{\mathbf{A}}[X]$ es un subuniverso que contiene a X, $B \subseteq S_g{}^{\mathbf{A}}[X]$. ∎

Sea **A** un álgebra. Asignando a cada subconjunto X de A el subuniverso [X] se obtiene una aplicación de $P(A)$ en $P(A)$. Esta aplicación tiene las siguientes propiedades. La demostración se deja como ejercicio (7.2.11).

7.2.5. **Teorema.** 1) $X \subseteq [X]$,

2) $[[X]] = [X]$,

3) si $X \subseteq Y$ entonces $[X] \subseteq [Y]$,

4) B es un subuniverso de **A** si y sólo si $B = [B]$.

Ejemplos

7.2.6 Sean B = (B,v,∧,´,0,1) un álgebra de Boole y X un subconjunto de B. Si
X = ∅,[X] es la intersección de todos los subuniversos de B, con lo cual [X] = {0,1}. Si X ≠ ∅, probaremos que los elementos de [X] son todos los de la forma

(1) $\left(x_{11} \wedge \ldots \wedge x_{1r_1}\right) v \left(x_{21} \wedge \ldots \wedge x_{2r_2}\right) v \ldots v \left(x_{n1} \wedge \ldots \wedge x_{nr_n}\right)$

con $x_{ij} \in X$ o $x_{ij}' \in X$, para todo i,j, $1 \leq i \leq n$ y $1 \leq j \leq r_i$.

Sea S el conjunto de los elementos de B de la forma (1).

Por el Teor. 7.2.4 $S \subseteq [X]$. Recíprocamente, si $a,b \in S$ es evidente que $avb \in S$ y, por la propiedad distributiva de ∧ con respecto a v, también $a \wedge b \in S$. Por las leyes de De Morgan y las propiedades distributivas, $a' \in S$. Tomando un $x \in S$, resulta que $0 = x \wedge x' \in S$ y $1 = x v x' \in S$. Además todo elemento x de X es de la forma (1) (tomando n=1, $r_1 = 1$ y $x_{11} = x$). Luego S es un subuniverso de B que contiene a X, con lo cual $[X] \subseteq S$.

7.2.7. Sean $S = (S,.)$ un semigrupo y X un subconjunto de S. Si X=∅, [X] es la intersección de todos los subuniversos de S. Como en S no hay operaciones 0-arias, ∅ es un subuniverso. Luego [X]=∅. Si X ≠ ∅, probaremos que [X] es el conjunto de todos los elementos de la forma (1) $x_1 . \ldots . x_n$, con $x_i \in X$ y n natural, $n \geq 1$.

Sea S´ el conjunto de los elementos de S de la forma (1). Por el Teor. 7.2.4, $S' \subseteq [X]$.

Además , si $a,b \in S'$, $a.b \in S'$ y $X \subseteq S'$. Luego, S´ es un subuniverso de *S* que contiene a X, con lo cual $[X] \subseteq S'$

7.2.8. Sean $\mathbf{M} = (M,.,1)$ un monoide y$X \subseteq M$. Si $X = \emptyset$,$[X] = \{1\}$, En caso contrario, razonando como en 7.2.7, es fácil ver que $[X] = \{1\} \cup \{x_1. \ ... \ ,x_n;$ $n \in N, n \geq 1, x_1,..., x_n \in X\}$.

7.2.9. Sean $G = (G,.,^{-1},1)$ un grupo y X un subconjunto de G. Si $X=\emptyset$,$[X]=$ {1}. En caso contrario, probaremos que [X] es el conjunto de los elementos de G de la forma

(1) $\qquad x_1. \ ... \ .x_n$, con $x_i \in X$ o $x_i^{-1} \in X$,

para todo i, i=1,...,n, y n natural, $n \geq 1$.

Sea S el conjunto de los elementos de la forma (1). Por el Teor. 7.2.4, $S \subseteq [X]$. Si $a,b \in S$, es inmediato que $a.b \in S$. Tomando $x \in S$, resulta que $1=x.x^{-1} \in S$.

Sea $a=x_1. \ ... \ x_n \in S$. Entonces $a^{-1} = x_n^{-1}, \ ... \ , x_1^{-1}$, de donde $a^{-1} \in S$. Como $X \subseteq S$,S es un subuniverso de G que contiene a X. Luego $[X] \subseteq S$.

Ejercicios

7.2.10. Sea A={a,b,c}, encontrar el submonoide del monoide de las transformaciones de A, generado por $\{f_1, f_2\}$ donde f1(z) =a, para todo $z \in A$ y f_2 toma los valores siguientes: $f_2(a)=b$, $f_2(b)=a$, $f_2(c)=b$.

7.2.11. Demostrar el teorema 7.2.5.

7.2.12. Describir el subreticulado generado por un conjunto X cuando X tiene un elemento y cuando X tiene dos elementos.
Idem para un álgebra de Boole.

7.3 Morfismos.

7.3.1. **Definición.** Sean $\mathbf{A} = (A,(f_i)_{i\in I})$ y $\mathbf{B} = (B,(g_i)_{i\in I})$ álgebras del mismo tipo. Un *morfismo u homomorfismo* de **A** en **B** es una aplicación h de A en B tal que, para todo $i\in I$, se cumple: si $n=\rho(i) >0$, para toda n -upla $(a_1,...,a_n)\in A^n$,
$h(f_i(a_1,...,a_n)) = g_i(h(a_1),...,h(a_n))$,
y si $\rho(i)=0$, $h(f_i(\varnothing)) = g_i(\varnothing)$.

Se escribirá h: $\mathbf{A} \rightarrow \mathbf{B}$ para designar a un morfismo h de **A** en **B**. Para demostrar que h es un morfismo de **A** en **B** se comprobará solamente la igualdad de 7.3.1 correspondiente al caso $\rho(i)>0$, pues el caso $\rho(i)=0$ sigue los mismos lineamientos que el anterior (basta reemplazar las n-uplas por $\varnothing$).

Sea h: $\mathbf{A} \rightarrow \mathbf{B}$ un morfismo. Si h es una aplicación inyectiva (resp. suryectiva, biyectiva) se dice que h es un *monomorfismo* (resp. epimorfismo, *isomorfismo*) de **A** en **B**. Un *endomorfismo* de **A** es un morfismo de **A** en **A**; un automorfismo de **A** es un isomorfismo de **A** en **A**. El álgebra **A** es *isomorfa* al álgebra **B** si existe un isomorfismo de **A** en **B**.

Ejemplos

7.3.2. Los morfismos de reticulados y los morfismos de álgebras de Boole, dados en 4.3 y en 5.3 respectivamente, son morfismos en el sentido de la definición 7.3.1.

7.3.3. Sean S =(S,.) y S' = (S,.) semigrupos. Un morfismo de S en S' es una función h: $S \rightarrow S'$ tal que, para todo par a,b de elementos de S, h(a.b)= h(a).h(b).

7.3.4. La función logaritmo, en una base determinada, es una biyección del conjunto R^+-{0} de los números reales mayores que 0 en el conjunto R de todos los números reales. Puesto que log (a.b)=log(a)+log(b), log. es un isomorfismo del semigrupo (R^+-{0},.) en el semigrupo (R,+).

7.3.5. Sean **M**=(M,.,1) y **M´** = (M´ ,.,1´) monoides. Un morfismo de **M** en **M´** es un morfismo h del semigrupo (M,.) en el semigrupo (M,.) tal que h(1)=1´.

7.3.6. Sea G=(G,.,$^{-1}$,1) y G´ =(G´ ,.,$^{-1}$,1´) grupos. Un morfismo de G en G´ es un morfismo h del monoide (G,.,1) en el monoide (G´,.,1´) tal que, para todo a∈G, h(a^{-1})=(h(a))$^{-1}$. Estas condiciones son superabundantes ya que h es un morfismo de G en G´ si y sólo si, para todo par a,b de elementos de G,

(1) h(a .b)=h(a).h(b)

(o, en forma equivalente, si y sólo si h es un morfismo del semigrupo (G,.) en el semigrupo (G´,.)).

En efecto, si vale la condición (1), h(1)=h(1.1)=h(1).h(1), con lo cual h(1) es idempotente en G´, de donde (6.2.16) h(1)=1´ . Por otra parte, para un elemento a de G,h(a^{-1}).h(a)=h(a^{-1}.a)=h(1)=1´y,análogamente, h(a). h(a^{1})=1´. Luego, por (6.2.13), h(a^{-1})=(h(a))$^{-1}$.

7.3.7. Sean **A** y **A´** anillos. Denotamos con + y ., respectivamente a la suma y al producto en **A** y en **A´**. De 7.3.6 y 7.3.3 se deduce que una aplicación h de A en A´ es un morfismo de **A** en **A´** si y sólo si para todo par a,b de elementos de A,

$$h(a+b)=h(a)+h(b) \quad y \quad h(a.b)=h(a).h(b).$$

7.3.8. **Teorema** *Si h es un isomorfismo de* **A** *en* **B**, *entonces* h^{-1} *es un isomorfismo de* **B** *en* **A**.

Demostración. Sean $\mathbf{A} = (A.(f_i)_{i\in I})$, $\mathbf{B} = (B,(g_i)_{i\in I})$, $i\in I$ y $n=\rho(i)$.

Si $(b_1,....,b_n)\in B^n$, se tiene

(1) $$h(h^{-1}(g_i(b_1,...,b_n)))= g_i(b_1,...,b_n).$$

Por otra parte, por ser h un morfismo de **A** en **B,**

$h(f_i(h^{-1}(b_1),...,h^{-1}(b_n))) = g_i(h(h^{-1}(b_1)),...,h(h^{-1}(b_n))) = g_i(b_1,...,b_n)$.

De (1), considerando que h es una función inyectiva, resulta

$h^{-1}(g_i(b_1,...,b_n)) = f_i(h^{-1}(b_1),...,h^{-1}(b_n))$. ∎

7.3.9. **Teorema.** *Si h es un morfismo de* **A** *en* **B** *y k es un morfismo de B en* ***C****, entonces koh es un morfismo de* **A** *en* **C.**

Demostración. Sean $\mathbf{A}=(A,(f_i)_{i\in I})$, $\mathbf{B}=(b,(g_i)_{i\in I})$, $\mathbf{C}=(C,(1_i)_{i\in I})$,e $i\in I$ tal que $\rho(i)=n$. Si $(a_1,...,a_n)\in A^n$, se tiene $(koh)(f_i(a_1,...,a_n)) = k(g_i(h(a_1),...,h(a_n))) = 1_i((koh)(a_1),...,(koh)(a_n))$. ∎

Para toda álgebra **A**, es inmediato que $id_{\mathbf{A}}$ es un automorfismo de **A**. Luego la relación $\mathbf{A} \approx \mathbf{B}$ si y sólo si **A** es isomorfa a **B**, es reflexiva y, por los teoremas precedentes, es simétrica y transitiva; luego, es una relación de equivalencia.

Sea End(**A**) el conjunto de los endomorfismos de un álgebra **A**.

Denotamos con o a la operación binaria sobre End(**A**) dada por (k,h)→koh. Por el teorema precedente, y teniendo en cuenta que la composición de funciones es asociativa resulta que (End(**A**),o,id) es un monoide.

Sea ahora Aut (**A**) el conjunto de los automorfismos de **A**. Si^{-1} denota a la función de A en A, que asigna a un automorfismo h el automorfismo inverso h^{-1}, resulta que $(Aut(\mathbf{A}),o,^{-1},id_{\mathbf{A}})$ es un grupo.

7.3.10 **Teorema.** *Sea h un morfismo de un álgebra* **A** *en un álgebra* **B** . *Si* A´ *es un subuniverso de* **A** *y* B´ *es un subuniverso de* **B**, *entonces* $h(A')$ *es un subuniverso de* **B** *y* h^{-1} *(***B´***) es un subuniverso de* **A**.

Demostración. Sean $(f_i)_{i\in I}$ y $(g_i)_{i\in I}$ las familias de operaciones fundamentales de **A** y **B** respectivamente.

Si g_i es una operación n-aria, y $b_1,...,b_n$ pertenecen a h(A´), existen $a_1,...,a_n \in A'$ tales que $h(a_i)=b_i$, para todo i, $1 \le i \le n$. Se tiene

$$g_i(b_1,...,b_n) = g_i(h(a_1),...,h(a_n)) = h(f_i(a_1,...,a_n)),$$

puesto que h es un morfismo. Siendo A´ un subuniverso de **A**, $f_i(a_1,...,a_n) \in A'$. Luego $g_i(b_1,...,b_n) \in h(A')$. Entonces h(A´) es un subuniverso de **B.**

Sean ahora f_i una operación n-aria y $a_1,...,a_n$ elementos de $h^{-1}(B')$. Entonces $h(a_i) \in B'$, para todo i, i=1,...,n. Como, por ser h un morfismo y B'un subuniverso, se tiene

$$h(f_i(a_1,...,a_n)=g_i(h(a_1),...,h(a_n)) \in B',$$

resulta que $f_i(a_1,...,a_n)$ pertenece a $h^{-1}(B')$. Luego $h^{-1}(B')$ es un subuniverso de **A**. ∎

7.3.11. **Teorema.** *Sea* **A** *un álgebra generada por un conjunto X. Si h y k son morfismos de* **A** *en un álgebra* **B** *tales que h y k coinciden en X. entonces h=k.*

Demostración. Sean $(f_i)_{i \in I}$ y $(g_i)_{i \in I}$ las familias de operaciones fundamentales de **A** y **B** respectivamente.

Sea Xo,...,Xr,Xr+1,... la sucesión de subconjuntos de A definida en 7.2.4. Puesto que Xo= X, h y k coinciden en Xo, por hipótesis. Supongamos que coinciden en Xr, para r≥0, y sea x un elemento de Xr+1 - Xr. Entonces existen i∈I y $x_1,...,x_n \in$Xr, donde n=ρ(i), tales que $x=f_i(x_1,...,x_n)$. Luego , $h(x)=g_i(h(x_1),...,h(x_n))$, y puesto que, $h(x_j)=k(x_j)$, para todo j, j=1...,n, resulta finalmente h(x)=k(x). ∎

Ejercicios

7.3.12. Sea f una aplicación de (R,+,-,0) en (R-{0},.,$^{-1}$,1) definida por f(a) = 2^a. Probar que f es un morfismo de grupos y que no es epimorfismo.

7.3.13. Probar que los monoides del ejercicio (6.2.18) son isomorfos.

7.3.14. Sea (S,.) un semigrupo. Se define la operación . en P (S) por : A.B={ a .b ; a ∈ A,b ∈ B}.
Probar que (P (S),.) es un semigrupo y que la función que a s ∈ S le asigna {s} ∈ P (S), es un monomorfismo de (S,.) en (P (S),.).

7.3.15. Sea G un grupo. Probar que si $a^2 = 1$, para todo a ∈ G, entonces G es abeliano.

7.3.16. Sean G un grupo y g un elemento fijo de G. Sea f la aplicación de G en G definida por f(x)= gxg^{-1}. Probar que f es un automorfismo de G.

7.3.17. Sean G y G´ dos grupos, B un conjunto generador de G y f una función de B en G.
Probar que si existe un morfismo de grupos de G en G´ tal que su restricción a B coincide con f, entonces este morfismo es único.

7.3.18. Sea $Z(2^{1/2})$ el anillo del ejercicio (6.3.11) y f la aplicación de este anillo en sí mismo, dada por $f(m + n.2^{1/2}) = m-n.2^{1/2}$. Probar que f es un morfismo de anillos. Establecer si f es monomorfismo o epimorfismo.

7.3.19. Sea A el conjunto de todas las funciones reales continuas definidas sobre el intervalo unitario cerrado, A es un anillo con las operaciones habituales de suma y multiplicación de funciones (teniendo en cuenta que la suma y el producto de dos funciones continuas es una función continua), la función opuesta, la función nula y la identidad.
Sean **R** el anillo de los reales y ϕ la aplicación de A en **R** dada por
ϕ (f(x)) = f (1/2).
Probar que ϕ es un morfismo de anillos. Encontrar el subconjunto de A cuya imagen por ϕ es 0.

7.4 Semigrupos, monoides y grupos cíclicos.

7.4.1. **Definición.** Sean **A** un semigrupo, monoide o grupo y a un elemento de A. Entonces la subálgebra generada por a se llama, respectivamente, el subsemigrupo, submonoide o subgrupo *cíclico* generado por a. Se dice que **A** es *cíclico* si A=[a], para algún elemento a de A.

Si $S = (S,.)$ es un semigrupo y $a \in S$, se define, para todo número entero $n>0$, la *potencia* n de a, poniendo

$$a^n = a. \ldots .a.$$
$$\text{n veces}$$

Si $\mathbf{M} = (M,.,1)$ es un monoide y $a \in M$, se define también la potencia *cero* de a, por : $a^0 = 1$. Finalmente, si $\mathbf{G} = (G,.,^{-1},1)$ es un grupo, se define las potencias *negativas* de a, poniendo, para todo entero $n>0$, $a^{-n} = (a^{-1})^n$.

7.4.2. **Teorema.** *Para todo elemento a de un grupo* G *y todo par de enteros m y n, se cumple que* $a^m . a^n = a^{m+n}$.

Demostración. Si m=0 o n=0, la igualdad del enunciado es evidente.

Supongamos m y n mayores que 0. Entonces,

$$a^m . a^n = (a. \ldots .a) . (a. \ldots .a) = a^{m+n}.$$
$$\text{m veces} \qquad \text{n veces}$$

$$a^{-m}. a^{-n} = (a^{-1})^m . (a^{-1})^n = (a^{-1})^{m+n} = a^{-(m+n)} = a^{-m-n} .$$

$$a^{-m} .a^n = (a^{-1})^m .a^n = (a^{-1} . \ldots . a^{-1}) (a. \ldots .a),$$
$$\text{m veces} \qquad \text{n veces}$$

lo que es igual, por la propiedad asociativa, a a^{-m+n}. ∎

De acuerdo con 7.2.7, si a es un elemento de un semigrupo S .

$$S_g^S [a] = \{ a^n; n>0\}.$$

Si a pertenece a un monoide **M**, por 7.2.8,

$$S_g^M [a] = \{ a^n ; n\geq 0\}.$$

Finalmente, si a pertenece a un grupo G, por 7.2.9 y 7.3.2,

$$S_g^G [a] = \{a^n ; n\in Z\}.$$

7.4.3. **Teorema.** *Si S = (S. .) es un semigrupo cíclico generado por un elemento a, entonces S es isomorfo al semigrupo (N-{0},+) o S es finito y existe un par de enteros r y m, r≥1 y m≥1, tales que S = {* $a,...,a^{r+m-1}$*}, cumpliéndose además que* $\{a^r,...,a^{r+m-1}\}$ *es el universo de un subsemigrupo de S isomorfo a (* Zm,+) (6.2.8).

Demostración. Caso 1. Para todo par r y s de enteros positivos, si $r\neq s$ entonces $a^r \neq a^s$.

La aplicaciòn de N-{0} en S=[a] dada por $n\rightarrow a^n$ es evidentemente biyectiva. Por el Teor. 7.4.2 a m+n le corresponde $a^{m+n} = a^m . a^n$, luego es un isomorfismo de (N{0},+) sobre *S* .

Caso 2. Existen enteros positivos r y s tales que $r\neq s$ y $a^r = a^s$.

Sea r el primer entero tal que $a^r = a^{r+x}$, para algún x>0, y sea m el primer entero tal que $a^r = a^{r+m}$. Entonces a,..., a^{r+m-1} son todos distintos.

Sea ahora t≥r+m. Luego, t-r≥m. Si q y p son el cociente y el resto, respectivamente, de la división de t-r por m, resulta t-r=mq+p, con 0≤p≤m, de donde t=r+mq+p, con lo cual $a^t = a^{r+mq}.a^p$

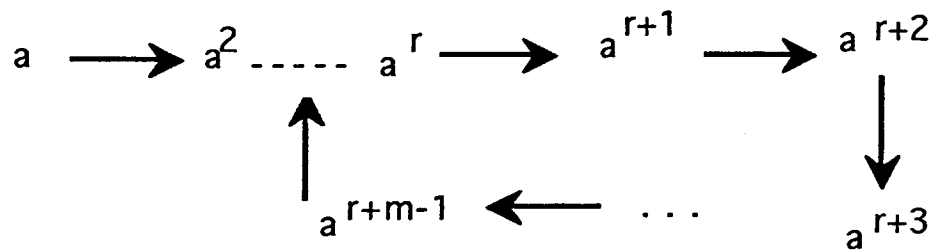
De $a^r = a^{r+m}$ resulta $a^r = a^{r+mq}$, y entonces, $a^t = a^{r+p}$, lo que muestra que $a^t \in \{a^r,...,a^{r+m-1}\}$. Luego $S = \{a,...,a^{r+m-1}\}$ y $B = \{a^r,...,a^{r+m-1}\}$ es un subuniverso de S .

Sea ahora $f:B \rightarrow Zm$ la aplicación dada por $f(a^{r+x}) = (r+x) \pmod m$.

Si $f(a^{r+x}) = f(a^{r+y})$ resulta que x-y es un múltiplo de m, de donde x=y por estar ambos números comprendidos entre 0 y m-1 . Puesto que $|B| = |Zm|$, f es biyectiva.

Por otra parte, $f(a^{r+x} \cdot a^{r+y}) = (r+x+r+y) \pmod m = (r+x) \pmod m + (r+y) \pmod m = f(a^{r+x}) + f(a^{r+y})$. con lo cual f es un isomorfismo del subsemigrupo (B,.) sobre (Zm,+). ∎

En el caso finito el semigrupo S puede representarse por el grafo Grm que muestra la figura siguiente



Grafo G_{rm} representativo de un semigrupo cíclico finito

Fig. 15

Para el caso de los monoides se obtiene el resultado siguiente, efectuando muy pocos cambios en la demostración precedente.

7.4.4. **Teorema.** *Si* **M**=(M,.,1) *es un monoide cíclico generado por un elemento a, entonces* **M** *es isomorfo a (* N,+,0) o M *es finito y existe un par de enteros* r≥0 y m≥1 *tal que* M={1,a,...,a^{r+m-1} }, *cumpliéndose además que* {a^r,...,a^{r+m-1}} *es el universo de un subsemigrupo de* (M, .) *isomorfo a (* Zm,+).

7.4.5. **Corolario.** *Todo semigrupo cíclico finito contiene un elemento idempotente. Todo monoide cíclico y finito , no isomorfo a (* Zm,+,0), *para algún* m≥1, *contiene un elemento idempotente además de la unidad.*

Demostración. Si a es un elemento generador de un semigrupo o de un monoide en las condiciones del enunciado se tiene que, para algún r≥1 y algún m≥1, $\{a^r,...,a^{r+m-1}\}$ es el universo de un subsemigrupo isomorfo a (Zm,+). Sea a^{r+x} el elemento correspondiente a 0 por el isomorfismo definido en 7.4.3 (es decir, r+x es un múltiplo de m). Entonces, a a^{r+x} .a^{r+x} le corresponde 0+0=0, con lo cual a^{r+x} .a $^{r+x} = a^{r+x}$. ∎

7.4.6. **Corolario.** *Para todo elemento* x *de un semigrupo, o monoide, finito, existe un entero* n *tal que* x^n *es idempotente.*

Demostración. Basta aplicar 7.4.5 al subsemigrupo o submonoide cíclico generado por x. ∎

7.4.7. **Teorema.** *Si* G *es un grupo cíclico entonces* G *es isomorfo al grupo de los enteros o* G *es finito y, para algún* m≥1, G *es isomorfo a* (Zm,+,-,0).

Demostración. Sea a un generador del grupo **G**.

Caso 1. Para todo par de enteros distintos r y s, $a^r \neq a^s$.

La aplicación de Z en G dada por $r \rightarrow a^r$ es un isomorfismo de grupos.

Caso 2. Existe un par de enteros distintos r y s tales que $a^r = a^s$.

Suponiendo r>s, $1=a^r .(a^s)^{-1}=a^{r-s}$, con r-s>0. Sea m el primer entero positivo tal que $1=a^m$. Entonces el monoide de las potencias de exponente mayor o igual que cero de a es isomorfo a (Zm,+,0).

Como $a^{m-1}=a^{-1}$, para todo n>0, $a^{-n}=(a^{-1})^n=(a^{m-1})^n=a^{(m-1)n}$.

Luego , toda potencia de exponente negativo coincide con una potencia de exponente positivo. Esto concluye la demostración del teorema. ∎

7.4.8. **Definición.** El orden de un elemento a de un grupo G es el cardinal del subgrupo cíclico generado por a.

Se deduce directamente de la definición 7.4.8 que un elemento a de un grupo G tiene orden finito m, si y sólo si, m es el menor entero, mayor o igual que 1, tal que $a^m=1$.

7.4.9. **Teorema.** *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Sean G un grupo cíclico generado por un elemento a y S un subgrupo de G.

Sea Z´ el conjunto de los enteros x tales que $a^x \in S$. Luego $0 \in Z'$ y si $x,y \in Z'$, se tiene $a^{x-y} = a^x(a^{-1})^y = a^x(a^y)^{-1}$, que es un elemento de S, con lo cual $(x-y) \in Z'$. Entonces Z´ es subuniverso de **Z**, de donde, por 7.1.6, Z´ está generado por un entero $m \geq 0$. Por lo tanto, todo elemento de S es de la forma a^{qm}, con $q \in Z$, es decir, es una potencia de a^m. ∎

Nota. No vale en general que un subsemigrupo (resp. submonoide) de un semigrupo cíclico (resp. monoide cíclico) es cíclico (ejercicio 7.4.13).

Ejemplos

7.4.10 Sea la relación sobre el conjunto X= {a,b,c,d}, R={(a,b),(b,c), (b,d),(c,d),(d,a),(d,c)}. Entonces, en el monoide de todas las relaciones binarias sobre X con respecto a la composición, R genera el submonoide cíclico: $\{R^0,R,...,R^6\}$. En este caso los números r y m del Teor. 7.4.4 son 6 y 1 respectivamente. Los elementos idempotentes son R^0= idx y R^6.

7.4.11. En Z_6 los órdenes de 1,2,3,4 y 5 son, respectivamente, 6,3,2,3 y 6. Si p es primo, todo elemento no nulo de Zp es generador, o equivalentemente, todo elemento no nulo tiene orden p. En efecto, si n es el orden de un elemento x de Zp se tiene que nx≡o (mod p), es decir: p | nx, con lo cual p | n, de donde n=p.

7.4.12. Sea R el grupo de las rotaciones en el plano, con respecto a la composición como operación binaria. Una rotación de ángulo $\alpha < 2\pi$ tiene orden finito si y sólo si, para un entero n, n>0, $n\alpha=2\pi$, es decir, $\alpha=2\pi/n$.

Ejercicios.

7.4.13. Mostrar que no es válido en general que un subsemigrupo (resp. submonoide) de un semigrupo cíclico (resp. monoide cíclico) es cíclico.

7.4.14. (Z,+,-,0) es un grupo cíclico generado por 1. Encontrar el submonoide de Z generado por 1.
Encontrar un subconjunto $A \subseteq Z$ tal que el submonoide de Z generado por A sea igual a Z.

7.4.15. a) Probar que un grupo cíclico de orden 5 tiene 4 generadores.
b) Probar que un grupo cíclico de orden p, p número primo, tiene p-1 generadores.

7.4.16. Sea a un elemento del grupo (Zp,+,-,0). probar que los subgrupos generados por a y por p-a coinciden.

7.4.17. Un semigrupo S se llama semigrupo *de torsión* si para todo $x \in S$ el subsemigrupo cíclico [x] generado por x es finito.
Un grupo *de torsión* es un semigrupo de torsión que además es un grupo.
Probar que G es un grupo de torsión si y sólo si todo subsemigrupo de G es un subgrupo de G.

7.4.18. Sea S un semigrupo y sea E(S) el conjunto de elementos idempotentes de S.
a) Probar que si S es conmutativo, entonces E(S) es un subsemigrupo de S.

b) Sean S_1 un semigrupo de torsión, S_2 un semigrupo y f de S_1 en S_2 un epimorfismo de semigrupos,
Probar que S_2 también es de torsión,
Probar que f $(E(S_1)) = E(S_2)$. (**Indicación:** Tener en cuenta que todo semigrupo cíclico finito contiene un elemento idempotente).

7.5 Representación de semigrupos monoides y grupos.

Sea A un conjunto. En 6.2.10 se definió en A^A (conjunto de todas las aplicaciones de A en A) las operaciones binarias o y ¤dadas por : fog(x)=f(g(x)) y f¤g(x)=g(f(x)).
A continuación de 6.2.12 se definió el semigrupo S^1 obtenido de un semigrupo S por adjunción de una unidad. Se tiene ahora el siguiente resultado.

7.5.1. **Teorema.** *Todo semigrupo S es isomorfo a un subsemigrupo de* $((S^1)^{S^1}, o)$ *y a un subsemigrupo de* $\left(\left(S^1\right)^{S^1}, ¤\right)$.

Demostración. Sea I: $S \to \left(S^1\right)^{S^1}$ la aplicación dada por: (I(x)) (r)= x.r, para todo $x \in S$ y todo $r \in S^1$, donde x.r designa el producto en S^1.
Entonces (I (x.y)) (r) = (x.y).r = x.(y.r) = x.(I (y)) (r) = (I(x)) ((I(y) (r)) = I(x)oI(y)(r). Luego, I (x.y) = I(x)oI(y), lo que muestra que I es un morfismo de semigrupos.
Por otra parte, si x e y son elementos distintos de S, se tiene que I(x) e I(y) son aplicaciones distintas, ya que I(x) (1) =x e I (y) (1) =y. Entonces I es un monomorfismo, con lo cual S es isomorfo al subsemigrupo I(S) de $(\left(S^1\right)^{S^1}$,o) (ver 7.3.10).

Definiendo la aplicación D: $S \to \left(S^1\right)^{S^1}$ por (D(x)) (r)=r.x, se obtiene, en forma análoga, que S es isomorfo al subsemigrupo D(S) de $(\left(S^1\right)^{S^1}$, ¤). ∎

Sea ahora **M**=(M,.,1) un monoide. Entonces M^1=M y para las aplicaciones I y D de la demostración precedente, se tiene, $I(1)=D(1)=id_{\mathbf{M}}$, con lo cual , **M** es isomorfo a I (M) y a D(M). Vale, por lo tanto, el siguiente teorema

7.5.2. **Teorema** . *Todo monoide* **M** *es isomorfo a un submonoide de* $(M^M,o,id\mathbf{M})$ *y a un submonoide de* $(M^M,¤id\mathbf{M})$.

Si A es un conjunto las biyecciones de A en A, o permutaciones de A, constituyen un grupo con respecto a las operaciones o y ¤(ver 6.2.10). Se tiene el siguiente teorema de representación de grupos

7.5.3. **Teorema.** (Cayley) *Todo grupo* **G** *es isomorfo a un grupo de permutaciones de* G.

Demostración. Sea I la aplicación de G en G^G definida en la demostración de 7.5.1. Si $x \in G$, $I(x) \circ I(x^{-1}) = I(x.x^{-1}) = I(1) = id_G$ y , análogamente, $I(x^{-1}) \circ I(x) = id_G$.

Luego, I(x) es una biyección de G en G. Entonces, por la demostración de 7.5.1, G es isomorfo al subgrupo I(G) del grupo de las permutaciones de G con respecto a la operación o. ∎

Las aplicaciones I y D se llaman representaciones regulares a izquierda y derecha respectivamente.

Ejemplos

7.5.4. Sea $A^d = (A,.)$ un semigrupo tal que A es no vacío y la operación binaria está definida por: a.b=b. Entonces, (I(a)) (1)=a.1=a y, para todo b,

(I(a)) (b)=a.b=b, es decir I(a) es la aplicación que vale a en 1 y que coincide con la identidad sobre todos los elementos de A.

Para la aplicación D(a) se tiene que (D(a)) (1)=a y, para todo b, (D(a)) (b)=a, es decir, D(a) es una aplicación constante.

7.5.5. En el monoide (P(E),∩,E) las aplicaciones I y D coinciden.
Ambas asignan a un subconjunto A de E la aplicación B→A∩B, de P(E) en P(E).

7.5.6. El grupo Zɜ es isoformo a un subgrupo de Sɜ mediante las aplicaciones I y D, que en este caso coinciden. Se tiene que I(0)=id, $I(1)=\begin{pmatrix}012\\120\end{pmatrix}$ y $I(2)=\begin{pmatrix}012\\201\end{pmatrix}$

Ejercicios

7.5.7. Sea x perteneciente a un conjunto finito A y sea f una permutación de los elementos de A, existen un entero positivo k tal que $f^k(x)=x$. El ciclo de f es el conjunto ordenado $(x,f(x),f^2(x),\ldots, f^{k-1}(x))$.

a) Sea $f=\begin{pmatrix}123456\\213564\end{pmatrix}$ una permutación de A = { 1,2,3,4,5,6}.

Para todo x $\in$ A encontrar el ciclo de x y escibir f como el producto de sus ciclos.

b) Sea g=(1 2 3) una permutación de {1,2,3}; verificar que g=(1 2) (1 3) = (3 1) (3 2).

c) Sea p= (1 2 3) (4 5) una permutación de { 1,2,3,4,5}. Encontrar el grupo generado por p.

7.5.8. Sea S_n el grupo de permutaciones de un conjunto con n elementos y sea G un subgrupo de S_n. Las permutaciones s y t de G se llaman *conjugadas* en G si existe un elemento g $\in$ G tal que $s=gtg^{-1}$.

a) Probar que la conjugación es una relación de equivalencia en G.

b) Sean s y t permutaciones conjugadas en S_n, tales que $s = gtg^{-1}$.

b_1) Probar que para todo ciclo $(a_1,...,a_k)$ de t, $(g(a_1),...,g(a_k))$ es un ciclo de s.

b_2) Sean $s=(a_1,...,a_k)\ (a_r,...,a_j)\ ...\ (a_i,...,a_m)$ y $t=(b_1,...,b_k)\ (b_r,...,b_j)\ ...\ (b_i,...,b_m)$ dos permutaciones de S_n con el mismo número de ciclos y de mismas longitudes respectivas.

Probar que s y t son conjugadas en Sn.

b_3) Qué conclusión se obtiene a partir de b_1) y b_2) ?

7.5.9. Sea G un grupo de permutaciones contenido en Sn. Probar que si G contiene una permutación impar t, es decir tal que su signo es sig(t)=-1, en-

tonces G contiene el mismo número de permutaciones pares que de impares. (**Indicación:** Probar que la aplicación ß de G en G definida por ß(g)=tg es una biyección y considerar la sumatoria $\sum sig(g)$ sobre todas las permutaciones $g \in G$.)

7.5.10. Representar $(Z_4,+,-,0)$ por un grupo de permutaciones sobre $\{0,1,2,3\}$.

7.5.11. a) Explicitar el subsemigrupo de N^N isoformo al semigrupo $(N-\{0\},+)$ por una representación regular.
b) Explicitar el submonoide de $P(E)^{P(E)}$ isoformo al monoide $(P(E),\cap,E)$, por una representación regular.

7.5.12. Sea M un monoide finito. Probar que si un elemento de M tiene inverso a izquierda (o tiene inverso a derecha) entonces éste es único y es el inverso a ambos lados.
(**Indicación:** Usar el teorema de Cayley).
Probar que el resultado enunciado no vale para monoides infinitos.
(**Indicación:** Considerar el monoide de las funciones de N en N).

Capítulo 8

Algebras cocientes y productos

Las congruencias en un álgebra son relaciones de equivalencia, en su conjunto subyacente, que permiten definir, en forma natural, un álgebra del mismo tipo sobre el conjunto cociente. Se estudian, en este capítulo, las congruencias en general y luego las específicas para semigrupos, grupos, anillos y álgebras de Boole.

Habiendo visto previamente los productos de reticulados y de álgebras de Boole, el lector no tendrá dificultades en asimilar y dar ejemplos del concepto de álgebras del mismo tipo que se expone a continuación.

8.1 Congruencias

8.1.1. **Definición.** Sea **A** un álgebra y R una relación de equivalencia en A. Entonces, R es *compatible* con respecto a una operación n-aria f_i de **A** si, dados $a_1,...,a_n$, $b_1,...,b_n$ en A tales que $a_j R b_j$, para todo j=1,...,n, entonces

$$f_i(a_1,...,a_n)\, R f_i(b_1,...,b_n).$$

Si R es compatible con todas la operaciones de **A**, se dice que R es una *congruencia* en **A**.
Es evidente que una relación de equivalencia es siempre compatible con las operaciones 0-arias del álgebra.

Ejemplos

8.1.2. R es una congruencia en un semigrupo (S..) o en un monoide (M,.,1) si y sólo si R es de equivalencia y

(1) a_1Rb_1 y a_2Rb_2 implica $a_1.a_2Rb_1.b_2$

8.1.3. R es una congruencia en un grupo $(G,.,^{-1},1)$ si y sólo si R es de equivalencia y vale (1) para toda cuaterna a_1,a_2,b_1,b_2 de elementos de G. En efecto, con respecto a la operación unaria $^{-1}$, se tiene que si aRb, como $a^{-1}Ra^{-1}$, por (1), $1Rb.a^{-1}$, y puesto que también $b^{-1}\ Rb^{-1}$, aplicando nuevamente (1), se obtiene $b^{-1}\ Ra^{-1}.s$

8.1.4. R es una congruencia en un anillo (A,+,.,-,0) o en un semianillo (A,+,.,0,1) si y sólo si, para toda cuaterna a_1, a_2, b_1, b_2 de elementos de A tales que a_iRb_i, i=1,2, se cumple $a_1+a_2Rb_1+b_2$ y $a_1.a_2\ Rb_1.b_2$ (la compatibilidad de R con respecto a la operación - resulta de 8.1.3.).

8.1.5.R es una congruencia en un reticulado (L,v,∧) o en un álgebra de Boole (B,v,∧,´,0,1) si y sólo si R es de equivalencia y $a_i R b_i$, para i=1,2 implica $a_1 v a_2 R b_1 v b_2$ y $a_1 \wedge a_2 R b_1 \wedge b_2$. Para ver que estas dos últimas condiciones implican la compatibilidad de R con respecto a la operación ´ del álgebra de Boole, sean a,b ∈ B tales que aRb. Puesto que a´ Ra´ , se tiene, 1Rbva´ . Como también b´ Rb´, resulta b´ R(bva´) ∧b´ . Por la propiedad distributiva, (bva´) ∧b´ = a´ ∧ b´ , con lo cual, b´ Ra´ ∧b´ . En la misma forma resulta a´Ra´ ∧b´ , de donde, por la transitividad y simetría de R, se obtiene a´ Rb´.

Denotaremos C_A al conjunto de todas las congruencias sobre el álgebra **A**. Recordamos (3.2) que E_A designa al conjunto de las relaciones de equivalencia sobre A.

8.1.6. **Teorema.** *El conjunto* $C_{\mathbf{A}}$, *ordenado por inclusión, es un subreticulado de* $(E_A, \subseteq)$.

Demostración Sean R_i, i=1,2, congruencias en **A**. Veremos que $R_1 \cap R_2$ y $[R_1 \cup R_2]$ (4.1.4) son también congruencias. Sean entonces f una operación n-aria en **A** y $a_1,...,a_n,b_1,...,b_n \in A$.

Si $a_i (R_1 \cap R_2) b_i$, para todo i, i=1,...,n), entonces

$$f(a_1,...,a_n)\, R_i f(b_1,...,b_n),\ i=1,2,$$

con lo cual,

$$f(a_1,...,a_n)\ R_1 \cap R_2 f\ (b_1,...,b_n).$$

Supongamos ahora que $a_i[R_1 \cup R_2]b_i$, para todo i, i=1,...,n.

Entonces, existen $x_1{}^i,...,xk_i{}^i$, i=1,..., n, en A, tales que,

$$a_i\ (R_1 \cup R_2)x_1{}^i,...,xk_i{}^i\ (R_1 \cup R_2)b_i,\ i=1,...,n.$$

Utilizando eventualmente la reflexividad de R_1 y R_2, puede obtenerse una sucesión $R_{j1},..., R_{jm}$ de relaciones, cada una igual a R_1 o a R_2, y, para cada i, i=1,...,n, una sucesión $z^i{}_1,...,z^i{}_{m-1}$, de elementos de A, tales que,

$$a_i\ R_{j1} z^i{}_1,...,z^i{}_{m-1} R_{jm} b_i.$$

Luego,

$f(a_1,...,a_n)\ R_{j1} f(z^1{}_1,...,z^n{}_1)...f(z^1{}_{m-1},...,z^n{}_{m-1}) R_{jm} f(b_1,...,b_n)$,

con lo cual , $f(a_1,...a_n)\ [R_1 \cup R_2] f(b_1,...,b_n)$. ∎

Si R es una congruencia en un álgebra **A**, para cada operación n-aria f de **A** queda definida una operación n-aria [f], sobre A/R, poniendo: $[f](R(a_1),...,R(a_n)) = R(f(a_1,...,a_n))$. La operación [f] está bien definida ya que R es compatible con f.

8.1.7. **Definición.** Sean $\mathbf{A} = (A,(f_i)_{i\in I})$ un álgebra y R una congruencia en **A**. El álgebra $(A/R,([f_i])_{i\in I})$ se denota **A**/R y se llama el *álgebra cociente de* **A** *por* R.

8.1.8. **Teorema.** *Sea* R *una congruencia en un álgebra* **A**. *Entonces, la aplicación canónica* $\rho : A \rightarrow A/R$ *es un epimorfismo del álgebra* **A** *sobre el álgebra* A/R.

Demostración. Si f es una operación n-aria de **A** y $a_1,...,a_n$ son elementos de A, de acuerdo con las definiciones de ρ y de [f], se tienen las siguientes igualdades,

$$\rho(f(a_1,...,a_n) = R(f(a_1,...,a_n))$$
$$= [f](R(a_1),...,R(a_n)) = [f]\ (\rho(a_1),...\rho(a_n)),$$

lo que prueba el enunciado. ∎

Según se definió en 3.1.5, la relación de equivalencia asociada a una aplicación f: $A \rightarrow B$ es la relación R_f sobre A dada por: aR_fa' si y sólo si $f(a) = f(a')$.

8.1.9. **Teorema** *Sea* h *un morfismo de un álgebra* **A** = $(A.(f_i)_{i\in I})$ *en un álgebra* **B**= $(B,(g_i)_{i\in I})$. *Entonces, la relación de equivalencia.* R_h, *asociada a* h *es una congruencia en* A.

Demostración. Sean f_i una operación n-aria en **A** y $a_1,...,a_n,a'_1,...,a'_n$ elementos de A tales que, para todo j, j=1,...,n, se cumple $a_jR_ha'_j$. entonces, por ser h un morfismo, y $h(a_j) = h(a'_j)$, para todo j, j=1....,n, resultan las siguientes igualdades

$h(f_i(a_1,...,a_n)) = g_i(h(a_1),...,h(a_n))$

$= g_i(h(a'_1),...,h(a'_n)) = h(f_i(a'_1,...,a'_n))$.

Luego,

$f_i(a_1,...,a_n) R_h f_i(a'_1,...,a'_n)$. ∎

8.1.10. **Teorema.** *Sean* h *un epimorfismo de un álgebra* $\mathbf{A} = (A.(f_i)_{i\in I})$ *sobre un álgebra* $\mathbf{B} = (B,(g_i)_{i\in I})$ *y* R_h *la relación de equivalencia asociada a* h. *Entonces, existe un isomorfismo* h′ *de* $\mathbf{A}/R_h$, *en* **B** *tal que.* $h'\circ\rho = h$, *donde* ρ *es la aplicación canónica de* A *sobre* A/R_h.

Demostración. La aplicación $h': A/R_h \to B$, dada por $h'(R_h(a)) = h(a)$, está bien definida (ver 3.2.8) y es biyectiva, ya que h es una suryección. Para verificar que es un morfismo, sea f_i una operación n-aria de **A** y $a_1,...,a_n$ elementos de A. Entonces aplicando las definiciones de $[f_i]$ y de h′ , y teniendo en cuenta que h es un morfismo, resulta

$h'([f_i]\,(R_h(a_1),...,R_h(a_n))) = h'(\,R_h(f_i(a_1,...,a_n)))$

$= h(f_i((a_1,...a_n))) = g_i(h(a_1),...,h(a_n))$

$= g_i(h'(R_h(a_1),...,R_h(a_n))$,

lo que prueba la aserción. ∎

Ejercicios.

8.1.11. Sean **A** un álgebra y R, S congruencias en **A** tales que $S \subseteq R$.
Sea $R/S = \{(S(a), S(b)) \in \mathbf{A}/S \times \mathbf{A}/S ; (a,b) \in R\}$. Probar que R/S es una congruencia en el álgebra cociente $\mathbf{A}/S$.

8.1.12. Sean R, S congruencias en un álgebra **A** tales que $S \subseteq R$, $\propto$ la aplicación de $(A/S)/(R/S)$ en A/R dada por $\propto((R/S)(S(a)) = R(a)$.
Probar que $\propto$ está bien definida y que es un isomorfismo.
($S(a)$ es un elemento de A/S y $(R/S)(S(a))$ denota la imagen de $S(a)$ por la relación R/S que, por (8.1.11), es una congruencia en $\mathbf{A}/S$).

8.1.13. Sean **A** un álgebra y S una congruencia en **A**. Se indica con $[S,1]$ el intervalo de extremos S y 1 en el reticulado $(C(\mathbf{A}), \subseteq)$ de las congruencias de **A**.
Sea $\propto$ la aplicación de $[S, 1]$ en $C(\mathbf{A}/S)$ dada por $\propto(R)=R/S$.
Probar que $\propto$ es un morfismo de orden de $([S,1], \subseteq)$ en $(C(\mathbf{A}/S), \subseteq)$ y que $\propto$ es inyectivo.

8.1.14. Sean **A** un álgebra, B un subuniverso de **A** y R una congruencia en **A**. Sea $B^R = \{ a \in \mathbf{A}$; aRb, para algún $b \in B\}$.
Demostrar que B^R es un subuniverso de **A**.

8.1.15. Sean **A** un álgebra con una sola operación unaria y B un subuniverso de **A**.
Sea R la relación dada por: aRb si y sólo si a=b o $\{a,b\}\subseteq B$.
Probar que R es una congruencia en **A.**

8.1.16. Sean S un semirreticulado y a un elemento de S.
Sea R_a = {(b,c) $\in S \times S$; las relaciones $a\leq b$, $a\leq c$ valen ambas o bien no vale ninguna de las dos }. Probar que R_a es una congruencia en S.

8.1.17. Si R es una congruencia en **A** y C (**A**) es un reticulado distributivo (resp. modular), probar que C (**A**/R) es también un reticulado distributivo (resp. modular).

8.2. Congruencias en semigrupos.

Es inmediato comprobar que si R es una congruencia en un semigrupo S = (S,.), el álgebra cociente, S /R, es también un semigrupo.

8.2.1. **Definición.** Un *ideal* de un semigrupo S = (S,.) es un subconjunto no vacío, I, de S tal que, para todo i de I y todo a de S, i.a y a.i pertenecen a I.

8.2.2. **Teorema.** *Si I es un ideal de un semigrupo S =(S,.) entonces la relación de equivalencia asociada a la partición {I}* $\cup$ { {a}, a $\in$ *S -I} es una congruencia en S.*

Demostración. Sea R la relación de equivalencia asociada a la partición del enunciado y sean $a_1,b_1,a_2,b_2 \in S$, tales que, $a_i R b_i$, i=1.2.

Si algún elemento del conjunto $\{a_1,a_2,b_1,b_2\}$, digamos a_1, pertenece a I, resulta que $b_1 \in I$, con lo cual, a_1,a_2 y $b_1.b_2$ pertenecen a I y, por lo tanto, $a_1.a_2\ R b_1.b_2$.

En caso contrario, $a_1=b_1$ y $a_2=b_2$, de donde, $a_1.a_2 = b_1.b_2$. ∎

El semigrupo cociente de un semigrupo *S* por la relación de equivalencia asociada a un ideal I se denotará *S* /I. Para toda clase de equivalencia [x], se tiene que [x].I=I.[x]=I

Ejemplos

8.2.3. Sea I un ideal del semigrupo (N,+). Si n es el primer elemento de I, resulta que n+1, n+2,... pertenecen a I, con lo cual I=[n,∞) = {x∈ N; n≤x}. El semigrupo cociente tiene n clases unitarias (las clases de 0,...,n-1) y la clase I.

8.2.4. Sea (S,≤) un semireticulado inferior. Un segmento inicial de S es un subconjunto J de S tal que, para , para todo x∈ S y todo j∈ J, si x≤ j entonces x∈ J. El conjunto de los segmentos iniciales no vacíos de S coincide con el conjunto de los ideales del semigrupo (S,∧). En efecto sea J un segmento inicial no vacío de S y sean j∈ J y x∈ S, entonces x∧j≤j, con lo cual, x∧j∈ J. Recíprocamente, si J es un ideal de (S,∧), j∈ J y x es un elemento de S tal que x ≤ j, resulta, x∧j=x, con lo cual x ∈ J.

8.2.5. De acuerdo con el ejemplo precedente, si X⊆A, P (X) es un ideal del semigrupo (P (A), ∩).

Nota. No toda congruencia en un semigrupo se obtiene a partir de un ideal como en 8.2.2. Por ejemplo, el único ideal de A^d (6.2.11) es A y toda relación de equivalencia en A es una congruencia en A^d.

Ejercicios

8.2.6. Sea S un semigrupo. Probar que:

a) Si A y B son subsemigrupos de S , entonces $A \cup B$ es un subsemigrupo de S si y sólo si $AB \cup BA \subseteq A \cup B$.

b) Si I es un ideal de S y T es un subsemigrupo de S , entonces $I \cap T$ es un ideal de T y $I \cup T$ es un subsemigrupo de S.

8.2.7. Sean S un semigrupo, I un ideal de S, R la congruencia asociada con la partición $\Pi = \{I\} \cup \{\{x\} ; x \in S - I\}$. Probar que para cualquier elemento i de I, la clase R(i) es un elemento cero de S /R.

8. 3 Congruencias en grupos.

Se verifica fácilmente que el álgebra cociente de un grupo por una congruencia es un grupo.

Las congruencias en grupos están relacionadas con los llamados subgrupos normales. Antes de definirlos introduciremos las siguientes notaciones: Si $(G,.,^{-1},1)$ es un grupo, $X \subseteq G$ y $a \in G$, pondremos

$$a.X = \{a.x;\ x \in X\} \quad y \quad X.a = \{x.a;\ x \in X\}.$$

Resulta inmediatamente, para subconjuntos A y B de G y elementos a,b de G, que

$$a.(b.A) = (a.b).A \quad y \quad (A.a).b = A.(a.b).$$

8.3.1. Teorema. *Sean* **G** *un grupo y* X *un subconjunto de* G. *Entonces las siguientes proposiciones son equivalentes*

a) $X.a = a.X$, *para todo* $a \in G$.

b) $a^{-1}.X.a = X$, *para todo* $a \in G$.

c) $a^{-1}.X.a \subseteq X$, *para todo* $a \in G$.

Demostración. De a) se obtiene b) multiplicando ambos miembros por a^{-1} y de b) se obtiene a) multiplicando ambos miembros por a. Claramente, b) implica c). Suponiendo ahora c) y reemplazando a por a^{-1}, resulta $a..X.a^{-1} \subseteq X$. Multiplicando por a^{-1} a la izquierda y por a a la derecha, resulta $X \subseteq a^{-1}.X.a$, con lo cual se obtiene b). ∎

8.3.2. Definición. Un subgrupo **N** de un grupo **G** es *normal* si, para todo elemento a de G, se cumple a.N = N.a.

De acuerdo con 8.3.1, **N** es normal si y sólo si, para todo $a \in G$, $a^{-1}.N.a \subseteq N$.

Evidentemente, si **G** es conmutativo todo subgrupo de **G** es normal.

8.3.3. Lema. *Si* **S** *es un subgrupo de un grupo* **G** *entonces las relaciones binarias, R y R', en G, dadas respectivamente por aRb si y sólo* $a^{-1}.b \in S$ *y*

$aR'b$ si y sólo si $a.b^{-1} \in S$, son de equivalencia en G, y, para todo $a \in G$, $R(a) = a.S$ y $R'(a) = S.a$.

Demostración. La relación R es reflexiva puesto que $a^{-1}.a = 1$, que es un elemento de S. Si $a^{-1}.b \in S$, se tiene, $(a^{-1}.b)^{-1} = b^{-1}.a \in S$, con lo cual R es simétrica. Finalmente si $a^{-1}.b$ y $b^{-1}.c$ pertenecen a S, entonces el producto, $a^{-1}.c$, es un elemento de S. Luego R es transitiva. En la misma forma resulta que la relación R' es también de equivalencia.

Por otra parte, de la definición de R resulta que $x \in R(a)$ si y sólo si $a^{-1}.x \in S$, que es equivalente a "$x \in a.S$". Análogamente $x \in R'(a)$ si y sólo si $x.a^{-1} \in S$, que equivale a "$x \in S.a$". ∎

La clase $R(a) = a.S$ (resp. $R'(a) = S.a$) se llama la *clase izquierda de a módulo S* (resp. *clase derecha de a módulo S*). Las relaciones R y R'serán llamadas relaciones *módulo S, a derecha y a izquierda*, respectivamente. Del Lema resulta inmediatamente que $R(1) = R'(1) = S$ y que si *S* es normal, entonces R= R', en cuyo caso se dirá que R es la relación *módulo S*.

8.3.4. **Teorema.** *Sean* **G** *un grupo y* R *una relación binaria en* G. *Entonces* R *es una congruencia en* **G** *si y sólo si* R *es la relación módulo un subgrupo normal de* **G**.

Demostración. Sea R una congruencia en el grupo **G**. Veremos primeramente que R(1) es el universo de un subgrupo normal de **G**.

Si a,b $\in$ R(1), entonces aR1 y bR1, con lo cual, a.bR1. Además a^{-1} Ra^{-1}, de donde $(a.a^{-1})R(1.a^{-1})$, es decir $a^{-1} \in R(1)$. Puesto que 1$\in$ R(1), resulta que R(1) es un subuniverso de G.

Sean ahora a $\in$ G y x$\in$ R(1). Puesto que a^{-1} Ra^{-1}, xR1 y aRa, resulta $(a^{1}.x.a)R(a^{1}.1.a)$, de donde, $a^{-1}.x.a \in R(1)$. Entonces $a^{-1}R(1)a \subseteq$ R(1), lo que demuestra que R(1) es el universo de un subgrupo normal.

Si aRb, puesto que $a^{-1}Ra^{-1}$, se tiene, $1R(a^{-1}.b)$, con lo cual $a^{-1}.b \in R(1)$. Recíprocamente de $a^{-1}.b \in R(1)$ se deduce aRb usando aRa. Esto muestra que R es la relación módulo R(1).

Recíprocamente, sean **N** un subgrupo normal de **G** y R la relación módulo **N**. Si a,b,c,d, son elementos de G tales que aRb y cRd, entonces, a $\in$ R(b) =b.N y c$\in$ R(d)=d.N, es decir, existen n y m en N, tales que,

$$a = b.n \quad y \quad c = d.m.$$

Entonces, a.c = (b.n). (d.m) = b. (n.d).m. Como **N** es normal, N.d = d.N (8.3.1), con lo cual existe n´ en N tal que n.d = d.n´, de donde, a.c = b.(d.n´).m = b.d.(n´. m) $\in$ (b.d).N. Por lo tanto, (a.c) R (b.d), lo que demuestra que R es una congruencia. ∎

Se comprueba fácilmente que la asignación R→R(1) establece un isomorfismo del conjunto de las congruencias de un grupo **G**, ordenado por inclusión, en el conjunto de los subgrupos normales de **G**, ordenado por

inclusión. El grupo cociente de G por R se lo denota indistintamente **G**/R o **G**/R(1).
Puesto que todo subgrupo de un grupo conmutativo es normal, se obtiene el siguiente resultado

8.3.5. **Corolario.** *Si* **G** *es un grupo conmutativo, el reticulado de las congruencias de* **G** *es isomorfo al reticulado de los subuniversos de* **G**.

Sean ahora **G** un grupo finito y **S** un subgrupo de **G** (no necesariamente normal). Sean R y R´ las relaciones módulo S, a izquierda y derecha respectivamente. Según 8.4.3, para todo elemento a de G, R(a) = a.S. De aquí resulta $|R(a)| = |S|$, puesto que si, para $s,s' \in S$, se tiene a.s = a.s´, resulta s=s´. Análogamente, $|R'(a)| = |S.a| = |S|$. Se tiene entonces

$$|G| = |G/R|\,|S| = |G/R'|\,|S|.$$

El número $|G/R| = |G/R'|$ se llama *índice* de *S* en **G**. Siendo el *orden* de un grupo finito el número de sus elementos, la igualdad precedente se expresa

8.3.6. **Teorema.** (Lagrange) *Si* **G** *es un grupo finito y S es un subgrupo de* **G**, *entonces el orden de* **G** *es igual al producto del orden de S por el índice de S en* **G**.

8.3.7. **Corolario.** *El orden de un subgrupo de un grupo finito* **G** *divide al orden de* **G**.

Ejemplos

8.3.8. El grupo de los enteros **Z** es conmutativo, luego todo subgrupo es normal. Si **S** es un subgrupo de **Z**, S es el conjunto de los múltiplos de un entero p (7.1.6). La congruencia R módulo S es entonces, aRb si y sólo si a-b es un múltiplo de p. Coincide, por lo tanto, con la congruencia módulo p (3.1.4). El álgebra cociente es, entonces, el grupo de los enteros módulo p(6.2.8).

8.3.9. Sea S_3 el grupo de las permutaciones del conjunto {1,2,3} (6.2.10). Las permutaciones

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

junto con la permutación idéntica forman un subgrupo normal N de S_3. Puesto que S_3 tiene seis elementos, el grupo cociente tiene dos elementos, de acuerdo con el Teor. 8.4.6. Es, por lo tanto, isomorfo a Z_2.

8.3.10. Sea h un morfismo de grupos de **G** en **G´**. Según 8.2.8, la relación de equivalencia, R_h, asociada a h es una congruencia en **G.** Por lo tanto $R_h(1)$ es un subgrupo normal de **G**. Ahora bien, xR_h1 si y sólo si $h(x)=h(1) = 1$, con lo cual $R_h(1) = \{x \in G;\ h(x) =1\}$. Este subgrupo normal de **G** se llama *núcleo de h* y se denota Ker h. De acuerdo con el Teor. 8.2.9, G/Ker h es isomorfo a h (G).

8.3.11. Sea C el conjunto de los números complejos. Entonces (C-{0},.,/,1) es un grupo, donde . designa a la multiplicación usual y / a la aplicación $\alpha \rightarrow 1/\alpha$ de C-{0} en C-{0}.

Sea f la aplicación de C-{0} en C-{0} dada por, $f(\alpha) = \alpha / |\alpha|$. Puesto que $f(\alpha.\beta) = (\alpha.\beta) / |\alpha.\beta| = \alpha / |\alpha|.\ \beta / |\beta|$, resulta que f es un morfismo de grupos. El núcleo de f es el conjunto de los números complejos α, $\alpha \neq 0$, tales que $\alpha / |\alpha| = 1$, lo que equivale a que α es un número real mayor que 0. Luego Ker $f = R^+-\{0\}=\{x\in R,x>0\}$.

De acuerdo con 8.3.10, $C-\{0\}/R^+ -\{0\}$ es isomorfo a la imagen de f, es decir al conjunto de los números complejos de módulo 1.

Ejercicios

8.3.12. Probar que H={f $_{ab}$; a es un número racional} es un subgrupo del grupo G de (6.2.20). Probar que K={f$_{1b}$; b es un número real} es un subgrupo normal de dicho grupo G.

8.3.13. Sean H y K subgrupos normales de un grupo G, probar que H∩K y H.K son también subgrupos normales de G.

8.3.14. Sean G un grupo y H un subgrupo de G. Sea N(H)={w∈G; wHw^{-1} = H}. Probar que:

a) N(H) es subgrupo de G.

b) H es subgrupo normal de N(H).

c) N(H) es el máximo subgrupo de G en el que H es normal.

d) H es un subgrupo normal de G si y sólo si N(H)=G.

8.3.15. Sean G un grupo y N, M dos subgrupos normales de G tales que N⊆M,

a) Probar que N es un subgrupo normal de M.

b) Probar que M/N es un subgrupo normal de G/N.

c) Sea f la aplicación de G/N en G/M dada por f(xN) = xM.

Probar que f está bien definida y que es un morfismo de grupos.

8.3.16. Sean G un grupo , H un subgrupo de G y g un elemento de G,
a) Probar que gHg^{-1} es un subgrupo de G.
b) Sea K el único subgrupo de orden o(K) en el grupo G.
Probar que K es subgrupo normal de G.

8.3.17. Sean G_1 y G_2 grupos y f un morfismo de grupos de G_1 en G_2. Probar que f es un monomorfismo (de grupos) si y sólo si el núcleo Ker f es igual a $\{1_{G1}\}$.

8.3.18. Sean G un grupo y L (G) el conjunto de todos los subgrupos de G,
a) Dados S , T $\in L$(G), probar que el conjunto S vT constituído por los elementos de la forma $s_1.t_1.s_2.t_2. \ldots .s_k.t_k$ con $k \geq 1$, $s_i \in S$ y $t_i \in T$, también pertenece a L(G).
b) Establecer si L(G) ordenado por inclusión, es o no un álgebra de Boole.

8.3.19. Sean G un grupo finito y $a \in G$, probar que $a^{o(G)} = 1_G$.

8.3.20. Probar que los subgrupos de un grupo finito de orden p son únicamente los subgrupos triviales si y sólo si p es un número primo. (**Indicaciones:** Usar el teorema de Lagrange. Considerar dos casos: el grupo es cíclico o no lo es).

8.4. Congruencias en anillos.

Sea $\mathbf{A} = (A,+,.,-,0)$ un anillo. De acuerdo con la definición una relación R en A es una congruencia en $\mathbf{A}$ si y sólo si R es una congruencia en el grupo $\mathbf{G_A} = (A,+,-,0)$ y una congruencia en el semigrupo $\mathbf{S_A} = (A,.)$. Según el Teor. 8.3.4, R es una congruencia en $\mathbf{G_A}$ si y sólo si R(0) es un subgrupo de $\mathbf{G_A}$ y R es la relación módulo R(0), es decir, aRb si y sólo si $a-b \in R(0)$.

8.4.1. **Definición.** Sea $\mathbf{A} = (A,+,.,-,0)$ un anillo. Un *ideal* de $\mathbf{A}$ es un subconjunto I de A tal que I es un subuniverso del grupo $\mathbf{G_A}$ y un ideal del semigrupo $S_{\mathbf{A}}$ (8.2.1.).

Entonces, un subconjunto I de A es un ideal de A si y sólo si
a) $0 \in I$,
b) $i,j \in I$ implica $i - j \in I$,
c) $i \in I$ y $a \in A$ implica $i.a, a.i \in I$.

Ejemplos

8.4.2. A y {0} son ideales de $\mathbf{A}$, llamados *ideales triviales.*

8.4.3. Si **A** es un anillo conmutativo y a ∈ A, el conjunto a.A = {a.x, x ∈ A} de los *múltiplos de a,* es un ideal de **A**. En efecto a.x-a.x´ = a.(x-x´) ∈ a.A, y z.(a.x) = a.(z.x), ya que **A** es conmutativo, con lo cual z.(a.x) ∈ a.A.
Los ideales de la forma a.A se llaman *principales.*
Teniendo en cuenta 7.1.6, resulta que todo ideal del anillo Z de los enteros es principal.

8.4.4. Todo ideal del anillo de los polinomios R[x] (6.3.7) es principal. En efecto, si I es un ideal de R[x], I ≠ {0}, sea g un polinomio de I de grado mínimo. Entonces $\{p.g, p \in R[X]\} \subseteq I$. Dado q ∈ I, existen p y r en R[x] tales que q = p.g+r. Si r ≠0, el grado de r es menor que el grado de g, pero, por otra parte, r = q-p.g, con lo cual r∈ I, lo que contradice la elección de g. Entonces, r=0, de donde, I = g.R[x].

8.4.5. Los únicos ideales de un cuerpo son los triviales. En efecto, sean K un cuerpo e I un ideal de K. Si I ≠ {0}, sea i ∈ I-{0}. Entonces, para todo k ∈ K se tiene k = (k.i^{-1}).i, con lo cual, k ∈ I. Luego I = K

8.4.6. Sean **B** = (B,v,∧,´,0,1) un álgebra de Boole y $\mathbf{A_B}$ = (B,Δ,∧,id_B,0) el anillo definido en 6.3.8. Veremos que un subconjunto I de B es un ideal de $\mathbf{A_B}$ si y sólo si verifica las siguientes condiciones

1) $0 \in I$,

2) $i,j \in I$ implica $ivj \in I$,

3) $i \in I$ y $a \leq i$ implican $a \in I$.

Sea I un ideal de $\mathbf{A}_{\mathbf{B}}$. Se verifica fácilmente que $ivj = (i\Delta j)\ \Delta(i \wedge j)$. Luego, si $i,j \in I$, resulta $ivj \in I$.

Sean ahora $i \in I$ y $a \in A$ tales que $a \leq i$. Entonces, $a \wedge i = a$. Luego $a \in I$.

Recíprocamente, supongamos que I cumple las condiciones 1), 2) y 3). Entonces, si $i,j \in I$, como $i \wedge j' \leq i$ y $i' \wedge j \leq j$, en virtud de 3) resulta, $i \wedge j'$, $j' \wedge i \in I$, de donde, por 2), $(i \wedge j') \vee (i' \wedge j) = i \Delta j \in I$.

Si $i \in I$ y $a \in B$, puesto que $a \wedge i \leq i$, por 3) resulta $a \wedge i \in I$.

Los ideales de $\mathbf{A}_{\mathbf{B}}$ se llaman también ideales del álgebra de Boole **B**.

Una relación similar a la que existe entre congruencias en un grupo **G** y subgrupos normales de **G** (8.3.4) se establece entre congruencias en un anillo **A** e ideales de **A**.

8.4.7. **Teorema.** *Sean* **A** *un anillo y* R *una relación binaria en* A. *Entonces* R *es una congruencia en* **A** *si y sólo si* R *es la relación módulo un ideal de* **A**.

Demostración. Sea R una congruencia en **A**. Entonces, R es una congruencia en el grupo abeliano $\mathbf{G}_{\mathbf{A}}$. De acuerdo con el Teor. 8.3.4, R(0) es un subgrupo de $\mathbf{G}_{\mathbf{A}}$ y R es la relación de equivalencia módulo R(0). Veremos

que R(0) es un ideal de **A**: si x $\in$R(0) y a$\in$A, se tiene que xR0 y aRa, de donde, (x.a)R(0.a), es decir x.a$\in$R(0). Resulta, análogamente, que a.x $\in$R(0). Sea ahora R la relación de equivalencia módulo un ideal I de **A**. Se cumple entonces que R es una congruencia en $\mathbf{G_A}$ y que, para todo par a,b de elementos de A, aRb si y sólo si a-b $\in$ I.

Sean a_1,a_2,b_1,b_2, elementos de A tales que $a_i R b_i$, i=1,2. Puesto que a_1-b_1 $\in$ I, resulta (a_1.a_2) - (b_1.a_2) $\in$ I y, en forma similar, (b_1.a_2) - (b_1.b_2) $\in$ I. Sumando estos elementos resulta (a_1.a_2)-(b_1.b_2) $\in$ I, es decir, (a_1.a_2) R (b_1.b_2). Luego, R es una congruencia en **A**. ∎

La asignación R→R(0) establece un isomorfismo entre el conjunto de las congruencias en el anillo **A**, ordenado por inclusión, y el conjunto de los ideales de **A** ordenado por inclusión (luego, este último conjunto ordenado es un reticulado en virtud de 3.1.6). El anillo cociente se denota indistintamente **A**/R o **A**/R (0). Según 8.3.3, A/R(0) = {a+R(0), a $\in$A}.

Ejemplos

8.4.8. Según 8.4.3, todo ideal del anillo **Z** de los enteros es principal. Luego, los anillos de la forma Z_p, de enteros módulo p, son los únicos anillos cocientes de **Z**.

8.4.9. En Z_8 {0,4} es un ideal principal. El anillo cociente tiene como conjunto subyacente a {{0,4}, {1,5}, {2,6} , {3,7}} y es isomorfo a $\mathbf{Z_4}$.

8.4.10. En el anillo de las funciones de R en R (6.3.9) el conjunto $I=\{f \in R^R$, $f(1)=0\}$ es un ideal. Las funciones f y g son equivalentes módulo I si y sólo si (f-g) (1)=0 o, equivalentemente, f(1)=g(1). La aplicación de R en R^R/I dada por $r \to \{f; f(1)=r\}$ es un isomorfismo.

8.4.11. Sea h un morfismo de anillos de **A** en **A´**. Según 8.2.8, la relación de equivalencia asociada, R_h, es una congruencia en **A**. Luego, $R_h(0)$ es un ideal de **A** y $R_h(0)=\{a \in A; h(a)=0\}$. Como en el caso de los grupos (8.3.10), $R_h(0)$ se llama *núcleo de h* y se denota Ker h. Aplicando el Teor. 8.2.9 se obtiene que **A**/Ker h es isomorfo a **A´**.

Sea **A** un anillo. En el reticulado de los ideales de **A**, los ideales triviales {0} y A son respectivamente el primer y el último elemento. Los coátomos de ese reticulado se llaman *ideales maximales* de **A**.

8.4.12. **Teorema.** *Sea* **A** *un anillo con unidad conmutativo e* I *un ideal de* **A**. *Entonces* **A**/I *es un cuerpo si y sólo si* I *es un ideal maximal.*

Demostración. Sea **A**/I un cuerpo y supongamos que I está contenido propiamente en un ideal I´. Luego, puede tomarse un elemento a en I´- I. Resulta entonces, a+I≠I.

Sea b ∈ A. Puesto que a+I es invertible en **A**/I, existe x ∈ A tal que (a+I). (x+I) = b+I. Luego, (a.x)+I = b+I.

Puesto que a∈ I´, a.x ∈I´ y como I⊆I' también (a.x)+I⊆I'.

Luego, b+I⊆I' de donde b ∈ I´. Esto muestra que I´= A, lo que implica que I es maximal.

Recíprocamente, supongamos que I es un ideal maximal de **A** y sea a+I un elemento no nulo de **A**/I, es decir a ∈ A-I. Se quiere probar que a+I es invertible, lo que equivale a probar la existencia de un elemento x de A tal que (a+I) (x+I) = 1+I, o equivalentemente, tal que a .x sea equivalente a 1 módulo I, o equivalentemente, tal que, para algún i de I, 1=a.x+i.

Sea I´ = {(a.x)+i; x ∈ A y i∈ I}. Se verá que I´ es un ideal de **A**. En efecto, 0=(a.0)+0 ∈ I´; si z=(a.x)+i y z´= (a.x´) + i´ son elementos de I´ , z-z´= a(x-x´) + (i-i´) que es un elemento de I´. Finalmente, para b∈ A, se tiene, z.b = (a.x.b) + i.b = ((a.b)x)+ i.b, por la conmutatividad de A, de donde z.b∈ I´.

Todo elemento i de I puede escribirse en la forma i=(a.0)+i, lo que muestra que I⊆I' . La inclusión es estricta ya que a=(a.1)+0, con lo cual a∈I´ - I. Siendo I maximal, debe cumplirse I´= A, de donde puede asegurarse la

existencia de x en A e i en I tales que 1=(a.x)+i. Por las consideraciones expresadas más arriba, a+I es invertible. ∎

Ejercicio

8.4.13. Sea $\mathbf{A}$= (A,+,.,-,0) un anillo, probar que una relación R en A es una congruencia en $\mathbf{A}$ si y sólo si R es una congruencia en el grupo $\mathbf{G_A}$ = (A,+,-,0) y R es una congruencia en el semigrupo $\mathbf{S_A}$= (A,.).

8.5 Congruencias en álgebras de Boole.

Sean $\mathbf{B}$=(B,∨,∧,′,0,1) un álgebra de Boole y $\mathbf{A_B}$ = (B,Δ,∧, id_B,0,1) el anillo con unidad definido en 6.3.8. El teorema siguiente muestra que las congruencias en $\mathbf{B}$ son exactamente las congruencias en $\mathbf{A_B}$.

8.5.1. **Teorema.** *Sean* $\mathbf{B}$ *un álgebra de Boole y* R *una relación binaria en* B. *Entonces* R *es una congruencia en* $\mathbf{B}$ *si y sólo si* R *es una congruencia en* $\mathbf{A_B}$.

Demostración. Sea R una congruencia en B. Veremos que R(0) es un ideal de $\mathbf{A_B}$.

Se tiene que $0 \in R(0)$. Sean $a,b \in R(0)$. Entonces $a\ R\ 0$ y $b\ R\ 0$, de donde, $a' R\ 1$ y $b' R\ 1$. Luego, $a \wedge b' R\ 0$ y $a' \wedge b\ R\ 0$. De aquí resulta $(a \wedge b') \vee (a' \wedge b)\ R\ 0$, es decir, $a \Delta b \in R(0)$. También, de $a\ R\ 0$ y $b\ R\ b$, se deduce $a \wedge b\ R\ 0$.

Veremos ahora que R coincide con la relación módulo el ideal R(0) en $\mathbf{A_B}$, lo que equivale a demostrar que $a \Delta b \in R(0)$ si y sólo si aRb, para todo par a,b de elementos de B.

Si aRb, puesto que $b' Rb'$ y R es una congruencia en **B**, resulta $a \wedge b'\ R\ 0$. Similarmente, considerando $a' Rb'$ y bRb, se tiene $a' \wedge b\ R\ 0$. Luego, $(a \wedge b') \vee (a' \wedge b)\ R\ 0$, es decir $a \Delta b\ R\ 0$.

Para demostrar la recíproca, veamos que de xR0 se deduce, para todo y, $x \Delta y$ R y. En efecto, considerando $y' Ry'$, se obtiene $x \wedge y'\ R0$ y, puesto que $x'\ R\ 1$, de yRy, se obtiene, $x' \wedge y\ R\ y$. Aplicando la operación v resulta la aserción.

Sea $a \Delta b\ R\ 0$. Por lo precedente, $(a \Delta b) \Delta b\ R\ b$, es decir aRb. De acuerdo con el Teor. 8.4.7, R es una congruencia en $\mathbf{A_B}$.

Sea ahora R una congruencia en $\mathbf{A_B}$. Supongamos que $a_i Rb_i$, para i=1,2. Entonces, $a_1 \Delta a_2\ R\ b_1 \Delta b_2$ y $a_1 \wedge a_2\ R\ b_1 \wedge b_2$. Puesto que, en general, $x \vee y = x \Delta y \Delta x \wedge y$, resulta $a_1 \vee a_2\ R\ b_1 \vee b_2$. De acuerdo con 8.1.5, esto finaliza la demostración de que R es una congruencia en **B**. ∎

8.6. Productos.

8.6.1. **Definición.** Sean $\mathbf{A} = (A,(f_i)_i \in I)$ y $\mathbf{B}=(B,(g_i)_i \in I)$ álgebras del mismo tipo. El *producto (o producto directo)* de **A** y **B**, denotado **AxB**, es el álgebra del mismo tipo cuyo universo es AxB y cuyas operaciones $(p_i)_i \in I$, están dadas por

$p_i\,(a_1,b_1),\ldots,(a_n,b_n)) = (f_i(a_1,\ldots,a_n),\ g_i\,(b_1,\ldots,b_n))$,

siendo n el rango de i.

8.6.2. **Teorema.** *Sean* $\mathbf{A} = (A,(f_i)_i \in I)$ y $\mathbf{B} = (B,(g_i)_i \in I)$ *álgebras del mismo tipo. Entonces, las proyecciones primera y segunda de* AxB *en* A *y* B, *respectivamente, son morfismos de* **AxB** *en* **A** *y de* **AxB** *en* **B**, *respectivamente.*

Demostración. Sea π_1 de AxB en A la primera proyección del producto cartesiano. Si n es el rango de i, $a_1,\ldots,a_n \in A$ y $b_1,\ldots,b_n \in B$, se tiene

$\pi_1(p_i\,((a_1,b_1),\ldots,(a_n,b_n)) = \pi_1\,(f_i\,(a_1,\ldots,a_n),g_1\,(b_1,\ldots,b_n)) = f_i\,(a_1,\ldots,a_n) = f_i(\pi_1(a_1,b_1),\ldots,\pi_1\,(a_n,b_n))$.

Luego, π_1 es un morfismo. Lo mismo vale para π_2. ∎

Ejercicios

8.6.3. Sean G un grupo y H y K dos subgrupos de G tales que $H \cap K = \{1_G\}$, $H.K = G$ y $xy = yx$ para todo $x \in H$ y para todo $y \in K$.
Probar que la aplicación f de HxK en G definida por $f((x,y)) = x.y$ es un isomorfismo.

8.6.4. Sea **A** un álgebra, se define una estructura algebraica sobre AxA de la siguiente manera:
Para cada operación n-aria f_i en A, se define un correspondiente operación n-aria f en AxA por :
$f((a_1,b_1),..., (a_n,b_n)) = (f_i(a_1,...,a_n),f_i (b_1,...,b_n))$ y además se agregan las operaciones 0-arias (a,a) para todo $a \in A$, una operación unaria s definida por s((a,b)) = (b,a) y una operación binaria t dada por t((a,b),(c,d)) = (a,d), si b=c y t((a,b),(c,d)) = (a,b), en caso contrario.
Probar que B es un subuniverso de ese álgebra definida sobre el conjunto AxA, si y sólo si B es una congruencia en A.

Capítulo 9

Algebras libres

En este capítulo se introducen las álgebras libres y se dan algunos resultados sobre ellas. Se caracterizan los semigrupos, monoides y grupos libres. Se definen los términos y el álgebra de los términos y se prueba que esta última es un álgebra libre.

9.1. Definición de álgebras libres.

9.1.1. **Definición.** Sea K una clase de álgebras de un tipo dado y U un álgebra del mismo tipo, generada por un conjunto X. Se dice que U está *libremente generada por* X, con respecto a la clase K, si se cumple la siguiente propiedad *universal*:
para toda álgebra $\mathbf{A} \in K$ y toda aplicación k: $X \to A$, existe un morfismo k^* de U en A que extiende a k (es decir, para todo $x \in X$, $k^*(x) = k(x)$).

El morfismo k^* de la definición precedente es único ya que si h: U→A es un morfismo con la misma propiedad, h y k^* coinciden sobre un conjunto de generadores de U (ver 7.3.11).

Ejemplos

9.1.2. Sea **N** el monoide de los números naturales, con la suma usual como operación binaria y 0 como unidad. Veremos que **N** está libremente generado por {1} con respecto a la clase K de todos los monoides. En efecto, **N** está generado por {1} y si **M** es un monoide y k: {1}→M una aplicación, poniendo, para todo n∈N, $k^*(n)=(k(1))^n$, se obtiene un morfismo de **N** en **M** que extiende a k. En la misma forma se prueba que el grupo **Z** de los enteros está libremente generado por {1} con respecto a la clase de todos los grupos.

9.1.3. En contraposición con los dos ejemplos precedentes, el grupo **Z**p, p>0, está generado por {1}, pero no está libremente generado por {1} con respecto a la clase de todos los grupos. Para comprobar esta aserción sea k: {1}→**Z** una aplicación tal que k(1)=a, con a>0, y supongamos que existe un morfismo h: $\mathbf{Z_p}$→**Z** que extiende k. Entonces, h(0)=h(1+ ...+1), donde 1 está

repetido como sumando p veces, con lo cual h(0)=ph(1)=pa. Luego, pa=0, en contradicción con la elección de a.

9.1.4. Un reticulado booleano de orden 2 (isomorfo al reticulado de las partes de un conjunto de 2 elementos, ordenado por inclusión) está libremente generado por el conjunto de los dos elementos incomparables, con respecto a la clase de todos los reticulados. En efecto, si a,b,0,1 son los elementos de un tal reticulado **B**, 1=avb y 0=a∧b, con lo cual {a,b} genera **B**. Si para un reticulado **L**, **k** es una aplicación de {a,b} en **L**, poniendo $k^*(a)=k(a)$, $k^*(b)=k(b)$, $k^*(1)=k(a)\vee k(b)$ y $k^*(0)=k(a)\wedge k(b)$ se obtiene un morfismo de **B** en **L** que extiende k. Es fácil comprobar que (B,v,∧,′,0,1) no está libremente generado por {a,b} con respecto a la clase de todas las álgebras de Boole.

9.1.5. **Teorema.** *Sean* $\mathbf{U_1}$ *y* $\mathbf{U_2}$ *álgebras libremente generadas por* X_1 *y* X_2, *respectivamente, con respecto a una clase* K. *Si* $\mathbf{U_1}$ *y* $\mathbf{U_2}$ *pertenecen a* K *y* X_1 *y* X_2 *son coordinables, entonces* $\mathbf{U_1}$ *y* $\mathbf{U_2}$ *son isomorfas.*

Demostración. Sea $\propto$ una biyección de X_1 sobre X_2. Sean K_1: $X_1 \to U_2$ la composición de $\propto$ con la inclusión de X_2 en U_2 y k_2: $X_2 \to U_1$ la composición de $\propto^{-1}$ con la inclusión de X_1 en U_1. Por las hipótesis del enunciado existen los morfismos k_1^* : $U_1 \to U_2$ y k_2^* : $U_2 \to U_1$ que extienden a k_1 y a k_2, respectivamente.

Para todo $x \in X_1$, se tiene que $k_2^* \circ k_1^* (x) = \alpha^{-1}(\alpha(x)) = x$, con lo cual $k_2^* \circ k_1^*$ es igual a la identidad sobre U_1, ya que coincide con la identidad sobre un conjunto de generadores. En la misma forma se prueba que $k_1^* \circ k_2^*$ es igual a la identidad sobre U_2. Luego, k_1^* es una biyección y, por lo tanto, un isomorfismo de U_1 sobre U_2.

∎

9.2. Semigrupos, monoides y grupos libres.

Sea X un conjunto. Se dirá que X es un *alfabeto* y que cada elemento de X es una l*etra.*

Una *palabra*, no vacía, sobre el alfabeto X es una sucesión finita, $p = x_1,...,x_n$, de elementos de X. Se denotará $p = x_1 \ldots x_n$ y se dirá que n es la longitud, l (p), de p. El conjunto vacío es la *palabra vacía.* Será denotado λ y se pondrá $l(\lambda)=0$.

Dadas las palabras $p_1 = x_1 \ldots x_m$ y $p_2 = y_1 \ldots y_n$ la *concatenación* de p_1 con p_2, denotada p_1p_2, es la palabra $x_1 \ldots x_m y_1 \ldots y_n$.

9.2.1. **Monoides libres.** Sea W(X) el conjunto de todas las palabras sobre el alfabeto X. Es inmediato que la concatenación es una operación binaria sobre **W**(X) y que λ es elemento neutro. Se tiene entonces un monoide que

será denotado **W**(X). Se verá que este monoide está libremente generado por X con respecto a la clase de todos los monoides.

De acuerdo con 7.2.8, **W**(X) está generado por X. Sean **M**=(M,.,1) un monoide y k una aplicación de X en M. Definimos k^* : W(X)→M poniendo : k^* (x)=k(x), para todo x∈X; k^* (λ)=1 y

$$k^* (x_1...x_n) = k(x_1).....k(x_n),$$

para toda palabra $x_1...x_n$ no vacía.

Por la asociatividad de la operación. de M , resulta inmediatamente que k^* es un morfismo·

9.2.2. **Semigrupos libres** Sea X un conjunto no vacío. Una demostración análoga a la precedente, permite afirmar que el conjunto W(X)-{λ}, de todas las palabras no vacías sobre el alfabeto X, con la concatenación como operación binaria, es un semigrupo libremente generado por X con respecto a la clase de todos los semigrupos.

9.2.3. **Grupos libres.** Sean X un conjunto y X´ un conjunto coordinable con X y tal que X∩X´ = ∅. Designemos, en general, x´ al elemento correspondiente a x por una biyección de X en X´ , para todo x∈X. Diremos que una palabra, sobre el alfabeto X∪X´ ,es *reducida,* si no tiene un par de letras consecutivas de la forma xx´ o x´ x.

Si p es una palabra perteneciente a $W(X \cup X')$, denotaremos r(p) a la palabra reducida, obtenida de p, suprimiendo reiteradamente las subpalabras de la forma xx' o $x'x$. Por ejemplo, si p es la palabra $ab'\ bb'cc'\ ba'$, $r(p) = \lambda$. Convendremos en escribir $x=(x')'$, para todo $x \in X$.

Sea G el conjunto de todas las palabras reducidas sobre $X \cup X'$. Definimos sobre G una operación binaria. poniendo: $p_1.p_2 = r(p_1p_2)$, y una operación unaria^{-1} dada por $(a_1...a_n)^{-1}=a_n'...a_1'$. Veremos que $(G,.,^{-1}, \lambda)$ es un grupo, para lo cual, observamos en primer lugar que la única propiedad que no se obtiene directamente de las definiciones es la asociatividad de la operación binaria.

Sean p_1, p_2 y p_3 palabras reducidas. Si alguna de ellas es vacía, es evidente que se cumple

$$(1)\quad (p_1.p_2).p_3 = p_1.(p_2.p_3).$$

Supongamos entonces $p_i \neq \lambda$, $i=1,2,3$, y sean $p_1=x_1...x_m$, $p_2= y_1...y_n$ y $p_3= z_1...z_q$.

Demostraremos (1) por inducción sobre $n=l(p_2)$. Si $n=1$, pongamos $y=y_1$.

Caso 1: $y \neq x_m'$, $y \neq z_1'$. Se tiene en este caso que ambos miembros de (1) son iguales a $x_1...x_m y\ z_1...z_q$.

Caso 2: $y=x_m'$, $y \neq z_1'$. Ambos miembros de (1) son iguales a $r(x_1...x_{m-1}\ z_1...z_q)$.

Caso 3: $y=x_m'$, $y=z_1'$. Luego, $x_m = z_1$. Ambos miembros de (1) son iguales a $x_1...x_{m-1}y'\ z_2 ... z_q$.

Supongamos ahora que vale (1) para toda palabra p_2 de longitud menor que n, con $n \geq 2$.

Puede escribirse $p_2 = y_1 \cdot p_2'$, siendo $p_2' = y_2 \ldots y_n$ Entonces, aplicando la hipótesis inductiva y lo demostrado para $l(y)=1$, resulta,

$(p_1 \cdot p_2) \cdot p_3 = (p_1 (y_1 \cdot p_2')) \cdot p_3 = ((p_1 \cdot y_1) \cdot p_2') \cdot p_3 = (p_1 \cdot y_1) \cdot (p_2' \cdot p_3) =$

$p_1 \cdot (y_1 \cdot (p_2' \cdot p_3)) = p_1 \cdot ((y_1 \cdot p_2') \cdot p_3) = p_1 \cdot (p_2 \cdot p_3)$.

Luego, **G** es un grupo. Aplicando 7.2.9, es inmediato que **G** está generado por X. Probaremos ahora que **G** está libremente generado por X con respecto a la clase de todos los grupos.

Sean $(H, ., ^{-1}, 1)$ un grupo y k una aplicación de X en H.

Definimos una aplicación k^* de **G** en H poniendo: $k^*(x) = k(x)$ y $k^*(x') = k(x)^{-1}$, para todo $x \in X$, $k^*(\lambda) = 1$, y, para toda palabra reducida $p = x_1 \ldots x_n$, $k^*(p) = k^*(x_1) \ldots k^*(x_n)$. Es fácil comprobar que $k^*(p_1 \cdot p_2) = k^*(P_1) \cdot k^*(p_2)$, por inducción sobre 1 (p_1), con lo cual, **G** verifica la propiedad universal.

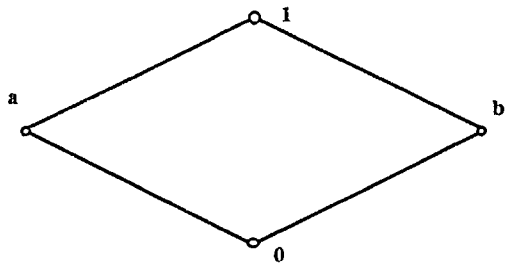
Ejercicios

9.2.4. Sea **A**= { a,b}, probar que el semigrupo $\mathbf{A}^d$ está generado por **A** y que no está libremente generado en la clase de todos los semigrupos, usando la propiedad universal.

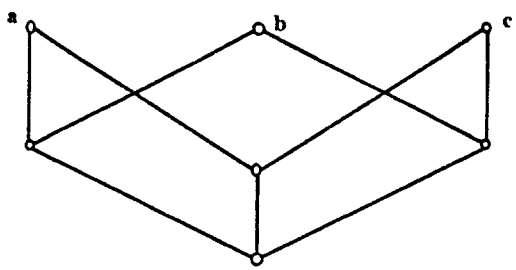
9.2.5. Sean **A**={a,b,c} un conjunto, Sl[**A**] el semigrupo libre generado por **A**, f la aplicación de **A** en (N-{0},+), dada por f(a) = f(b) = f(c) = 1 y f′ de Sl[A] en (N-{0},+) la extensión de f a Sl[A].
Demostrar que el conjunto cociente obtenido por la congruencia asociada a f′ es isomorfo a (N-{0},+). Expresar cómo queda caracterizada cada clase, y dada una clase, cuántas palabras contiene.

9.2.6. Utilizando la propiedad universal, establecer que la propiedad de que un morfismo de grupos es un monomorfismo si y sólo si su núcleo tiene como único elemento a la identidad, no vale en general para monoides.

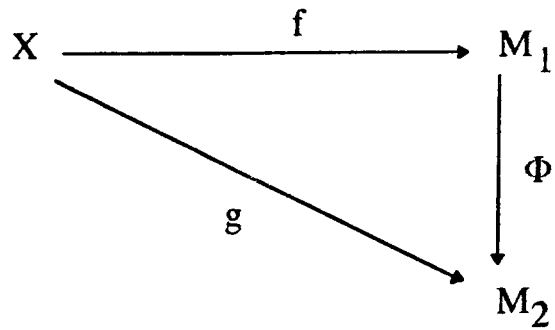
9.2.7. Establecer si el álgebra de Boole de la figura está libremente generada por el conjunto **X**={a,b} con respecto a la clase de todas las álgebras de Boole.



9.2.8. Probar que el semirreticulado de la figura está libremente generado por el conjunto {a,b,c} en la clase de todos los semirreticulados inferiores.



9.2.9. Sean **X** un conjunto no vacío, $(\mathbf{M}_1,.,1)$, $(M_2,.,1)$ dos monoides, f una aplicación de **X** en $\mathbf{M}_1$ y **g** una aplicación de **X** en $\mathbf{M}_2$. Probar que si $\mathbf{M}_1$ está libremente generado en la clase de todos los monoides y además $\mathbf{R}_f \subseteq \mathbf{R}_g$, ($R_f$ y R_g son las relaciones de equivalencia asociadas a f y g respectivamente, ver 3.1.5) entonces existe un único morfismo φ de $\mathbf{M}_1$ en $\mathbf{M}_2$ tal que el diagrama siguiente conmuta.



9.3. Términos

Según se definió en 6.1 un tipo de álgebras es una función ρ de un conjunto I en el conjunto N de los números naturales. Para todo $n \in N$ pondremos $I_n = \rho^{-1}(n)$, es decir, I_n es igual al conjunto de los símbolos funcionales de rango n.

9.3.1. **Definición.** Sean X un conjunto de *variables* y ρ un tipo de álgebras con dominio I. El conjunto T(X) de *términos de tipo ρ sobre* X es el menor conjunto de palabras sobre el alfabeto $X \cup I$ tal que

1) $X \cup I_0 \subseteq T(X)$,

2) si $p_1,\ldots, p_n \in T(X)$ e $i \in I_n$, entonces $ip_1\ldots p_n \in T(X)$

Si . tiene rango 2, suele escribirse $p_1.p_2$ en lugar de . p_1 p_2, en cuyo caso se agregan paréntesis cuando es necesario.

Ejemplos

9.3.2. Si X={x,y} e I consta de un único símbolo operacional . cuyo rango es 2, son ejemplos de términos: x, y, x .y, x.x, (x.x).y, x .(x.y).

9.3.3. Sea ρ el tipo de álgebras cuyo dominio I consta de dos símbolos binarios,+ y ., un símbolo unario - y de todos los números reales, cada uno de rango 0. Si X={x}, todo polinomio a coeficientes reales en la indeterminada x es un término.

Sea ρ un tipo de álgebras con dominio I y X un conjunto . Definimos, por inducción una aplicación v del conjunto W(XUI)) - {λ}, de todas las palabras no vacías sobre el alfabeto XUI, en Z , en la forma siguiente:
para una letra $x \in X$, $v(x)=-1$; para una letra $i \in I$, $v(i)=\rho(i)-1$, y para una palabra $p=a_1\ldots a_n$, $v(p) = \sum_{k=1}^{n} v(a_k)$

Si p es la palabra $a_1\ldots a_n$, una *palabra inicial* de p es una palabra de la forma $a_1\ldots a_k$, con $k \leq n$. Si $k < n$ se dirá que la palabra inicial es *propia*.

9.3.4. **Lema.** Sean ρ un tipo de álgebras con dominio I y X un conjunto. Si p es una palabra sobre XUI que pertenece a T(X) entonces se cumplen las dos condiciones siguientes

1) $v(p) = -1$

2) para toda palabra inicial propia p´ de p, $v(p') \geq 0$.

Demostración. Sea $p \in T(X)$. Si $l(p)=1$, entonces $p=a$, donde $a \in X$ o $a \in I$. En ambos casos $v(p)=-1$.

Supongamos que, para todo término p de longitud menor que n, $n \geq 2$, se cumple $v(p)=-1$ y que $v(p') \geq 0$, para toda palabra inicial propia p´ de p.

Sea ahora p un término de longitud n. Entonces $p=ip_1...p_k$, donde $i \in I_k$ y $p_1,...,p_k \in T(X)$.

Luego, $v(p) = (k-1)+v(p_1)+... +v(p_k) = (k-1)-k = -1$, por la hipótesis inductiva.

Sea ahora p´ una palabra inicial propia de p. Entonces p´ es de la forma $p'=ip_1..p_rp'_{r+1}$, donde $r<k$ y p'_{r+1} es la palabra vacía o una palabra inicial propia de p_{r+1}. Resulta entonces $v(p') = (k-1)-r+v(p'_{r+1}) \geq 0$, puesto que k-r-1 y $v(p'_{r+1})$ son no negativos. ∎

9.3.5. **Corolario.** *Una palabra inicial propia de un término no es un término.*

Demostración. Si p´ es una palabra inicial propia de un término, se tiene, $v(p') \geq 0$, mientras que para todo término p, $v(p)=-1$. ∎

9.3.6. **Corolario.** Si p y q son términos de la forma p= $ip_1...p_n$, q = $jq_1...q_m$, entonces p=q implica que i=j, n=m y, para todo k, k=1,... n, $p_k=q_k$.

Demostración. Si las palabras p y q son iguales, entonces i=j, de donde $\rho(i)=\rho(j)$, con lo cual n=m. Si l (p_1) ≠ l (q_1), p_1 es una palabra inicial propia de q_1, o q_1 lo es de p_1, lo cual contradice el corolario precedente. Luego l (p_1)=l (q_1) y, por lo tanto $p_1=q_1$. Repitiendo el razonamiento se prueba que $p_2=q_2,...,p_n=q_n$. ∎

9.4. El álgebra de los términos.

9.4.1. **Definición.** Sean ρ un tipo de álgebras con dominio I y X un conjunto tales que X∪Io≠∅. *El álgebra de los términos de tipo ρ sobre* X es el álgebra de tipo ρ, (T(X), $(t_i)_{i\in I}$), tal que,

$$t_i(\emptyset) = i, \text{ para } i \in Io,$$

$t_i(p_1,...,p_n) = ip_1...p_n$, para $i \in I_n$ y $p_1,...,p_n \in T(X)$.

(Es claro que la condición X∪Io≠∅ se impone para que T(X)≠∅.)

9.4.2. **Teorema**. *Sean ρ un tipo de álgebras con dominio I y X un conjunto tales que X∪Io≠∅. Si X∩Io=∅, entonces el álgebra T(X), de los términos de*

tipo ρ sobre X, está libremente generada por X con respecto a todas las álgebras de tipo ρ.

Demostración. Veremos que $\mathbf{T}(X)$ está generada por X

Con la notación de 7.2.4, $S_g^{\mathbf{T}(X)}(X) = \bigcup_{n=0}^{\infty} X_n$. Puesto que $X_o=X$ y $I_o \subseteq X_1$, resulta que $X \cup I_o \subseteq S_g^{\mathbf{T}(X)}(X)$. Sean $p_1,...,p_n \in S_g^{\mathbf{T}(X)}(X)$ e i un símbolo funcional de rango n. Puesto que existe k tal que $p_1,...,p_n \in X_k$, $t_i(p_1,...,p_n) = ip_1...p_n)$ pertenece a X_{k+1} y, por lo tanto a $S_g^{\mathbf{T}(X)}(X)$. Siendo T(X) el menor conjunto con esas propiedades, resulta lo afirmado.

Sean ahora $(A,(f_i)_{i\in I})$ un álgebra de tipo ρ y k una aplicación de X en A. Definimos k^* : T(X)→A, por inducción sobre la longitud de los términos, en la forma siguiente

para todo $x\in X$, $k^*(x)=k(x)$, y, para todo $i\in I_o$, $k^*(i)=f_i(\varnothing)$.

Supuesta definida k^* sobre los términos de longitud menor que r, con $r\geq 2$, sea p un término de longitud r. Entonces p es de la forma $p=ip_1...p_n$, donde cada p_j, j=1,...,n, es un término de longitud menor que r. Por la unicidad de la escritura de p (9.3.6), puede definirse $k^*(p) = f_i(k^*(p_1),...,k^*(p_n))$.

Es evidente que k^* es una aplicación que extiende a k. Para comprobar que es un morfismo, sean i un símbolo funcional de rango n y $p_1,...,p_n \in \mathbf{T}(X)$. Entonces $k^*(t_i(p_1,...,p_n)) = k^*(ip_1...p_n) = f_i(k^*(p_1),...,k^*(p_n))$. Esto termina la demostración del teorema. ∎

Indice de términos.

Bibliografia.

1. M.A. Arbib (ed), Algebraic Theory of Machines Languages and Semigroups. Academic Press (1968).

2. C. Berge, Graphes et Hypergraphes, Dunod, Paris, (1970).

3. G.Birkhoff and T. Bartee, Modern Applied Algebra. MacGraw-Hill (1970).

4. S. Burris and H. P. Sankappanavar, A Course in Universal Algebra. Springer (1982).

5. M.Carvallo, Monographie des treillis et algèbres de Boole. Gauthier-Villars, Paris (1966).

6. A.H. Clifford and G. B. Preston, The Algebraic Theory of Semigroups. Am. Math. Soc., Vol.1, Math. Surveys 7, (1962).

7. R. Faure et E. Heurgon, Structures ordonnées et algèbres de Boole. Gauthier -Villars, Paris (1971).

8. A. Gill, Applied Algebra for the Computer Sciences. Prentice-Hall (1976).

9. I.N. Herstein, Algebra Moderna, Trillas, México, (1974).

10. S. Lang, Algebra, Aguilar, España, (1971).

11. R.N. McKenzie, G.F. McNulty and W. F Taylor, Algebras, Lattices, Varieties, Vol. 1 Wadsworth & Brooks/Cole (1987).

12. L. Oubiña, Introducción a la Teoría de Conjuntos, EUDEBA, Buenos Aires, (1976).

13. R. E. Prather, Discrete Mathematical Structures for Computer Science. Haughton Mifflin Company, U.S.A. (1976).

14. K.A. Ross, C.R.B. Wright, Matemáticas Discretas, Prentice-Hall Hispanoamérica, México (1990).

15. D.E. Rutherford, Introduction to Lattice Theory, Oliver and Boyd, Edinburgh and London, (1965).

La tarea de difundir el conocimiento científico,misión esencial de la Universidad,deviene en un compromiso ineludible en el caso de la Facultad de Ciencias Exactas de la Universidad Nacional de la Plata,en cuyos Centros,Institutos y Laboratorios desarrolla su actividad un muy numeroso grupo de docentes e investigadores de reconocido prestigio científico y académico.
La Editorial Exacta constituye el órgano editorial de la Fundación Ciencias Exactas - entidad creada para apoyar el funcionamiento de la Facultad de Ciencias Exactas de la Universidad Nacional de la Plata y su objetivo es el de propiciar la difusión de obras de relevancia científica de la autoría de los docentes e investigadores de dicha Unidad Académica.

FUNDACION
CIENCIAS
EXACTAS
LA PLATA

Existen en la actualidad varios temas de la informática que necesitan para su desarrollo del uso de nociones algebraicas no triviales.
Entre ellos pueden citarse: sistemas de reestructura, tipos abstractos de datos, bases de datos, desarrollos sistemáticos de programas.
Este texto pretende dar al estudiante de informática el material algebraico necesario para que pueda abordar sin dificultades el tratamiento de esos y de otros temas.
Se ha acompañado las definiciones y teoremas, expuestos con todo el rigor y la claridad de la matemática, con numerosos ejemplos que permiten comprender el significado de los conceptos abstractos y adquirir un manejo fluído de los mismos.
Cada apartado incluye varios ejercicios que son considerados una parte importante del texto.

FUNDACION
CIENCIAS
EXACTAS
LA PLATA