CAPÍTULO 8 ANÁLISIS COMBINATORIO EN LOS CONJUNTOS PARCIALMENTE ORDENADOS

En los capítulos 2 . . . 7 de este libro se han descrito sistemáticamente los métodos de resolución de los problemas combinatorios. Sin embargo, se hace cada vez más evidente (en particular, cuando se trata de resolver problemas de tipo extremal) la necesidad imperiosa de analizar más profundamente la estructura de los conjuntos discretos. De esto depende directamente la posibilidad del desarrollo ulterior de la teoría combinatoria general, como también, sobre todo, de las aplicaciones de la misma. El objetivo de este capítulo consiste en introducir al lector en el dominio de las tentativas modernas de extender el análisis combinatorio a los conjuntos de naturaleza más general. Las principales de las propiedades estructurales de los conjuntos, que estudiaremos aquí, son las de ordenación y de independencia.

El capítulo comienza por la descripción de los conjuntos discretos con ordenaciones parciales definidas sobre los mismos. A continuación se analizan más detalladamente los retículos que representan una clase de conjuntos más estrecha, pero muy importante para el análisis combinatorio. Para poder operar con conjuntos parcialmente ordenados se introducen las álgebras de incidencia. Una atención especial se presta en este caso a la operación de inversión y a la función de Moebius relacionada con dicha operación. Por fin, en el capítulo han sido incluidos los fundamentos de la teoría de los matroides la cual representa amplias generalizaciones, que permiten ligar las bases de la teoría combinatoria con toda una serie de ramas de las matemáticas, en primer lugar, con el álgebra moderna y con la topología.

8.1. CONJUNTOS PARCIALMENTE ORDENADOS

Sea $(A, \leqslant)$ un conjunto ordenado parcialmente. Si $|A| < \infty$, el conjunto parcialmente ordenado se denomina *finito*. Si a y b son elementos del conjunto parcialmente ordenado A y si, además, $a \leqslant b$, entonces el conjunto

$$[a, b] = \{x \mid a \leqslant x \leqslant b\}$$

lleva el nombre de *intervalo*. El conjunto parcialmente ordenado $(A, \leqslant)$ es *localmente finito*, siempre que $|[a, b]| < \infty$, cualesquiera que sean $a, b \in A$. Los conjuntos parcialmente ordenados $(A, \leqslant)$ y $(B, \leqslant)$ se llaman *isomorfos* y se designan $(A, \leqslant) \cong (B, \leqslant)$, si existe tal aplicación biunívoca φ del conjunto A sobre el B que la expresión $a_1 \leqslant a_2$ tiene lugar cuando y sólo cuando

$\varphi(a_1) \leqslant \varphi(a_2)$. Indiquemos que la biunívocidad de la aplicación φ puede deducirse de la última condición.

Recordemos que los elementos a y b se llaman *comparables*, si $a \leqslant b$, o bien $b \leqslant a$. De lo contrario, a y b se llaman *incomparables* y se designan: $a \| b$. Así pues, la *cadena* es un conjunto parcialmente ordenado, en el cual no hay elementos incomparables. Se denomina *anticadena* a un conjunto parcialmente ordenado, en el cual $a \| b$ para todo $a \neq b$.

Sea $(A, \leqslant)$ un conjunto ordenado parcialmente, y sea B un subconjunto no vacío del conjunto citado. Entonces, en B existe un orden natural parcial $\leqslant_B$ inducido por la relación $\leqslant$. Llamemos $(B, \leqslant_B)$ *subconjunto parcialmente ordenado* del conjunto $(A, \leqslant)$.

Antes de introducir definiciones nuevas, veamos una serie de ejemplos importantes de los conjuntos parcialmente ordenados que nos harán falta en la exposición ulterior de la materia.

EJEMPLO 1. Un conjunto trivial parcialmente ordenado (o una anticadena), es decir, un conjunto en el que $a \leqslant b$, si y sólo si $a = b$.

EJEMPLO 2. Un conjunto N de todos los números naturales de orden corriente, es decir, $n \leqslant m$ cuando y sólo cuando $m - n$ es no negativo. El conjunto $(N, \leqslant)$ es linealmente ordenado y localmente finito.

EJEMPLO 3. Un conjunto de números reales con orden corriente. Es linealmente ordenado, pero no es parcialmente ordenado y localmente finito.

EJEMPLO 4. Un conjunto $\mathscr{P}(S)$ de todos los subconjuntos del conjunto S, ordenado por inclusión, es decir, si $A, B \in \mathscr{P}(S)$, entonces $A \leqslant B$ en $\mathscr{P}(S)$ cuando y sólo cuando $A \subseteq B$ (A es un subconjunto del conjunto B). El conjunto $(\mathscr{P}(S), \subseteq)$ no es linealmente ordenado; por ejemplo, los subconjuntos arbitrarios de un solo elemento no son comparables. Si $|S| < \infty$, entonces $(\mathscr{P}(S), \subseteq)$ es también finito. De lo contrario, $(\mathscr{P}(S), \subseteq)$ ni siquiera será conjunto localmente finito.

EJEMPLO 5. Un conjunto Z de números enteros ordenados por divisibilidad, es decir, $a \leqslant b$ cuando y sólo cuando $a \mid b$ (a divide a b). El conjunto $(Z, \mid)$ es localmente finito, pero no es linealmente ordenado.

EJEMPLO 6. Un conjunto $D(n)$ de todos los divisores de un número entero n ordenado por divisibilidad. Este conjunto es un subconjunto parcialmente ordenado del conjunto $(Z, \mid)$.

EJEMPLO 7. Un conjunto $P(n)$ de particiones de un número natural n (se denomina partición de un número natural n a toda sucesión finita no creciente de números naturales $\lambda_1, \lambda_2, \ldots, \lambda_r$, para la cual $\sum_{i=1}^{r} \lambda_i = n$; los números λ_i suelen llamarse partes de la partición), ordenadas de un modo tal que si $\lambda, \mu \in P(n)$, entonces $\lambda \leqslant \mu$ cuando y sólo cuando al sumar las partes separadas de la partición λ, puede obtenerse la partición μ. Por ejemplo, $3 + 1 + 1 = (1^2, 3)$; $4 + 1 = (1, 4)$; $3 + 2 = (2, 3)$ son particiones del número 5, y, además, $(1^2, 3) \leqslant (1, 4)$ y $(1^2, 3) \leqslant (2, 3)$, mientras que $(1, 4)$ y $(2, 3)$ son incomparables en $P(5)$.

EJEMPLO 8. Se denomina partición no ordenada de un conjunto finito S a la colección $\pi = \{\pi_1, \pi_2, \ldots\}$ de sus subconjuntos no vacíos disjuntos dos a dos, cuya unión es igual a S; los subconjuntos π_i llevan el nombre de bloques de la partición. Veamos un conjunto $B(S_n)$ de todas las particiones no ordenadas del conjunto S_n, compuesto por n elementos y ordenados conforme a la unión de bloques, es decir, $\pi \leqslant \tau$ cuando y sólo cuando cada bloque π_i, perteneciente a π, está contenido en cierto bloque τ_j, perteneciente a τ (o bien, dicho de otro modo, cada bloque τ_j se obtiene «pegando» ciertos bloques de π).

EJEMPLO 9. Un conjunto de todos los subespacios del espacio vectorial n-dimensional $V_n(q)$ sobre un campo de q elementos ordenados por inclusión, es decir, si U y V son los subespacios de $V_n(q)$, entonces $U \leqslant V$ cuando y sólo cuando U es un subespacio de V.

EJEMPLO 10. Un conjunto de todas las caras de un poliedro convexo d-dimensional (por poliedro convexo d-dimensional se entiende un conjunto acotado d-dimensional de puntos del espacio euclídeo que puede ser representado como una intersección de un número finito de semiespacios), ordenadas por inclusión.

Los conjuntos parcialmente ordenados mencionados en los ejemplos 6 . . . 10 son finitos.

Se llama *cadena* C en un conjunto parcialmente ordenado $(A, \leqslant)$ su subconjunto no vacío el cual, siendo parcialmente ordenado, constituye una cadena. Recibe el nombre de *anticadena* en un conjunto parcialmente ordenado un subconjunto no vacío suyo el cual, siendo parcialmente ordenado, constituye una anticadena. La *longitud* $l(C)$ de una cadena finita C es un número igual a $|C| - 1$. Se dice que el conjunto parcialmente ordenado A es de *longitud* n (la designación es $l(A) = n$), si en A existe una cadena de longitud n y todas las demás cadenas en A tienen una longitud no superior a n. Diremos que el conjunto parcialmente ordenado A tiene una longitud finita, si su longitud es igual a n, y $n \neq \infty$. Diremos que la *anchura* de un conjunto parcialmente ordenado A es igual a n, si existe en A una anticadena compuesta de n elementos, mientras que todas las anticadenas restantes de A contienen no más de n elementos. Observemos que la longitud de un conjunto linealmente ordenado A es igual a $|A| - 1$, y la anchura, a 1.

Sea S un conjunto de n elementos. Hallemos la anchura del booleano $\mathscr{P}(S)$, es decir del conjunto parcialmente ordenado del ejemplo 4. La respuesta a esta pregunta la da el teorema siguiente que se debe a Sperner.

Teorema 1. Sea $\mathscr{P}(S)$ un booleano, $|S| = n$. Entonces, la anchura de $\mathscr{P}(S)$ es igual a $\binom{n}{[n/2]}$, donde $[x]$ es una parte entera de x.

La demostración del teorema se desprende directamente del siguiente lema.

Lema 1. Sea $(A_1, A_2, \ldots, A_m)$ una anticadena arbitraria en $\mathscr{P}(S)$, donde

$|S| = n$. En este caso se verifica la desigualdad

$$\sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \leqslant 1.$$

Demostración del lema. Examinemos en $\mathcal{P}(S)$ las cadenas $\varnothing = B_0 \subset B_1 \subset \ldots \subset B_n = S$, tales que $|B_k| = k$ para $k = 1, 2, \ldots, n$. El número de todas estas cadenas en $\mathcal{P}(S)$ es igual a $n!$. Veamos entre dichas cadenas aquellas que «pasan» por el subconjunto A_i, $i = 1, 2, \ldots, m$. Sea $|A_i| = r$. Entonces, las cadenas citadas tienen la forma siguiente:

$$B_0 \subset B_1 \subset \ldots \subset B_{r-1} \subset A_i \subset B_{r+1} \subset \ldots \subset B_n.$$

El número de subcadenas $B_0 \subset B_1 \subset \ldots \subset B_{r-1}$ es igual a $|A_i|! = r!$, mientras que el número de subcadenas $B_{r+1} \subset \ldots \subset B_n$ es igual a $(n - |A_i|)! = (n - r)!$. Por consiguiente, el número total de cadenas que tienen la longitud n y que pasan por A_i es igual a $|A_i|!(n - |A_i|)!$.

Cuando $i \neq j$, las cadenas que pasan por A_i y A_j son diferentes. Efectivamente, supongamos que A_i, A_j $(i \neq j)$ pertenecen a una misma cadena. Existen, pues, tales elementos B_k y B_l de la cadena que $A_i = B_k$ y $A_j = B_l$. Pero, en este caso, o bien $A_i \subset A_j$, lo que contradice la suposición sobre la incomparabilidad de A_i y A_j.

De aquí, el número total de cadenas de longitud n que pasan por todos los subconjuntos de la anticadena es igual a

$$\sum_{i=1}^{m} |A_i|!(n - |A_i|)!$$

Mas esta magnitud no sobrepasa el número total de todas las cadenas de longitud n, por lo cual

$$\sum_{i=1}^{m} |A_i|!(n - |A_i|)! \leqslant n!.$$

De aquí proviene la desigualdad[1)]

$$\sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \leqslant 1,$$

lo que se trataba de demostrar.

Demostración del teorema 1. Sea $(B_1, \ldots, B_k)$ una familia de todos los subconjuntos del conjunto S, compuestos de $\left[\frac{n}{2}\right]$ elementos. Entonces,

[1)] Muy a menudo en la literatura esta desigualdad se denomina de Lubel, quien la demostró en 1966. Sin embargo, fue obtenida con anterioridad, independientemente, por Yamamoto (1954) y L. Meshalkin (1963).

evidentemente, esta familia, siendo un subconjunto de $\mathscr{P}(S)$ será una anticadena y $k = \binom{n}{\left[\frac{n}{2}\right]}$. Demostremos ahora que todas las demás anticadenas en $\mathscr{P}(S)$ no son superiores en potencia a k.

Efectivamente, sea $(A_1, \ldots, A_m)$ una anticadena arbitraria de $\mathscr{P}(S)$. Entonces, en virtud del lema 1 y la desigualdad evidente

$$\binom{n}{|A_i|} = k \leqslant \binom{n}{\left[\frac{n}{2}\right]}$$

tenemos

$$\frac{m}{\binom{n}{\left[\frac{n}{2}\right]}} \leqslant \sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \leqslant 1.$$

Por consiguiente, $m \leqslant \binom{n}{\left[\frac{n}{2}\right]} = k$, lo que se requería de demostrar. Desempeña un papel importante el principio siguiente referente a los conjuntos finitos parcialmente ordenados. Dicho principio confirma la existencia de una numeración concordada con el orden.

Teorema 2. Sea $(A, <)$ un conjunto finito parcialmente ordenado. En este caso los elementos de A pueden numerarse de un modo tal: $A = \{a_1, a_2, \ldots, a_n\}$ que de $a_i < a_j$ se deduzca $i < j$.

Demostración. Pongamos $X_m = \{b_1, b_2, \ldots, b_m\}$, donde la numeración primaria $A = \{b_1, b_2, \ldots, b_n\}$ está elegida de una manera cualquiera. Construyamos una sucesión de aplicaciones biunívocas φ_m de los conjuntos $\{1, 2, \ldots, m\}$ sobre sí mismo, tal que cada subconjunto X_m, numerado por medio de $\varphi_m: X_m = \{a_1^m, \ldots, a_m^m\}$, donde $a_i^m = b_{\varphi_m(i)}$, satisfaga la afirmación enunciada en el teorema: de $a_i^m < a_j^m$ se deduce que $i < j$.

Cuando $m = 1$, la aplicación biunívoca φ_1 se construye unívocamente. Supongamos que una aplicación biunívoca

$$\varphi_{n-1}: \{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}$$

con la propiedad requerida ya está construida. Designemos con k el número menor de aquellos números i que poseen la propiedad $b_n < a_i^{n-1}$. Construyamos una aplicación biunívoca $\varphi_n: \{1, \ldots, n-1, n\} \to \{1, \ldots, n-1, n\}$ del modo siguiente:

$$\varphi_n(i) = \begin{cases} i, & \text{si } i < k; \\ n, & \text{si } i = k; \\ i+1, & \text{si } i > k. \end{cases}$$

En otras palabras, introduzcamos b_n entre a_k^{n-1} y a_k^{n-1}. Comprobemos que

φ_n posee las propiedades requeridas. Si $a_i^n < a_j^n$, y $\{a_i^n, a_j^n\} \subset X_{n-1}$, entonces, por hipótesis de la inducción, $i < j$. Si $b_n = a_k^n < a_j^n$, entonces $k < j$ por construcción. En fin, si $a_i^n < a_k^n = b_n$, entonces $a_i^n < a_k^n < a_{k+1}^n$, de donde $a_i^n < a_{k+1}^n$, por ser transitiva la relación de orden, y por fin, $i < k + 1$ por hipótesis de la inducción, puesto que $\{a_i^n, a_{k+1}^n\} \subset X_{n-1}$. Por consiguiente, también aquí $i < k$ (el caso de $i = k$ es imposible); la demostración del teorema queda terminada.

En los conjuntos parcialmente ordenados resulta útil resaltar los elementos de ciertos tipos especiales. El elemento M del conjunto parcialmente ordenado A se denomina *máximo* (último elemento), si en A no existe un elemento a «*mayor*» que M, es decir, $a \geqslant M$ no se verifica, cualquiera que sea $a \in A$, distinto de M. Por analogía, un elemento $m \in A$ se denomina *mínimo* (primer elemento), si en A no existe un elemento $a \in A$, distinto de m, y tal que $a \leqslant m$. El elemento $a \in A$ se llama *maximal* si para cada $c \in A$: $c \leqslant a$. El elemento $b \in A$ se llama *minimal* si para cada $c \in A$: $c \geqslant b$. Para los elementos maximal y minimal de un conjunto parcialmente ordenado se usarán también las designaciones I (unidad) y 0 (cero), respectivamente. Es fácil comprobar que todo elemento máximal es máximo y todo elemento minimal es mínimo. La afirmación recíproca, hablando en general, no tiene lugar. Así, por ejemplo, en un conjunto trivial parcialmente ordenado todo elemento es tanto máximo, como mínimo. Otro ejemplo de elementos mínimos pero no minimales nos lo dan los números primos en el conjunto de números positivos enteros $\{2, 3, 4, 5, 6, \ldots\}$, ordenado por divisibilidad igual que en el ejemplo 5. El cero en el conjunto $P(n)$ del ejemplo 7 será (1^n); en el booleano $\mathscr{P}(S)$, el conjunto vacío $\varnothing$, y en belliano $B(S_n)$, la partición $\{a_1\}, \{a_2\}, \ldots, \{a_n\}$. Las unidades en estos conjuntos parcialmente ordenados también existen y son iguales a n, S y S_n, respectivamente.

Observemos que la definición de elemento minimal se obtiene de la definición de elemento maximal sustituyendo simplemente el símbolo $\leqslant$ por $\geqslant$. De este mismo modo están relacionados los conceptos de elementos máximo y mínimo. En general, al disponer de una afirmación referente a un conjunto parcialmente ordenado y al sustituir $\leqslant$ por $\geqslant$, obtenemos una afirmación nueva. Las afirmaciones relacionadas entre sí mediante el modo citado se llaman *duales*.

Sea $(A, \leqslant)$ un conjunto parcialmente ordenado. La relación $\geqslant$ (donde $a \geqslant b$ significa que $b \leqslant a$) es también relación de orden sobre A. De este modo, $(A, \geqslant)$ es también un conjunto parcialmente ordenado que se llama *dual* respecto del conjunto parcialmente ordenado $(A, \leqslant)$. Ahora, si Φ es una afirmación referente a los conjuntos parcialmente ordenados, entonces, al sustituir todos los signos $\leqslant$ por $\geqslant$, obtendremos una afirmación dual respecto de la afirmación Φ.

Principio de dualidad. Si una afirmación Φ es cierta para todos los conjuntos parcialmente ordenados, la afirmación dual respecto a Φ también será lícita para todos los conjuntos parcialmente ordenados.

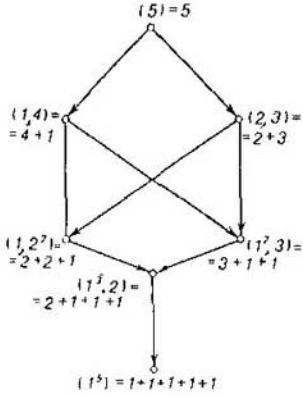

Fig 8.1.

Este principio es válido por la simple razón de que Φ tiene lugar en el conjunto parcialmente ordenado $(A, \leqslant)$ cuando y sólo cuando la afirmación dual respecto de Φ tiene lugar en el conjunto parcialmente ordenado $(A, \geqslant)$.

Sea $(A, \leqslant)$ un conjunto parcialmente ordenado. Diremos que un elemento $a \in A$ *cubre* el elemento $b \in B$, o bien b *se cubre* por el elemento a (la designación es: $a \succ\!\!- b$, o bien $b -\!\!\prec a$), si $a > b$ y no existe $c \in A$, tal que se verifique $a > c > b$. El elemento a se llama *átomo*, si $a \succ\!\!- 0$, y *coátomo*, si $a -\!\!\prec 1$. Para el caso en que a cubre b o coincide con éste, la designación será $a \succcurlyeq b$.

Se denomina *diagrama de Hasse* de un conjunto parcialmente ordenado A a un grafo orientado, cuyos vértices son los elementos del conjunto A, mientras que el arco (a, b) está presente cuando y sólo cuando a cubre b en el conjunto parcialmente ordenado A. Se acostumbra a representar los arcos en este grafo en dirección hacia abajo. En la fig. 8.1 se muestra el diagrama de Hasse del conjunto parcialmente ordenado $P(5)$ del ejemplo 7.

Los coátomos en $P(5)$ son (1, 4) y (2, 3); el átomo es $(1^3, 2)$. En $P(5)$ se tienen en total 7 elementos. Los valores de $|P(n)|$ crecen muy rápidamente a medida que aumente n; por ejemplo: $|P(6)| = 11$, $|P(10)| = 42$, $|P(20)| = 627$, $|P(50)| = 204\,226$, $|P(100)| = 190\,569\,292$.

Los diagramas de Hasse para el boolcano $\mathcal{P}(S)$, donde $S = \{1, 2, 3, 4\}$ y para el conjunto parcialmente ordenado $D(20)$ del ejemplo 6 se aducen en las figs. 8.2 y 8.3, respectivamente. En el primer conjunto los átomos son todos los subconjuntos de un solo elemento, a saber, {1}, {2}, {3}, {4}, y en el segundo, los números 2 y 5.

Sea A un conjunto finito parcialmente ordenado. Entonces su diagrama de Hasse es un grafo orientado sin contornos. Por analogía con la teoría de los grafos, se denomina *matriz de adyacencia* del diagrama de Hasse de un conjunto parcialmente ordenado A a la matriz cuadrada $\|k_{ij}\|$ de orden $|A|$, en la que $k_{ij} = 1$, si (a_i, a_j) es un arco en el diagrama de Hasse (o bien, lo que es equivalente, $a_j -\!\!\prec a_i$ en A), y $k_{ij} = 0$, en el caso contrario. Esta matriz coincide con la matriz de la función de recubrimiento del álgebra estándar de incidencia $S(A)$ (véase más abajo el párrafo 8.3).

Detengámonos brevemente en los métodos de numeración, concordada con el orden, cuya existencia se garantiza por el teorema 2. Diremos que el elemento a es un *ascendiente* del elemento b, o que b es un *descendiente* de a, siempre que $a > b$ en A.

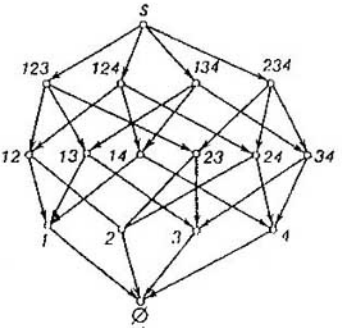

Fig.8.2.

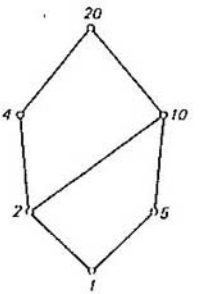

Fig.8.3.

Veamos el problema siguiente que es de importancia en las aplicaciones:

Divídanse todos elementos de un conjunto parcialmente ordenado A en capas de un modo tal que:

a) todos los elementos de una capa dada no tengan descendientes en la capa siguiente;

b) los elementos de la primera capa no tengan descendientes, y los de la capa última no tengan ascendientes;

c) cada capa constituya una anticadena en A.

He aquí uno de los métodos de resolución de este problema. Sea K una matriz de adyacencia del diagrama de Hasse de un conjunto parcialmente ordenado A. Denotemos con $\bar{a}$, b los vectores columna de esta matriz. Calculemos el vector $\bar{a}_1 = \sum_{a \in A} \bar{a}$, y agreguémoslo a la matriz K escribiéndolo a la derecha. Designemos con A_1 un subconjunto del conjunto A, a cuyos elementos en el vector columna $\bar{a}_1$ corresponden ceros. Estos ceros significan que los elementos del conjunto A_1 no tienen descendientes. Por eso el conjunto A_1 forma la primera capa.

Calculemos ahora el vector $\bar{a}_2 = \bar{a}_1 - \sum_{a \in A_1} \bar{a}$. A los ceros de este vector columna $\bar{a}_2$ corresponden los elementos del conjunto A_2 que forman la segunda capa. Calculemos el vector $a_3 = \bar{a}_2 - \sum_{a \in A_2} \bar{a}$, y consideremos los elementos del conjunto A_3, correspondientes a los ceros del vector columna, ubicados en la tercer capa. Seguiremos con los cálculos hasta que se obtenga un vector columna compuesto exclusivamente por ceros. Consideremos todos los elementos restantes del conjunto A situados en la última capa. Para demostrar que la partición obtenida es la buscada, observemos que en cada etapa del cálculo hallamos los elementos del conjunto sin descendientes.

Ilustremos este método con un ejemplo concreto. Sea A un conjunto

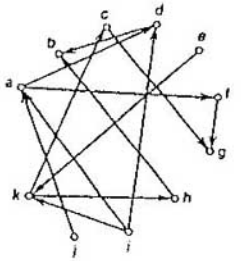

Fig.8.4.

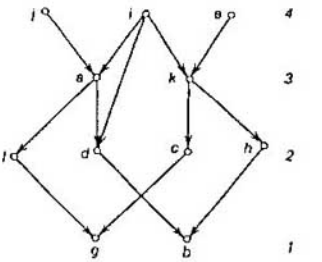

Fig.8.5.

parcialmente ordenado cuyo diagrama de Hasse se expone en la fig. 8.4. Todos los cálculos para la resolución del problema se aducen en la tabla. El diagrama de Hasse se da en la fig. 8.5.

Tabla 8.1

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	A_1	A_2	A_3	A_4
a	0	0	0	1	0	1	0	0	0	0	0	2	2	0	X
b	0	0	0	0	0	0	0	0	0	0	0	0	X	X	X
c	0	0	0	0	0	0	1	0	0	0	0	1	0	X	X
d	0	1	0	0	0	0	0	0	0	0	0	1	0	X	X
e	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0
f	0	0	0	0	0	0	1	0	0	0	0	1	0	X	X
g	0	0	0	0	0	0	0	0	0	0	0	0	X	X	X
h	0	1	0	0	0	0	0	0	0	0	0	1	0	X	X
i	1	0	0	1	0	0	0	0	0	0	1	3	3	2	0
j	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0
k	0	0	1	0	0	0	0	1	0	0	0	2	2	0	X
	Capa											1	2	3	4
	Elementos											*b, g*	*c, d, f, h*	*a, k*	*e, i, j*

Observación. Al realizar el método examinado de partición en capas con ayuda de un ordenador, hace falta agregar a la matriz K la matriz

$$E = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

con el fin de distinguir los ceros (0) y lugares vacíos (X). En este caso los ceros se harán unidades, y las X, ceros.

Al numerar arbitrariamente los elementos de un conjunto parcialmente ordenado A dentro de la capa 1, luego, dentro de la capa 2, etc., obtendremos una numeración concordada con el orden del conjunto A. Por ejemplo, los elementos de un conjunto parcialmente ordenado cuyo diagrama de Hasse se expone en la fig. 8.4, podemos numerarlos así: *bghcdfkaeij*, o bien *gbcdhfakeji*, o bien *bgfdchakjie*, etc. Hemos de notar que, aceptada tal numeración de los elementos, K será una matriz triangular superior.

Es prácticamente imposible numerar, con ayuda del método aducido, todas las permutaciones de los elementos del conjunto parcialmente ordenado A concordadas con el orden de A. Por eso, recomendamos que el mismo lector elabore, a título de ejercicio, el método de numeración de las permutaciones de los elementos de un conjunto parcialmente ordenado concordadas con el orden del mismo, mas dicha recomendación ha de realizarse después de estudiar el material del § 8.3.

Una cadena, en la que cada subconjunto no vacío posee un elemento mínimo, se llama *bien ordenada*. Un conjunto bien ordenado constituye una cadena finita. Un conjunto de números naturales, ordenado de un modo natural, es también bien ordenado. Un conjunto de todos los números enteros no está bien ordenado con relación al orden natural, puesto que no tiene el elemento mínimo. Sin embargo, se hace bien ordenado, si el orden se establece del modo siguiente:

$$1<2<3<4< \ldots <0<-1<-2<-3<-4< \ldots,$$

donde todos los números positivos preceden a los restantes. Otro ejemplo de una cadena que no está bien ordenada es el segmento [0, 1], pues, por ejemplo, el intervalo $\left(\frac{1}{2}, 1\right)$ no contiene el elemento minimal.

La importancia de los conjuntos bien ordenados consiste en la posibilidad de aplicar el *método* de inducción, o sea de la llamada *inducción transfinita* que se conoce por los conjuntos numerables y finitos en el caso de los conjuntos bien ordenados. La esencia de este método consiste en lo siguiente: sea P una afirmación concerniente a los elementos de un conjunto bien ordenado A. Si P se cumple para el elemento mínimal (o «primero») del conjunto A, y de la validez de la afirmación P para todo $x<a$ se deduce su validez para el elemento a, entonces la afirmación P se cumple para todos los elementos del conjunto bien ordenado A.

En efecto, supongamos cumplidas las premisas de la condición de inducción. Veamos un subconjunto B de todos los elementos de A, para los cuales no se cumple la afirmación P. Si la conclusión de la inducción no tiene lugar, entonces B es no vacío. Por cuanto A es bien ordenado, en B se tiene el elemento mínimo a. Según la condición, este elemento no puede ser elemento minimal del conjunto A. Si $x<a$, entonces $x \in B$, y, por lo tan-

to, para x es válida la afirmación P según la condición. Mas en este caso para a es válida la afirmación P. Hemos llegado a una contradicción. Esto quiere decir, que el conjunto B es vacío y la afirmación P es válida para todo $b \in A$.

Se dice que un conjunto parcialmente ordenado A satisface la *condición de mínimo (de máximo*, respectivamente), si cada subconjunto no vacío del conjunto A es un conjunto parcialmente ordenado que contiene elementos minimales (maximales).

Cualquier conjunto bien ordenado A satisface la condición de minimal, y el conjunto A^*, dual respecto de A, satisface la condición de maximal. Como ejemplo de tal conjunto interviene el conjunto de números naturales de orden corriente que satisface la condición del mínimo, pero no satisface la del máximo.

Diremos que un conjunto parcialmente ordenado satisface la *condición de rotura de las cadenas decrecientes* (la *condición de rotura de las cadenas crecientes*, respectivamente), si para una sucesión numerable arbitraria $\{a_n \mid n = 1, 2, \ldots\}$ de elementos de A tal que $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant \ldots$ ($a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n \leqslant \ldots$, respectivamente) existe un número k, tal que $a_n = a_k$ para todo $n \geqslant k$.

Teorema 3. En un conjunto parcialmente ordenado A la condición de mínimo (de máximo, respectivamente) es equivalente a la condición de rotura de las cadenas decrecientes (crecientes).

Demostración. Supongamos que se cumple la condición de mínimo y que $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant \ldots$ es una cadena numerable de elementos de A. Sea a el elemento mínimo en un subconjunto $\{a_n \mid n = 1, 2, \ldots\}$ del conjunto A. Entonces, $a = a_k$ para cierto k, y, por consiguiente, $a_n = a = a_k$ para todo $n \geqslant k$.

Al contrario, supongamos que se cumple la condición de rotura de las cadenas decrecientes y que B es un subconjunto no vacío del conjunto A. En este caso B contiene el elemento a_1, y si a_1 no es mínimo en B, existe un elemento $a_2 \in B$ tal que $a_1 > a_2$. Supongamos que existen tales $a_1, \ldots, a_n \in B$ que $a_1 > a_2 > \ldots > a_n$. En este caso, o bien a_n es mínimo en B, o bien existe un elemento $a_{n+1} \in B$ tal que $a_n > a_{n+1}$. De aquí concluimos que o bien B tiene un elemento mínimo, o bien existe una cadena infinita $a_1 > a_2 > \ldots > a_n > \ldots$ de elementos de B. Por hipótesis, es posible sólo el primer caso.

De un modo dual se establece la validez de la parte restante del teorema, el cual queda, pues, completamente demostrado.

Ejercicio. Demuéstrese que

1. Si una cadena C y otra cadena, dual respecto de C, en un conjunto dual parcialmente ordenado están bien ordenadas, entonces C contiene un número finito de elementos.
2. Si un conjunto parcialmente ordenado no contiene ni cadenas infinitas ni anticadenas infinitas, es finito.
3. Un conjunto finito satisface las condiciones de mínimo y de máximo.

4. Si una cadena no es bien ordenada, contiene una subcadena que es dual respecto de una serie natural.

5. Un conjunto ordenado local finito parcialmente satisface la condición del mínimo.

Si A es un conjunto parcialmente ordenado, entonces el conjunto de todas las cadenas será parcialmente ordenado de por sí con ayuda de una inclusión teórico-multiplicativa. Los elementos máximos de este último conjunto, si existen, se denominan cadenas máximas del conjunto A. En otras palabras, una cadena C del conjunto parcialmente ordenado A se llama cadena máxima, si para todo elemento a de A, no perteneciente a C, el subconjunto $C \cup \{a\}$ ya no es una cadena.

Al estudiar los conjuntos infinitos hemos de emplear frecuentemente el siguiente *axioma de elección:*

Dado un conjunto A, existe una función φ que a todo conjunto no vacío B de A le hace corresponder un elemento determinado $\varphi(B)$ de este subconjunto.

Dicho de otro modo, la función φ marca el único elemento en cada uno de los subconjuntos no vacíos del conjunto A.

Las numerosas investigaciones matemáticas se apoyan en el axioma de elección. La cuestión sobre las bases lógicas de este axioma y la legitimidad de su empleo pertenece a los problemas más difíciles y discutibles en la argumentación de la teoría de conjuntos. En la exposición ulterior que viene más adelante el axioma de elección se supondrá válido. Para los conjuntos numerables el axioma de elección puede ser fácilmente demostrado. En efecto, si los elementos del conjunto A están numerados con números naturales, obtenemos la función requerida al marcar en cada subconjunto B de A aquel elemento suyo que lleva el número minimal.

Sea A un conjunto en el que vienen definidas dos relaciones de orden parcial: $\leqslant$ y $\rightrightarrows$. Diremos que el orden $\rightrightarrows$ es una prolongación del orden $\leqslant$, si para cualesquiera $a, b \in A$ la relación $a \leqslant b$ lleva consigo la correlación $a \rightrightarrows b$.

Teorema 4. Sea A un conjunto parcialmente ordenado que satisface la condición de mínimo. Entonces, su orden parcial puede prolongarse hasta el orden que transforma A en un conjunto bien ordenado.

Antes de pasar a la demostración del teorema, demos a conocer algunas definiciones. Se denomina *segmento* de cierto conjunto bien ordenado A a todo subconjunto suyo B que contiene, junto con cualquier elemento suyo b, todos los $x \in A$, tales que $x \leqslant b$. Un conjunto de elementos que preceden estrictamente a cierto elemento a de A es un segmento auténtico del conjunto A, es decir, un segmento, distinto del propio A, con el cual se agotan todos los *segmentos auténticos*: si B es un segmento de tal índole, él se compone de todos los elementos que preceden estrictamente al elemento mínimo del complemento $A \setminus B$, es decir, B se define por dicho elemento. Convengamos en considerar un subconjunto vacío como segmento auténtico del

conjunto A; éste se determina por el elemento mínimo del conjunto citado.

Demostración del teorema 4. Sea A un conjunto parcialmente ordenado que satisface la condición de mínimo. Marquemos en cada subconjunto suyo no vacío B un solo elemento $\varphi(B)$, al poner $\varphi(B)$ igual a uno de sus elementos mínimos. Esto siempre puede realizarse en virtud de la condición de mínimo y del axioma de elección. Llamaremos marcado al subconjunto no vacío B de A, si el orden inducido de B puede ser prolongado hasta el orden que lo convierte en un conjunto bien ordenado y, además, de una manera tal que para todo $a \in B$ tenemos: $a = \varphi(A \setminus B')$, donde B' es un segmento del conjunto B en la ordenación total citada que se define por el elemento a. Los conjuntos marcados existen en A; tal es, por ejemplo, un subconjunto $\{\varphi(A)\}$, puesto que $\{\varphi(A)\}' = \varnothing$, y $\varphi(A) = \varphi(A \setminus \varnothing)$.

Sean B y C dos subconjuntos marcados, para los cuales están elegidas las ordenaciones totales que poseen la propiedad indicada en el parágrafo antecedente. Entonces, ambos subconjuntos mencionados tienen $\varphi(A)$ en calidad de primer elemento, razón por la cual poseen segmentos coincidentes no vacíos. La reunión D de todos los segmentos coincidentes de estos dos subconjuntos será, evidentemente, un segmento en cada uno de ellos; este es el segmento mayor entre los segmentos coincidentes. Si el segmento D fuese distinto tanto de B, como de C, entonces, de conformidad con la definición de subconjunto marcado, el segmento D se definiría en B y en C por el elemento $\varphi(A \setminus D)$, y en este caso B y C poseerían un segmento coincidente mayor que D, el cual consta de D y del elemento $\varphi(A \setminus D)$. Esta contradicción con la definición de D demuestra que uno de los dos subconjuntos marcados B y C es un segmento del otro.

De aquí se desprende que la reunión S de todos los subconjuntos marcados de A será marcada también. En efecto, si b y c de S pertenecen a los subconjuntos marcados B y C, respectivamente, entonces ambos yacen en el mayor de los subconjuntos citados, por ejemplo, en B. Suponiendo $b \geqslant c$ en S, si $b \geqslant c$ en este A, obtendremos en S una ordenación lineal, la cual será, incluso, ordenación total: toda cadena decreciente de elementos en S está contenida íntegramente en cierto subconjunto marcado B, por lo cual ha de romperse. Por fin, si $b \in S$, entonces b está contenido en cierto subconjunto marcado B y define tanto en S, como en B un mismo segmento B', con la particularidad de que $b = \varphi(A \setminus B')$. Con ello queda demostrado el hecho de que S está marcada.

Para finalizar la demostración del teorema nos resta señalar que si S fuese distinto de A, entonces en la contradicción con la definición de S obtendríamos un subconjunto marcado superior a S, agregando a S el elemento $\varphi(A \setminus S)$ y considerando este elemento el siguiente tras todos los elementos de S. El teorema queda demostrado.

Del teorema 4 se deduce inmediatamente el

Teorema 5 (Zermelo). En todo conjunto no vacío puede definirse un orden que lo convierte en un conjunto bien ordenado.

Más aún, del teorema 5 proviene el axioma de elección. En efecto, si A es cierto conjunto no vacío, entonces, conforme al teorema 5, puede considerarse bien ordenado. Si B es un subconjunto no vacío del conjunto A, entonces, al designar con $\varphi(B)$ el elemento minimal del conjunto B, nos convencemos de que $\varphi(B)$ satisface al axioma de elección. De este modo, se ha demostrado la equivalencia del teorema 4, del axioma de elección y del teorema de Zermelo.

Véanse [33, 90, 91] para familiarizarse más detalladamente con el axioma de elección y los teoremas equivalentes a él.

Veamos un sistema $\{A_\alpha \mid \alpha \in L\}$ de conjuntos parcialmente ordenados, suponiendo que el conjunto L es también parcialmente ordenado. Convengamos en considerar que los diferentes conjuntos del sistema a examinar no tienen puntos comunes. Esto, sin embargo, no impide que algunos de ellos sean diferentes ejemplares de un mismo conjunto. Denotemos con A una reunión teórico-multiplicativa de conjuntos de este sistema y con P, el producto directo de los conjuntos del sistema $\{A_\alpha \mid \alpha \in L\}$, es decir, el conjunto de funciones a que a todo conjunto A_α le hace corresponder un elemento $a_\alpha \in A_\alpha$. Las funciones a pueden concebirse como una fila (a_α), donde α recorre el conjunto L. La existencia de tales funciones se desprende de la aplicación del axioma de elección $a \bigcup_{\alpha \in L} A_\alpha$. Por consiguiente, el producto directo de cualquier sistema de conjuntos no vacíos es no vacío. Definamos sobre P una relación $\prec$, haciendo $a \prec b$, si de $a_\alpha \not\leqslant b_\alpha$, para cierto $\alpha \in L$ se deduce que existe tal $\beta \in L$ que $\beta < \alpha$, y $a_\beta < b_\beta$.

Teorema 6. Si un conjunto parcialmente ordenado L satisface la condición del mínimo, la relación $\preccurlyeq$ en P, definida por la condición

$$a \preccurlyeq b, \text{ si } a = b, \text{ o bien } a \prec b,$$

es un orden.

Demostración. La reflexividad de la relación $\preccurlyeq$ es obvia. Supongamos que $a \preccurlyeq b$ y $b \preccurlyeq a$, pero $a \neq b$. Entonces, existe tal índice $\alpha \in L$, que $a_\alpha \not\leqslant b_\alpha$, y $a_\beta < b_\beta$ para cierto $\beta < \alpha$. Pero, $b_\beta \not\leqslant a_\beta$ y $b \prec a$. Por consiguiente, se encontrará $\beta_1 < \alpha$ tal que $b_{\beta_1} < a_{\beta_1}$. De aquí, $a_{\beta_1} \not\leqslant b_{\beta_1}$, y $a \prec b$. Por eso, existe $\beta_2 < \beta_1$ tal que $a_{\beta_1} < b_{\beta_1}$. Continuando este proceso, obtendremos una sucesión decreciente infinita

$$\alpha > \beta > \beta_1 > \beta_2 > \ldots$$

de elementos de L, mas esto contradice la condición del mínimo de L (véase teorema 3). Esto quiere decir que $a = b$ y el carácter antisimétrico de la relación $\preccurlyeq$ está demostrado.

Comprobemos ahora la transitividad de nuestra relación. Supongamos que $a \preccurlyeq b$ y $b \preccurlyeq c$. Si $a = b$ ó $b = c$, la transitividad es obvia. En cambio, si $a \prec b$ y $b \prec c$, pero no que $a \prec c$, se encontrará tal índice $a \in L$ que $a_\alpha \not\leqslant c_\alpha$ y $a_\beta \not\leqslant c_\beta$ para todos los $\beta < \alpha$. De aquí se deduce que $a_\alpha \not\leqslant b_\alpha$, o bien $b_\alpha \not\leqslant$

c_α. Pongamos $\alpha_1 = \alpha$, y supongamos están elegidos los índices

$$\alpha_1 > \alpha_2 > \ldots > \alpha_n$$

de un modo tal que para cada α_i $(i = 1, 2, \ldots, n)$ tiene lugar $a_{\alpha_i} \not\leqslant b_{\alpha_i}$, o bien $b_{\alpha_i} \not\leqslant c_{\alpha_i}$. Si, por ejemplo, $a_{\alpha_n} \not\leqslant b_{\alpha_n}$, entonces para cierto $\beta < \alpha_n$ debe ser $a_\beta < b_\beta$. Si $b_\beta \leqslant c_\beta$, entonces $a_\beta < c_\beta$. Por cuanto $\beta < \alpha_n < \alpha$, esto contradice la elección de α. Por consiguiente, $b_\beta \not\leqslant c_\beta$, lo que nos permite poner $\alpha_{n+1} = \beta$. Así pues, se ha obtenido de nuevo una sucesión decreciente infinita de elementos de L: $\alpha_1 > \alpha_2 > \ldots > \alpha_n > \ldots$, lo que contradice la condición de mínimo de L. Por lo tanto, la transitividad de la relación $\prec$ está demostrada y la demostración del teorema queda terminada.

El producto directo P, dotado de un orden descrito en el teorema 6 lleva el nombre de *producto ordenado* de los conjuntos parcialmente ordenados A_α.

Determinemos también sobre el conjunto A la relación $\prec$, poniendo $a \prec b$, cuando y sólo cuando $a, b \in A_\alpha$, y $a \leqslant b$ en A_α, o bien $a \in A_\alpha$, $b \in A_\beta$ y $\alpha < \beta$ en L. Comprobemos que la relación $\prec$ es un orden en $A = \bigcup_{\alpha \in L} A_\alpha$. Efectivamente, es obvio que $\prec$ es una relación reflexiva. Si $a \prec b$ y $b \prec a$, es evidente que $a, b \in A_\alpha$ para cierto $\alpha \in L$, y, por lo tanto, $a = b$. Si $a \prec b$ y $b \prec c$, entonces $a \in A_\alpha$, $b \in A_\beta$, $c \in A_\gamma$, y la desigualdad $a \prec c$ se establece mediante un examen no complejo de los siguientes cuatro casos:

1) $\alpha = \beta$, $\beta = \gamma$; 2) $\alpha = \beta$, $\beta < \gamma$; 3) $\alpha < \beta$, $\beta < \gamma$; 4) $\alpha < \beta$, $\beta = \gamma$.

De modo que $(A, \prec)$ es realmente un conjunto parcialmente ordenado, el cual se llama *suma ordenada* de los conjuntos parcialmente ordenados A_α.

Si L es una anticadena, entonces la suma ordenada recibe el nombre de *suma cardinal* y el producto ordenado, de *producto directo*. En el caso de un producto directo es evidente que $a \prec b$, cuando y sólo cuando $a_\alpha \leqslant b_\alpha$ en A_α para todo $\alpha \in L$. Si L es una cadena, la suma ordenada de los conjuntos parcialmente ordenados se llama *suma ordinal*. Un producto ordenado, en el caso cuando L es un conjunto bien ordenado, se denomina *lexicográfico*.

Una suma ordenada A contiene naturalmente sus sumandos en calidad de subconjuntos. Esto nos permite decir que *A se descompone en una suma ordenada* de sus subconjuntos. Un conjunto parcialmente ordenado, que no puede ser representado en forma de una suma ordinal (cardinal, respectivamente) de sus propios subconjuntos, se denomina ordinalmente (cardinalmente) *indescomponible*.

Al contrario, los factores A_α de los productos ordenados P no admiten interpretación tan natural como sus subconjuntos. Verdad es que A_α se encajan en el producto ordenado P, mas son muchos tales encajes.

Una información más detallada sobre las sumas y los productos ordenados puede sacarse de [33]. Enunciemos aquí, en forma de ejercicios, una serie de sus propiedades.

Ejercicios. Demuéstrese que

6. Cada conjunto parcialmente ordenado es una suma cardinal (ordinal, respectivamente) de sus subconjuntos cardinalmente (ordinalmente) indescomponibles.

7. Cada conjunto parcialmente ordenado es una suma ordenada de conjuntos de un solo elemento.

8. Un conjunto parcialmente ordenado es una suma cardinal (ordinal, respectivamente) de conjuntos de un solo elemento, cuando y sólo cuando es una anticadena (cadena).

9. La adición ordinal es no conmutativa.

10. Una suma ordenada de los conjuntos bien ordenados $\{A_\alpha \mid \alpha \in L\}$ es bien ordenada, si, y sólo si, L es un conjunto bien ordenado.

11. Una suma ordenada de los conjuntos parcialmente ordenados $\{A_\alpha \mid \alpha \in L\}$ satisface la condición de mínimo si y sólo si esta condición la satisfacen L y todos los A_α.

12. Un producto ordenado de una familia finita de conjuntos parcialmente ordenados A_α satisface la condición del mínimo si y sólo si esta condición la satisfacen todos los A_α.

13. Un producto lexicográfico de las cadenas es una cadena.

14. Un producto lexicográfico de una familia finita de conjuntos bien ordenados es bien ordenado.

Al concluir este párrafo detengámonos en algunos resultados referentes a los conjuntos parcialmente ordenados, donde la atención principal se presta a las cadenas y anticadenas. Para tal análisis resulta típico el problema de búsqueda del número mínimo de cadenas, en el que puede partirse un conjunto finito parcialmente ordenado. La respuesta la da el siguiente teorema que se debe a Dilworth.

Teorema 7. Sea P un conjunto finito parcialmente ordenado. El número mínimo de cadenas disjuntas, que contienen todos los elementos de P, es igual a la anchura de P.

Demostración. Supongamos que $d(P)$ es el número mínimo de cadenas disjuntas que contienen todos los elementos del conjunto parcialmente ordenado P; $U(P)$ es la familia de todas las anticadenas en P, y $s(P)$, la anchura del conjunto parcialmente ordenado P, es decir, $s(P) = \max_{A \in U(P)} |A|$. En estas condiciones el teorema afirma que $d(P) = s(P)$. Demostrémoslo.

Es evidente que $d(P) \geqslant s(P)$, puesto que no existe ninguna cadena que contenga más de un elemento de la anticadena. La desigualdad inversa se demuestra por inducción según el número de elementos del conjunto parcialmente ordenado P, es decir, $|P|$. Si $|P| = 1$, la afirmación es cierta. Supongamos que es cierta para todos los conjuntos parcialmente ordenados Q tales que $|Q| < |P|$. Pongamos $s(P) = n$ y examinemos dos casos.

Caso 1. Sea una anticadena $A \in U(P)$, $|A| = n$, que no contiene ni la anticadena $A_{\min}$ de todos los elementos mínimos de P, ni tampoco la anticadena $A_{\max}$ de todos los elementos máximos de P. Definamos dos conjuntos:

$$P^+ = \{x \in P \mid \exists a \in A : x \geqslant a\};$$
$$P^- = \{x \in P \mid \exists a \in A : x \leqslant a\}.$$

De conformidad con las suposiciones referentes a la anticadena A tenemos:

$P^+ \cap P^- = A$, $P^+ \cup P^- = P$, $P^+ \neq P$, y $P^- \neq P$. Por consiguiente, $|P^-| < |P|$ y $|P^+| < |P|$. Entonces, con arreglo a la suposición de inducción, tenemos $d(P^-) \leqslant s(P^-) = n$, y $d(P^+) \leqslant s(P^+) = n$, es decir, cada uno de los dos conjuntos parcialmente ordenados P^- y P^+ puede ser representado en forma de una reunión de n cadenas disjuntas:

$$P^+ = \bigcup_{i=1}^{n} C_i^{(1)} \quad \text{y} \quad P^- = \bigcup_{i=1}^{n} C_i^{(2)}.$$

Cada elemento a de la anticadena A es, a la vez, un elemento mínimo en P^+ y máximo, en P^-. Pegando las cadenas $C_i^{(1)}$ y $C_i^{(2)}$, que contienen el elemento a, obtenemos una cadena C_a. Por cuanto todo elemento a de la anticadena A, siendo mínimo en P^+ y máximo en P^-, es maximal para una de las cadenas $C_i^{(1)}$ y minimal para una de las cadenas $C_i^{(2)}$, entonces, pegando las cadenas de recubrimiento de P^- y P^+ por los elementos comunes de la anticadena A, llegamos a que $P = P^- \cup P^+ = \bigcup_{a \in A} C_a$; $|A| = n$, es decir, existe un recubrimiento del conjunto parcialmente ordenado P mediante las n cadenas.

Caso 2. Cada anticadena de potencia n del conjunto parcialmente ordenado P contiene o bien todos sus elementos máximos o bien todos sus elementos mínimos. Por consiguiente, existen, como máximo, dos anticadenas de esta índole: una que contiene todos los elementos máximos, y la otra que contiene todos los elemento mínimos. Tomemos al azar un elemento $a \in A_{\text{mín}}$ y elijamos $b \in A_{\text{máx}}$ de un modo tal que $b \geqslant a$ (b puede ser igual a a). Sea $Q = P \setminus \{a, b\}$. Es evidente que $|Q| < |P|$. Por consiguiente, según la hipótesis de inducción, Q puede descomponerse en $s(Q)$ cadenas, mas $s(Q) = n - 1$, en virtud de la hipótesis. De aquí, al agregar a dichas cadenas una cadena $\{a, b\}$, obtendremos una descomposición de P en n cadenas. Por consecuencia, en este caso $d(P) \leqslant n = s(P)$. La demostración del teorema queda establecida.

Es lícita también la afirmación dual.

Teorema 8. Sea P un conjunto finito parcialmente ordenado. Entonces, el número mayor de elementos en la cadena de P es igual al número mínimo de anticadenas disjuntas que contienen todos los elementos del conjunto P.

Demostración. Sea $t(P)$ el número mínimo de anticadenas disjuntas que cubren todos los elementos del conjunto finito parcialmente ordenado P; $C(P)$ es una familia de todas las cadenas en P, y $m(P) = \max_{C \in C(P)} |C|$. Se necesita demostrar que $t(P) = m(P)$ para todo P.

Es obvio que $m(P) \leqslant t(P)$, puesto que ninguna anticadena contiene más de un elemento de la cadena. Por inducción respecto de $m = m(P)$ demostremos la desigualdad inversa. Cuando $m = 1$ ella, evidentemente, se verifica. Sea $t(Q) \leqslant m(Q)$ para todos los conjuntos parcialmente ordenados Q tales que $m = m(Q) < n$. Entonces, si $m(P) = n$, analicemos la anticadena A que incluye todos los elementos máximos de P. Está claro que

$A \neq \varnothing$, puesto que el elemento máximo de cada cadena máxima está contenido en A. Veamos un conjunto parcialmente ordenado $P \setminus A$. Es fácil mostrar que $m(P \setminus A) = n - 1$. En efecto, sea $x_1 < x_2 < \ldots < x_n$ una cadena de potencia n en $(P \setminus A)$. Puesto que $m(P) = n$, esta cadena es máxima y, por lo tanto, $x_n \in A$, lo que contradice la suposición: $x_n \in (P \setminus A)$. Entonces, en $(P \setminus A)$ no hay cadenas de n elementos, y, por hipótesis de inducción, llegamos a que $t(P \setminus A) \leqslant m(P \setminus A) = n - 1$. De aquí, $t(P) \leqslant m(P)$ y el teorema queda demostrado.

El teorema 7 fue enunciado por primera vez por Dilworth [92] en 1950 y demostrado con motivo del análisis de los retículos distributivos (véase § 8.2). Sin embargo, muy pronto se comprendió que este teorema tiene un campo de aplicación mucho más amplio. Más aún, el teorema resultó ser equivalente a varios teoremas de mini-máx del análisis combinatorio, por ejemplo, al teorema de P. Hall sobre el sistema de representantes distintos (§ 3.2), al de Ford y Fulkerson sobre el flujo máximo expresado en números enteros y el corte mínimo (§ 6.4), al de Menger sobre la separación de los vértices y a otros. Merced a las numerosas interpretaciones, los razonamientos aducidos más arriba ocupan en el análisis combinatorio uno de los lugares centrales.

Enunciemos ahora una serie de teoremas y, a continuación, interpretándolos de tal o cual modo, demostremos la equivalencia entre algunos de ellos.

Recordemos que se denomina grafo bipartido a un grafo $G = G(V, L)$, en el cual el conjunto de vértices $V = S \cup T$ se divide en dos conjuntos disjuntos S y T de un modo tal que cada arista (a, b) une cierto vértice $a \in S$ con el vértice $b \in T$. El grafo G es bipartido cuando y sólo cuando todos los ciclos simples de él tienen longitud par.

Cualquier relación binaria $R \subseteq S \times T$ sobre los conjuntos finitos S y T puede considerarse como un grafo orientado bipartido $G(S \cup T, R)$, en el que todas las aristas están orientadas de S a T, con la particularidad de que (a, b) es un arco en G, si y sólo si $a \in S$, $b \in T$, y $(a, b) \in R$, y viceversa. Por eso, en adelante no distinguiremos la relación binaria $R \subseteq S \times T$ y el grafo bipartido correspondiente $G(S \cup T, R)$, empleándolos como entes intercambiables. Cualquier familia $\{A_i \mid i \in T\}$ de subconjuntos del conjunto S engendra una relación binaria $R \subseteq S \times T$, a saber, $(a, i) \in R$ cuando y sólo cuando $a \in A_i$ y cualquier relación binaria puede, obviamente, considerarse en este sentido como un sistema de conjuntos.

Sea $G(S \cup T, R)$ un grafo bipartido. Se llama *combinación de pares* en el grafo G a un conjunto E de aristas, de las cuales no hay ningún par que tengan vértices comúnes. Denotemos con $S(E)$ y $T(E)$ los conjuntos de vértices de la combinación de pares E, situados en los conjuntos S y T, respectivamente. Un subconjunto $A \subseteq S$ se denomina *transversal parcial* en S, si existe tal combinación de pares E que $A = S(E)$. Del modo análogo se define también la transversal parcial para $B \subseteq T$.

Dicho de otro modo, el conjunto $A \subseteq S$ es una transversal parcial del grafo $G(S \cup T, R)$ cuando y sólo cuando existe un encaje φ: $A \to T$ tal que $(a, \varphi(a)) \in R$, cualquiera que sea $a \in A$.

El teorema de P. Hall sobre el sistema de representantes distintos (véase § 3.2) puede ahora enunciarse en términos de los grafos bipartidos.

Teorema 9. Sea $G(S \cup T, R)$ un grafo bipartido con conjuntos finitos de vértices S y T. Entonces, $A \subseteq S$ será una transversal parcial, si, y sólo si, $|B| \leqslant |R(B)|$ para todo $B \subseteq A$, donde

$$R(B) = \bigcup_{a \in B} \{y \in T \mid (a, y) \in R\}.$$

Efectivamente, sea $\{A_i \mid i \in T\}$ una familia finita de subconjuntos del conjunto S; aquí, los subconjuntos A_i no son forzosamente distintos. Definamos una relación binaria:

$$(i, a) \in R, \text{ siempre que } a \in A_i.$$

Entonces, $R(J) = \bigcup_{j \in T} A_j$ para todo $J \subseteq T$; ahora, del teorema 9 obtenemos el teorema de P. Hall del § 3.2:

Teorema 10 (P. Hall). Una familia de conjuntos $\{A_i \mid i \in T\}$ tiene transversal (o bien un sistema de representantes distintos) cuando y sólo cuando

$$\left| \bigcup_{j \in J} A_j \right| \geqslant J \text{ para todo } J \subseteq T.$$

Recordemos la formulación del teorema sobre el flujo máximo y el corte mínimo (véase teorema 4 del § 6.5).

Teorema 11 (Ford, Fulkerson). Para cualquier red con una capacidad de paso expresada en números enteros, el valor máximo de un flujo de la entrada s a la salida t es igual a la capacidad de paso mínima del corte que separa s de t.

En el § 6.4 se ha deducido, del teorema sobre el flujo máximo y corte mínimo, el teorema de Konig, a saber:

Teorema 12. Sea $G = G(S \cup T, R)$ un grafo bipartido arbitrario. Entonces, el número máximo de aristas de la combinación de pares en el grafo G es igual a la potencia mínima del conjunto (S, T)-separador de los vértices del grafo G.

Recordemos que el conjunto de vértices en un grafo arbitrario $G(V, E)$ recibe el nombre de conjunto *(S, T)-separador de vértices*, donde $S, T \subseteq V$ y $S \cap T = \varnothing$, si al eliminar estos vértices del grafo, junto con las aristas incidentes (o con los arcos) se rompen todas las cadenas (o caminos) que llevan de los vértices del conjunto S a los del conjunto T. Diremos que dos cadenas (o dos caminos) del vértice a al vértice b del grafo G no tienen vértices comunes, si ellas tienen de común sólo los vértices a y b. Llamemos conjunto (S, T)-separador de aristas (o de arcos) a tal familia de aristas (o de arcos) del grafo G, cuya eliminación de G rompe todas las cadenas (caminos) que llevan de los vértices del conjunto S a los del conjunto T.

Interpretemos ahora el teorema de Konig en términos de las matrices. Sea $A = \|a_{ij}\|$ una matriz rectangular arbitraria con elementos reales. Nos será de interés sólo una cuestión: ¿es igual o no a cero el elemento de la matriz? Llamemos líneas de la matriz tanto sus filas, como las columnas. El conjunto de elementos de la matriz distintos de cero se llamará *transversal* de la matriz, si ningún par de ellos yace en una línea. Diremos que el conjunto M de líneas cubre todos los elementos no nulos, si cada elemento no nulo de la matriz A yace por lo menos en una línea de M. A la matriz A se le hace corresponder un grafo bipartido, tomando como vértice el conjunto de filas y el de columnas de la matriz A y haciendo $(b_i, c_j) \in R$ cuando y sólo cuando $a_{ij} \neq 0$. Aquí, con b_i y c_j están designadas la i-ésima columna y j-ésima fila, respectivamente, de la matriz A. Entonces, del teorema 12 obtenemos el teorema de Konig del § 4.1.

Teorema 13. La potencia mayor de la transversal en una matriz es igual al número mínimo de líneas que cubren todos los elementos distintos de cero.

En el § 4.1 hemos demostrado la equivalencia de los teoremas 10 y 13. Así pues, los teoremas 9, 10, 12 y 13 son equivalentes. Demostremos que les son equivalentes también los teoremas 7, 8. Con este fin deduzcamos el teorema de Dilworth del teorema de Konig, y luego, viceversa. Mas, renunciemos con anterioridad el teorema de Dilworth en términos de los grafos.

Recordemos que el diagrama de Hasse de cualquier conjunto finito parcialmente ordenado representa un grafo orientado sin contornos. Sea G un grafo orientado sin contornos. La descomposición del grafo en cadenas es tal partición del conjunto de vértices y arcos del grafo G, que cada vértice de G pertenece a una y sólo una cadena. La descomposición con un número mínimo de cadenas se denomina mínima. Diremos que a es mayor que b, si se tiene una cadena orientada de a a b. Dos vértices de un grafo orientado sin contornos se llaman incomparables (o independientes), si no se verifican las desigualdades $a < b$ y $b < a$.

Ahora el teorema 7 puede enunciarse del modo siguiente:

Teorema 14. El número máximo de vértices recíprocamente incomparables en un grafo orientado sin contornos es igual al número de cadenas en la descomposición mínima del grafo.

Los teoremas 7 y 12 *son equivalentes.* Demostremos que del teorema de Konig se deduce el de Dilworth. Sea P un conjunto finito parcialmente ordenado. Construyamos un grafo bipartido $G(P \cup P', R)$ sobre el conjunto de vértices $P \cup P'$, donde P' es un ejemplar más del conjunto P. Además, los vértices x e y', donde y' es la copia de y en P', los unimos con una arista solamente en el caso, cuando $x < y$ en el conjunto parcialmente ordenado P.

Lema 2. Para toda combinación de pares M en el grafo $G(P \cup P', R)$ existe una descomposición D del conjunto parcialmente ordenado P en cadenas, para la cual $|M| + |D| = n$, donde $n = |P|$.

Demostración. Sea $M = \{(x_1, x_2'), (x_3, x_4'), \ldots, (x_{2k-1}, x_{2k}')\}$, entonces $x_1 < x_2$, $x_3 < x_4$, $\ldots$, $x_{2k-1} < x_{2k}$ en P, y sea que podemos agrupar diferentes elementos del conjunto $\{x_1, x_2, \ldots, x_{2k-1}, x_k\}$ en cadenas de un modo tal que cada una de éstas contenga dos o más elementos. Las cadenas construidas son disjuntas dos a dos, puesto que M es una combinación de pares en el grafo G. Agregando a ellas como cadenas de un solo elemento todos los elementos del conjunto P, que no figuran en las cadenas construidas, obtendremos la descomposición D del conjunto P en cadenas. Si el número de elementos del conjunto P que integran la i-ésima cadena de D es igual a l_i, entonces $n = |P| = \sum_{i=1}^{|D|} l_i = \sum_{i=1}^{|D|} (l_i - 1) + |D| = |M| + |D|$, puesto que $l_i - 1$ es igual al número de aristas de la combinación de pares M del grafo bipartido G que participan en la formación de la i-ésima cadena de D.

Lema 3. Sea X tal conjunto de vértices, que cubren todas las aristas del grafo G, que ya ninguno de sus subconjuntos cubre todas las aristas del grafo G. Entonces, existe en el conjunto parcialmente ordenado P una cadena A, tal que $|X| + |A| = n$, donde $n = |P|$.

Demostración. Sea $X = \{x_1, \ldots, x_i, y_1, \ldots, y_j\}$ un conjunto mínimo de vértices del grafo G que cubre todas las aristas. Entonces, $x_i \neq y_j$, cualesquiera que sean i y j. Demostremos esto por reducción al absurdo. Sea, por ejemplo, $x_i = y_1$. Puesto que X es el conjunto mínimo de vértices que cubre todas las aristas del grafo G, existen las aristas (x, y'), donde $x \notin X$, y (x_1, y'), donde $y' \notin X$. Mas, en virtud de la propiedad de transitividad para la relación del orden en P, y de la construcción del grafo bipartido G, llegamos a que (x, y') es una arista en el grafo G, lo que contradice la suposición de que X cubre todas las aristas del grafo G. Por consiguiente, todos los elementos en el conjunto $\{x_1, \ldots, x_i, y_1, \ldots, y_j\}$ son distintos. Por cuanto X cubre todas las aristas del grafo G, entonces $A = P \setminus X$ será una anticadena en P. Además, $|X| + |A| = |P| = n$. El lema queda demostrado.

Supongamos ahora que M es una combinacion de pares máxima en el grafo $G(P \cup P', R)$, y X es el recubrimiento de vértice mínimo de las aristas del grafo G. Entonces, en virtud del teorema 12, tenemos $|M| = |X|$. De aquí, considerando los lemas 2 y 3, $|D| = |A|$, puesto que $|D| = n - |M|$, y $|A| = n - |X|$. Pero, $|A| \leqslant |D|$ para cualesquiera A, $D \subseteq P$, puesto que ningún par de elementos incomparables pueden yacer en una misma cadena. Por consiguiente, $\max_A |A| = \min_D |D|$, es decir, la deducción del teorema 7 a partir del teorema 12 queda establecida.

Para demostrar la afirmación inversa de que el teorema 7 tiene por resultado el teorema 12, es suficiente al grafo bipartido $G(S \cup T, R)$ hacerle corresponder el conjunto parcialmente ordenado $S \cup T$ con la relación del orden parcial $<: x < y$ cuando y sólo cuando $(x, y) \in R$. La implicación re-

querida se desprende ahora de las siguientes dos afirmaciones que se comprueban con facilidad:

1) Para cualquier descomposición D del conjunto $S \cup T$ en cadenas existe una combinación de pares M en el grafo $G(S \cup T, R)$, para la cual $|D| + |M| = |S \cup T|$ (a título de M hace falta tomar un conjunto de todas las cadenas de D compuestas por dos elementos).

2) Para toda anticadena A de un conjunto parcialmente ordenado $S \cup T$ existe un recubrimiento de vértice X de las aristas del grafo G, para el cual $|A| + |X| \leqslant |S \cup T|$, puesto que el complemento a la anticadena A en el conjunto $S \cup T$ contiene el recubrimiento de vértice X de las aristas del grafo G. De este modo queda establecida la equivalencia de los teoremas 7 y 12.

Ejercicio 15. Sea $G(V, E)$ un grafo orientado tal que para s y $t \in V$ es válida la igualdad

$$k = |\Gamma(s)| - |\Gamma^{-1}(s)| = |\Gamma^{-1}(t)| - |\Gamma(t)|,$$

y para cualquier $v \in V - \{s, t\}$, la igualdad

$$|\Gamma(v)| = |\Gamma^{-1}(v)|.$$

Demuéstrese que en el grafo G hay k caminos del vértice s al vértice t que no se intersecan por arcos.

Sea $D(G)$ un grafo orientado obtenido del grafo no orientado G sustituyendo en éste cada arista por un par de arcos inversamente orientados que son incidentes respecto de los mismos vértices. Señálese que

16. Existe una correspondencia biunívoca entre las cadenas en el grafo G y los caminos en $D(G)$.

17. Para cualesquiera dos vértices s y t, el número mínimo de aristas, cuya supresión en el grafo G rompe todas las cadenas de s a t, es igual al número mínimo de arcos cuya eliminación rompe todos los caminos de s a t en el grafo $D(G)$.

Continuamos la deducción y la demostración de los resultados combinatorios equivalentes.

Lema 4. Sea $G(V, E)$ una red de entrada s y salida t, a cada arco de la cual se le asigna una capacidad específica de paso. En este caso son válidas las siguientes igualdades:

1) el valor del flujo máximo en la red G es igual al número máximo de caminos de s a t que no se intersecan por los arcos;

2) la capacidad de paso del corte mínimo en la red G es igual al número mínimo de arcos, cuya eliminación rompe todos los caminos de s a t.

Demostración. 1) Sea v cierto flujo máximo en la red G, y sea G^* un grafo orientado obtenido de G por eliminación de todos los arcos libres del flujo v. Por cuanto las capacidades de paso de todos los arcos de la red G son iguales a 1, entonces para todos los arcos e de la red G^* tenemos: $f(e) = 1$. De aquí, en virtud de la definición de flujo en una red (véase

§ 6.4), para todos los arcos e en la red G^*, distintos de s y t, tenemos: $|\Gamma(e)| = |\Gamma^{-1}(e)|$, mientras que para la entrada s y la salida t, $v = |\Gamma(s)| - |\Gamma^{-1}(s)| = |\Gamma^{-1}(t)| - |\Gamma(t)|$. Pero, en virtud de la afirmación citada en el ejercicio 15, en la red G^*, y, por lo tanto, en la red G existen v caminos de s a t que no se intersecan por los arcos. De aquí llegamos a que el valor v del flujo máximo en la red G no es superior a k (el número máximo de caminos de s a t que no se intersecan por los arcos).

Supongamos ahora que $P_1, P_2, \ldots, P_k$ es un juego de un número máximo de caminos de s a t en la red G que no se intersecan por los arcos. Definamos en G el flujo f del modo siguiente:

$$f(e) = \begin{cases} 1, \text{ si existe tal } i \text{ que } e \in P_i; \\ 0, \text{ en el caso contrario.} \end{cases}$$

Es evidente que el valor de tal flujo es igual a k, y el valor del flujo máximo no es inferior a k. Por consiguiente, $v \leqslant k$, y, debido a la desigualdad antecedente, $v \geqslant k$. De este modo, $v = k$, y la primera afirmación del lema queda demostrada.

2. Eliminemos en la red G todos los arcos del corte mínimo que separa la entrada s de la salida t. Entonces, en el grafo orientado obtenido no habrá ningún camino de s a t. Por eso, la potencia de este corte no es inferior al número mínimo de arcos cuya eliminación rompe todos los caminos de s a t. Para finalizar la demostración de la segunda afirmación del lema, demostremos que es cierta también la relación inversa. En efecto, sea T un conjunto de arcos cuya eliminación rompe todos los caminos de s a t en la red G, y sea S un conjunto de vértices que pueden ser alcanzados partiendo de la entrada s, con ayuda de los caminos que no contienen un arco del conjunto T. Está claro que $(S, V \setminus S)$ es un corte en la red G. Además, $(S, V \setminus S) \subseteq T$. Por eso, la potencia del corte mínimo no sobrepasa $|(S, V \setminus S)|$ y, por consiguiente, $|T|$. El lema está demostrado.

Enunciemos ahora una serie de *teoremas de Menger* y demostrémoslos tanto para los grafos orientados, como no orientados, haciendo uso del teorema 11 sobre el flujo máximo y el corte mínimo.

Teorema 15. Sean s y t dos vértices en un grafo orientado G. El número máximo de caminos de s a t, en G que no se intersecan por los arcos es igual a la potencia mínima del conjunto (s, t)-separador de arcos del grafo G.

Demostración. Vamos a considerar el grafo G como una red de entrada s y salida t, a todo arco del cual le está asignada la capacidad de paso unitaria. Entonces, el teorema en consideración es un corolario del lema 4 y del teorema 11.

Supongamos que para un grafo no orientado G existe el grafo orientado $D(G)$, obtenido de G sustituyendo cada arista de éste por un par de arcos inversamente orientados, que son incidentes respecto de los mismos vértices. Entonces, en virtud de los ejercicios 16 y 17, se deduce la validez del teorema 15 para el grafo no orientado.

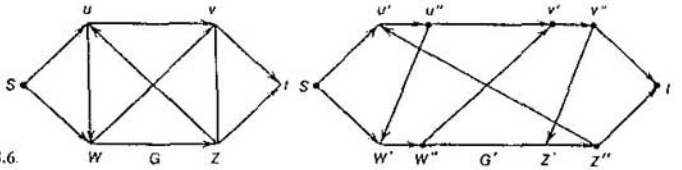

Fig.8.6.

Teorema 16. Sean s y t dos vértices de un grafo no orientado G. El número máximo de cadenas en G que van de s a t y no se intersecan por las aristas es igual a la potencia mínima del conjunto (s, t)-separador de aristas del grafo G.

Formulemos los análogos de los teoremas 15 y 16 para los vértices.

Teorema 17. Sean s y t dos vértices no adyacentes en un grafo orientado G. Entonces, la potencia mínima del conjunto (s, t)-separador de vértices en el grafo G es igual al número máximo de caminos que van de s a t y que no tienen vértices comunes.

Con el fin de demostrar el teorema 17 construyamos un grafo orientado G' a partir del grafo orientado $G(V, E)$ con dos vértices no adyacentes s y t. Dividamos para ello los vértices $v \subseteq V \setminus \{s, t\}$ en dos nuevos vértices v' y v'', uniéndolos con un arco (v', v''). Luego, sustituyamos cada arco del grafo G con el vértice terminal $v \in V \setminus \{s, t\}$ por un arco nuevo que tiene v' en calidad de vértice terminal; sustituyamos, además, cada arco con el vértice inicial $v \in V \setminus \{s, t\}$ por un arco que tiene v'' en calidad de vértice inicial. El grafo G y el G', construido a partir de G, se representan en la fig. 8.6.

Ejercicios. Demuéstrese que para los grafos construidos más arriba:

18. Todo camino de s a t en el grafo G' corresponde al camino de s a t en el grafo G que se obtiene por contracción de todos los arcos del tipo (v', v''), y viceversa, cada camino de s a t en el grafo G corresponde al camino de s a t en el grafo G' obtenido por división de todos los vértices del camino, distintos de s y t.

19. El número máximo de caminos que van de s a t en el grafo G' y que no se intersecan por las arcos es igual al número máximo de caminos de s a t que no tienen vértices comunes.

20. Dos caminos de s a t en el grafo G' no se intersecan por los arcos, cuando y sólo cuando los caminos que les corresponden en el grafo G no se intersecan por vértices.

21. La potencia mínima de un conjunto (s, t)-separador de arcos en el grafo G' es igual a la potencia mínima del conjunto (s, t)-separador de vértices del grafo G.

La validez del teorema 17 se deduce de las afirmaciones, fácilmente comprobables, enunciadas en los ejercicios 18 . . . 21.

Teorema 18. Sean s y t dos vértices no adyacentes de un grafo no orien-

tado G. Entonces, la potencia mínima del conjunto (s, t)-separador de vértices en el grafo G es igual al número máximo de cadenas que van de s a t y que no tienen vértices comunes.

Demostración. Es suficiente aplicar el teorema 17 al grafo $D(G)$.

Los teoremas 17 y 18 se generalizan fácilmente.

Teorema 19. Sea $G(V, E)$ un grafo orientado y supongamos que S, $T \subseteq V$. Entonces, la potencia mínima del conjunto (S, T)-separador de vértices es igual al número máximo de caminos que van de los vértices del conjunto S a los del conjunto T y que no tienen vértices comúnes.

Demostración. Agreguemos al grafo G dos vértices nuevos s^* y t^*, como también todos los arcos del tipo (s^*, s), donde $s \in S$, y todos los arcos del tipo (t, t^*), donde $t \in T$. Del teorema 17, aplicado al nuevo grafo construido, se deduce el teorema 19.

Razonando análogamente, del teorema 18 obtenemos el siguiente resultado.

Teorema 20 (Menger). Sea $G(V, E)$ un grafo no orientado y S, $T \subseteq V$. Entonces, la potencia mínima del conjunto (S, T)-separador de vértices es igual al número máximo de cadenas que van de los vértices del conjunto S a los del conjunto T y que no tienen vértices comunes.

Es obvio que si en los teoremas 19 y 20 suponemos que $S = \{s\}$, $T = \{t\}$, es decir, que S y T son conjuntos de un solo elemento, obtendremos las afirmaciones de los teoremas 17 y 18.

Deduzcamos ahora el *teorema* 11 *sobre el flujo máximo expresado en números enteros* y *el corte mínimo, basándonos en los teoremas de tipo de Menger.* Sea $G(V, E)$ una red de entrada s y salida t, en cuyos arcos vienen dadas las capacidades de paso que se expresan en números enteros. Construyamos una red nueva G' sobre el mismo conjunto de vértices, sustituyendo cada arco $e \in E$ con una capacidad de paso $c(e)$ por $c(e)$ de los arcos igualmente orientados y borrando todos los arcos con capacidades de paso nulas. La red G y la red nueva G', construida a partir de G, están representadas en la fig. 8.7, donde los números en los arcos del grafo G expresan sus capacidades de paso.

Sean R y R' los cortes que separan la entrada s de la salida t en las redes G y G', respectivamente, y que están definidas por un mismo conjunto de vértices. Entonces

$$|R'| = \sum_{e \in R} c(e),$$

donde c son las capacidades de paso de los arcos de la red G. Así pues, al poner $N = \min_{R} \sum_{e \in R} c(e)$, llegamos a que $|R'| \geqslant N$. Entonces, en virtud del teorema 15, existen N (y este número es máximo) caminos de s a t en la red G' que no se intersecan por los arcos.

Sea $f(e)$ el número de arcos paralelos al arco e en la red G', ocupados por dichos caminos. En este caso $f(e)$ es el flujo de s a t de magnitud N

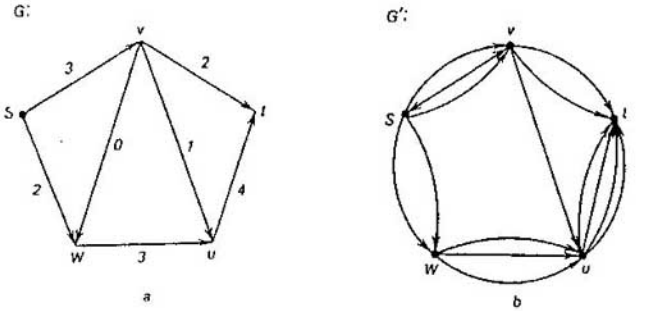

Fig.8.7. a b

en la red $G(V, E)$ (aquí se han empleado también los resultados del lema 4). La implicación requerida está demostrada.

Demostremos que *del teorema* 20 (*de Menger*) *se deduce la validez del teorema* 12 (*de Konig*). Sea $G(S \cup T, R)$ un grafo bipartido sobre el conjunto de vértices $S \cup T$, $S \cap T = \varnothing$. Obviamente, el conjunto de vértices A cubre todas las aristas del grafo G, cuando y sólo cuando A es un conjunto (S, T)-separador de vértices del grafo G. Para toda combinación de pares de n aristas en el grafo G pueden elegirse n cadenas que van de los vértices del conjunto S a los del conjunto T, y viceversa, k cadenas de S a T, que no tienen vértices comúnes y contienen k aristas del grafo G que no se intersecan por las vértices. Por consiguiente, el número máximo de cadenas de S a T, que no tienen vértices comúnes, es igual al número máximo de aristas de la combinación de pares en el grafo G. Pero, en virtud del teorema 20, el número máximo de cadenas que van de los vértices del conjunto S a los del conjunto T y que no tienen vértices comúnes, es igual a la potencia mínima del conjunto (S, T)-separador de vértices. Por consiguiente, el teorema 12 queda demostrado.

Todas las implicaciones establecidas en el libro, entre los teoremas de Menger, Konig, P. Hall, Dilworth y el de Ford-Fulkerson sobre el flujo máximo expresado en números enteros y el corte mínimo están reunidas en el grafo orientado (véase fig. 8.8), en el cual los vértices corresponden a los teoremas, y el arco (A, B) está presente en el grafo cuando y sólo cuando queda demostrado que el teorema B se deduce del teorema A. Según podemos ver en el grafo que se muestra en la fig. 8.8, para finalizar la demostración de la equivalencia entre los teoremas citados es sifuciente, por ejemplo, deducir uno de los teoremas de Menger a partir del teorema de Konig.

Deduzcamos el teorema 18 (*de Menger*) *del teorema 12* (*de Konig*), recurriendo al método de inducción matemática. La idea de tal demostración surge de las obras [134, 135]. Con ello acabemos la comprobación de la equivalencia entre los teoremas de Ford-Fulkerson, Menger, König, P. Hall y Dilworth y también ilustramos con un ejemplo concreto la idea de la de-

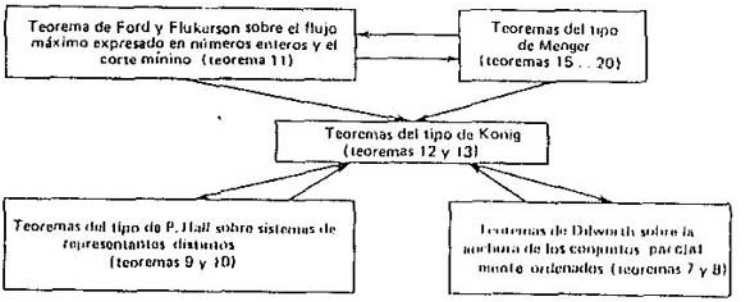

Fig.8.8.

mostración de los teoremas de Menger por el método de inducción matemática.

Lema 5. Supongamos que $G(V, E)$ es un grafo no orientado arbitrario, en el que se distinguen dos vértices no adyacentes s, $t \in V$, y que $X \subseteq V$ es un conjunto mínimo (s, t)-separador de vértices del grafo G, tal que $|X| = k$. Entonces, en $G(V, E)$ existen k cadenas de s a t que no se intersecan por los vértices.

Demostración. Un vértice del grafo G, distinto de s y t, y no adyacente a ninguno de ellos, recibe el nombre de vértice interior del grafo G. Demostremos el lema por inducción respecto de n (el número de vértices interiores del grafo G). Sea $n = 0$, es decir, en G no hay vértices interiores. Entonces, el grafo G tiene la forma mostrada en la fig. 8.9. Sean $x_1, x_2, \ldots, x_p$ los vértices del grafo G que son adyacentes tanto a s, como a t, simultáneamente. Es evidente que $x_1, x_2, \ldots, x_p \subseteq X$. Por eso, cuando $p = k$, el sistema buscado de k cadenas que no se intersecan por los vértices se halla en seguida. Si $p < k$, construyamos un subgrafo G', del grafo G, suprimiendo todos los vértices $x_1, x_2, \ldots, x_p$ junto con las aristas incidentes. Ahora, para demostrar el lema, basta con encontrar en el subgrafo G', $k - p$ cadenas de s a t, que no se intersecan por vértices.

Así pues, sea $p < k$, y sean A y $T \subseteq V \setminus \{x_1, x_2, \ldots, x_p\}$ los conjuntos de vértices del subgrafo G', adyacentes a los vértices s y t, respectivamente. Examinemos un grafo bipartido auxiliar $G^*(S \cup T, R)$ sobre el conjunto de vértices $S \cup T$, $S \cap T = \varnothing$, en el cual $(x, y) \in R$ cuando y sólo cuando $x \in S$, $y \in T$, y $(x, y) \in E$ (fig. 8.10).

En el grafo G^* $(S \cup T, R)$ se encontrará una combinación de pares con $k - p$ aristas. Demostrémoslo por reducción al absurdo. Supongamos que en el grafo G^* $(S \cup T, R)$ no hay combinaciones de pares con $k - p$ aristas, es decir, la potencia máxima de las combinaciones de pares del grafo G^* es inferior a $k - p$. Entonces, en virtud del teorema 12 (de Konig), en $G^*(S \cup T, R)$ existe un conjunto (S, T)-separador $X_0 \subseteq S \cup T$, cuyo número de vértices

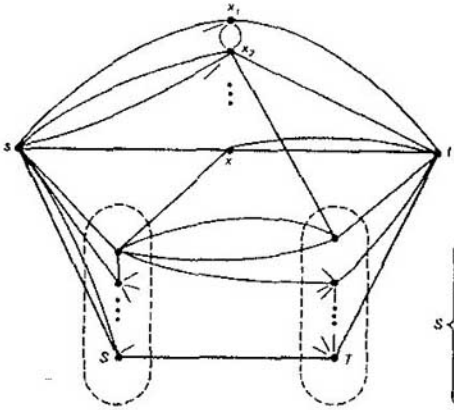

Fig.8.9.

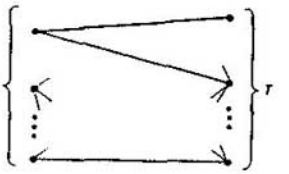

Fig.8.10.

es menos de $k - p$. Pero $X_0 \cup \{x_1, \ldots, x_p\}$ será, evidentemente, un conjunto (s, t)-separador de vértices en el grafo G con un número de vértices inferior a k. Hemos llegado, pues, a una contradicción con la hipótesis del lema. De este modo, en $G^*(S \cup T, R)$ existe una combinación de pares con $k - p$ aristas, y en el grafo G, k cadenas de s a t que no se intersecan por los vértices. El lema está demostrado para todos los grafos sin vértices interiores.

Admitamos que el lema está demostrado para todos los grafos con un número de vértices interiores inferior a $n_0 > 0$. Veamos un grafo arbitrario $G(V, E)$ con un número de vértices interiores igual a n_0 y un conjunto mínimo (s, t)-separador de los vértices X, donde $|X| = k$. Sea x_1 uno de los vértices interiores de este grafo. En el grafo G', obtenido de G por eliminación del vértice x_1 junto con las aristas incidentes, las condiciones del lema se cumplen como antes. Pero, en el grafo G' el número de vértices interiores ya es inferior a n_0, y, por lo tanto, en virtud de la hipótesis de inducción, se encontrarán k cadenas de s a t, que no se intersecan por los vértices, en G', y por consiguiente, en el grafo G. El incumplimiento de las condiciones del lema significa que $x_1 \in X$. Supongamos que G_0 es un subgrafo del grafo G engendrado por el conjunto de vértices $V \setminus X$; V_s es el conjunto de vértices del subgrafo G_0 unidos con el vértice s en G_0, y $V_t = (V \setminus X) \setminus V_s$. Sean G_s y G_t los subgrafos del grafo G engendrados por los conjuntos de vértices $V_s \cup X$ y $V_t \cup X$, respectivamente. Sobre el conjunto de vértices $V_1 = V_s \cup X \cup \{t'\}$ construyamos un grafo G_1, a partir del grafo G_s, adicionando un nuevo vértice t' y todas las aristas del tipo (x, t'), donde $x \in X$. Además, sobre el conjunto de vértices $V_2 = V_t \cup X \cup \{s'\}$ construyamos el grafo G_2, a partir del grafo G_t, juntando un nuevo vértice s' y agregando todas las aristas del tipo (s', x), donde $x \in X$. Los grafos G y G_1, G_2, cons-

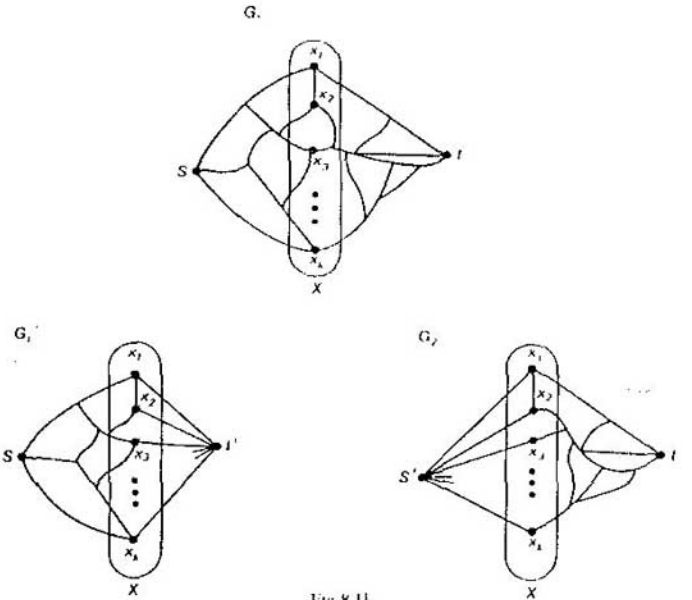

Fig. 8.11.

truidos a partir de G, se exponen en la fig. 8.11. Por construcción, en el grafo G_1 se tiene un conjunto mínimo (s, t')-separador de k vértices, y en el grafo G_2, un conjunto mínimo (s', t)-separador de k vértices, puesto que es precisamente tal, por ejemplo, el propio conjunto X.

En el grafo G_1 los vértices s y t' no son adyacentes, puesto que $s \notin X$. Además, cada vértice interior de G_1 es también interior en G, pero, al mismo tiempo x_1, siendo vértice interior en G, no lo es en G_1. Por eso el número de vértices interiores del grafo G_1 es inferior a n_0. Mas en este caso, por la hipótesis de inducción, se encontrarán k cadenas de s a t' en el grafo G_1, las cuales no se intersecan por los vértices. De un modo análogo mostramos que se encontrarán k cadenas de s' a t en el grafo G_2, las cuales no se intersecan por los vértices. De la construcción de los grafos G_1 y G_2 obtenemos automáticamente k cadenas de s a t en el grafo G, las cuales no se intersecan por los vértices. De este modo, el lema queda demostrado.

Si en el grafo G con dos vértices no adyacentes s y t se tiene un sistema de k cadenas de s a t que no se intersecan por los vértices, entonces el conjunto (s, t)-separador de vértices ha de contener por lo menos un vértice de cada cadena, o bien, dicho de otro modo, la potencia de cada conjunto (s, t)-separador de vértices del grafo G no debe ser inferior a k. De aquí y del

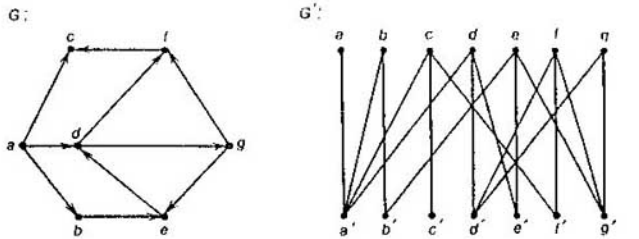

Fig.8.12.

lema 5 obtenemos directamente el teorema 18. Así pues, la implicación está demostrada y, por consiguiente, queda establecida la equivalencia de los teoremas de Ford-Fulkerston, Konig, P. Hall, Menger y Dilworth.

Es de interés el problema de buscar (las demostraciones de) todas las implicaciones entre los teoremas recién citados del análisis combinatorio. Proponemos que el mismo lector halle las implicaciones que faltan. En otras palabras, proponemos que el lector termine de construir el grafo mostrado en la fig. 8.8, hasta que se obtenga un grafo orientado completo sin lazos. Una parte de las implicaciones que faltan o las demostraciones nuevas de las implicaciones ya establecidas pueden encontrarse en las obras [1, (cap. 8, § 1), 8, 25 (caps 7 y 12), 28, 114 (cap. 5), 120, 122, 123 (§ 15.7), 124 (cap. IV, § 4) y 133, 135]. Así, por ejemplo, en [122] Harary obtuvo, partiendo del teorema original de Menger [119] (véase el teorema 18), diferentes teoremas de tipo de Menger, incluidos teoremas sobre el flujo máximo expresado en números enteros y el corte mínimo, de Konig, P. Hall, Dilworth y otros. En [120] se da un resumen de los teoremas de tipo de P.Hall sobre el sistema de representantes distintos (véase el teorema 10). Ford y Fulkerson [28] obtuvieron, basándose en su teorema sobre el flujo máximo de números enteros y el corte mínimo, los teoremas de Konig, Menger, Dilworth y P. Hall (véanse las teoremas 4.1, 4.2, cap. II, § 8 y teorema 10.1 [28]). En [121] el teorema sobre el flujo máximo y el corte mínimo se deduce del teorema de Menger, y en [25] se exponen detalladamente las correlaciones entre los teoremas de Menger y de Konig sobre las combinaciones de pares para los grafos bipartidos.

Sea $G(V, E)$ un grafo orientado finito y supongamos que S, $T \subseteq V$ son tales que $|S| = |T| = k$. Construyamos un grafo bipartido $G'(V \cup V', E')$ sobre un conjunto de vértices $V \cup V'$, donde V' es un ejemplar más del conjunto V. Con $v' \in V'$ denotemos el vértice que corresponde al vértice $v \in V$, y con $T' \subseteq V'$, el conjunto correspondiente a $T \subseteq V$. El conjunto de aristas E' en el grafo bipartido G' se define mediante la relación

$$E' = \{(v, v') \mid v \in V\} \cup \{(v, u') \mid (u, v) \in E\}.$$

El grafo G y el G', construido a partir de G, están representados en la fig. 8.12.

Lema 6. Sea $G(V, E)$ un grafo orientado finito y S, $T \subseteq V$, tales que $|S| = |T| = k$. En el grafo G hay k caminos de S a T, que no se intersecan por los vértices, cuando y sólo cuando existe en el grafo G' una combinación de pares $M = \{(y_1, x_1'), \ldots, (y_n, x_n')\}$ tal que $\{x_1, x_2, \ldots, x_n\} = V \setminus T$, $\{y_1, y_2, \ldots, y_n\} = V \setminus S$.

Demostración. Sea $P_1, P_2, \ldots, P_k$ una familia de caminos de S a T que no se intersecan por los vértices, donde $|S| = |T| = k$. Definamos φ: $V' \setminus T' \to V \setminus S$, haciendo

$$\varphi(u') = \begin{cases} u, \text{ si } u \notin P_i \text{ para todo } i,\ i = 1, \ldots, k; \\ v, \text{ si } u \in P_i, \text{ y } v \text{ sigue tras } u \text{ en } P_i. \end{cases}$$

Es evidente que φ es una aplicación biunívoca y que para todo $u' \in V' \setminus T'$ tenemos $(\varphi(u'), u') \in E'$. De este modo, $M = \{(\varphi(u'), u') \mid u' \in V' \setminus T'\}$ es una combinación de pares y $\{\varphi(u') \mid u' \in V' \setminus T'\} = V \setminus S$.

Demostremos la afirmación inversa. Sea $M = \{(y_1, x_1'), \ldots, (y_n, x_n')\}$ una combinación de pares en el grafo G', donde $\{y_1, \ldots, y_n\} = V \setminus S$, y $\{x_1, \ldots, x_n\} = V \setminus T$. La aplicación isomorfa φ: $V' \setminus T' \to V \setminus S$ se define de una manera evidente, a saber: $y_i = \varphi(x_i')$ para cualquier $x_i \in V \setminus T$. Definamos, para cada $s \in S$, el camino P_s en el grafo G que va del vértice s a uno de los vértices del conjunto T. Si $s \in S \cap T$, entonces $P_s = \{a\}$. Si $s \notin ST$, entonces $s \notin T$. Por eso siempre existe un vértice $s' \in V' \setminus T'$ tal que $\varphi(s') = u_1 \in V \setminus S$. Si $u_1 \in T$, suponemos que $P_s = \{s, u_1\}$. Si $u_1 \notin T$, entonces, por ser φ inyectiva, se encontrará un vértice $u_2 = \varphi(u_1') \in V \setminus S$, tal que $u_2 \neq u_1$. Si $u_2 \in T$, suponemos $P_s = \{s, u_1, u_2\}$. Si $u_2 \notin T$, entonces, por ser φ inyectiva, se encontrará un vértice $u_3 = \varphi(u_2') = V \setminus S$, tal que $u_3 \neq u_2$. Continuamos este proceso hasta que se encuentre por primera vez el vértice $u_j \in T$, y entonces suponemos $P_s = \{s, u_1, u_2, \ldots, u_j\}$. Por ser la aplicación φ inyectiva, deducimos que los caminos P_s, construidos para diferentes $s \in S$, no se intersecan por los vértices. De este modo queda demostrado el lema.

Para el grafo G (expuesto en la fig. 8.12) con $S = \{a, f, g\}$ y $T = \{c, d, f\}$ se tienen tres itinerarios que no se intersecan por los vértices: $P_a = \{a, c\}$, $P_f = \{f\}$, $P_g = \{g, e, d\}$ que van de los vértices de conjunto S a los del conjunto T, y a estos caminos les corresponde, según el lema 6, una combinación de pares $M = \{(b, b'), (c, a'), (d, e'), (e, g')\}$, tal que $\{b, c, d, e\} = V \setminus S$, y $\{b', a', e', g'\} = V' \setminus T'$.

El lema 6 se emplea para generalizar los matroides transversales con los grafos bipartidos $G(S \cup T, R)$ (véase § 8.4, como también el concepto de ganimoide en [1]).

Ejercicios 22. Dedúzcanse los teoremas 17 y 19 a partir del lema 6 y del teorema 12.

23. Demuéstrese el teorema 17 por el método de inducción matemática según el número de vértices interiores del grafo.

8.2. RETÍCULOS

Sea $(A, \leqslant)$ un conjunto arbitrario parcialmente ordenado, y sea B un subconjunto no vacío del conjunto citado. El elemento $a \in A$ se denomina *cota superior exacta* (*supremo*) del conjunto B, siempre que $a \geqslant b$ para todo $b \in B$, y si de la validez de la relación $v \geqslant b$ para todo $b \in B$ se deduce que $v \geqslant a$. De un modo dual se define la *cota inferior exacta* (*ínfimo*) del conjunto B: el elemento $a \in A$ se llama cota inferior exacta, si $a \leqslant b$ para todo $b \in B$, y si de la condición $u \leqslant b$ para todo $c \in B$ se deduce que $u \leqslant a$. Las cotas exactas superior e inferior del conjunto B en el conjunto parcialmente ordenado $(A, \leqslant)$ las designaremos con los símbolos $\sup_A B$ y $\inf_A B$, respectivamente. A veces, sin embargo, el índice A se omitirá. Directamente de las definiciones se desprende la validez de las siguientes afirmaciones:

a) Si $a \leqslant b$, entonces $\sup\{a, b\} = b$, e $\inf\{a, b\} = a$.

b) Sea $B \subseteq C$. Si existen $\sup B$ y $\sup C$ ($\inf B$ e $\inf C$, respectivamente), entonces $\sup B \leqslant \sup C$ ($\inf B \geqslant \inf C$, respectivamente).

c) Si $A \subseteq \mathscr{P}(S)$, entonces $\sup A$ coincide con la unión de todos los subconjuntos de la familia A, e $\inf A$, con su intersección.

Se propone que el lector mismo compruebe la validez de estas afirmaciones.

Un conjunto parcialmente ordenado $(A, \leqslant)$ se denomina *retículo* (o *estructura*), si para cualesquiera $a, b \in A$ existen $\sup\{a, b\}$ e $\inf\{a, b\}$. El retículo no tiene que tener obligatoriamente 0 y 1. Son retículo toda cadena, un conjunto de todos los conjuntos ordenado por inclusión (véase el ejemplo 4 del § 8.1) y algunos otros conjuntos parcialmente ordenados cuyos ejemplos se darán a conocer más abajo.

Si un conjunto parcialmente ordenado $(A, \leqslant)$ es un retículo, entonces el conjunto parcialmente ordenado $(A, \geqslant)$, dual respecto del primero, es también un retículo. Así pues, el principio de dualidad es aplicable para los retículos.

Emplearemos las siguientes designaciones:

$$a \wedge b = \inf\{a, b\}, \quad a \vee b = \sup\{a, b\}$$

denominando $\wedge$ *intersección* y $\vee$, *unión*. Los símbolos $\wedge$ y $\vee$ en los retículos representan operaciones binarias que poseen las siguientes propiedades:

a) $a \wedge a = a$, $a \vee a = a$ (idempotencia);

b) $a \wedge b = b \wedge a$, $a \vee b = b \vee a$ (conmutatividad);

c) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$ (asociatividad);

d) $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$ (absorción).

La relación de orden $\leqslant$ en los retículos puede ser caracterizada con ayuda de las operaciones $\wedge$ y $\vee$. A saber,

$$a \leqslant b \Leftrightarrow a \wedge b = a,$$

o bien

$$a \leqslant b \Leftrightarrow a \vee b = b.$$

Tales caracteristicas permiten considerar los retículos como conjuntos con dos operaciones binarias $\wedge$ y $\vee$, las cuales satisfacen las propiedades de idempotencia, conmutatividad, asociatividad y absorción.

Observemos que el requisito de idempotencia no es obligatorio, puesto que la idempotencia de las operaciones es un corolario de ambas propiedades de absorción. En efecto, usando sucesivamente diferentes propiedades de absorción, llegamos a que $a \vee a = a \vee (a \wedge (a \vee a)) = a$, y $a \wedge a = a \wedge (a \vee (a \wedge a)) = a$.

Teorema 21. Sea A un conjunto con dos operaciones binarias $\wedge$ y $\vee$, las cuales son idempotentes, conmutativas, asociativas y satisfacen las propiedades de absorción. Supongamos que $a \leqslant b$ significa que $a \vee b = b$. Entonces, la relación $\leqslant$ es relación de orden en el conjunto A, y un conjunto parcialmente ordenado que surge resulta ser un retículo, con la particularidad de que

$$a \vee b = \sup\{a, b\}$$
$$a \wedge b = \inf\{a, b\}.$$

Demostración. La reflexividad de la relación $\leqslant$ se desprende de la idempotencia de la unión. Si $a \leqslant b$, y $b \leqslant a$, es decir, $a \vee b = b$, y $b \vee a = a$, entonces, en virtud de la conmutatividad, $a = b$, es decir, la relación $\leqslant$ resulta antisimétrica. Si $a \vee b = b$, y $b \vee c = c$, entonces, en virtud de la asociatividad, tenemos

$$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c,$$

lo que demuestra la transitividad de la relación $\leqslant$. Por consiguiente, la relación $\leqslant$ es una relación de orden parcial en el conjunto A. Luego, $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$ (aquí se han empleado sucesivamente las propiedades de asociatividad e idempotencia) y

$$b \vee (a \vee b) = b \vee (b \vee a) = (b \vee b) \vee a = b \vee a = a \vee b$$

(se han aprovechado sucesivamente las propiedades de conmutatividad, asociatividad, idempotencia y, de nuevo, la propiedad de conmutatividad). De aquí, $a \leqslant a \vee b$ y $b \leqslant a \vee b$. Si $a \leqslant v$ y $b \leqslant v$, entonces, haciendo uso de la idempotencia, conmutatividad y asociatividad de la operación de unión, tenemos: $(a \vee b) \vee v = a \vee (b \vee v) = a \vee v = v$, es decir, $a \vee b \leqslant v$. Recordando la definición de la cota superior exacta, nos convencemos de que $a \vee b = \sup\{a, b\}$. Por fin, de las propiedades de conmutatividad y absorción tenemos

$$(a \wedge b) \vee a = a \vee (a \wedge b) = a$$

y

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

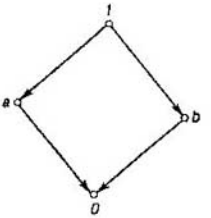

Fig.8.13.

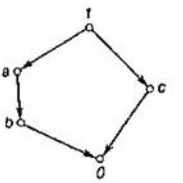

Fig.8.14.

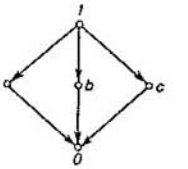

Fig.8.15.

es decir, $a \wedge b \leqslant a$, y $a \wedge b \leqslant b$. Si $u \leqslant a$ y $u \leqslant b$, entonces, en virtud de las propiedades de asociatividad y absorcion y por definicion de la relación $\leqslant$, obtenemos

$$u \wedge (a \wedge b) = (u \wedge a) \wedge b = (u \wedge (u \vee a)) \wedge b = u \wedge b = u \wedge (u \vee b) = u.$$

De aquí, en virtud de las propiedades de conmutatividad y absorción, se deduce que

$$u \vee (a \wedge b) = (u \wedge (a \wedge b)) \vee (a \wedge b) = (a \wedge b) \vee ((a \wedge b) \wedge u) = (a \wedge b),$$

es decir, $a \wedge b \geqslant u$. De este modo, $a \wedge b = \inf\{a, b\}$ y el teorema queda demostrado.

Observemos que los razonamientos duales permiten llegar a las mismas deducciones que se obtienen al definir la relación $\leqslant$ por la condición $a \leqslant b$, si $a \wedge b = a$.

Así pues, cualquier retículo finito siempre puede ser descrito con ayuda de una tabla de intersecciones/uniones o del diagrama de Hasse. Por ejemplo, sea $A = \{0, a, b, 1\}$ cuyo diagrama de Hasse viene expuesto en la fig. 8.13. Entonces, el retículo A se define completamente mediante la siguiente tabla de intersecciones/uniones:

Tabla 8.2

$\vee$ \ $\wedge$	0	a	b	1
0	0	0	0	0
a	a		0	a
b	b	1		b
1	1	1	1	

Los valores en la diagonal están omitidos en esta tabla, ya que $x \vee x = x$, y $x \wedge x = x$ para todos los $x \in A$. Además, en virtud de la conmutatividad de las operaciones $\wedge$ y $\vee$, esta tabla define por completo el retículo. Para convencerse de esto, basta comprobar sólo las identidades de asociatividad y absorción. El mismo lector puede hacerlo.

Al describir los retículos, emplearemos los métodos que combinan ambos métodos citados. Describamos, como ejemplo, dos retículos en un conjunto de cinco elementos 0, a, b, c, 1, cuyos diagramas de Hasse están ex-

puestos en las figs 8.14 y 8.15. El retículo expuesto en la fig. 8.14, con $b<a$, $c\vee b = 1$, y $a\wedge c = 0$, recibe el nombre de *pentágono*. La descripción aducida del pentágono es completa, pues todas las demás relaciones del pentágono se deducen de las aducidas. El retículo expuesto en la fig. 8.15, con $a\wedge b = a\wedge c = b\wedge c = 0$, y $a\vee b = a\vee c = b\vee c = 1$, se llama *diamante*. El subconjunto B del retículo A se denominará también pentágono o diamante, si es un subretículo que, al ser un conjunto parcialmente ordenado, es isomorfo al pentágono o diamante, respectivamente. De este modo, al afirmar que $B = \{b_1, b_2, b_3, b_4, b_5\}$ es un pentágono (diamante, respectivamente), suponemos que la aplicación φ: $b_1 \to 0$, $b_2 \to a$, $b_3 \to b$, $b_4 \to c$, $b_5 \to 1$ es un isomorfismo del retículo B sobre el retículo que se muestra en la fig. 8.14 (en 8.15, respectivamente).

Precisemos el concepto de isomorfismo de los retículos. Corrientemente, para los retículos se introducen dos conceptos equivalentes de isomorfismo.

1. Los retículos $(L_0, \leqslant)$ y $(L_1, \leqslant)$ se denominan isomorfos, si son isomorfos como conjuntos parcialmente ordenados. Ya hemos empleado esta definición de isomorfismo de los retículos.

2. Los retículos $(L_0; \wedge, \vee)$ y $(L_1; \wedge, \vee)$ se denominan isomorfos, si existe un isomorfismo φ del conjunto L_0 sobre el L_1, tal que para cualesquiera a, $b \in L_0$:

$$\varphi(a\wedge b) = \varphi(a)\wedge\varphi(b);$$
$$\varphi(a\vee b) = \varphi(a)\vee\varphi(b).$$

Pese a la equivalencia de estas definiciones, en lo que sigue adelante se distinguirán estos dos conceptos de isomorfismo de los retículos con el fin de evitar toda clase de confusión al generalizarlos.

Renunciaremos también a las designaciones $(L; \wedge, \vee)$ y $(L, \leqslant)$ para los retículos y conjuntos parcialmente ordenados y escribiremos simplemente letras mayúsculas, indicando los conjuntos principales, a excepción de los casos en que esto sea necesario para una mejor asimilación del texto.

El isomorfismo de los conjuntos parcialmente ordenados se generaliza del modo siguiente.

Una aplicación φ: $A_0 \to A_1$ se llama *isótona* (o bien conservadora del orden) de un conjunto parcialmente ordenado A_0 en otro conjunto parcialmente ordenado A_1, siempre que $a \leqslant b$ en A_0 lleva consigo $\varphi(a) \leqslant \varphi(b)$ en A_1. Un ejemplo de aplicación isótona φ: $L_0 \to L_1$ se aduce en la fig. 8.16, donde $\varphi(0) = 0$, $\varphi(a) = \varphi(b) = c$, $\varphi(1) = 1$.

Se llama *homomorfismo* del retículo $(L_0; \wedge, \vee)$ en el retículo $(L_1; \wedge, \vee)$ la aplicación φ: $L_0 \to L_1$ que satisface las condiciones

$$\varphi(a\vee b) = \varphi(a)\vee\varphi(b);$$
$$\varphi(a\wedge b) = \varphi(a)\wedge\varphi(b),$$

cualesquiera que sean, a, $b \in L_0$.

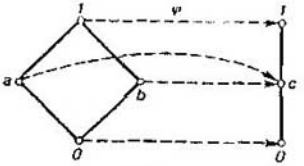

Fig.8.16.

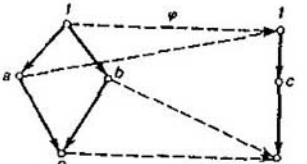

Fig.8.17.

En la fig. 8.17 se expone el ejemplo del homomorfismo φ: $L_0 \to L_1$.

Todo homomorfismo de los retículos es una aplicación isótona. En efecto, si φ: $L_0 \to L_1$ es un homomorfismo, entonces $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$ para cualesquiera $a, b \in L_0$. Sea $x, y \in L_0$, y $x \leqslant y$ en L_0. Entonces, $y = x \vee y$, y por consiguiente, $\varphi(y) = \varphi(x \vee y) = \varphi(x) \vee \varphi(y)$, es decir, $\varphi(x) \leqslant \varphi(y)$ en L_1. Así pues, el homomorfismo φ es también una aplicación isótona.

Lo recíproco no es cierto. Por ejemplo, la aplicación isótona φ: $L_0 \to L_1$ expuesta en la fig. 8.16 no es un isomorfismo, puesto que

$$\varphi(a \vee b) = \varphi(1) = 1 \neq c = c \vee c = \varphi(a) \vee \varphi(b)$$

Recordemos que llamamos producto directo $P \times Q$ de los conjuntos parcialmente ordenados P y Q al conjunto de todos los pares del tipo (x, y), donde $x \in P$, $y \in Q$, con la particularidad de que $(x_1, y_1) \leqslant (x_2, y_2)$ en $P \times Q$ cuando y sólo cuando $x_1 \leqslant x_2$ en P, $y_1 \leqslant y_2$ en Q (véase § 8.1).

Teorema 22. El producto directo $P \times Q$ de cualesquiera dos retículos P y Q es un retículo.

Demostración. Sean (x_1, y_1) y (x_2, y_2) elementos arbitrarios del conjunto parcialmente ordenado $P \times Q$. Por cuanto P y Q son retículos, para todo elemento $(x_1 \vee x_2, y_1 \vee y_2)$ del conjunto parcialmente ordenado $P \times Q$ tenemos: $(x_1 \vee x_2, y_1 \vee y_2) \geqslant (x_1, y_1)$ y $(x_1 \vee x_2, y_1 \vee y_2) \geqslant (x_2, y_2)$. Sea $(u, v) \geqslant (x_2, y_2)$, o bien, lo que es equivalente, $u \geqslant x_i$ en P, y $v \geqslant y_i$ en Q, siendo $i = 1, 2$. De aquí, en virtud de la definición de cota superior exacta, $u \geqslant x_1 \vee x_2$, y $v \geqslant y_1 \vee y_2$, así que $(u, v) \geqslant (x_1 \vee x_2, y_1 \vee y_2)$ en $P \times Q$. Esto demuestra que

$$(x_1 \vee x_2, y_1 \vee y_2) = (x_1, y_1) \vee (x_2, y_2).$$

De aquí se desprende que la unión situada en el segundo miembro existe.

Mediante los razonamientos duales llegamos a que

$$(x_1 \wedge x_2, y_1 \wedge y_2) = (x_1, y_1) \wedge (x_2, y_2),$$

por lo cual $P \times Q$ es un retículo y el teorema queda demostrado.

Un retículo que satisface la identidad

$$(a \wedge b) \vee (a \wedge c) = a \wedge (b \vee (a \wedge c))$$

o bien (lo que es equivalente) la condición siguiente: $a \geqslant b$, lleva consigo $(a \wedge c) \vee b = a \wedge (b \vee c)$ y se llama *modular*. Un ejemplo importante de retículos modulares es el de subespacios de un espacio lineal (véase el ejemplo 9

en el § 8.1). En efecto, si A, B, C son subespacios y si $A \supseteq B$, entonces, evidentemente, $(B + C) \cap A \supseteq B + (A \cap C)$. Viceversa, si el vector a se dispone en $(B + C) \cap A$, entonces $a = b + c$, donde $b \in B$ y $c \in C$. De aquí, $c(a - b) \in (C \cap A)$, es decir, $a \in (B + (A \cap C))$ y, por lo tanto, $(B + C) \cap A \subseteq B + (A \cap C)$. De un modo análogo se comprueba que también son modulares los retículos de los divisores normales de un grupo arbitrario, de los ideales de un anillo y de los submódulos del módulo. Un ejemplo típico de un retículo no modular es el diagrama que se expone en la fig. 8.14.

Demos a conocer ahora una representación intuitiva de un «retículo más general» que está engendrado por cierto conjunto de elementos y que satisface ciertas correlaciones. Los «retículos más generales» se denominarán en adelante *libres*. Estos retículos se construirán por formación sucesiva de elementos «nuevos» con ayuda de las operaciones de unión e intersección hasta que se obtenga un retículo. Además, los elementos «nuevos» se identificarán con los «antiguos», si y sólo si las igualdades entre ellos pueden deducirse o bien de las identidades del retículo, o bien de las correlaciones prefijadas. Ilustremos lo dicho con un ejemplo de construcción de un «retículo más general» que está engendrado por los elementos a, b, c y que satisface la relación $b < a$. Formemos, ante todo, las uniones e intersecciones $a \vee c$, $b \vee c$, $a \wedge c$, $b \wedge c$. Ha de notarse que $a \vee b \vee c = (a \vee b) \vee c = a \vee c$, puesto que $a \vee b = a$; análogamente, $a \wedge b \wedge c = b \wedge c$. Demostremos ahora que los siete elementos a, b, c, $a \vee c$, $b \vee c$, $a \wedge c$ y $b \wedge c$, de los que ya disponemos, son distintos dos a dos. Recordemos que dos de ellos serían iguales, si la igualdad entre ellos se deduciera de la relación $b < a$ y de los axiomas del retículo. Por eso, para mostrar que cualesquiera dos de los elementos citados son distintos, basta encontrar un retículo con los elementos a, b, c que satisfaga la relación $b < a$, en la que estos dos elementos son distintos. Por ejemplo, para mostrar que $a \neq a \vee c$, tomemos un retículo: $\{0, 1, 2\}$, donde $0 < 1 < 2$, y pongamos: $b = 0$, $a = 1$, $c = 2$, $b = 0 < 1 = a$. Entonces, $a = 1 \neq 2 = 1 \vee 2 = a \vee c$. El paso siguiente consiste en la formación, a base de estos elementos, de las nuevas uniones e intersecciones, tales como $b \vee (a \wedge c)$, $(b \vee c) \wedge a$. Es fácil notar que todas las demás uniones e intersecciones son iguales a uno de los elementos introducidos, por ejemplo, $b \wedge (a \wedge c) = b \wedge c$, $a \vee (a \wedge c) = a$. Demostremos ahora que los nueve elementos a, b, c, $a \vee c$, $b \vee c$, $a \wedge c$, $b \wedge c$, $b \vee (a \wedge c)$ y $a \wedge (b \vee c)$ forman un retículo. Con este fin hace falta demostrar que de estos nueve elementos ya no obtendremos elementos nuevos con ayuda de las operaciones de unión e intersección. Todas las $\binom{9}{2} = 36$ uniones y el mismo número de intersecciones, que han de ser comprobadas, se calculan de un modo trivial. Por ejemplo, $a \vee (b \vee (a \wedge c)) = (a \vee b) \vee (a \wedge c) = a$ en virtud de la propiedad de absorción, y puesto que $a \vee b = a$; análogamente, $c \wedge (a \wedge (b \vee c)) = (c \wedge a) \wedge (b \vee c) = a \wedge c$, puesto

que $c \wedge a \leqslant b \vee c$. El «retículo más general» obtenido se muestra en la fig. 8.18.

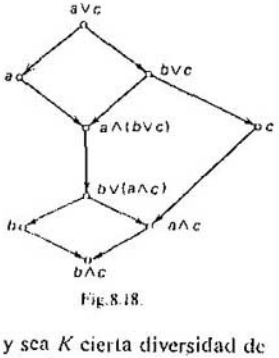

Fig. 8.18.

Se llama *diversidad* de retículos a una clase de todos los retículos, cada uno de los cuales satisface cierto juego de identidades prefijado. La clase de todos los retículos o la clase de todos los retículos modulares son ejemplos de la diversidad de retículos.

Demos ahora a conocer la definición estricta de «retículo más general» o de retículo libre respecto a cierta diversidad de retículos.

Sea A un conjunto parcialmente ordenado y sea K cierta diversidad de retículos. Un retículo $F_K(A)$ se denomina libre en la diversidad K, engendrada por el conjunto parcialmente ordenado A, si se cumplen las siguientes condiciones:

a) $F_K(A) \in K$;

b) $A \subseteq F_K(A)$ y para cualesquiera $a, b, c \in A$: $\inf_A \{a, b\} = c$ ($\sup_A \{a, b\} = c$) cuando y sólo cuando $a \wedge b = c$ en $F_K(A)$ ($a \vee b = c$ en $F_K(A)$, respectivamente);

c) A es el conjunto generador del retículo $F_K(A)$;

d) Sea $L \in K$ y $\varphi: A \to L$, una aplicación isótona tal que si $a, b, c \in A$ e $\inf_A \{a, b\} = c$ ($\sup_A \{a, b\} = c$, respectivamente), entonces $\varphi(a) \wedge \varphi(b) = \varphi(c)$ en L ($\varphi a) \vee \varphi(b) = \varphi(c)$ en L, respectivamente). Entonces la aplicación puede ser prolongada hasta que se obtenga un homomorfismo reticular Ψ: $F_K(A) \to L$, es decir, un isomorfismo tal que $\varphi(a) = \Psi(a)$ para todo $a \in A$.

El retículo $F_K(A)$ se llama también retículo K-libre sobre el conjunto parcialmente ordenado A.

Cuando K coincide con la diversidad de todos los retículos, omitiremos el índice K y al retículo libre sobre A lo llamaremos $F(A)$. Si A es una anticadena y $|A| = n$, denotaremos $F_K(n)$ ó $F(n)$ y llamaremos este retículo K-libre o, simplemente, libre de n elementos generadores. En 1900 Dedekind mostró que un retículo modular libre $F_M(3)$ de tres elementos generadores tiene 28 elementos y su diagrama tiene la forma expresada en la fig. 8.19, donde los elementos generadores están designados con x, y, z, mientras que

$$a = (x \vee y) \wedge (y \vee z) \wedge (x \vee z),\ b = (x \wedge y) \vee (y \wedge z) \vee (x \wedge z),$$
$$x_1 = (x \wedge a) \vee b,\ y_1 = (y \wedge a) \vee b,\ z_1 = (z \wedge a) \vee b.$$

En el teorema que sigue se da una caracterización muy útil de los retículos modulares.

Teorema 23. Un retículo L es modular, si y sólo si no contiene pentágonos.

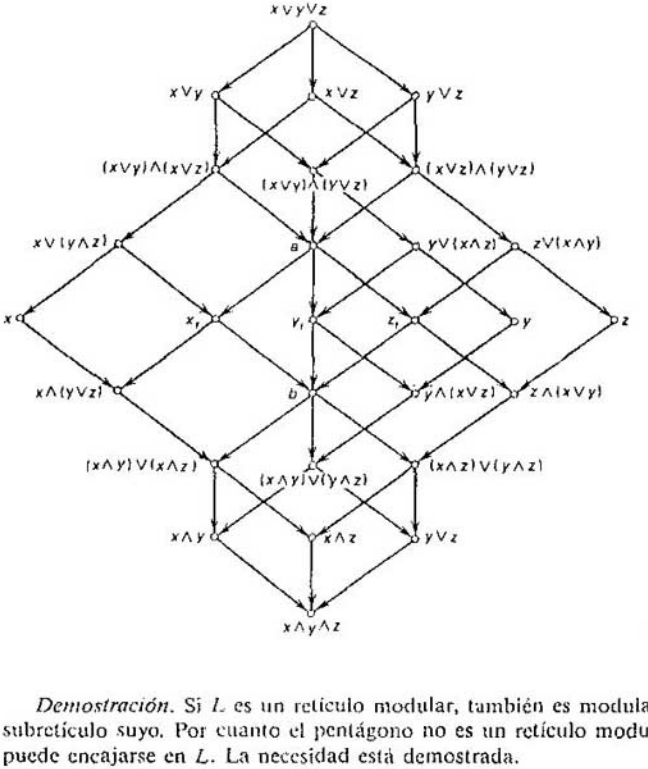

Fig 8.19.

Demostración. Si L es un retículo modular, también es modular todo subretículo suyo. Por cuanto el pentágono no es un retículo modular, no puede encajarse en L. La necesidad está demostrada.

A la inversa, sea L un retículo no modular. En este caso existen los elementos $a, b, c \in L$, tales que $b \leqslant a$ y $(a \wedge c) \vee b \neq a \wedge (c \wedge b)$. El retículo libre que está engendrado por los elementos a, b, c, y que satisface la relación $b < a$ se muestra en la fig. 8.18. Un subretículo en L, engendrado por los elementos a, b, c, debe ser una imagen homomorfa de este retículo libre. Los siguientes cinco elementos del retículo libre: $a \wedge c$, $b \vee (a \wedge c)$, $a \wedge (b \vee c)$, c y $b \vee c$ forman un pentágono y no pueden identificarse para un homomorfismo correspondiente, puesto que al identificar cualesquiera dos de los elementos citados, serán identificados también los elementos $b \vee (a \wedge c)$ y $a \wedge (c \vee b)$, lo que contradice nuestra suposición. El teorema queda pues demostrado.

Un retículo que satisface una de las siguientes identidades equivalentes:

$$(a \wedge b) \vee (a \wedge c) = a \wedge (b \vee c);$$
$$(a \vee b) \wedge (a \vee c) = a \vee (b \wedge c),$$

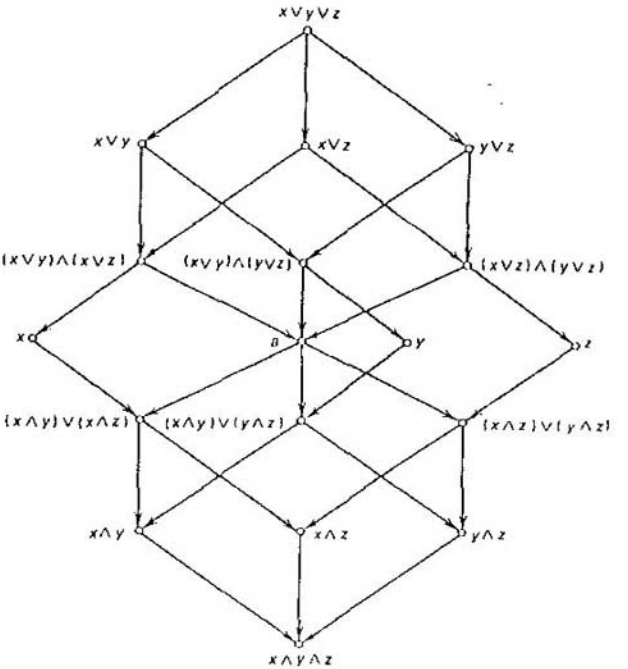

Fig.8.20.

se denomina *distributivo*. Es evidente que un retículo, dual respecto del retículo distributivo, es también distributivo. Un ejemplo muy importante de un retículo distributivo es el booleano, es decir el retículo $\mathcal{P}(S)$ de todos los subconjuntos de un conjunto arbitrario S. Es también retículo distributivo cualquier cadena. Cabe notar que cualquier retículo distributivo es modular. Sin embargo, no todo retículo modular es distributivo. Por ejemplo, un retículo modular de todos los subespacios del espacio lineal no es distributivo. Los retículos cuyos diagramas se dan en las figs. 8.14 y 8.15 no son distributivos. Una familia de todos los retículos distributivos forma una diversidad de retículos. Un retículo distributivo libre $F_D(3)$ de tres elementos generadores tiene 18 elementos y su diagrama se expone en la fig. 8.20. No es difícil ver que el diagrama $F_D(3)$ se obtiene del diagrama $F_M(3)$ (véase fig. 8.19) «pegando»

$x\vee(y\wedge z)$ con $(x\vee y)\wedge(x\vee z)$; $x\wedge(y\vee z)$ con $(x\wedge y)\vee(x\wedge z)$;
$y\vee(x\wedge z)$ con $(x\vee y)\wedge(y\vee z)$; $y\wedge(x\vee z)$ con $(x\wedge y)\vee(y\wedge z)$;
$z\vee(x\wedge y)$ con $(x\vee z)\wedge(y\vee z)$; $z\wedge(x\vee y)$ con $(x\wedge z)\vee(y\wedge z)$

(estos pares de elementos coinciden debido a la distributividad). Al realizarse tal «pegado», los elementos a, x_1, y_1, z_1 y b del retículo modular libre también «se pegan» formando un elemento. Así pues, en el retículo distributivo

$$(x \vee y) \wedge (x \vee z) \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z).$$

El mismo lector puede convencerse de esto.

Teorema 24. Un retículo modular L es distributivo, si y sólo si no contiene diamantes.

Demostración. Si L es un retículo distributivo, todo subretículo suyo será también distributivo. Por cuanto el diamante no es un retículo distributivo, a él no se le puede encajar en L. La necesidad está demostrada.

Viceversa, sea L un retículo modular, pero no distributivo. Entonces, se encontrarán tales elementos $x, y, z \in L$ que $x \wedge (y \vee z) \neq (x \wedge y) \vee (x \wedge z)$. Un retículo modular libre engendrado por x, y, z está representado en la fig. 8.19. Del diagrama de este retículo se ve que sus elementos a, b, x_1, y_1, z_1 forman un diamante. Por eso, en cualquier retículo modular dichos cinco elementos forman un subretículo que es isomorfo a la imagén homomorfa del diamante. Pero, el diamante tiene sólo dos imágenes homomorfas: el propio diamante y el retículo de un solo elemento. En el primer caso la suficiencia del teorema está demostrada. Al tratar el segundo caso, observemos que al pegar los elementos a y b, se pegan también los elementos $x \wedge (y \vee z)$ y $(x \wedge y) \vee (x \wedge z)$, lo que contradice nuestra suposición. Por consecuencia, todo retículo no distributivo contiene un diamante y el teorema queda demostrado.

De los teoremas 23 y 24 obtenemos las siguientes caracterizaciones útiles de los retículos distributivos y modulares:

Teorema 25. Un retículo L es distributivo cuando y sólo cuando no contiene pentágonos ni tampoco diamantes.

Corolario 1. a) El retículo L es distributivo cuando y sólo cuando para cualesquiera $a, b, c \in L$ de las relaciones $a \wedge c = b \wedge c$ y $a \vee c = b \vee c$ se deduce que $a = b$.

b) El retículo L es modular cuando y sólo cuando para todos los $a, b, c \in L$ de las relaciones $b \geqslant a$, $a \wedge c = b \wedge c$ y $a \vee c = b \vee c$ se deduce que $a = b$.

La propiedad más importante de la modularidad se expresa por la siguiente afirmación.

Teorema 26. Si a y b son elementos de un retículo modular L, los intervalos $[a \wedge b, a]$ y $[b, a \vee b]$ son isomorfos. En este caso el isomorfismo se realiza mediante las aplicaciones:

$$\varphi(x) = x \vee b \qquad (a \wedge b \leqslant x \leqslant a)$$
$$\psi(y) = a \wedge y \qquad (b \leqslant y \leqslant a \vee b).$$

Demostración. Está claro que φ y ψ son aplicaciones isótonas, con la particularidad de que $\psi(\varphi(x)) = a \wedge (x \vee b) = x \vee (a \wedge b) = x$ (en virtud de la

identidad de la modularidad y merced a la condición $x \geqslant a \wedge b$) y $\varphi(\psi(y)) = (a \wedge y) \vee b = (a \vee b) \vee y = y$ (en virtud de la identidad de la modularidad y merced a la condición $y \leqslant a \vee b$). Por consiguiente, φ y ψ son isomorfismos, lo que se trataba de demostrar.

Dos intervalos $[x, y]$ y $[x', y']$ del retículo L se denominan *transpuestos*, si $[x, y] = [a, a \vee b]$ y $[x', y'] = [a \wedge b, b]$ para ciertos $a, b \in L$. Diremos que los intervalos $[x, y]$ y $[x', y']$ son *proyectivos* (la designación es $[x, y] \sim [x', y']$), si existe una sucesión finita de intervalos

$$[x, y], [x_1, y_1], \ldots, [x_n, y_n], [x', y'],$$

en la cual cualesquiera dos intervalos vecinos son transpuestos.

Ejercicio 1. Sea $\mathscr{P}(S)$ un booleano. Demuéstrese que dos intervalos $[A, B]$ y $[C, D]$ del retículo de Boole $\mathscr{P}(S)$ son proyectivos cuando y sólo cuando $B - A = D - C$, donde $A, B, C, D \subseteq S$.

Directamente del teorema 26 se desprende que en un retículo modular los intervalos proyectivos son isomorfos. De aquí se deduce el siguiente resultado.

Teorema 27 (*de Jordan-Hölder para retículos modulares*). Cualesquiera dos cadenas máximas que unen los elementos maximal y minimal de un retículo modular finito son de longitud igual. Si $a_0, a_1, \ldots, a_{n-1}, a_n$, y $b_0 = a_0, b_1, \ldots, b_{n-1}, b_n = a_n$ representan un par de tales cadenas máximas, existe una permutación σ de índices $\{1, 2, \ldots, n\}$, tal que $[a_{i-1}, a_i] \sim [b_{\sigma(i)-1}, b_{\sigma(i)}]$ para $i = 1, 2, \ldots, n$. Además, si el retículo en consideración es distributivo, la permutación σ está unívocamente definida.

Así pues, una familia $\mathscr{S} = \{[a_{i-1}, a_i]\ i = 1, \ldots, n\}$ de intervalos de la cadena máxima $a_0, a_1, \ldots, a_{n-1}, a_n$ de un retículo distributivo finito es unívoca con una exactitud de hasta una proyectividad. Sobre $\mathscr{S}$ puede introducirse una relación de orden $\leqslant$: para $[x, y]$ y $[z, w] \in \mathscr{S}$ diremos que $[x, y] \leqslant [z, w]$, si para cualquier cadena máxima $a_0, a_1, \ldots, a_{n-1}, a_n$ existen p y q, tales que $p \leqslant q$ y $[a_p, a_{p+1}] \sim [x, y]$, $[a_q, a_{q+1}] \sim [z, w]$.

Del teorema 27 obtenemos

Corolario 2. Supongamos que S es un conjunto finito; L, un subretículo del retículo de Boole $\mathscr{P}(S)$; S^-, el elemento minimal y S^+, un complemento en S del elemento maximal del retículo L. Si $A_0 = S^-$, $A_1, \ldots, A_n = S - S^+$ es la cadena máxima en L y $\mathscr{S} = \{A_i - A_{i-1}\}$; $i = 1, \ldots, n\}$, entonces

$$(S^-, \{F : F \in \mathscr{S}\}, S^+)$$

es una partición del conjunto S, la cual no depende de la elección de la cadena máxima. Además, los conjuntos S^- y S^+ pueden ser vacíos, y todos los $F \in \mathscr{F}$ no vacíos.

Cabe notar que $F \leqslant F'$, donde $F, F' \in \mathscr{S}$, cuando y sólo cuando para todo $A \in L$ de $F' \subseteq A$ se deduce que $F \subseteq A$.

Un conjunto parcialmente ordenado A se llama *retículo completo*, si ca-

da subconjunto suyo no vacío B tiene $\sup_A B$ e $\inf_A B$. Los retículos completos son: el segmento [0, 1] de orden corriente; el conjunto de todos los subconjuntos de cierto conjunto ordenado por inclusión; toda cadena finita. Un retículo completo lo constituye también un conjunto parcialmente ordenado $B(S_n)$ de todas las particiones no ordenadas del conjunto finito S_n (véase el ejemplo 8 del § 8.1). Está claro que cualquier retículo completo ha de tener 0 y 1. Por eso, un retículo de números enteros de orden corriente no es un retículo completo.

Por una partición dada π se puede determinar la relación de equivalencia ϱ, suponiendo $a\varrho b$ cuando y sólo cuando a y b se contienen en un mismo bloque de la partición π. Viceversa, si ϱ es una relación de equivalencia, entonces la familia de clases contiguas de equivalencia ϱ en el conjunto A (se llama clase contigua de equivalencia ϱ, definida por el elemento $a \in A$, al subconjunto $\{x \in A \mid x \varrho a\}$) es la partición del conjunto A. Así pues, existe una correspondencia biunívoca entre las particiones y las relaciones de equivalencia. Por lo tanto, el conjunto de todas las relaciones de equivalencia, definidas sobre el conjunto A y ordenado del modo siguiente: $\varrho \leqslant \tau$, si $a\varrho b$, lleva consigo $a\tau b$, y forma un retículo completo.

Ejercicios. Compruébese que

2. El conjunto de todas las particiones del conjunto A, ordenado según la reunión de los bloques, es un retículo completo.

3. Una suma ordenada de retículos completos $\{A_\alpha \mid \alpha \in L\}$, donde L es un retículo completo, es retículo completo.

4. Un producto directo de los retículos completos es retículo completo.

5. Un producto ordenado de retículos completos $\{A_\alpha \mid \alpha \in L\}$, donde L es un retículo completo que satisface la condición de mínimo, es un retículo completo.

Un retículo L se denomina *retículo con complementos relativos*, si para todo elemento c perteneciente a cualquier intervalo $[a, b]$ existe un elemento d, tal que $c \vee d = b$, y $c \wedge d = a$. Este elemento d recibe el nombre de *complemento* del elemento c en el intervalo $[a, b]$. El complemento se define de una manera no unívoca. Por ejemplo, en el retículo expuesto en la fig. 8.21 los elementos c y d son complementos del elemento b en el intervalo $[s, 1]$. No obstante, los elementos a y s sirven uno para otro de únicos complementos en el intervalo $[a, b]$. Un retículo con 0 y 1 se denomina *retículo con complementos*, si cada uno de sus elementos tiene complemento en el intervalo [0, 1]. Los complementos en el intervalo [0, 1] se llaman simplemente *complementos*. Debido al corolario 1, en cualquier intervalo dado $[a, b]$ del retículo distributivo L el elemento c puede tener, como máximo, un único complemento relativo. Cada retículo modular L con complementos es un retículo con complementos relativos. El pentágono (véase fig. 8.14) es un retículo no modular con complementos, siendo éstos, sin embargo, no relativos.

Se denomina *retículo de Boole* un retículo distributivo con complementos.

Teorema 28. En un retículo de Boole L cualquier elemento x tiene uno

y sólo un complemento x. Además, para cualesquiera x, $y \in L$, tienen lugar las relaciones:

a) $x \wedge x = 0$, $x \vee x = 1$ (de complementariedad);

b) $\bar{\bar{x}} = x$ (de involución);

c) $\overline{x \wedge y} = \bar{x} \vee \bar{y}$, $\overline{x \vee y} = \bar{x} \wedge \bar{y}$ (leyes de Morgan)

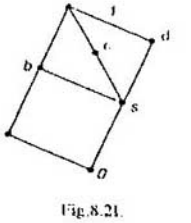

Fig. 8.21.

Demostración. Por ser distributivo el retículo de Boole L, la correspondencia $x \to \bar{x}$ es unívoca. Pero, en vista de que el concepto de complemento es simétrico, x es un complemento para $\bar{x}$, de donde $x = \bar{\bar{x}}$ en virtud de la unicidad de los complementos en L. La propiedad de involución queda demostrada. Por consiguiente, la correspondencia $x \to \bar{x}$ es biunívoca.

Demostremos ahora que

(*) $x \wedge a = 0$, cuando y sólo cuando $x \leqslant \bar{a}$.

En efecto, si $x \leqslant \bar{a}$, entonces $x \wedge a \leqslant \bar{a} \wedge a = 0$, y si $x \wedge a = 0$, tendremos $x = x \wedge 1 = x \wedge (a \vee \bar{a}) =$ (debido a la distributividad) $= (x \wedge a) \vee (x \wedge \bar{a}) = 0 \vee (x \wedge \bar{a}) = x \wedge \bar{a}$. De este modo (*) queda demostrada.

Si $a \leqslant b$, entonces $b \wedge \bar{a} \leqslant b \wedge \bar{b} = 0$ y por lo tanto, en virtud de (*), $b \leqslant \bar{a}$. Dicho de otro modo, la correspondencia biunívoca $x \to \bar{x}$ invierte el orden. Por cuanto la correspondencia $x \to \bar{x}$ también invierte el orden, entonces $x \to \bar{x}$ es un isomorfismo autodual, lo que demuestran las leyes de Morgan.

Del teorema 28 se deduce que cada retículo de Boole es autodual (es decir, es isomorfo respecto de un retículo dual hacia sí mismo). Por cuanto los complementos en el retículo de Boole son únicos, éste puede considerarlo como un álgebra con dos operaciones binarias $\vee$, $\wedge$, una operación de complementariedad — y dos elementos marcados: 0 y 1. Se llama *álgebra de Boole* a un álgebra con las operaciones $\vee$, $\wedge$ y dos fronteras universales: 0 y 1, que satisfacen las propiedades de: idempotencia, conmutatividad, asociatividad, absorción (véase la definición de retículo), modularidad (retículo modular), distributividad (retículo distributivo), fronteras universales (retículo con 0 y 1), complementariedad (retículo con complementos), involución y leyes de Morgan (retículo de Boole) (véase § 2.1). Por ejemplo, el conjunto $\mathscr{P}(S)$ de todos los subconjuntos del conjunto S (booleano) es un álgebra de Boole. Luego, cualquier subálgebra de un álgebra de Boole es de por sí un álgebra de Boole. Las álgebras de Boole son un producto directo de las álgebras de Boole y los intervalos de las álgebras de Boole.

Ejercicios. Demuéstrese que

6. Un conjunto de números enteros no negativos, ordenado respecto de la divisibilidad (véase el ejemplo 5 del § 8.1) es un retículo distributivo (consideramos que 0 divide a 0; aquí, $\sup\{a, b\}$ es el mínimo común múltiplo de los números a y b; $\inf\{a, b\}$ es el máximo común divisor de los números a y b).

7. Un retículo de Boole finito es isomorfo al retículo de todos los subconjuntos de un cierto conjunto finito.

8. Cualquier retículo distributivo se encaja en un retículo de Boole.

9. Todo retículo modular con complementos únicos es un retículo de Boole.

Teorema 29. En un retículo L de longitud finita y complementos relativos, cada elemento a es una unión de átomos contenidos en él.

Demostración. Si $a>0$, entonces o bien a es un átomo, o bien $a>b>0$ para cierto $b\in L$. Sea c un complemento relativo del elemento b en el intervalo $[0, a]$. Por inducción a lo largo del intervalo $[0, a]$ se demuestra que los elementos b y c son ambos una unión de átomos. Pero, en tal caso, esto es lícito también para $a = b\vee c$. El teorema está demostrado.

Colorario 3. En un retículo modular de longitud finita con complementos cada elemento es una unión de átomos contenidos en él.

Se dice que un retículo L satisface la condición de recubrimiento por arriba, si para cualesquiera sus elementos a, b ($a \neq b$) las condiciones $a\wedge b \prec b$ y $a\wedge b \prec a$ llevan consigo $a \prec a\vee b$, y $b \prec a\vee b$. La condición de recubrimiento por debajo se define de un modo dual: el retículo L satisface la condición de recubrimiento por debajo, si para cualesquiera a, $b\in L$ ($a \neq b$) las condiciones $a \prec a\vee b$ y $b \prec a\vee b$ traen consigo $a\wedge b \prec a$ y $a\wedge b \prec b$. Del teorema 26 se deduce que el retículo modular posee las condiciones de recubrimiento tanto por arriba, como por debajo.

Un retículo L se llama *semimodular*, si satisface la condición de recubrimiento por arriba, o bien (lo que es equivalente) si para cualesquiera a, b, $c\in L$ la condición $a \prec b$ trae consigo $a\vee c \prec b\vee c$, o bien $a\vee c = b\vee c$. Son ejemplos de retículos semimodulares los retículos modúlares y algunos retículos importantes que aparecen en las geometrías (véase § 8.4). Dos ejemplos más de retículos semimodulares se exponen en la fig. 8.22.

Sea A un conjunto parcialmente ordenado con 0. Definamos en él una *función de altura* (o de *rango*) del modo siguiente: $r(a)$ es igual a la longitud de la cadena más larga en el intervalo $[0, a]$ (si tal cadena no existe, suponemos $r(a) = \infty$). Si A es un conjunto parcialmente ordenado de longitud finita N, entonces, $0\leqslant r(a)\leqslant N$ para cualquier elemento $a\in A$. En un retículo semimodular de longitud finita el rango $r(a)$ coincide con la longitud de la cadena máxima arbitraria en el intervalo $[0, a]$. Esto se deduce del siguiente teorema muy importante.

Teorema 30 (condición de Jordan—Hölder). En un retículo semimodular L de longitud finita, cualesquiera dos cadenas máximas entre a, $b\in L$ arbitrarios, tales que $a\leqslant b$, son de longitud igual.

Demostración. Sea $a = a_0 \prec a_1 \prec \ldots \prec a_n = b$ una cadena máxima de longitud n en $[a, b]$. Demostremos, por inducción respecto de n, que cualquier otra cadena máxima es de longitud n. Para $n = 0$, la afirmación es obvia. Si $n = 1$, entonces $a \prec b$, y por lo tanto, la cadena máxima en $[a, b]$ es única. Supongamos que nuestro teorema es lícito para todos los subretículos $[a, b]$ de longitud inferior a n, donde $n\geqslant 2$. Sea $a = b_1 \prec b_2 \prec \ldots \prec b_m = b$ otra cadena máxima en $[a, b]$. Si $a_1 = b_1$, entonces en el retículo semimodular $[a_1, b]$ la cadena máxima $a_1 \prec \ldots \prec a_n = b$ es de una longitud igual a $n - 1$; por consiguiente, la cadena máxima $a_1 \prec b_2 \prec \ldots \prec b_m = b$ ha de tener una longitud igual a $n - 1$;

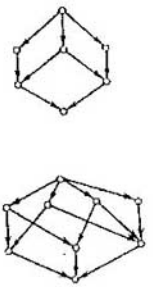

Fig.8.22.

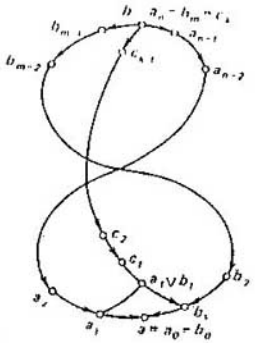

Fig.8.23.

por eso $n = m$. Si $a_1 \neq b_1$ (véase fig. 8.23), entonces examinemos una cadena máxima de longitud k en $[a_1 \vee b_1, b]$. Por ser el retículo semimodular, tenemos $(a_1 \vee b_1) > a_1$ y $(a_1 \vee b_1) > b_1$. Por consiguiente, $a_1 \prec (a_1 \vee b_1) \prec c_1 \prec c_2 \prec \ldots \prec c_k = b$ es la cadena máxima de longitud $k + 1$ en $[a_1, b]$, y $a_1 \prec a_2 \prec \ldots \prec a_n = b$ es también una cadena máxima, pero de longitud $n - 1$ en $[a_1, b]$. De este modo, en virtud de la suposición inductiva, $k + 1 = n - 1$. Análogamente, $k + 1 = m - 1$, por lo cual $n = m$. El teorema está demostrado.

De un modo dual se demuestra que en todo retículo L de longitud finita, que satisface la condición de recubrimiento por debajo, cualesquiera dos cadenas máximas entre los elementos arbitrarios a, $b \in L$ tienen igual longitud, es decir, se cumple la condición de Jordan—Hölder para cadenas.

Ejercicios. Demuéstrese que

10. Si en un conjunto parcialmente ordenado A con 0 se cumple la condición de Jordan—Hölder para cadenas, su función de rango $r(a)$, definida para todo $a \in A$, satisface las siguientes condiciones:

a) $r(0) = 0$;

b) de $a \prec b$ se deduce que $r(b) = r(a) + 1$.

11. Si en un conjunto parcialmente ordenado A está definida una función r, tal que $r(0) = 0$ y de $a \prec b$ se deduce que $r(b) = r(a) + 1$, entonces A satisface la condición de Jordan—Hölder para las cadenas y esta función coincide con su función de rango.

La modularidad y la semimodularidad pueden caracterizarse en términos de función de rango.

Teorema 31. Sea L un retículo de longitud finita con 0. El retículo L es semimodular cuando y sólo cuando satisface la condición de Jordan—Hölder para cadenas y para todos los a, $b \in L$ tiene lugar la desigualdad

$$r(a) + r(b) \geqslant r(a \wedge b) + r(a \vee b),$$

donde r es la función de rango del retículo L.

Demostración. Por ser L semimodular en el retículo L se cumple la con-

dición de Jordan—Hölder para las cadenas. Sea $a \wedge b = c_0 \prec c_1 \prec \ldots \prec c_t = b$ una cadena máxima en el intervalo $[a \wedge b, b]$. De acuerdo con la condición de Jordan—Hölder, la longitud de esta cadena es igual a $r(b) - r(a \wedge b)$. Teniendo presente la condición de recubrimiento por arriba para los retículos semimodulares, llegamos a que para L

$$a \vee (a \wedge b) = a = (a \vee c_0) \preccurlyeq (a \vee c_1) \preccurlyeq \ldots \preccurlyeq (a \vee c_t) = a \vee b$$

es también una cadena máxima, pero en el intervalo $[a, a \vee b]$. La longitud de esta cadena no sobrepasa la de la primera cadena (algunos elementos pueden coincidir), es decir, no es superior al número: $r(b) - r(a \wedge b)$. Por otra parte, de acuerdo con la condición de Jordan—Hölder, la longitud de esta cadena es igual a $r(a \vee b) - r(a)$. Por eso, $r(b) - r(a \wedge b) \geqslant r(a \vee b) - r(a)$. La necesidad está demostrada.

Demostremos ahora la suficiencia. Sean $a, b \in L$ tales que $a \succ (a \wedge b)$, $b \succ (a \wedge b)$ y $a \neq b$. Entonces, en virtud de la condición de Jordan—Hölder (véase ejercicio 10): $r(a) = r(b) = r(a \wedge b) + 1$. Sustituyamos estas igualdades en la desigualdad mencionada en la hipótesis del teorema y obtendremos: $r(a \vee b) \leqslant r(a) + 1$, $r(a \vee b) \leqslant r(b) + 1$. De aquí se desprende directamente que $(a \vee b) \geqslant a$, y $(a \vee b) \leqslant b$. Demostremos que $a \vee b \neq a$. Por reducción al absurdo tenemos: sea $a \vee b = a$. Entonces, $a > b$ y $a \wedge b = b$; mas esto contradice a que $b \succ (a \wedge b)$. Por consiguiente, $(a \vee b) \succ a$. Análogamente se comprueba que $(a \vee b) \succ b$. El teorema está demostrado.

Del teorema 31 y de la dualidad de las condiciones de recubrimiento por arriba y por debajo obtenemos el siguiente resultado:

Corolario 4. Si en un retículo L de longitud finita con 0 se cumple la condición de recubrimiento por debajo, entonces para cualesquiera $a, b \in L$ tiene lugar la desigualdad: $r(a) + r(b) \leqslant r(a \wedge b) + r(a \vee b)$.

Otra aplicación del teorema 31 es la siguiente afirmación:

Corolario 5. Para un retículo L de longitud finita son equivalentes las siguientes afirmaciones:

a) L es un retículo modular;

b) el retículo L satisface las condiciones de recubrimiento tanto por arriba, como por debajo;

c) L no contiene pentágonos;

d) para cualesquiera $a, b \in L$ se verifica la igualdad

$$r(a) + r(b) = r(a \wedge b) + r(a \vee b).$$

Demostración. Ya se ha establecido que a) trae consigo b). El teorema 31 y el corolario 4 estipulan que de b) se deduce d). La equivalencia entre a) y c) está demostrada en el teorema 23. Para finalizar la demostración del corolario demostremos que de d) se deduce c). Por reducción al absurdo: supongamos que el retículo L contiene un pentágono $\{0, a, b, c, 1\}$ (véase fig. 8.14) y para este retículo se cumple la condición d). Entonces

$$r(a) + r(c) = r(a \vee c) + r(a \wedge c) = r(1) + r(0)$$
$$= r(b \vee c) + r(b \wedge c) = r(b) + r(c).$$

De donde, $r(a) = r(b)$, lo que es imposible, puesto que $b < a$. El corolario está demostrado.

Sea L un retículo con 0. El subconjunto I del conjunto $L \setminus \{0\}$ se denomina *independiente*, si para cualesquiera subconjuntos finitos A y B suyos es válida la igualdad

$$\inf\{\sup A, \sup B\} = \sup(A \cap B).$$

Teorema 32. Un subconjunto finito I del retículo L es independiente cuando y sólo cuando la aplicación φ: $A \to \sup A$, definida para todos los $A \in \mathcal{P}(I)$, es un isomorfismo entre el retículo del booleano $\mathcal{P}(I)$ y el subretículo del retículo L, generado por el conjunto I.

Demostración. Tenemos $\sup\{\sup A, \sup B\} = \sup\{A \cup B\}$, y por eso, si el conjunto I es independiente (es decir, si $\inf\{\sup A, \sup B\} = \sup\{A \cap B\}$, entonces φ es un homomorfismo de los retículos. Si la aplicación φ no es biunívoca, entonces $\sup A = \sup B$ para algunos subconjuntos $A \subseteq I$, $B \subseteq I$, $A \neq B$. Sea, por ejemplo, $A \not\subseteq B$ y $a \in (A \setminus B)$. Entonces, $a \leqslant \sup B$, $a \notin B$; por eso, $a = \inf\{a, \sup B\} = \inf\{\sup\{a\}, \sup B\} = \sup(\{a\} \cap B) = \sup \varnothing = 0$, lo que es imposible. Por consiguiente φ es un isomorfismo.

Dejemos al lector la demostración de la afirmación recíproca.

Es evidente que el subconjunto de un elemento $\{a\}$ es siempre independiente. Un subconjunto $\{a, b\}$ es independiente cuando y sólo cuando $a \wedge b = 0$ ($a, b \in (L \setminus \{0\})$, $a \neq b$). Para que sea independiente un subconjunto $\{a, b, c\}$, donde $a, b, c \in (L \setminus \{0\})$ y todos los elementos a, b, c son distintos dos a dos, es necesario exigir que se verifiquen las siguientes igualdades:

$$a \wedge (b \vee c) = 0; \qquad (a \vee b) \wedge (a \vee c) = a;$$
$$b \wedge (a \vee c) = 0; \qquad (b \vee c) \wedge (b \vee a) = b;$$
$$c \wedge (a \vee b) = 0, \qquad (c \vee a) \wedge (c \vee b) = c.$$

En los retículos modulares y semimodulares podemos limitarnos a un número menor de relaciones.

Teorema 33. Si L es un retículo modular con cero 0, entonces un subconjunto de n elementos $\{a_1, \ldots, a_n\} \subseteq L - \{0\}$ es independiente cuando y sólo cuando $(a_1 \vee \ldots \vee a_i) \wedge a_{i+1} = 0$ para todo $i = 1, 2, \ldots, n-1$.

Demostración. La necesidad de las condiciones del teorema se obtendrá al suponer $A = \{a_1, \ldots, a_i\}$, $B = \{a_{i+1}\}$. Supongamos ahora que el subconjunto $\{a_1, \ldots, a_n\}$ satisface las condiciones del teorema. Sea A, $B \subseteq \{a_1, \ldots, a_n\}$, $A \cap B = \varnothing$. Entonces, $\inf\{\sup A, \sup B\} = 0$. Efectivamente, sea $a_k \in A \cup B$ con el índice máximo k. Sea, por ejemplo, $a_k \in B$. En este caso, por ser el retículo L modular para cualesquiera $x, y, z \in I$, tenemos $x \wedge (y \vee z) = x \wedge ((y \wedge (x \vee z)) \vee z)$. Al sustituir en la última igualdad x por $\sup A$, y por

a_k, y z por $\sup(B - \{a_k\})$, obtenemos

$$\inf\{\sup A,\ \sup B\} = \sup A \wedge (a_k \vee \sup(B - \{a_k\})) =$$
$$= \sup A \wedge ((a_k \wedge (\sup A \vee \sup(B - \{a_k\}))) \vee \sup(B - \{a_k\})) =$$
$$= \sup A \wedge \sup(B - \{a_k\}) = \inf\{\sup A,\ \sup(B - \{a_k\})\},$$

puesto que $a_k \wedge (\sup A \vee \sup(B - \{a_k\})) \leqslant (a_1 \vee \ldots \vee a_{k-1}) \wedge a_k = 0$.

Procediendo de este modo, podemos eliminar todos los elementos a_i que figuran en el conjunto $A \cup B$, y obtener, como resultado, la igualdad

$$\inf\{\sup A,\ \sup B\} = \sup \varnothing = 0.$$

En el caso general, en virtud de la modularidad y de la condición $A \cap \cap(B - A) = \varnothing$, tenemos

$$= x_1 \wedge [y_1 \vee (b \wedge (x_2 \vee y_2))] = x_1 \wedge [y_1 \vee (b \wedge [a_n \wedge (x_2 \vee y_2)])] =$$
$$= x_1 \wedge [y_1 \vee ((a_1 \vee a_2 \vee \ldots \vee a_{n-1}) \wedge a_n \wedge (x_2 \vee y_2))] = x_1 \wedge [y_1 \vee (0 \wedge (x_2 \vee y_2))] =$$

lo que se trataba de demostrar.

Ejercicios 12. Demuéstrese que la afirmación del teorema 33 es lícita para los retículos semimodulares con 0.

Sea L un retículo modular con 0. Demuéstrese que

13. Si $a_i \leqslant b_i$, $a_i,\ b_i \in L$, $i = 1, 2, \ldots, n$, y $b_1, b_2, \ldots, b_n$ son independientes, entonces $a_1, a_2, \ldots, a_n$ son también independientes.

14. Si $a_1, a_2, \ldots, a_n$ son elementos independientes del retículo L y $a_i = a_{i_1} \vee a_{i_2} \vee \ldots \vee a_{i_{k_i}}$, donde $a_{i_1}, a_{i_2}, \ldots, a_{i_{k_i}}$ son elementos independientes del retículo L e $i = 1, 2, \ldots, n$, entonces los elementos $a_{11}, \ldots, a_{1k_1}, a_{21}, \ldots, a_{2k_2}, \ldots, a_{nk_n}$ son independientes.

Teorema 34. Si $a_1, \ldots, a_n$ son elementos independientes de un retículo modular L con cero 0, entonces un subretículo H del retículo L generado por los intervalos $[0, a_i]$, donde $i = 1, \ldots, n$, es isomorfo al producto directo $[0, a_1] \times [0, a_2] \times \ldots \times [0, a_n]$.

Demostración. Sea H' un subretículo del retículo L generado por los intervalos $[0, a_1], \ldots, [0, a_{n-1}]$, $b = a_1 \vee a_2 \vee \ldots \vee a_{n-1}$, y

$$M = \{x_1 \vee x_2 \mid x_1 \in H',\ x_2 \leqslant a_n\}.$$

Por cuanto $[0, a_i] \subseteq [0, b]$ para $i = 1, 2, \ldots, n$, entonces $H' \subseteq [0, b]$, por lo que $x_1 \wedge b = x_1$ para todo $x_1 \in H'$. Haciendo uso de la independencia de los elementos $a_1, a_2, \ldots, a_n$ y de la ley modular, obtenemos para cualesquiera $x_1, y_1 \in H'$ y $x_2, y_2 \in [0, a_n]$:

$$= x_1 \wedge (y_1 \vee x_2 \vee y_2) = (x_1 \wedge b) \wedge (y_1 \vee x_2 \vee y_2) = x_1 \wedge [b \wedge (y_1 \vee (x_2 \vee y_2))] =$$
$$= x_1 \wedge [y_1 \vee (b \wedge (x_2 \vee y_2))] = x_1 \wedge [y_1 \vee (b \wedge [a_n \wedge (x_2 \vee y_2)])] =$$
$$= x_1 \wedge [y_1 \vee ((a_1 \vee a_2 \vee \ldots \vee a_{n-1}) \wedge a_n \wedge (x_2 \vee y_2))] = x_1 \wedge [y_1 \vee (0 \wedge (x_2 \vee y_2))] =$$
$$= x_1 \wedge [y_1 \vee 0] = x_1 \wedge y_1$$

y

$$x_2 \wedge (y_1 \vee x_1 \vee y_2) = (x_2 \wedge a_n) \wedge (y_1 \vee x_1 \vee y_2) = x_2 \wedge [a_n \wedge ((x_1 \vee y_1) \vee y_2)] =$$
$$= x_2 \wedge [y_2 \vee (a_n \wedge (x_1 \vee y_1))] = x_2 \wedge [y_2 \vee [a_n \wedge (b \wedge (x_1 \vee y_1))] =$$

$$= x_2 \wedge [y_2 \vee [a_n \wedge (a_1 \vee a_2 \vee \ldots \vee a_{n-1}) \wedge (x_1 \vee y_1)]] =$$
$$= x_2 \wedge [y_2 \vee (0 \wedge (x_1 \vee y_2))] = x_2 \wedge [y_2 \vee 0] = x_2 \wedge y_2.$$

Sirviéndonos de la ley modular, de estas igualdades deducimos que

$$(x_1 \vee x_2) \wedge (y_1 \vee y_2) = (x_1 \vee x_2) \wedge [(y_1 \vee x_2 \vee y_2) \wedge (y_1 \vee y_2)] =$$
$$= [(x_1 \vee x_2) \wedge (y_1 \vee x_2 \vee y_2)] \wedge (y_1 \vee y_2) = [x_2 \vee [x_1 \wedge (y_1 \vee x_2 \vee y_2)]] \wedge (y_1 \vee y_2) =$$
$$= [x_2 \vee (x_1 \wedge y_1)] \wedge (y_1 \vee y_2) = (x_1 \wedge y_1) \vee [x_2 \wedge (y_1 \vee y_2)] =$$
$$= (x_1 \wedge y_1) \vee [x_2 \wedge [(y_1 \vee y_2) \wedge (y_1 \vee x_1 \vee y_2)]] =$$
$$= (x_1 \wedge y_1) \vee [(y_1 \vee y_2) \wedge (x_2 \wedge (y_1 \vee x_1 \vee y_2))] = (x_1 \wedge y_1) \vee [(y_1 \vee y_2) \wedge (x_2 \wedge y_2)] =$$
$$= (x_1 \wedge y_1) \vee (x_2 \wedge y_2).$$

Así pues, el conjunto M queda cerrado también respecto de la intersección y, por lo tanto, coincide con el subretículo H. Más aún, la última igualdad, junto con la igualdad evidente

$$(x_1 \vee x_2) \vee (y_1 \vee y_2) = (x_1 \vee y_1) \vee (x_2 \vee y_2)$$

señalan que

$$\varphi(x,\ y) = x \vee y$$

es un homomorfismo reticular del producto directo $H' \times [0,\ a_n]$ sobre H. Si $x_1 \vee x_2 = y_1 \vee y_2$, entonces, por cuanto

$$x_2 \wedge (a_1 \vee \ldots \vee a_{n-1}) \leqslant a_n \wedge (a_1 \vee \ldots \vee a_{n-1}) = 0$$

y

$$y_2 \wedge (a_1 \vee \ldots \vee a_{n-1}) \leqslant a_n \wedge (a_1 \vee \ldots \vee a_{n-1}) = 0,$$

con ayuda de la ley modular obtenemos:

$$x_1 = x_1 \wedge (x_1 \vee x_2) \wedge (a_1 \vee \ldots \vee a_{n-1}) = x_1 \wedge (y_1 \vee y_2) \wedge (a_1 \vee \ldots \vee a_{n-1}) =$$
$$= x_1 \wedge [(y_1 \vee y_2) \wedge (a_1 \vee \ldots \vee a_{n-1})] = x_1 \wedge [y_1 \vee (y_2 \wedge (a_1 \vee \ldots \vee a_{n-1}))] =$$
$$= x_1 \wedge [y_1 \vee 0] = x_1 \wedge y_1 = y_1 \wedge x_1 = y_1 \wedge [x_1 \vee 0] =$$
$$= y_1 \wedge [x_1 \vee (x_2 \wedge (a_1 \vee \ldots \vee a_{n-1}))] = y_1 \wedge [(x_1 \vee x_2) \wedge (a_1 \vee \ldots \vee a_{n-1})] =$$
$$= y_1 \wedge (y_1 \vee y_2) \wedge (a_1 \vee \ldots \vee a_{n-1}) = y_1.$$

De un modo análogo se establece que $x_2 = y_2$. De este modo, φ resulta ser un isomorfismo. Aprovechando la suposición de inducción, llegamos a que

$$H \cong H' \times [0,\ a_n] \cong [0,\ a_1] \times \ldots \times [0,\ a_{n-1}] \times [0,\ a_n].$$

El teorema está demostrado.

Ejercicios. Sea L un retículo modular, $a,\ b,\ c \in L$. Demuéstrese que

15. (Von J. Neumann [114]). Un subretículo en L generado por los elementos $a,\ b,\ c \in L$, es distributivo cuando y sólo cuando

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

16. (Birkhoff [115]). Sean C_0, C_1 las cadenas en L. Entonces, un subretículo en L generado por el conjunto $C_0 \cup C_1$ es distributivo.

17. Un subretículo en L generado por $[a\wedge b,\ a]\cup[a\vee b,\ b]$ es isomorfo al retículo $[a\wedge b,\ a]\times[a\wedge b,\ b]$.

18. Compruébese que un subretículo generado por $[a\wedge b,\ a]\cup[a\wedge b,\ b]$ no coincide con $[a\wedge b,\ a\vee b]$. Demuéstrese que para la coincidencia es suficiente exigir que el retículo L sea distributivo.

Más abajo señalaremos que los resultados, formulados en los ejercicios 15...17, se emplean para resolver los problemas combinatorios de optimización. Si se encuentran dificultades en la resolución de los ejercicios, recomendamos referirse al libro de Grätzer (véase cap. 4, § 1[32]).

Teorema 35. Sea L un retículo semimodular con 0 y con una función de rango r. El conjunto de átomos $I=\{a_1, a_2, \ldots, a_n\}$ del retículo L es independiente cuando y sólo cuando

$$r(a_1\vee\ldots\vee a_n)=n.$$

Demostración. Supongamos que $(a_1\vee\ldots\vee a_i)\wedge a_{i+1}=0$ para todo $i=1, 2, \ldots, n-1$. Demostremos por inducción respecto de i que $r(a_1\vee\ldots\vee a_i)=i$. Para $i=1$ la afirmación es válida. Si $r(a_1\vee\ldots\vee a_i)=i$, entonces, por ser el retículo semimodular, tenemos $(a_1\vee\ldots\vee a_i)\prec(a_1\vee\ldots\vee a_i\vee a_{i+1})$ y por eso $r(a_1\vee\ldots\vee a_i\vee a_{i+1})=r(a_1\vee\ldots\vee a_i)+1=i+1$. Con esto queda demostrada la necesidad.

Para demostrar la suficiencia mostremos que el conjunto de átomos I satisface la condición del teorema 32. De la condición $r(a_1\vee\ldots\vee a_n)=n$ tenemos $r(\sup A)=|A|$ para cualquier subconjunto $A\subseteq I$, de modo que la aplicación $\varphi: A\to\sup A$ es biunívoca. Es evidente que la aplicación φ conserva las uniones. Tomemos ahora $A, B\subseteq I$, y sea $a=\inf\{\sup A, \sup B\}$, $b=\sup\{A\cup B\}$. Entonces $a\geqslant b$, y de la condición de semimodularidad tenemos

$$r(\sup A)+r(\sup B)\geqslant r(a)+r(\sup\{A\cup B\}),$$

de modo que $|A|+|B|\geqslant r(a)+|A\cup B|$. De aquí concluimos que

$$r(a)\leqslant|A|+|B|-|A\cup B|=|A\cap B|.$$

Por otro lado, $r(a)\geqslant r(b)=|A\cap B|$, por consiguiente, $r(a)=r(b)$, y $a=b$, es decir, $\inf\{\sup A, \sup B\}=\sup(A\cap B)$. De aquí proviene que φ es un isomorfismo, y, en virtud del teorema 32, el conjunto de átomos I es independiente. El teorema está demostrado.

Un retículo semimodular atómico completo (es decir, cualquier elemento lo representamos en forma de una reunión de átomos) sin cadenas infinitas se llama *geométrico* o *matroidal*.

Demos a conocer algunas definiciones.

Sea $\mathscr{P}(S)$ un conjunto de todos los subconjuntos de S. Diremos que sobre el conjunto S está dado el *operador de clausura*, si a todo elemento de $A\in\mathscr{P}(S)$ se la hace corresponder unívocamente un determinado elemento de $A\in\mathscr{P}(S)$, llamado clausura de A, con la particularidad de que dicha correspondencia satisface, para todos los $A, B\in\mathscr{P}(S)$, las condiciones

siguientes:

1. $A \subseteq \bar{A}$;
2. Si $A \subseteq B$, entonces $\bar{A} \subseteq \bar{B}$ (propiedad de conservación del orden);
3. $\bar{\bar{A}} = \bar{A}$ (idempotencia).

El conjunto A se llama *cerrado*, si coincide con su clausura.

Se denomina *pregeometría* (o *matroide*) $G(S)$ a un conjunto S con un operador de la clausura $\bar{}$, que satisface las propiedades:

a) de sustitución: para cualesquiera $p, q \in S$ y para todo $A \in \mathscr{P}(S)$, de $p \in \bar{A} \cup \{q\}$ y $p \notin A$ se deduce que $q \in \bar{A} \cup \{p\}$;

b) de base finita: para todo $A \in \mathscr{P}(S)$ existe un subconjunto finito $A_f \subseteq A$ tal que $\bar{A}_f = \bar{A}$.

Se denomina *geometría combinatoria* (en adelante, siempre geometría) a una pregeometría en la que todos los subconjuntos de un solo elemento, como también el conjunto vacío, son cerrados.

La definición de una geometría sobre el conjunto S se diferencia de la definición de una topología sobre S en que no se requiere el cumplimiento de la condición $\overline{A \cup B} = \bar{A} \cup \bar{B}$ para todos los A, $B \in \mathscr{P}(S)$, pero subsiste la propiedad de sustitución, la cual, en general, puede no cumplirse para la clausura de la topología.

Llamemos superficie a todo conjunto cerrado de una geometría. Las superficies de una geometría G, ordenadas por inclusión, forman un retículo completo $L(G)$ con operaciones binarias $\vee$ y $\wedge$: $A \wedge B = A \cap B$, $A \vee B = \overline{A \cup B}$, donde A y B son las superficies de la geometría G.

Teorema 36. Sea $G = (S, \bar{})$ una geometría. Entonces, el retículo $L(G)$ es geométrico. Viceversa, si L es un retículo geométrico, S, un conjunto de átomos del retículo L, y el conjunto $\{a \in S \mid a \leqslant \sup A\}$ es la clausura $\bar{A}$ de cualquier subconjunto $A \subseteq S$, entonces $G = (S, \bar{})$ es una geometría y el retículo de ella L es isomorfo a $L(G)$.

Demostración. Sea $G = (S, \bar{})$ una geometría. El hecho de que el retículo $L(G)$ es completo, sin cadenas infinitas y atómico se comprueba sin dificultad alguna. Por eso proponemos que el lector mismo lo haga individualmente a título de ejercicio. Demostremos que $L(G)$ es un retículo semimodular. Supongamos que $A, B \in L(G)$, $B = \bar{A} \cup \{p\}$ y $p \notin A$. Afirmamos que en este caso $A \prec\!\!\!\cdot\, B$. En efecto, si $C \in L(G)$ y $A \subset C \subseteq B$, entonces existe un elemento $q \in (C \setminus A)$ y $q \in C \subseteq B = \bar{A} \cup \{p\}$; por eso, según la propiedad de sustitución, $p \in \bar{A} \cup \{q\} \subseteq C$. Por consiguiente, $B = \bar{A} \cup \{p\} \subseteq C$. Resulta que $B = C$; de aquí, $A \prec\!\!\!\cdot\, B$. Sea ahora $D \in L(G)$. Entonces, $B \vee D = \overline{B \cup D} = \overline{\bar{A} \cup D \cup \{p\}}$ y $A \vee D = \overline{A \cup D}$; de aquí, o bien $p \in \overline{A \cup D}$ y, por eso, $A \vee D = B \vee D$, o bien $p \notin \overline{A \cup D}$, y en este caso, $A \vee D \prec\!\!\!\cdot\, B \vee D$. El teorema queda demostrado en una dirección.

Al contrario, sea L un retículo geométrico; S, un conjunto de átomos en L y $\bar{A} = \{a \in S \mid a \leqslant \sup A\}$ para todo $A \subseteq S$. Está claro que $A \to \bar{A}$ es un operador de clausura. Efectivamente, sea $a \in \bar{A}$. Para cada $A \subseteq S$ se cumple la desigualdad $a \leqslant \sup A$. Por lo tanto, $A \subseteq \bar{A}$. Si $A \subseteq \bar{B}$ para A, $B \subseteq S$, y

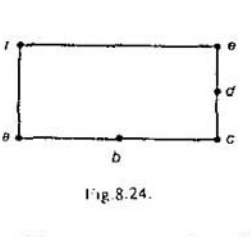

Fig.8.24.

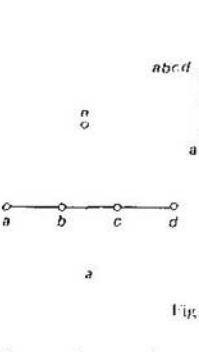

Fig.8.25.

$a \in A$, entonces $a \leqslant \sup B$. De aquí, $\sup A \leqslant \sup B$, y, por consiguiente, $A \subseteq B$.

La definición de retículo geométrico asegura el cumplimiento de las condiciones de base finita y de carácter cerrado de los subconjuntos de un solo elemento y del conjunto vacío. Comprobemos el cumplimiento de la propiedad de sustitución. Sea $p \in \overline{A \cup \{q\}}$ y $p \notin \overline{A}$. Por cuanto $\{q\}$ es un átomo, entonces, por ser el retículo semimodular $\overline{A \cup \{q\}} = (\overline{A} \vee \{q\}) \multimap \overline{A}$, por lo que de $A \subset \overline{A \cup \{p\}} \subseteq \overline{A \cup \{q\}}$ se deduce $\overline{A \cup \{p\}} = \overline{A \cup \{q\}}$; de este modo $q \in \overline{A \cup \{p\}}$. Con ello queda establecido que $(S, \bar{\ })$ es una geometría.

Demostremos ahora que los retículos son isomorfos. Denotemos con φ la aplicación $A \to \sup A$, donde $A \subseteq S$, $A \in L(G)$. Entonces ella aplica, pues, $L(G)$ en L. Por cuanto cada elemento del retículo L es una reunión de átomos, entonces la inclusión $A \subseteq B$ es equivalente a la desigualdad $A \leqslant \sup B$. Por eso φ es la aplicación biunívoca «sobre», y ambas aplicaciones φ y φ^{-1} son monótonas. Por consiguiente, φ es un isomorfismo. El teorema está demostrado.

Así pues, el retículo de un subespacio define por completo una geometría, y viceversa. Los diagramas de los retículos geométricos son, por regla general, muy engorrosos para que puedan utilizarse. Sin embargo, a menudo se presta la posibilidad de dibujar la geometría, asociando el dibujo con el retículo. Los elementos de rango k ($k \geqslant 0$) se denominarán k-superficies. En tal caso las 1-superficies se llamarán puntos; 2-superficies, rectas; 3-superficies, planos, etc. Observemos que un plano es una unión reticular de cualquier recta suya y un punto suyo no dispuesto en dicha recta, etc. Lo último puede formularse del modo siguiente:

(**) toda k-superficie y una 1-superficie, no situada en la primera, yacen en la única $(k + 1)$-superficie.

Al representar las geometrías, las rectas se dibujan en forma de segmentos (o las curvas). Dibujaremos sólo aquellas k-superficies, que no pueden

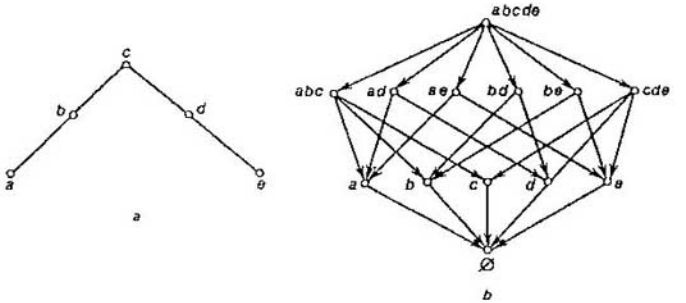

Fig.8.26.

ser restablecidas unívocamente según el dibujo, si sólo se emplea la propiedad (*). Aclaremos esto con un ejemplo. En la fig. 8.24 está representada una geometría de rango 3 con un conjunto de puntos $\{a, b, c, d, e, f, g\}$, con la particularidad de que las rectas *ad, ae, ag, bd, be, bf, bg, cf, cg, df, dg, eg* y los planos *abcg, afg, cdeg, efg, adg, aeg, bdg, beg, bfg, cfg, dfg* no están trazados, puesta que pueden obtenerse con ayuda de la propiedad (**).

En las figs. 8.25a . . . 8.28a están representadas las geometrías, y en las figs. 8.25b . . . 8.28b, los diagramas de sus retículos, respectivamente.

Hemos de notar que las representaciones de las geometrías son mucho más sencillas en comparación con los diagramas complejos de sus retículos.

Los matroides (o geometrías) surgen en gran cantidad, sobre todo en el álgebra, teoría de los grafos, geometría, teoría de las transversales, análisis combinatorio, etc. El estudio de ellos comenzó por el conocido problema de los siete puentes de Königsberg resuelto por Euler hace 200 años. La exposición de la teoría de los matroides la continuaremos en el § 8.4, donde daremos a conocer otros ejemplos de matroides y de sus aplicaciones.

Detengámonos brevemente en los resultados referentes a la anchura de los retículos geométricos enunciados a tenor con el teorema 1 (de Sperner).

Sea L un retículo geométrico finito. Designemos con $E(i)$ el conjunto

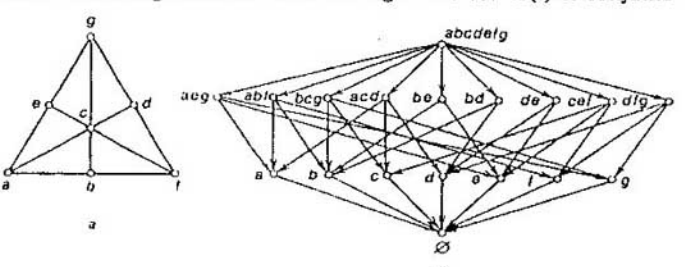

Fig.8.27.

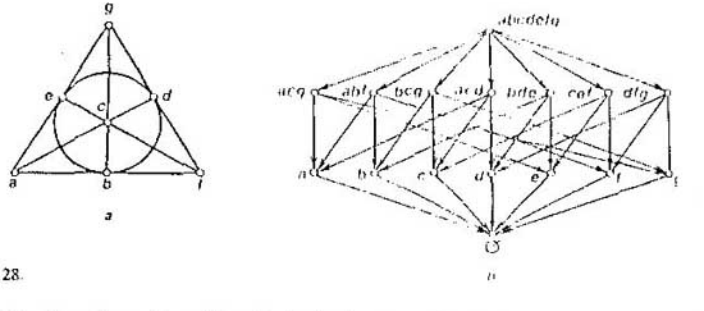

Fig.8.28.

de todos los elementos del retículo L de rango i, y sea

$$W_i = |E(i)|.$$

Observemos que el conjunto $E(i)$ es una anticadena del retículo L.

Teorema 37. Sea L un retículo geométrico finito en el cual todo elemento a de rango i se cubre por k_i elementos y cubre m_i elementos (los números k_i y m_i sólo dependen del rango i). Entonces, la anchura de L es igual a $\max\limits_{0 \leq i \leq r(L)} W_i$.

Demostración. Supongamos que $n = r(L)$ y $\max\limits_{0 \leq i \leq n} W_i = W_k$. En este caso $E(k)$ es una anticadena con W_k elementos. Resta por demostrar que si A es una anticadena arbitraria en L, entonces $|A| \leqslant W_k$. Para cualquier $a \in L$ designemos mediante $s(a)$ el número de todas las cadenas máximas que pasan por a. Es evidente que si $r(a) = i$, tendremos $s(a) = m_1 m_2 \ldots m_i k_i \ldots k_{n-1}$. Por consiguiente, $s(a)$ depende solamente del rango i. Por cuanto cada cadena máxima tiene exactamente un solo elemento de rango i, el número S de todas las cadenas máximas en L será igual a $s(a)\, W_i$. De aquí, la desigualdad $W_i \leqslant W_k$ nos dicta que $s(a) = \dfrac{S}{W_i} \geqslant \dfrac{S}{W_k}$. Por fin, cada cadena máxima pasa por un elemento a lo sumo de la anticadena A. Por consiguiente,

$$S \geqslant \sum_{a \in A} s(a) \geqslant |A| \cdot \frac{S}{W_k},$$

es decir, $|A| \leqslant W_k$, lo que se trataba de demostrar.

Un retículo geométrico finito L de rango n se llama *unimodal*, si para cierto número k se verifican las desigualdades $W_1 \leqslant \ldots \leqslant W_{k-1} \leqslant W_k$ y $W_k \geqslant W_{k+1} \geqslant \ldots \geqslant W_{n-1}$. Sean A y B unos subconjuntos del retículo L. Diremos que entre A y B existe una *paridad*, si existe una aplicación biunívoca φ: $A \to B$ (o bien φ: $B \to A$, si $|A| \geqslant |B|$), tal que para todo $a \in A$ (para todo $a \in B$, respectivamente) son comparables los elementos a y $\varphi(a)$.

Teorema 38. Sea L un retículo geométrico finito de rango n. Si L es uni-

modal y existe paridad entre $E(i)$ y $E(i+1)$ para todo $i<n$, entonces la anchura de L es igual a W_k, donde

$$W_1 \leqslant \ldots \leqslant W_k, \quad W_k \geqslant \ldots \geqslant W_{n-1}.$$

Demostración. Para cualquier subconjunto $A \subseteq L$ el número

$$d(A) = \max_{a,b \in A} (r(a) - r(b))$$

se denominará diámetro del subconjunto A. Sea A una anticadena del retículo L. La desigualdad $|A| \leqslant W_k$ se demostrará por inducción respecto del diámetro $d(A)$. Si $d(A) = 0$, entonces $A \subseteq E(i)$ para cierto i. De aquí, $|A| \leqslant W_i \leqslant W_k$. Supongamos ahora que $d(A) > 0$, y la desigualdad es válida para las anticadenas de menor diámetro. Por cuanto $d(A) > 0$, en la anticadena A siempre existe un elemento a, tal que $r(a) \neq k$; admitamos, para concretar, $r(a) < k$. Sea $i = \min_{a \in A} r(a)$, y $A = A_0 \cup A_1$, donde $A_1 = A \cap E(i)$ y $A_0 = A \setminus A_1$. Por hipótesis, $i < k$, por eso $|E(i)| \leqslant |E(i+1)|$, y, por lo tanto, existe una paridad $\varphi: E(i) \to E(i+1)$. Hagamos $A' = A_0 \cup \varphi(A_1)$. Los conjuntos A_0 y $\varphi(A_1)$ no se intersecan. En efecto, si $a \in (A_0 \cap \varphi(A_1))$, es decir, $a = \varphi(b)$ para cierto $b \in A_1$, entonces $a, b \in A$, $a \neq b$, y a, b son comparables, lo que es imposible, puesto que A es una anticadena. Por consiguiente, $|A'| = |A|$. Además, A' es una anticadena. En efecto, si $a, b \in A'$, $a \neq b$ y a, b son comparables, entonces $a \in A_0$ y $b = \varphi(A_1)$, es decir, $b = \varphi(c)$ para cierto $c \in A_1$. Por cuanto $r(b) = i + 1$, resulta que $r(b) < r(a)$. Por consecuencia, $b < a$, pero esto contradice la condición de que $c \leqslant b$ y $c \| a$. Esto quiere decir que A' es una anticadena. Pero, $d(A') = d(A) - 1$, por lo que, en virtud de la suposición de inducción, $|A| = |A'| \leqslant W_k$. El teorema está demostrado.

Aduzcamos sin demostración algunos resultados más sobre los números W_k en los retículos geométricos.

Teorema 39. Sea L un retículo geométrico finito de rango n. Entonces

$$W_1 \leqslant W_t \text{ para } t = 2, 3, \ldots, n-1$$

y

$$W_1 + \ldots + W_k \leqslant W_{n-k} + \ldots + W_{n-1} \text{ para } k = 1, 2, \ldots, n-2.$$

Teorema 40. Sea L un retículo geométrico finito de rango n. Entonces, cualquiera que sea $k = 1, \ldots, n-2$, la igualdad

$$W_1 + \ldots + W_k = W_{n-k} + \ldots + W_{n-1}$$

se verifica cuando y sólo cuando el retículo L es modular.

Teorema 41. Sea L un retículo geométrico modular finito de rango n. Entonces, para cualesquiera $0 \leqslant k \leqslant n$ se verifica la igualdad

$$W_k = W_{n-k}.$$

Ejercicios 19. Demuéstrese el teorema 1, haciendo uso del a) teorema 37; b) teorema 38.
20. Generalícese el teorema 37 a los conjuntos parcialmente ordenados.

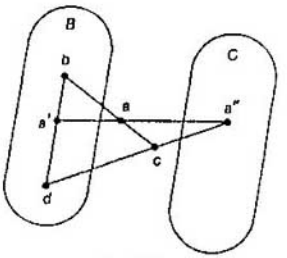

Fig.8.29.

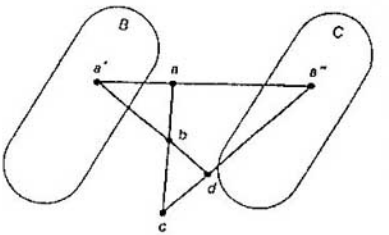

Fig.8.30.

En el capítulo 5 se ha analizado el *espacio proyectivo* como un par (A, L), donde A es un conjunto de puntos, y L, una familia de rectas, para la cual se cumplen las siguientes condiciones:

a) una recta $l \in L$ tiene no menos de dos puntos;

b) para cualesquiera dos puntos $a, b \in A$ existe sólo una recta $l \in L$, tal que $a, b \in l$;

c) para cualesquiera puntos $a, b, c, d, e \in A$ y rectas $l_1, l_2 \in L$, que satisfacen las condiciones: $a, b, d \in l_1$, y $b, c, e \in l_2$, existe un punto $f \in A$ y las rectas $l_3, l_4 \in L$, tales que $a, c, f \in l_3$, y $d, e, f \in l_4$.

Detengámonos ahora brevemente en la descripción del espacio proyectivo por medio de sus subespacios lineales. Para cualesquiera $a, b \in A$ (donde $a \neq b$) designemos con $a + b$ una recta que contiene los puntos a y b. Un subconjunto $B \subseteq A$ se denomina *subespacio lineal del espacio proyectivo*, si junto con cualesquiera dos puntos de B, le pertenece también una recta definida por los puntos citados. Dicho de otro modo, B es un espacio lineal, si $a, b \in B$ lleva consigo $a + b \subseteq B$. Sean B, C subespacios lineales. Pongamos $B + C$ igual a la unión de todas las rectas $b + c$, tales que $b \in B$, $c \in C$.

Lema 7. Para cualesquiera subespacios lineales B y C de un espacio proyectivo el conjunto $B + C$ es un subespacio lineal.

Demostración. Tomemos los puntos a, b y c, tales que $c \in a + b$, y $a, b \in B + C$. Demostremos que $c \in B + C$. Si $a, b \in B$, ó $a, b \in C$, tenemos: $c \in B \cup C \subseteq B + C$, puesto que B, C son subespacios lineales. Si $a \in B$ y $b \in C$ (o bien, viceversa), entonces por definición de $B + C$, $c \in B + C$. De este modo, podemos suponer que $a \notin B \cup C$, por lo que existen los puntos $a' \in B$ y $a'' \in C$, tales que $a \in a' + a''$. Son posibles dos casos. En el primero $b \in B \cup C$; sea, para concretar, $b \in B$. Veamos las rectas $b + a'$, $b + a$, $a + a'$ y $c + a''$ (véase fig. 8.29). Convengamos en considerar que todos los puntos b, a, a', a'' y c son dinstintos. Esto quiere decir que la recta $c + a''$ tiene un punto que yace tanto en $b + a$, como en $a + a''$. Por consiguiente, en virtud del punto c) en la definición de espacio proyectivo, existe un punto $d \in B$, tal que $d \in b + a'$, y $d \in c + a''$. Si $d = a''$, entonces $a \in B$, lo que es imposible. De aquí, $d \neq a''$, y por eso, $c \in d + a'' \in B + C$.

En el segundo caso $b \notin B \cup C$. Aprovechemos ahora la condición c) para las rectas $a + a'$, $a + b$, $a' + b$ y $a'' + c$ (véase fig. 8.30). Existe un punto $d \in a' + b$, tal que $c \in d + a''$. Por analogía con el primer caso tenemos $d \in B + C$, y, por lo tanto, $c \in B + C$. El lema está demostrado.

Teorema 42. Los subespacios lineales del espacio lineal forman un retículo geométrico modular.

Demostración. Por cuanto la intersección de cualquier número de subespacios lineales es un subespacio lineal, tenemos un espacio de clausuras $(A, \bar{\ })$. La clausura $\overline{X}$ del subconjunto $X \subseteq A$ se describe del modo siguiente: $\overline{X} = \bigcup_i X_i$, donde $X_0 = X$, $X_1 = X + X$, ..., $X_n = X_{n-1} + X_{n-1}$, ...

De aquí se deduce que $(A, \bar{\ })$ es un espacio de clausuras con las propiedades de una base finita. Por eso, sus subespacios lineales forman un retículo completo y para cualesquiera subespacios lineales X y Y queda válida la siguiente igualdad: $X \vee Y = \overline{X \cup Y}$.

Si X, Y, Z son subespacios lineales y $X \supseteq Z$, entonces, evidentemente, $X \wedge (Y \vee Z) \supseteq (X \wedge Y) \vee Z$. Mostremos que es válida también la inclusión inversa. Sea $p \in Y \vee Z$, es decir, $p \in X$ y $p \in Y \vee Z$. Por cuanto $p \in Y \vee Z = Y + Z$, existen los puntos $p' \in Y$ y $p'' \in Z$, tales que $p \in p' + p''$. De la inclusión $X \supseteq Z$ proviene que p, $(p'' \in X$. Si $p = p''$, entonces $p \in Z$, por lo que $p \in (X \wedge Y) \vee Z$. Si $p \neq p''$, entonces, $p' \in p + p'' \subseteq X$. Por consiguiente, $p' \in X \wedge Y$ y $p'' \in Z$; de aquí se desprende que $p \in (X \wedge Y) \vee Z$, con lo que queda demostrada la modularidad del retículo. Las propiedades restantes de la definición de pregeometría (matroide) o ya están comprobadas, o bien son triviales. La propiedad de sustitución se deduce de la modularidad. El teorema está demostrado.

Por consiguiente, los espacios proyectivos ofrecen ejemplos de matroides modulares y, de hecho, incluso de geometrías combinatorias modulares.

Dos elementos a y b de un retículo con complementos L se denominan *perspectivos*, si disponen de un complemento común, es decir, $a \vee c = b \vee c = 1$, y $a \wedge c = b \wedge c = 0$ para cierto elemento $c \in L$. El elemento c recibe el nombre de *eje de la perspectiva*.

Sea L un retículo modular con complementos, a, $b \in L$. Si a y b son perspectivos, el empleo sucesivo de las aplicaciones mencionadas en el teorema 26,

$$[0, a] = [a \wedge c, a] \to [c, a \vee c] = [c, b \vee c] \to [b \wedge c, b] = [0, b],$$

permite establecer un isomorfismo entre los intervalos $[0, a]$ y $[0, b]$, el cual se llama *aplicación perspectiva con el eje de la perspectiva* c y se designa con $P(a \to b; c)$. No es difícil comprender que $P(a \to b; c)$ aplica un elemento $x \in [0, a]$ sobre otro elemento $y = (x \vee c) \wedge b \in [0, b]$. Si L es un retículo compuesto por un conjunto vacío, los puntos y las rectas del plano proyectivo y por el propio plano, la aplicación perspectiva $P(a \to b; c)$ pone en correspondencia al punto x en la recta a y al punto y en la recta b (fig. 8.31). Preci-

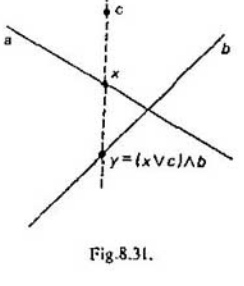

Fig.8.31.

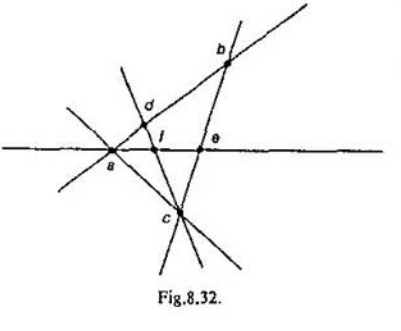

Fig.8.32.

samente a esta circunstancia se debe la denominación. Además, se ha establecido aquí que los intervalos $[0, a]$ y $[0, b]$ son proyectivos. Por eso, por analogía con la proyectividad de los intervalos, emplearemos, para la notación de los elementos perspectivos a y b, la designación $a \sim b$.

Lema 8. Sean a y b los puntos distintos (átomos) del retículo geométrico modular L. Entonces, $a \vee b$ contiene el tercer punto c cuando y sólo cuando a y b son perspectivos.

Demostración. Cualquier tercer punto en $a \vee b$ es un complemento relativo común para a y b en el intervalo $[0, a \vee b]$. En este caso, el elemento $c \vee (\overline{a \vee b}) = x$ será complemento común para a y b, cualquiera que sea el complemento $(\overline{a \vee b})$ del elemento $a \vee b$.

Viceversa, sean a y b perspectivos. Entonces, $1 = a \vee x = b \vee x$ cubre x. Pongamos $c = (a \vee b) \wedge x$. Tendremos

$$r(c) = r(a \vee b) + (r(x) - r(a \vee b \vee x)) = 2 - 1 = 1,$$

puesto que $a \vee b \vee x = 1$ cubre x. Quiere decir que $d \leqslant a \vee b$ es un punto, y además, distinto de a y b, puesto que $d \leqslant x$, y $a \wedge x = b \wedge x = 0$. Este es precisamente el tercer punto en $a \vee b$. El lema está demostrado.

Lema 9. En un retículo geométrico modular L la perspectividad es una relación de equivalencia.

Demostración. Es evidente que en cada retículo con complementos la perspectividad es una relación reflexiva y simétrica. Demostremos que en los retículos geométricos modulares la relación de perspectividad es también transitiva. En efecto, en virtud del lema 8, si $a \sim b$ y $b \sim c$, entonces (a excepción de un caso trivial en que $a = b$ ó $b = c$) existen los puntos d en $a \vee b$ y e en $b \vee c$, tales que se forma una configuración expuesta en la fig. 8.32. Construyamos ahora una «recta» $d \vee e$. Es evidente que

$$r((d \vee e) \wedge (a \vee c)) = r(d \vee e) + r(a \vee c) - r(d \vee e \vee a \vee c) \geqslant 2 + 2 - 3 = 1,$$

puesto que $d \vee e \vee a \vee c \leqslant a \vee b \vee c$. Esto significa que $d \vee e$ y $a \vee c$ tienen un punto común f. Pero, está claro que la recta $d \vee e$ no puede contener a, de lo

contrario ella contendría $a \vee d$, y, por consiguiente, el punto b, y junto con éste punto, $b \vee c$, y, por lo tanto, c, de donde se obtendría $r(a \vee b \vee c) = r(d \vee e) = 2$. De un modo análogo llegamos a que $d \vee e$ no puede contener c. Por eso, f es el tercer punto en $a \vee c$, y, de este modo, según el lema, tenemos $a \sim c$, lo que se trataba de demostrar.

De aquí se desprende que en cualquier retículo geométrico modular L la relación de perspectividad parte el conjunto de todos los puntos (átomos) del retículo en clases de equivalencia E_i, tales que para $a \in E_i$ y $b \in E_j$ se cumple la condición $a \sim b$, cuando y sólo cuando $i = j$.

Sean ahora $E_1, E_2, \ldots, E_k$ las clases de equivalencia que se componen de puntos recíprocamente perspectivos, y $a_i = \sup E_i$ para $i = 1, \ldots, k$.

Lema 10. En un retículo modular de dimensión finita con complementos los elementos a_i, que acabamos de encontrar, son independientes.

Demostración. Para demostrar la igualdad

$$(a_1 \vee \ldots \vee a_{n-1}) \wedge a_n = 0, \quad n = 2, 3, \ldots, k$$

es suficiente observar que ningún punto de a_n puede contenerse en $a_1 \vee \ldots \ldots \vee a_{n-1}$, puesto que E_i no se intersecan, y que todo elemento $x > 0$ contiene un punto del retículo. El lema queda demostrado.

De los teoremas 29 y 34, como también del lema 10, obtenemos el siguiente resultado importante.

Teorema 43. Cualquier retículo modular de longitud finita con complementos es un producto directo $[0, a_i]$, donde $a_i = \sup E_i$, y E_i son diferentes clases de relación de perspectividad de los puntos del retículo L.

Ejercicios. Demuéstrese que

21. Todo retículo geométrico es isomorfo al producto directo de retículos geométricos directamente indescomponibles.

22. Un retículo geométrico es directamente indescomponible cuando y sólo cuando cualesquiera dos átomos suyos son perspectivos.

23. En un retículo geométrico la relación de perspectividad de los puntos (átomos) es transitiva.

24. Los retículos geométricos distributivos son álgebras de Boole, y sólo álgebras de Boole, de rango finito.

25. La clase de retículos geométricos modulares está formada por productos directos de los retículos de espacios proyectivos y sólo por éstos.

Las afirmaciones de los ejercicios 21. . .23 caracterizan las propiedades estructurales de los retículos geométricos. Fueron obtenidas por primera vez por F.Maeda [117], y, en una forma más estricta, por Sasaki U. y Fujiwara S. [118]. Los resultados de los ejercicios 24. . .25 son características completas de las clases de retículos geométricos distributivos y de los retículos geométricos modulares (se obtienen con facilidad de los ejercicios 21. . .23). Las demostraciones de la mayoría de dichos resultados pueden hallarse en [1, 31, 32 y 116].

Los retículos L que para cualesquiera $a_0, a_1, a_2, b_0, b_1, b_2 \in L$ satisfacen la desigualdad

$$(a_0 \vee b_0) \wedge (a_1 \vee b_1) \wedge (a_2 \vee b_2) \leqslant ((c \vee a_1) \wedge a_0) \vee ((c \vee b_1) \wedge b_0),$$

donde $c = ((a_0 \vee a_1) \wedge (b_0 \vee b_1)) \wedge (((a_0 \vee a_2) \wedge (b_0 \vee b_2)) \vee ((a_1 \vee a_2) \wedge (b_1 \vee b_2)))$, se llaman *arguesanos*. Esta desigualdad representa una forma teórico-reticular del teorema de Desargues (véase teorema en el cap. 5). Efectivamente, tiene lugar el siguiente resultado:

Teorema 44. Un retículo geométrico modular L es arguesano cuando y sólo cuando en la geometría proyectiva, asociada con el retículo, es lícito el teorema de Desargues.

La demostración del teorema citado no es difícil, por lo cual se omite aquí. Los que desean, pueden encontrarla en [32]. En la misma obra se aduce la demostración del siguente resultado que representa el teorema bien conocido de la geometría.

Teorema 45. Sea L un retículo geométrico modular y supongamos que la geometría proyectiva, asociada con L, es regular (es decir, cada recta tiene no menos de tres puntos). Si el rango del retículo L no es inferior a 4, el retículo será arguesano.

Ejercicios. Demuéstrese que

26. La arguesidad de un retículo predetermina su modularidad.

27. Un conjunto parcialmente ordenado $B(S_n)$ (véase ejemplo 8 en el § 8.1) de todas las particiones no ordenadas del n = conjunto S_n es un retículo geométrico. Este retículo se llama, a menudo, belliano.

28. Un belliano $B(S_n)$ es modular, si y sólo si $n \leqslant 3$.

29. Cualquier retículo distributivo finito es encajable en un belliano.

Se denomina *representación* del retículo L a un encaje de dicho retículo en cierto belliano. Las representaciones de los retículos finitos es uno de los más antiguos problemas no resueltos por completo en la teoría de los retículos. Sólo para clases particulares de los retículos existen actualmente respuestas a este problema. El ejercicio 29, como también los teoremas 44 y 45, sirven de ilustración para algunos resultados en este sentido.

Hemos aclarado aquí sólo algunos de los aspectos de la teoría de los retículos. Para un estudio ulterior de esta teoría recomendamos los libros [31. . .33].

En conclusión de este párrafo detengámonos en las propiedades estructurales de resolución de algunos problemas de la optimización combinatoria. En el § 6.3, al analizar el algoritmo «ávido», hemos mostrado que él es correcto, es decir, resuelve correctamente cualquier problema concreto de optimización combinatoria sobre el sistema de conjuntos $\mathscr{S}$, cuando y sólo cuando $\mathscr{S}$ es un matroide, o bien, dicho de otro modo, forma un retículo geométrico (véanse los teoremas 2 del § 6.3 y 60 del § 8.4). Resulta que también muchos otros problemas de optimización combinatoria poseen propiedades estructurales muy interesantes. Mostremos esto, pero ante todo establezcamos el teorema de tipo de Jordan—Hölder para las funciones submodulares en los retículos distributivos.

Sea K un retículo distributivo con cero 0 y unidad 1. Recordemos que un booleano $\mathscr{P}(S)$, es decir, un conjunto de todos los subconjuntos de cierto conjunto finito S, forma un retículo distributivo en el que el cero 0 está

representado por un conjunto vacío $\varnothing$, y la unidad 1, por todo el conjunto S. Una función real μ, definida en K, se denomina submodular, si para todos los $x, y \in K$ se cumple la desigualdad

$$\mu(x) + \mu(y) \geqslant \mu(x \vee y) + \mu(x \wedge y).$$

Si para todos los $x, y \in K$ es válida la igualdad

$$\mu(x) + \mu(y) = \mu(x \vee y) + \mu(x \wedge y),$$

la función μ se denomina *modular*. Son funciones submodulares, por ejemplo, las dimensiones de los subespacios en espacios vectoriales y en las geometrías proyectivas, las funciones de rango en los matroides y polimatroides [128. . .132], la potencia de los subconjuntos u otras. Más aún, las funciones de dimensión de los subespacios en los espacios vectoriales y en las geometrías proyectivas son funciones modulares.

Supongamos que μ es una función submodular sobre un retículo distributivo K con cero 0 y unidad 1; L, un subretículo del retículo K con elemento mínimal a^- y elemento maximal a^+, y que

$$\mathscr{S} = \{[a_i, a_{i+1}] \mid i = 1, 2, \ldots, n-1\},$$

donde $a^- = a_1, a_2, \ldots, a_{n-1}, a_n = a^+$ es una cadena máxima arbitraria que en el subretículo L va de a^- a a^+. En cada uno de los intervalos de la familia $\mathscr{S}$ definamos, para todo $x \in [a_i, a_{i+1}]$ y $i = 1, 2, \ldots, n-1$, una función μ_i, al poner

$$\mu_i(x) = \mu(x) - \mu(a_i).$$

Además, si los intervalos $[0, a^-]$ y $[a^+, 1]$ no son conjuntos vacíos, entonces, pongamos, para $x \in [0, a^-]$, $\mu^-(x) = \mu(x)$, y para $x \in [a^+, 1]$, $\mu^+(x) = \mu(x) - \mu(a^+)$.

Elijamos ahora en L alguna otra cadena máxima que va de a^- a a^+, por ejemplo, $a^- = a_1', a_2', \ldots, a_{n-1}', a_n' = a^+$, y definamos, para todo $x \in [a_i', a_{i+1}']$, $i = 1, 2, \ldots, n-1$, una función

$$\mu_i'(x) = \mu(x) - \mu(a_i').$$

Resulta fácil comprobar que las funciones μ_i y μ_i', definidas más arriba, son submodulares.

En virtud del teorema 27, existe una permutación τ de índices $\{1, 2, \ldots, n-1\}$, definida unívocamente, tal que para todo i, $i = 1, 2, \ldots, n-1$, tiene lugar la correlación $[a_i, a_{i+1}] \sim [a_{\tau(i)}', a_{\tau(i)+1}']$.

Sea π_i: $[a_i, a_{i+1}] \to [a_{\tau(i)}', a_{\tau(i)+1}']$ un isomorfismo natural condicionado por la proyectividad de los intervalos de la cadena del retículo. Diremos que para una función submodular μ sobre K *se cumple la condición* (***), si para cualesquiera dos cadenas máximas de a^- a a^+ del subretículo L, a saber: $a^- = a_1, a_2, \ldots, a_{n-1}, a_n = a^+$ y $a^- = a_1' a_2', \ldots, a_{n-1}', a_n' = a^+$, se verifica, para todo $x \in [a_i, a_{i+1}]$, donde $i = 1, 2, \ldots, n-1$, la igualdad

$$\mu_i(x) = \mu(x) - \mu(a_i) = \mu(\pi_i(x)) - \mu(a_{\tau(i)}') = \mu_{\tau(i)}'(\pi_i(x)).$$

En otras palabras, la condición (***) significa que la definición de una «nueva» función submodular μ_l no depende en cierto sentido de la elección de la cadena máxima en un subretículo del retículo distributivo K.

Lema 11. Sean a, b unos elementos arbitrarios del subretículo L, tales que $\mu(a) + \mu(b) = \mu(a \vee b) + \mu(a \wedge b)$, donde μ es una función submodular sobre el retículo distributivo K. Entonces, para todo $x \in [a \wedge b,\ a \vee b]$ se verifican las desigualdades:

$$1)\ \mu(x) + \mu(a) = \mu(x \vee a) + \mu(x \wedge a);$$
$$2)\ \mu(x) + \mu(b) = \mu(x \vee b) + \mu(x \wedge b);$$
$$3)\ \mu(x \wedge a) + \mu(x \wedge b) = \mu(x) + \mu(a \wedge b);$$
$$4)\ \mu(x \vee a) + \mu(x \vee b) = \mu(a \vee b) + \mu(x);$$

Demostración. Por ser la función μ submodular, tenemos

$$\mu(x \wedge a) + \mu(x \wedge b) \geqslant \mu((x \wedge a) \vee (x \wedge b)) + \mu((x \wedge a) \wedge (x \wedge b))$$

y

$$\mu(x \vee a) + \mu(x \vee b) \geqslant \mu((x \vee a) \vee (x \vee b)) + \mu((x \vee a) \wedge (x \vee b)).$$

Por cuanto $x \in [a \wedge b,\ a \vee b]$, entonces $(x \wedge a) \vee (x \wedge b) = x \wedge (a \vee b) = x$; $(x \vee a) \wedge (x \vee b) = x \vee (a \wedge b) = x$ (aquí se han aprovechado la propiedad de distributividad de las operaciones reticulares y el hecho de que $x \leqslant a \vee b$, y $x \geqslant a \wedge b$) y $(x \wedge a) \wedge (x \wedge b) = x \wedge (a \wedge b) = a \wedge b$, $(x \vee a) \vee (x \vee b) = x \vee (a \vee b) = a \vee b$ (aquí se han aprovechado las propiedades de asociatividad, conmutatividad e idempotencia de las operaciones reticulares y el hecho de que $x \geqslant a \wedge b$, y $x \leqslant a \vee b$). Por consiguiente,

$$\mu(x \wedge a) + \mu(x \wedge b) \geqslant \mu(x) + \mu(a \wedge b),$$
$$\mu(x \vee a) + \mu(x \vee b) \geqslant \mu(a \vee b) + \mu(x).$$

Además, por ser submodular μ, tenemos:

$$\mu(x) + \mu(a) \geqslant \mu(x \vee a) + \mu(x \wedge a)$$
$$\mu(x) + \mu(b) \geqslant \mu(x \vee b) + \mu(x \wedge b).$$

Sumemos las últimas cuatro desigualdades y obtendremos

$$\mu(a) + \mu(b) \geqslant \mu(a \vee b) + \mu(a \wedge b),$$

pero, por hipótesis del lema, $\mu(a) + \mu(b) = \mu(a \vee b) + \mu(a \wedge b)$. Por consiguiente, en todas las cuatro desigualdades los segundos miembros son iguales a los primeros. El lema está demostrado.

Lema 12. Sea L un subretículo del retículo distributivo finito L, tal que para todos los a, $b \in L$ se verifica la igualdad

$$\mu(a) + \mu(b) = \mu(a \vee b) + \mu(a \wedge b).$$

Entonces, para todo par de intervalos proyectivos $[a, a']$ y $[b, b']$, donde a, a', b, $b' \in L$, y para cada $x \in [a, a']$ resulta válida la igualdad $\mu(x) -$

$- \mu(\pi(x)) = \mu(a) - \mu(b) = \mu(a') - \mu(b')$, donde π es un isomorfismo natural de $[a, a']$ en $[b, b']$ condicionado por la proyectividad de los intervalos.

Demostración. Si demostramos la validez del lema para los intervalos transpuestos, entonces, en virtud de la definición de intervalos proyectivos, el lema será válido también para cualquier par de intervalos. Por eso, demostremos el lema para los intervalos transpuestos. Sea $a, b \in L$. En virtud del teorema 26, la aplicación $\varphi(x) = x \wedge a = y$, definida para todo $x \in [b, a \vee b]$, prefija una aplicación isomorfa del intervalo $[b, a \vee b]$ en $[a \wedge b, a]$. Debido a la igualdad 3), del lema 11 tenemos, para todo $x \in [b, a \vee b]$:

$$\mu(a \wedge b) + \mu(x) = \mu(x \wedge a) + \mu(x \wedge b) = \mu(\varphi(x)) + \mu(b).$$

De aquí, $\mu(x) - \mu(\varphi(x)) = \mu(b) - \mu(a \wedge b) = \mu(a \vee b) - \mu(a)$. De este modo, el lema es lícito para cualesquiera intervalos transpuestos $[b, a \vee b]$ y $[a \wedge b, a]$. Con ello queda demostrado el lema.

Directamente del lema 12 y del teorema 27 obtenemos el siguiente resultado importante.

Teorema 46 (*del tipo de Jordan—Hölder para funciones submodulares sobre un retículo distributivo*). Sea L un subretículo del retículo distributivo finito K, y sea μ una función submodular sobre K. La condición (***) para la función submodular μ tiene lugar cuando y sólo cuando para todos los $a, b \in L$ se verifica la igualdad

$$\mu(a) + \mu(b) = \mu(a \wedge b) + \mu(a \vee b)$$

El subretículo L del retículo distributivo K se denomina *μ-esqueleto*, si la función submodular μ, definida sobre K, es modular en L, es decir, si para todos los $a, b \in L$ se cumple la igualdad

$$\mu(a) + \mu(b) = \mu(a \vee b) + \mu(a \wedge b).$$

De este modo, el teorema 46 afirma que la condición (***) para una función submodular μ se cumple cuando y sólo cuando el subretículo L es un μ-esqueleto.

Supongamos que S es un conjunto finito; μ, una función submodular definida sobre $\mathfrak{P}(S)$; L, un μ-esqueleto del booleano $\mathfrak{P}(S)$; $(S^-, \{F \mid F \in \mathcal{F}\}, S^+)$, una partición del conjunto S (véase el corolario 2) que no depende de la elección de la cadena máxima de S^- a $S - S^+$ en el subretículo L, donde S^- es el elemento minimal, y $S - S^+$, el elemento maximal del subretículo L. Entonces, en virtud del teorema 46, cada cadena máxima $S^- = A_1, A_2, \ldots, A_{n-1}, A_n = S - S^+$ en L prefija un mismo conjunto $\{\mu^-, \{\mu^F \mid F \in \mathcal{F}\}, \mu^+\}$ de funciones submodulares, donde

$$\mu^-(X) = \mu(X) \text{ para } X \subseteq S^-;$$

$$M^F(X) = \mu(X \cup A_i) - \mu(A_i) \text{ para } X \subseteq A_{i+1} - A_i = F \in \mathcal{F}, \text{ donde}$$

$$i = 1, \ldots, n-1;$$

$$\mu^+(X) = \mu(X \cup (S - S^+)) - \mu(S - S^+) \text{ para } X \subseteq S^+.$$

De aquí llegamos al siguiente

Corolario 6. Sea μ una función submodular sobre el booleano $\mathcal{P}(S)$. Si L es un μ-esqueleto, entonces la familia $\{\mu^-, \{\mu^F \mid F \in \mathcal{S}\}, \mu^+\}$ de funciones submodulares no depende de la elección de las cadenas máximas en el subretículo L.

Las propiedades de los μ-esqueletos de retículos distributivos se examinan en [128]. No vamos a detenernos en ellas y pasemos al análisis de los problemas de optimización combinatoria enunciados en términos de minimización de la función submodular μ sobre el retículo distributivo K:

$$\mu(x) = \sum_{i=1}^{m} c_i \mu_i(x),$$

donde $\mu_i(x)$ es una función submodular sobre el retículo distributivo K, y c_i, unos coeficientes reales positivos, $i = 1, 2, \ldots, m$.

Proposición 1. Sea $\min \{\mu(x) \mid x \in K\} = w$, $\mu(y_1) = \mu(y_2) = w$. Entonces, $\mu(y_1 \vee y_2) = \mu(y_1 \wedge y_2) = w$.

Demostración. Tenemos $2w = \mu(y_1) + \mu(y_2) = \sum_{i=1}^{m} c_i \mu_i(y_1) + \sum_{i=1}^{m} c_i \mu_i(y_2) = \sum_{i=1}^{m} c_i(\mu_i(y_1) + \mu_i(y_2)) \geqslant$ (por ser las funciones μ_i submodulares) $\geqslant \sum_{i=1}^{m} c_i(\mu_i(y_1 \vee y_2) + \mu_i(y_1 \wedge y_2)) = \sum_{i=1}^{m} c_i \mu_i(y_1 \vee y_2) + \sum_{i=1}^{m} c_i \mu_i(y_1 \wedge y_2) = \mu(y_1 \vee y_2) + \mu(y_1 \wedge y_2) \geqslant$ (puesto que w es el valor mínimo de $\mu(x)$) $\geqslant w + w = 2w$.

Por cuanto $\mu(y_1 \vee y_2) + \mu(y_1 \wedge y_2) = 2w$, $\mu(y_1 \vee y_2) \geqslant w$, y $\mu(y_1, y_2) \geqslant w$, entonces, $\mu(y_1 \vee y_2) = \mu(y_1 \wedge y_2) = w$.

De la desigualdad

$$\sum_{i=1}^{m} c_i(\mu_i(y_1) + \mu_i(y_2)) = \sum_{i=1}^{m} c_i(\mu_i(y_1 \vee y_2) + \mu_i(y_1 \wedge y_2)),$$

tenemos (en virtud de que para todo $i = 1, 2, \ldots, m$, los coeficientes $c_i > 0$):

$$\mu_i(y_1) + \mu_i(y_2) = \mu_i(y_1 \vee y_2) + \mu_i(y_1 \wedge y_2).$$

Llegamos, pues, al

Corolario 7. Una familia L de todos los elementos del retículo distributivo K, sobre los cuales la función submodular $\mu(x)$ alcanza su valor mínimo, forma un μ-esqueleto del retículo K. Más aún, el subretículo L es también μ_i-esqueleto del retículo K para todo $i = 1, 2, \ldots, m$.

El $(\mu_1, \ldots, \mu_m)$-esqueleto L del retículo K obtenido, depende, evidentemente, no sólo de las funciones submodulares μ_i, sino también de los coeficientes positivos c_i. Por eso, el esqueleto L del retículo K se denotará también con $L(c_1, \ldots, c_m)$, subrayando su dependencia de $c_1, c_2, \ldots, c_m$.

Es obvio que para todo $\lambda > 0$ tenemos la igualdad

$$L(\lambda c_1, \lambda c_2, \ldots, \lambda c_m) = L(c_1, c_2, \ldots, c_m).$$

Veamos un símplice $(m-1)$-dimensional S^{m-1} [124], en el cual cada

punto tiene las coordenadas $\left(\frac{c_1}{c_0}, \frac{c_2}{c_0}, \ldots, \frac{c_m}{c_0}\right)$, donde $c_0 = c_1 + \ldots + c_m$. Entonces, el esqueleto L del retículo K puede considerarse como función en el símplice S^{m-1} con valores en la familia de todos los subretículos del retículo distributivo K. Observemos que en este caso el conjunto de puntos en S^{m-1}, a los cuales corresponde un retículo fijo del retículo K, forma un poliedro convexo [124]. Además, si los poliedros, correspondientes a los esqueletos L_1 y L_2, tienen una arista común en S^{m-1}, entonces el subretículo generado por los elementos de $L_1 \cup L_2$ es el esqueleto del retículo K correspondiente a dicha arista común. Así pues, el símplice $(m-1)$-dimensional S^{m-1} está dotado de la estructura del complejo poliédrico.

Si algunas de las funciones submodulares $\mu_i(x)$ son monótonas, la estructura del complejo poliédrico puede caracterizarse de un modo aún más detallado.

En efecto, supongamos que $\mu_1, \mu_2, \ldots, \mu_p$ son funciones submodulares no decrecientes, y $\mu_{p+1}, \mu_{p+2}, \ldots, \mu_q$, funciones submodulares no crecientes sobre un retículo distributivo K. Veamos dos vértices (es decir, aristas 0-dimensionales) del complejo, cuyas coordenadas $(c_1, c_2, \ldots, c_m)$ y $(c_1', c_2', \ldots, c_m')$ son de tal género que

$$\begin{aligned} c_i &\geqslant c_i' \quad \text{para } i = 1, 2, \ldots, p; \\ c_i &\leqslant c_i' \quad \text{para } i = p+1, \ldots, q; \\ c_i &= c_i' \quad \text{para } i = q+1, \ldots, m. \end{aligned}$$

Sea $w = \min \left\{ \sum_{i=1}^{m} c_i \mu_i(x) \mid x \in K \right\}$, y $w' = \min \left\{ \sum_{i=1}^{m} c_i' \mu_i(x) \mid x \in K \right\}$.

Proposición 2. Si $y \in L(c_1, \ldots, c_m)$ e $y' \in L(c_1', \ldots, c_m')$, entonces

$$y \wedge y' \in L(c_1, \ldots, c_m), \; y \vee y' \in L(c_1', \ldots, c_m')$$

y para todo i, $i = 1, \ldots, m$, se verifican las igualdades

$$\mu_i(y) + \mu_i(y') = \mu_i(y \vee y') + \mu_i(y \wedge y').$$

Demostración. Si $y \in L(c_1, \ldots, c_m)$ e $y' \in L(c_1', \ldots, c_m')$, entonces

$$\sum_{i=1}^{m} c_i \mu_i(y) = w \text{ y } \sum_{i=1}^{m} c_i' \mu_i(y') = w'.$$

Por consiguiente, $w + w' = \sum_{i=1}^{m} c_i \mu_i(y) + \sum_{i=1}^{m} c_i' \mu_i(y') = \sum_{i=1}^{p} [(c_i - c_i')\mu_i(y) + c_i'(\mu_i(y) + \mu_i(y'))] + \sum_{i=p+1}^{q} [c_i(\mu_i(y) + \mu_i(y')) + (c_i' - c_i)\mu_i(y')] + \sum_{i=q+1}^{m} c_i(\mu_i(y) + \mu_i(y')) \geqslant$ (por ser submodulares las funciones $\mu_i(x)$) $\geqslant \sum_{i=1}^{p} [(c_i - c_i')\mu_i(y) + c_i'(\mu_i(y \vee y') + \mu_i(y \wedge y'))] + \sum_{i=p+1}^{q} [c_i(\mu_i(y \vee y') + \mu_i(y \wedge y')) + (c_i' - c_i)\mu_i(y')] + \sum_{i=q+1}^{m} c_i(\mu_i(y \vee y') + \mu_i(y \wedge y')) =$ (sumemos y reste-

mos de las sumas obtenidas $\sum_{i=1}^{p} c_i\mu_i(y\wedge y')$ y $\sum_{i=p+1}^{q} c_i'\mu_i(y\vee y'))$ =

$$= \sum_{i=1}^{m} c_i\mu_i(y \wedge y') + \sum_{i=1}^{m} c_i'\mu_i(y \vee y') + \sum_{i=1}^{p} [(c_i - c_i')\mu_i(y) + c_i'\mu_i(y\wedge y') -$$

$$- c_i\mu_i(y \wedge y')] + \sum_{i=p+1}^{q} [(c_i' - c_i)\mu_i(y') + c_i\mu_i(y \vee y') - c_i'\mu_i(y \vee y')] =$$

$$= \sum_{i=1}^{m} c_i\mu_i(y \wedge y') + \sum_{i=1}^{m} c_i'\mu_i(y \vee y') + \sum_{i=1}^{p} (c_i - c_i')(\mu_i(y) - \mu_i(y \wedge y')) +$$

$$+ \sum_{i=p+1}^{q} (c_i' - c_i)(\mu_i(y') - \mu_i(y\vee y') \geqslant$$

(en virtud de que para $i = 1, 2, \ldots, p$ se verifican las desigualdades $c_i - c_i' \geqslant 0$, y $\mu_i(y) - \mu_i(y\wedge y') \geqslant 0$, puesto que μ_i es una función submodular no decreciente e $y \geqslant y\wedge y'$ en el retículo K; y para $i = p + 1, \ldots, q$ se verifican las desigualdades $c_i' - c_i \geqslant 0$, y $\mu_i(y') - \mu_i(y\vee y') \geqslant 0$, puesto que μ_i son funciones submodulares no crecientes e $y' \leqslant y\vee y'$ en el retículo K, y, por consiguiente, en virtud de que la segunda y tercera sumas en la última expresión son no negativas) $\geqslant \sum_{i=1}^{m} c_i\mu_i(y\wedge y') + \sum_{i=1}^{m} c_i'\mu_i(y\vee y') \geqslant w + w'$, puesto que $w =$

$= \min \left\{ \sum_{i=1}^{m} c_i\mu_i(x) \mid x\in K \right\}$ y $w' = \min \left\{ \sum_{i=1}^{m} c_i'\mu_i(x) \mid x\in K \right\}$.

De aquí, por cuanto las expresiones primera y última son iguales, tenemos

$$\sum_{i=1}^{m} c_i\mu_i(y\wedge y') + \sum_{i=1}^{m} c_i'\mu_i(y\vee y') = w + w'.$$

Por consiguiente, puesto que

$$w = \min \left\{ \sum_{i=1}^{m} c_i\mu_i(x) \mid x\in K \right\} \text{ y } w' = \min \left\{ \sum_{i=1}^{m} c_i'\mu_i(x) \mid x\in K \right\},$$

llegamos a que $\sum_{i=1}^{m} c_i\mu_i(y\wedge y') = w$, y $\sum_{i=1}^{m} c_i'\mu_i(y\vee y') = w'$. De este modo, hemos establecido que $y\wedge y' \in L(c_1, \ldots, c_m)$ e $y\vee y' \in L(c_1', \ldots, c_m')$. Además, queda demostrado que

$$\sum_{i=1}^{m} c_i\mu_i(y) + \sum_{i=1}^{m} c_i'\mu_i(y') = \sum_{i=1}^{m} c_i\mu_i(y\wedge y') + \sum_{i=1}^{m} c_i'\mu_i(y\vee y')$$

y también

$$\sum_{i=1}^{p} c_i(\mu_i(y) + \mu_i(y')) + \sum_{i=p+1}^{q} c_i(\mu_i(y) + \mu_i(y')) + \sum_{i=q+1}^{m} c_i(\mu_i(y) +$$

$$+ \mu_i(y')) = \sum_{i=1}^{p} c_i(\mu_i(y\vee y') + \mu_i(y\wedge y')) + \sum_{i=p+1}^{q} c_i(\mu_i(y\vee y') +$$

$$+ \mu_i(y\wedge y')) + \sum_{i=q+1}^{m} c_i\mu_i(y\vee y') + \mu(y\wedge y')).$$

Teniendo presente la última igualdad, la submodularidad de las funciones $\mu_i(x)$ y el hecho de que $c_i > 0$, $c_i' > 0$, llegamos a que para todos los i, $i = 1, 2, \ldots, m$ son válidas las igualdades

$$\mu_i(y) + \mu_i(y') = \mu_i(y \vee y') + \mu_i(y \wedge y').$$

La proposición está demostrada.

Directamente de la proposición 2 se deduce el

Corolario 8. El conjunto $L(c_1, \ldots, c_m) \cup L(c_1', \ldots, c_m')$ constituye un $(\mu_1, \ldots, \mu_m)$-esqueleto del retículo K.

Al demostrar la proposición 2, se ha establecido que

$$\sum_{i=1}^{p} (c_i - c_i')[\mu_i(y) - \mu_i(y \wedge y')] = 0,$$

$$\sum_{i=p+1}^{q} (c_i' - c_i)[\mu_i(y') - \mu_i(y \vee y')] = 0.$$

De aquí, en virtud de que para todo i, $i = 1, 2, \ldots, p$, $c_i \geqslant c_i'$ y μ_i son funciones submodulares no decrecientes y de que para todo i, $i = p + 1, \ldots, q$, $c_i \leqslant c_i'$ y μ_i son funciones submodulares no crecientes, tenemos

$$(c_i - c_i')(\mu_i(y) - \mu_i(y \wedge y')) \text{ para } i = 1, 2, \ldots, p,$$
$$(c_i' - c_i)(\mu_i(y') - \mu_i(y \vee y')) \text{ para } i = p + 1, \ldots, q.$$

Si para $i = 1, 2, \ldots, p$ ponemos $c > c_i'$, obtendremos que $\mu_i(y) = \mu_i(y \wedge y')$. Análogamente, si para $i = p + 1, \ldots, q$ ponemos $c_i' > c_i$, resultará que $\mu_i(y') = \mu_i(y \vee y')$. De este modo, para $i = 1, 2, \ldots, p$, si $c_i > c_i'$ y μ_i son funciones submodulares estrictamente decrecientes, tenemos $y = y \wedge y'$, y para $i = p + 1, \ldots, q$, si $c_i' > c_i$ y μ_i son funciones submodulares estrictamente crecientes, entonces $y' = y \vee y'$. En otras palabras, esto quiere decir que todos los elementos del esqueleto $L(c_1, \ldots, c_m)$ son inferiores o iguales a los elementos del esqueleto $L(c_1', \ldots, c_m')$ respecto del orden del retículo K.

Así pues, la proposición 2 y el corolario 8 permiten obtener, a partir de las soluciones ya conocidas de dos diferentes problemas de optimización, nuevas soluciones para cada uno de los mismos. Si $\mu_i(x)$ son funciones submodulares en el booleano $\mathscr{P}(S)$, el conjunto de soluciones del problema de minimización de la función $\mu(x) = \sum_{i=1}^{m} c_i \mu_i(x)$, donde $c_i > 0$, forma un subretículo L del booleano $\mathscr{P}(S)$ (corolario 7). Cada cadena máxima que une los elementos minimal y maximal de L prefija las particiones del conjunto S (corolario 2) y de la función submodular $\mu(x)$ (corolario 6), las cuales no dependen de la elección de la cadena máxima. Esto resulta ser útil al resolver problemas prácticos (véanse [128...132 y 136]).

8.3. FUNCIONES DE INCIDENCIA E INVERSIÓN DE MOEBIUS

Sea P un conjunto parcialmente ordenado y localmente finito y sea K un campo de característica 0 (comúnmente, el campo de números reales). Estudiemos la clase $A(P)$ de funciones $f(x, y)$ que toman valores en el campo K y que están definidas para todos los $x, y \in P$. Exijamos que $f(x, y) = 0$, si no se cumple la condición $x \leqslant y$. La suma de tales dos funciones, como también la multiplicación por los escalares, se definirán del modo siguiente:

$$(f + g)(x, y) = f(x, y) + g(x, y);$$

$$(\alpha \cdot f)(x, y) = \alpha \cdot f(x, y);$$

y el producto (o convolución) $f*g$, del modo siguiente:

$$(f*g)(x, y) = \sum_{z:\, x \leq z \leq y} f(x, z)g(z, y).$$

El producto citado está definido correctamente, puesto que por ser el conjunto P localmente finito, el número de sumandos en el segundo miembro es finito y $(f*g)(x, y) = 0$ cada vez que $x \not\leqslant y$.

Un conjunto $A(P)$ con operaciones de adición, multiplicación (o convolución) y multiplicación por escalares recibe el nombre de *álgebra de incidencia* del conjunto parcialmente ordenado P sobre K, mientras que los elementos de dicho conjunto se llaman funciones de incidencia del conjunto P.

No es difícil notar que la multiplicación de las funciones de incidencia es asociativa y distributiva, mientras que de elemento neutro con relación a la multiplicación (convolución) sirve la función de Kronecker (o función delta):

$$\delta(x, y) = \begin{cases} 1, \text{ si } x = y; \\ 0, \text{ en el caso contrario.} \end{cases}$$

Demostremos, por ejemplo, que la operación de multiplicación (convolución) es asociativa. Sea $f, g, h \in A(P)$. Entonces,

$$(f*(g*h)) = \sum_{z:\, x \leq z \leq y} f(x, z)(g*h)(z, y) = \sum_{z:\, x \leq z \leq y} f(x, z) \left(\sum_{t:\, z \leq t \leq y} g(z, t)h(t, y) \right) =$$

$$= \sum_{t:\, x \leq t \leq y} \left(\sum_{z:\, x \leq z \leq y} f(x, z)g(z, t) \right) h(t, y) = \sum_{t:\, x \leq t \leq y} (f*g)(x, t)h(t, y) =$$

$$= ((f*g)*h)(x, y).$$

En vista de las observaciones citadas, se ve que el álgebra de incidencia es realmente un álgebra asociativa sobre el campo K. Además, $A(P)$ es conmutativa cuando y sólo cuando el conjunto parcialmente ordenado P es una anticadena, es decir, cuando dicho conjunto está ordenado de un modo trivial.

Teorema 47. Una función de incidencia f en $A(P)$ tiene funciones inver-

sas tanto izquierda, como derecha, cuando y sólo cuando $f(x, x) \neq 0$ para todo $x \in P$. Más aún, las funciones inversas derecha e izquierda coinciden.

Demostración. Sea

$$\sum_{x \leq z \leq y} f(x, z)g(z, y) = \delta(x, y).$$

Por cuanto $1 = \delta(x, x) = f(x, x)g(x, x)$ para todo x de P, la condición $f(x, x) \neq 0$ para todo $x \in P$ será, evidentemente, necesaria.

Viceversa, sea $f(x, x) \neq 0$ para todo $x \in P$. Entonces, $g(x, x) = \dfrac{1}{f(x, x)}$ para todo $x \in P$. Hallemos, ahora, $g(x, y)$ para $x < y$. Supongamos, sin restringir la generalidadde los razonamientos, que ya tenemos los valores de $g(z, y)$ para todos los z tales que $x < z \leqslant y$. Para $x < y$ tenemos

$$(f*g)(x, y) = \delta(x, y) = 0 = \sum_{x \leq z \leq y} f(x, z)g(z, y),$$

y, por consiguiente,

$$-f(x, x)g(x, y) = \sum_{x < z \leq y} f(x, z)g(z, y).$$

De aquí podemos hallar $g(x, y)$, puesto que $f(x, x) \neq 0$, y todos los sumandos de la suma finita en el segundo miembro de la última igualdad son conocidos. Así pues, no sólo hemos demostrado que f tiene función inversa derecha, sino que obtuvimos también la fórmula recurrente para su cálculo.

Análogamente, de la relación $(g*f)(x, y) = \delta(x, y)$ obtenemos la fórmula recurrente para determinar la función inversa izquierda para f.

Supongamos ahora que g_1 y g_2 son funciones inversas para f de $A(P)$, derecha e izquierda, respectivamente, es decir, $f*g_1 = g_2*f = \delta$. Por ser asociativa la multiplicación de las funciones de incidencia, $g_2 = g_2*\delta = g_2*(f*g_1) = (g_2*f)*g_1 = \delta*g_1 = g_1$, es decir, las funciones inversas izquierda y derecha coinciden. La demostración queda terminada.

Una función, inversa de f, se denotará con f^{-1}. Introduzcamos, además, las siguientes designaciones: $f^0 = \delta$, $f^1 = f$, $f^2 = f*f$, $f^3 = f*f^2$, . . . , $f^k = f*f^{k-1}$, . . . y $f^{-k} = (f^{-1})^k$.

Además de la función de Kronecker $\delta(x, y)$, ya analizada, se destacan a menudo, entre otras funciones de incidencia en $A(P)$, las siguientes:

$$\text{zeta-función } \zeta(x, y) = \begin{cases} 1, \text{ si } x \leqslant y; \\ 0, \text{ en el caso contrario;} \end{cases}$$

$$\text{lambda-función } \lambda(x, y) = \begin{cases} 1, \text{ si } x = y, \text{ o bien } y \text{ cubre } x; \\ 0, \text{ en el caso contrario;} \end{cases}$$

función de cadenas (eta-función)

$$\eta(x, y) = \zeta(x, y) - \delta(x, y);$$

función de recubrimiento (kappa-función)

$$\varkappa(x, y) = \lambda(x, y) - \delta(x, y);$$

función de Moebius (my-función)

$$\mu(x, y) = \zeta^{-1}(x, y);$$

función de longitud (rho-función)

$\varrho(x, y) = l(x, y)$, donde $l(x, y)$ es la longitud del intervalo $[x, y]$ en P. Las razones, por las que se destacan dichas funciones y sus denominaciones se harán claras, si estudiamos las propiedades de estas funciones de incidencia. La definición de la función de Moebius $\mu(x, y)$, como función inversa de la zeta-funcion $\zeta(x, y)$ de $A(P)$ es correcta. En efecto, $\zeta(x, x) = 1 \neq 0$ para todo $x \in P$. Por eso, en virtud del teorema 47, ζ tiene su inversa μ, la cual es para ζ tanto la inversa izquierda, como la derecha. Más aún, en virtud del teorema 47, la función de Moebius $\mu(x, y)$ del conjunto finito local parcialmente ordenado P puede ser calculada para $x, y \in P$ fijos, tales que $x < y$ de un modo recurrente con ayuda de las fórmulas

$$\mu(x, y) = -\sum_{x \leq z < y} \mu(x, z) = -\sum_{x < z \leq y} \mu(z, y) \qquad (1)$$

tomándose en consideración las condiciones de que $\mu(x, x) = 1$ para cualquier $x \in P$.

Sea P^* un conjunto parcialmente ordenado, dual respecto a P. Entonces, si $\zeta(x, y) \in A(P)$, y $\zeta^*(x, y) \in A(P^*)$, tendremos $\zeta^*(x, y) = \zeta(x, y)$ para cualesquiera x, y de P. Es evidente que las igualdades análogas tienen lugar para las lambda-funciones, las funciones de Kronecker, de cadenas, de recubrimiento y de longitud; además, en virtud del teorema 47 y la propiedad análoga de la zeta-función, también son válidas para las funciones de Moebius. De este modo, las funciones de incidencia mencionadas no cambian, si en lugar de P examinamos P^*.

Para comprender mejor el sentido de las definiciones introducidas, analicemos las representaciones matriciales de las funciones de incidencia. Con este fin prolonguemos al principio la relación de orden parcial $\leqslant$ sobre el conjunto ordenado y localmente finito P, hasta que se obtenga una relación de orden $<$, que convierte P en un conjunto bien ordenado (esto es siempre realizable en virtud del teorema 4), luego hagamos uso del conjunto bien ordenado para marcar con índices los elementos del conjunto P. Resultará en este caso que si $x_\alpha \leqslant x_\beta$, entonces $\alpha < \beta$. Ahora, a toda función de incidencia $f(x, y)$ de $A(P)$ se le hace corresponder una matriz $F = \|f_{\alpha\beta}\|$ con elementos del campo K, en la cual las filas y las columnas están concordadas con los índices del conjunto P, a saber, $f_{\alpha\beta} = f(x_\alpha, x_\beta)$. Hablando en general, la matriz obtenida puede ser también de orden infinito. En el caso de un conjunto finito parcialmente ordenado P las matrices de funciones de incidencia serán de orden $|P|$, mientras que como conjunto de índices en este caso pueden elegirse los números naturales de 1 a $|P|$ (véase teorema 2).

La matriz de las funciones de incidencia $f(x, y) \in A(P)$, obtenida de este modo, es, obviamente, una matriz triangular superior, es decir, en la que debajo de la diagonal principal solamente hay ceros.

Veamos unos cuantos ejemplos. Sea Z una matriz de la zeta-función de $A(P)$. Si $P = \mathscr{P}(S)$, donde $S = \{a, b, c\}$, entonces

$$Z = \begin{pmatrix} \varnothing & a & b & c & ab & bc & ac & abc \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} \varnothing \\ a \\ b \\ c \\ ab \\ bc \\ ac \\ abc \end{matrix}$$

Si P es una cadena de 5 elementos, entonces

$$Z = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Si P es una anticadena de 5 elementos, entonces

$$Z = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Sean $F = \|f_{\alpha\beta}\|$ y $G = \|g_{\alpha\beta}\|$ matrices de las funciones de incidencia f y g de $A(P)$, respectivamente, de cuyos índices sirven los elementos del conjunto bien ordenado $(P, \leqslant)$. Entonces, si $h(x, y) = f(x, y) + g(x, y)$, $t(x, y) = \alpha \cdot f(x, y)$ y $p(x, y) = (f * g)(x, y)$, tendremos $H = F + G$, $T = \alpha \cdot F$, y $P = F \cdot G$. Las primeras dos igualdades son evidentes. Comprobemos que $P = F \cdot G$, es decir, $p_{\alpha\beta} = \sum_{\gamma} f_{\alpha\gamma} g_{\gamma\beta}$. Efectivamente,

$$\sum_{\gamma} f_{\alpha\gamma} g_{\gamma\beta} = \sum_{\gamma} f(x_\alpha, x_\gamma) g(x_\gamma, x_\beta) = \sum_{j:\alpha \leqslant j \leqslant \beta} f(x_\alpha, x_j) g(x_j, x_\beta) =$$

$= $ (aprovechemos el hecho de que, para $\gamma < \alpha$, $f(x_\alpha, x_\gamma) = 0$, y, para $\beta < \gamma$, $g(x_\gamma, x_\beta) = 0$) $= \sum_{x_\alpha \leqslant x_\gamma \leqslant x_\beta} f(x_\alpha, x_\gamma) g(x_\gamma, x_\beta) = p(x_\alpha, x_\beta) = p_{\alpha\beta}$.

De aquí, si P es un conjunto finito parcialmente ordenado, $A(P)$ puede considerarse como una subálgebra del álgebra de todas las matrices triangulares superiores de orden $|P|$. Las representaciones matriciales facilitan considerablemente el estudio de los conjuntos parcialmente ordenados y la comprensión de la esencia de introducción de las álgebras de incidencia sobre ellos.

Inmediatamente de las definiciones de las funciones de incidencia se deducen las siguientes identidades:

$$\text{a) } f = f*\delta = \delta*f; \qquad \text{b) } \delta^k = \delta^{k-1} = \ldots = \delta;$$

$$\text{c) } \zeta^n(x, y) = \sum_{i=0}^{n} \binom{n}{i} \eta^i(x, y); \quad \eta^n(x, y) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \zeta^i(x, y);$$

$$\text{d) } \lambda^n(x, y) = \sum_{i=0}^{n} \binom{n}{i} \varkappa^i(x, y); \quad \varkappa^n(x, y) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \lambda^i(x, y);$$

e) $(x*\zeta)(x, y)$ = al número de todos los átomos en el intervalo $[(x, y)]$ de P.

f) $(\zeta*x)(x, y)$ = al número de todos los coátomos en el intervalo $[x, y]$ de P.

Para obtener las identidades c) y d) hace falta servirse también del binomio de Newton:

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Comprobemos la validez de la identidad e). Tenemos $(x*\zeta)(x, y) = \sum_{z: x \leq z \leq y} x(x, z)\zeta(z, y) =$ (por cuanto $x(x, z) \neq 0$ sólo cuando $x \multimap z$) $= \sum_{z: x \multimap z \leq y} x(x, z)\zeta(z, y) =$ (puesto que $\zeta(z, y) = 1$ para todo $z \leqslant y$) $= \sum_{z: x \multimap z \leq y} x(x, z)$. Pero si $x(x, z) \neq 0$, entonces $x(x, z) = 1$. La identidad e) queda demostrada. La identidad f) se obtiene de e) de un modo dual.

Además,

$$f^2(x, y) = (f*f)(x, y) = \sum_{z_1: x \leq z_1 \leq y} f(x, z_1) f(z_1, y);$$

$$f^3(x, y) = (f*f^2)(x, y) = (f*(f*f))(x, y) =$$

$$= \sum_{z_1: x \leq z_1 \leq y} f(x, z_1) \left(\sum_{z_2: z_1 \leq z_2 \leq y} f(z_1, z_2) f(z_2, y) \right) =$$

$$= \sum_{z_1, z_2: x \leq z_1 \leq z_2 \leq y} f(x, z_1) f(z_1, z_2) f(z_2, y).$$

Ahora, por inducción obtenemos la identidad

$$\text{g) } f^k(x, y) = \sum_{z_1, z_2, \ldots, z_{k-1}: x \leq z_1 \leq \ldots \leq z_{k-1} \leq y} f(x, z_1) f(z_1, z_2) \ldots f(z_{k-1}, y).$$

Directamente de g) y de las definiciones de las funciones de incidencia ζ, η, x del conjunto parcialmente ordenado y localmente finito P obtenemos las identidades:

h) $\eta^k(x, y)$ = al número de todas las cadenas de longitud k entre x e y en P (puesto que $\eta(x, z_1)\eta(z_1, z_2) \ldots \eta(z_{k-1}, y) = 1$ cuando y sólo cuando $x < z_1 < z_2 < \ldots < z_{k-1} < y$);

i) $\varkappa^k(x, y)$ = al número de todas las cadenas máximas de longitud k entre x e y en P (puesto que $\varkappa(x, z_1)\varkappa(z_1, z_2) \ldots \varkappa(z_{k-1}, y) = 1$ cuando y sólo cuando $x \prec z_1 \prec z_2 \prec \ldots z_{k-1} \prec y$);

j) $\zeta^2(x, y) = |[x, y]|$ (puesto que $\zeta(x, z)\zeta(z, y) = 1$ cuando y sólo cuando $x \leqslant z \leqslant y$).

Introduzcamos las designaciones especiales para algunos elementos más del álgebra de incidencia $A(P)$. Sea $x, y, u, v \in P$. Pongamos

$$e_x(u, v) = \begin{cases} 1, \text{ si } u = v = x, \\ 0, \text{ en el caso contrario;} \end{cases}$$

$$\delta_{x,y}(u, v) = \begin{cases} 1, \text{ si } u = x, v = y, \\ 0, \text{ en el caso contrario.} \end{cases}$$

Ejercicios. Sea $f \in A(P)$. Demuéstrese que

1. Si $g = \delta_{x,y} * f$, entonces $g(u, v) = \begin{cases} 0, \text{ si } u \neq x, \\ f(u, v), \text{ si } u = x. \end{cases}$

2. Si $g = f * \delta_{z,w}$, entonces $g(u, v) = \begin{cases} 0, \text{ si } v \neq w; \\ f(u, z), \text{ si } v = w \end{cases}$

3. Si $g = \delta_{xy} * f * \delta_{z,w}$, entonces $g(u, v) = \begin{cases} 0, \text{ si } u \neq x \text{ y } v \neq w, \\ f(y, z), \text{ si } u = x \text{ y } v = w. \end{cases}$

Es evidente que $\delta_{x,y} * \delta_{u,v} = \begin{cases} \delta_{x,v}, \text{ si } y = u; \\ 0, \text{ si } y \neq u. \end{cases}$

Observemos que $e_x = \delta_{x,x}$. De aquí, $e_x^2 = e_x$, es decir, e_x son idempotentes en $A(P)$.

Haciendo uso de las funciones introducidas, podemos escribir

$$f = \sum_{x,y \in P: x \leqslant y} f(x, y)\delta_{x,y}.$$

Esta igualdad puede entenderse de tal manera, que para todos los $u, v \in P$ se tiene

$$f(u, v) = \sum_{x,y \in P: x \leqslant y} f(x, y)\delta_{x,y}(u, v)$$

(cualesquiera que sean u y v, la suma en el segundo miembro contiene un solo sumando no nulo). Mostremos que $e_x * f * e_y = f(x, y)\delta_{x,y}$. En efecto,

$$e_x * \sum_{u,v \in P: u \leqslant v} f(u, v)\delta_{u,v} * e_y = \sum_{u,v \in P: u \leqslant v} f(u, v)\delta_{x,x} * \delta_{u,v} * \delta_{y,y} = f(x, y)\delta_{x,y}.$$

Recordemos algunos resultados y definiciones que nos harán falta a continuación. Se denomina *ideal derecho* a un subgrupo I del grupo aditivo de un anillo R si, junto con cualquier elemento $a \in I$ y cualquier $x \in R$, el elemento ax también está contenido en I. Si, en las mismas condiciones, xa

se contiene en I, entonces I recibe el nombre de *ideal izquierdo*. El subconjunto I del anillo R, que es ideal izquierdo y derecho simultáneamente, se denomina *ideal bilateral*. Un elemento x del anillo R es *casi regular a la derecha*, si existe un elemento $y \in R$ tal que $x + y - xy = 0$. Cabe notar que en un anillo con la unidad 1 el elemento x es casi regular a la derecha cuando y sólo cuando $1 - x$ es invertible a la derecha. Efectivamente, $x + y - xy = 0 \Leftrightarrow 1 - (x + y - xy) = 1 \Leftrightarrow (1 - x)(1 - y) = 1$. Un ideal derecho será casi regular, si todos los elementos suyos son casi regulares a la derecha. Se llama *radical de Jacobson* del anillo R (se denota rad R) al ideal maximal derecho casi regular del anillo R. El radical de Jacobson del anillo R es un ideal bilateral. En el anillo R con la unidad 1 el elemento $x \in \text{rad } R$ cuando y sólo cuando para todos los $a, b \in R$ el elemento $1 - axb$ es invertible [137].

Ejercicio 4. Demuéstrese que un idempotente casi regular a la derecha de cualquier anillo es igual a cero.

Proposición 3. El radical de Jacobson de un algebra de incidencia $A(P)$ del conjunto parcialmente ordenado y localmente finito P sobre el campo K contiene todas las funciones $f \in A(P)$ tales que $f(x, x) = 0$ para todo $x \in P$.

Demostración. El elemento $f \in A(P)$ es casi regular cuando y sólo cuando $1 - f$ es invertible en $A(P)$. En virtud del teorema 47, el elemento $1 - f$ es invertible cuando y sólo cuando para todos los $x \in P$ tiene lugar $(1 - f)(x, x) \neq 0$, o bien $f(x, x) \neq 1$. El álgebra de incidencia es un anillo con la unidad 1 (la función delta es un elemento unidad). Por eso, $f \in \text{rad} A(P)$ en aquel y sólo en aquel caso cuando para todos los $g, h \in A(P)$ el elemento $1 - g*f*h$ es invertible, o bien, que es lo mismo, $g*f*h$ es casi regular. En particular, para $g = h = e_x$ tenemos $e_x*f*e_x = f(x, x)e_x \in \text{rad } A(P)$. De aquí, para todo $x \in P$, $f(x, x) = 0$, puesto que en el radical no hay idempotentes, salvo 0 (véase ejercicio 4). La proposición está demostrada.

Observemos que las álgebras de incidencia de dos conjuntos parcialmente ordenados son isomorfas como anillos, cuando y sólo cuando son isomorfos los propios conjuntos parcialmente ordenados. En una dirección esta afirmación es evidente. Demostrémosla en la otra dirección.

Teorema 48 (Stanley). Sean P y Q los conjuntos parcialmente ordenados y localmente finitos, y sea K un campo. Entonces, del isomorfismo de las álgebras de incidencia $A_K(P)$ y $A_K(Q)$ se desprende que P y Q son isomorfos como conjuntos parcialmente ordenados.

Demostración. Demostremos cómo se puede restablecer unívocamente el conjunto parcialmente ordenado P, a partir del anillo $A(P)$. Al factorizar $A(P)$ según el conjunto de elementos de la forma $\sum_{x<y} \lambda_{x,y}\delta_{x,y} = \text{rad} A(P)$, obtendremos $\sum_x \lambda_{x,x}\delta_{x,x} + \text{rad } A(P)$.

De este modo, los elementos $A(P)/\text{rad}A(P)$ tienen por expresión $\bar{f} = \sum_{x \in P} \lambda_x \bar{e}_x$. Una aplicación $\varphi: \sum_{x \in P} \lambda_x \bar{e}_x \to (\lambda_x)_{x \in P}$ es un isomorfismo $\overline{A(P)} = A(P)/\text{rad}A(P) \to \prod_{x \in P} K_x$ (producto directo de ejemplares del campo $K =$

$= K_x$, por uno para cada x de P). Así pues, $A(P)/\mathrm{rad}\, A(P) \cong \prod_{x \in P} K_x$ y se genera por los idempotentes e_x que son ortogonales ($e_x \cdot e_y = 0$ para $x \neq y$) y mínimos (es decir, son mínimos los ideales izquierdos generados por ellos). Demostremos que otros idempotentes mínimos b $A(P)$ no existen. Enel producto $\prod_{x \in P} K_x\, \bar{e}_x = (0, \ldots 1 \ldots 0)$. Si $\bar{r} \cdot \bar{e}_x = (0 \ldots \lambda \ldots 0)$ es un potente, entonces $\lambda^2 = \lambda$. De aquí, $\lambda = 0$ ó a 1. El ideal generado por $\bar{e}_x$ tiene la forma $(0 \ldots \lambda \ldots 0)$. Por consiguiente, el juego de $\bar{e}_x$ se define unívocamente por el álgebra $A(P)$, puesto que si dos álgebras de incidencia $A(P)$ y $A(Q)$ son isomorfas, en las álgebras $\overline{A(P)}$ y $\overline{A(Q)}$ los idempotentes mínimos corresponden uno al otro.

Sea un conjunto f_x de idempotentes mínimos a la derecha y a la izquierda en $A(P)$ tales que $\bar{f}_x = \bar{e}_x$. Introduzcamos en el conjunto f_x un orden, suponiendo que $f_x \leqslant f_y$, cuando y sólo cuando $f_x * A(P) * f_y \neq 0$. El teorema quedará demostrado, si mostramos que $f_x \leqslant f_y$ cuando y sólo cuando $x \leqslant y$. Tenemos: $f_x = e_x + \sum_{u<v} \lambda_{u,v} \delta_{u,v}$. Es fácil mostrar que $u \leqslant x \leqslant v$, de lo contrario no tendremos el mínimo. En efecto, de f_x podemos obtener $e_x * f_x$ (multiplicando a la izquierda), mientras que de $e_x * f_x$ (si $u \not\leqslant x$) no se puede obtener f_x. Por consiguiente, el ideal izquierdo f_x no es mínimo. Así pues, $u \leqslant x$. De un modo análogo se demuestra que $v \geqslant x$, cualquiera que sea v (siempre que $\lambda_{u,v} \neq 0$).

Sea $x \leqslant y$. Mostremos que en este caso $f_x * A(P) * f_y \neq 0$. Con este fin basta comprobar que $f_x * \delta_{x,y} * f_y \neq 0$. Efectivamente, $f_x * \delta_{x,y} * f_y = \left(e_x + \sum_{\substack{u \leqslant x \leqslant u \\ u<v}} \lambda_{u,v} \delta_{u,v}\right) * \delta_{x,y} * \left(e_y + \sum_{\substack{s \leqslant y \leqslant t \\ s<t}} \mu_{s,t} \delta_{s,t}\right) = e_x * \delta_{x,y} * e_y + \ldots = \delta_{x,y} + \ldots) \neq \neq \lambda \delta_{x,y}$. Por cuanto $\delta_{x,y}$ puede obtenerse después de abrir los paréntesis de un solo modo: $e_x * \delta_{x,y} * e_y$, este sumando no puede reducirse junto con los otros. Por eso, el segundo miembro no es igual a 0.

Sea $x \not\leqslant y$. Mostremos que en este caso $f_x * A(P) * f_y$, donde $f_x = \sum_{u \leqslant x \leqslant y} \lambda_{u,v} \delta_{u,v}$ y $f_y = \sum_{s \leqslant y \leqslant t} \mu_{s,t} \delta_{s,t}$. Con este fin basta demostrar que para todos los p, q tiene lugar la relación $f_x * \delta_{p,q} * f_y = 0$, puesto que todo elemento $f \in A(P)$ puede ser representado en la forma $\sum_{p \leqslant q} \lambda_{p,q} \delta_{p,q}$. Sea $f_x * \lambda_{p,q} * f_y \neq 0$. Entonces, sólo un sumando es distinto de cero: $\delta_{u,v} * \delta_{p,q} * \delta_{s,t} \neq 0$ (aquí se omite el coeficiente). Pero, $\delta_{u,v} * \delta_{p,q} * \delta_{s,t} \neq 0$, si y sólo si $u \leqslant x \leqslant v = p \leqslant q = s \leqslant y \leqslant t$, es decir, cuando $x \leqslant y$. Hemos llegado a una contradicción con eso de que $x \not\leqslant y$. Por consiguiente $f_x * \delta_{p,q} * f_y = 0$. El teorema está demostrado.

Ocurre a menudo que en las aplicaciones se examina no todo el álgebra de incidencias $A(P)$ en su integridad, sino sólo determinadas subálgebras

de ésta, exigiendo de las funciones de incidencia, o bien valores constantes sobre los intervalos isomorfos del conjunto parcialmente ordenado P, o bien la llamada multiplicatividad.

Sea $A(P)$ un álgebra de incidencia del conjunto parcialmente ordenado localmente finito P. Veamos un subconjunto de todas las funciones de incidencia $f \in A(P)$, para las cuales del isomorfismo de todos los intervalos $[x, y]$ y $[a, b]$ en P se deduce: $f(x, y) = f(a, b)$. Denotemos este subconjunto con $S(P)$. Es evidente que $S(P)$ es un subálgebra del algebra de incidencia $A(P)$ que se llama *álgebra estándar* del conjunto parcialmente ordenado P. En efecto, si $f, g \in A(P)$, y φ es cierto isomorfismo del intervalo $[x, y]$ en $[a, b]$, entonces

$$(f + g)(x, y) = f(x, y) + g(x, y) = f(a, b) + g(a, b) = (f + g)(a, b);$$

$$(\alpha f)(x, y) = \alpha f(x, y) = \alpha f(a, b) = (\alpha f)(a, b);$$

$$(f * g)(x, y) = \sum_{z:\, x \leq z \leq y} f(x, z) g(x, y) = \sum_{z:\, x \leq z \leq y} f(\varphi(x), \varphi(z)) g(\varphi(z), \varphi(y)) =$$

$$= \sum_{z:\, a = \varphi(x) \leq \varphi(z) \leq \varphi(y) = b} f(a = \varphi(x), \varphi(z)) g(\varphi(z), b = \varphi(y)) = (f * g)(a, b).$$

Directamente del teorema 47 obtenemos el sigueinte resultado:

Corolario 9. Sea $S(P)$ un álgebra estándar del conjunto parcialmente ordenado P. Si la función de incidencia pertenece a $S(P)$ y es invertible en $A(P)$, será invertible tambien en $S(P)$.

Es fácil comprobar que las funciones ϱ, δ, ζ, λ, η, $\varkappa$, definidas más arriba, yacen en $S(P)$ y, en virtud del corolario 9, la función de Moebius μ también está situada en $S(P)$.

Sea P un retículo. La función de incidencia $f \in A(P)$ se llama *multiplicativa*, si para todos los $x, y \in P$ de la condición

$$[x \wedge y, x \vee y] \cong [x \wedge y, x] \times [x \wedge y, y]$$

se deduce que

$$f(x \wedge y, x \vee y) = f(x \wedge y, x) f(x \wedge y, y).$$

Son ejemplos de funciones multiplicativas de incidencia para los retículos las funciones δ, ζ y ζ^2 (véase la identidad j)).

Corolario 10. Sea f una función invertible multiplicativa de $A(P)$. Entonces, $f(x, x) = 1$ para todo $x \in P$.

Demostración. De $[x \wedge x, x \vee x] \cong [x \wedge x, x] \times [x \wedge x, x]$ tenemos: $f(x, x) = f(x, x) f(x, x)$. Debido a la invertibilidad, $f(x, x) \neq 0$ para todo $x \in P$. Por consiguiente, $f(x, x) = 1$.

Teorema 49. Sea P un retículo. Entonces, todas las funciones inversibles multiplicativas pertenecientes a $S(P)$, forman un grupo con relación a la operación de multiplicación (convolución).

Demostración. Sean f y g las funciones inversibles multiplicativas de incidencia del álgebra estándar $S(P)$. Comprobemos que la función $f * g$ tam-

bién será multiplicativa. Admitamos que

$$[x\wedge y,\ x\vee y]\cong[x\wedge y,\ x]\times[x\wedge y,\ y].$$

En este caso $(f*g)(x\wedge y,\ x\vee y)=\sum\limits_{z:x\wedge y\leqslant z\leqslant x\vee y} f(x\wedge y,\ z)g(z,\ x\vee y)=$ (puesto que $[x\wedge y,\ z]\cong[x\wedge y,\ z\wedge x)]\times[x\wedge y,\ z\wedge y]$, $[z,\ x\vee y]\cong[z,\ z\vee x)]\times[z,\ z\vee y]$ y f, g son funciones multiplicativas) $=\sum\limits_{z:x\wedge y\leqslant z\leqslant x\vee y} f(x\wedge y,\ z\wedge x)f(x\wedge y,\ z\wedge y)g(z,\ z\vee x)\times$ $\times g(z,\ z\vee y)=$ (puesto que $[z,\ z\vee x]\cong[z\wedge x,\ x]$, $[z,\ z\vee y]\cong[z\wedge y,\ y]$ y f, $g\in S(P))=\sum\limits_{z:x\wedge y\leqslant z\leqslant x\vee y}(f(x\wedge y,\ z\wedge x)g(z\wedge x,\ x))(f(x\wedge y,\ z\wedge y)g(z\wedge y,\ y))=$ (denotemos $z\wedge x$ y $z\wedge y$ con u y v respectivamente; entonces, $x\wedge y\leqslant u\leqslant x$ y $x\wedge y\leqslant v\leqslant y$, puesto que $x\wedge(x\wedge y)=x\wedge y$, $y\wedge(x\wedge y)=(x\wedge y)$, $x\wedge(x\vee y)=x$, $y\wedge(x\vee y)=y$) $=\sum\limits_{u:x\wedge y\leqslant u\leqslant x} f(x\wedge y,\ u)g(u,\ x)\sum\limits_{v:x\wedge y\leqslant v\leqslant y} f(x\wedge y,\ v)g(v,\ y)=(f*g)(x\wedge y,\ x)(f*g)(x\wedge y,\ y)$, es decir, $f*g$ es una función multiplicativa.

Comprobemos que f^{-1} es también una función multiplicativa. Demostremos por inducción respecto de l que la condición de multiplicatividad se cumple para todos los intervalos de longitud no superior a l. Para $l=0$, esto es evidente. Supongamos que la afirmación dada es válida para $l-1$; demostremos su validez para l. Analicemos cierto intervalo $[x\wedge y,\ x\vee y]$ de longitud l. Tenemos, pues,

$$0=\delta(x\wedge y,\ x\vee y)=(f^{-1}*f)(x\wedge y\ ,\ x\vee y)=\sum_{z:x\wedge y\leqslant z\leqslant x\vee y} f^{-1}(x\wedge y,\ z)f(z,\ x\vee y)=$$

$$=\sum_{z:x\wedge y\leqslant z\leqslant x\vee y} f^{-1}(x\wedge y,\ z)f(z,\ x\vee y)+f^{-1}(x\wedge y,\ x\vee y)f(x\vee y,\ x\vee y)=$$

(en virtud de la hipótesis de inducción, y teniendo presente que $f(x\vee y,\ x\vee y)=1$) $=\sum\limits_{z:x\wedge y\leqslant z\leqslant x\vee y} f^{-1}(x\wedge y,\ z\wedge x)f^{-1}(x\wedge y,\ z\wedge y)f(z,\ z\vee x)f(z,\ z\vee y)+$ $+f^{-1}(x\wedge y,\ x\vee y)=$ (en virtud de que $[z,\ z\vee x]\cong[z\wedge x,\ x]$, $[z,\ z\vee y]\cong[z\wedge y,\ y]$ y f, $f^{-1}\in S(P))=\sum\limits_{z:x\wedge y\leqslant z\leqslant x\vee y} f^{-1}(x\wedge y,\ z\wedge x)f(z\wedge x,\ x)f^{-1}(x\wedge y,\ z\wedge y)f(z\wedge y,\ y)+$ $+f^{-1}(x\wedge y,\ x\vee y)=$ (denotemos $z\wedge x$ y $z\wedge y$, con u y v, respectivamente, teniendo presente que $[x\wedge y,\ x\vee y]\cong[x\wedge y,\ x]\times[x\wedge y,\ y]$ y $f(x,\ x)=1$ para todo $x\in P)=\sum\limits_{u:x\wedge y\leqslant u<x} f^{-1}(x\wedge y,\ u)f(u,\ x)\sum\limits_{v:x\wedge y\leqslant v<y} f^{-1}(x\wedge y,\ v)f(v,\ y)+f^{-1}(x\wedge y,\ x)\times$ $\times\sum\limits_{v:x\wedge y\leqslant v<y} f^{-1}(x\wedge y,\ x)f(v,\ y)+f^{-1}(x\wedge y,\ y)\sum\limits_{u:x\wedge y\leqslant u<x} f^{-1}(x\wedge y,\ u)f(u,\ x)+$ $+f^{-1}(x\wedge y,\ y)\sum\limits_{u:x\wedge y\leqslant u<x} f^{-1}(x\wedge y,\ u)f(u,\ x)+f^{-1}(x\wedge y,\ x\vee y)=$ (en virtud de las fórmulas del teorema 47 y de la igualdad $f(x,\ x)=1$ para todo $x\in P)=(-f^{-1}(x\wedge y,\ \ |x))(-f^{-1}(x\wedge y,\ \ y))+f^{-1}(x\wedge y,\ \ x)(-f^{-1}(x\wedge y,\ y))+f^{-1}(x\wedge y,\ y)(-f^{-1}(x\wedge y,\ x))+f^{-1}(x\wedge y,\ x\vee y)$. De este modo, llegamos a que

$$f^{-1}(x\wedge y,\ x\vee y)-f^{-1}(x\wedge y,\ x)f^{-1}(x\wedge y,\ y)=0.$$

Por consiguiente,

$$f^{-1}(x\wedge y,\ x\vee y) = f^{-1}(x\wedge y,\ x)f^{-1}(x\wedge y,\ y)$$

y la demostración del teorema queda establecida.

Calculemos la función de Moebius para algunos conjuntos parcialmente ordenados aducidos en el § 8.1.

EJEMPLO 1. Sea A un conjunto parcialmente ordenado trivial. Es obvio que

$$\mu(a,\ b) = \begin{cases} 1, \text{ si } a = b; \\ 0, \text{ en el caso contrario.} \end{cases}$$

EJEMPLO 2. Sea $N = \{0,\ 1,\ 2,\ \ldots,\ k\}$ un subconjunto de números enteros con orden ordinario. En virtud del corolario 10, $\mu(n,\ n) = 1$ para todo $n \in N$. Aprovechemos las fórmulas (1) y obtengamos que $\mu(n,\ n+1) = -1$, y $\mu(n,\ n+k) = 0$, cualesquiera que sean $n,\ k \in N$ y $k \geqslant 2$. De este modo,

$$\mu(n,\ m) = \begin{cases} 1, \text{ si } n = m; \\ -1, \text{ si } m - n = 1; \\ 0, \text{ en los casos restantes.} \end{cases}$$

EJEMPLO 3. Sea $\mathscr{P}(S_n)$ un booleano (véase ejemplo 4 del § 8.1), donde $S_n = \{s_1,\ s_2,\ \ldots,\ s_n\}$. Veamos una familia de todos los binarios n-dimensionales $\bar{a} = (a_1,\ \ldots,\ a_n)$ con una relación de orden: $\bar{a} \leqslant \bar{b}$ cuando y sólo cuando $a_i \leqslant b_i$ para todo $i = 1,\ 2,\ \ldots,\ n$. Designemos este conjunto parcialmente ordenado con Σ_n. No es difícil comprobar que

$$\mathscr{P}(S_n) \cong \Sigma_n$$

En efecto, si $X \subseteq S_n$, definamos $\varphi(X) = (x_1,\ \ldots,\ x_n)$, donde

$$x_i = \begin{cases} 0, \text{ si } s_i \notin X; \\ 1, \text{ si } s_i \in X. \end{cases}$$

Es fácil ver que φ es un isomorfismo. Más aún,

$$\Sigma_n \cong \Sigma_1 \times \Sigma_1 \times \ldots \times \Sigma_1.$$

En virtud del ejemplo 2, para Σ_1 e $y \geqslant x$ tenemos $\mu(x,\ y) = (-1)^{y-x}$, puesto que existen solamente dos posibilidades: $x = y$, o bien $x = 0$ e $y = 1$. Sea $X \subseteq Y \subseteq S_n$, $\varphi(X) = (x_1,\ \ldots,\ x_n)$ y $\varphi(Y) = (y_1,\ \ldots,\ y_n)$ en el isomorfismo $\mathscr{P}(S_n) \cong \Sigma_1 \times \ldots \times \Sigma_1$. Entonces,

$$\mu(X,\ Y) = \mu((x_1,\ \ldots,\ x_n),\ (y_1,\ \ldots,\ y_n)) = \prod_{i=1}^{n} \mu(x_i,\ y_i) =$$

$$= (-1)^{\sum_{i=1}^{n} y_i \quad \sum_{i=1}^{n} x_i} = (-1)^{|Y| - |X|}.$$

EJEMPLO 4. Sea $D(n)$ un conjunto de todos los divisores del número natural n, ordenado respecto de la divisibilidad (véase ejemplo 6 del § 8.1). De

acuerdo con el teorema sobre la unicidad de la descomposición de un número en factores primos,

$$D(n) \cong D(p_1^{\alpha_1}) \times D(p_2^{\alpha_2}) \times \ldots \times D(p_s^{\alpha_s}).$$

Por consiguiente, es suficiente calcular la función de Moebius para $D(p^\alpha)$, donde p es un número primo, y α, un número entero. Pero, el conjunto parcialmente ordenado $D(P^\alpha)$ es una cadena $1 \mid p \mid p^2 \mid \ldots \mid p^\alpha$ isomorfa al subconjunto de números enteros $\{0, 1, 2, \ldots \alpha\}$ con orden ordinario, cuya función de Moebius se ha calculado en el ejemplo 2. Por eso

$$\mu(p^i, p^j) = \begin{cases} 1, \text{ si } i = j; \\ -1, \text{ si } j - 1 = 1; \\ 0, \text{ en todos los casos restantes.} \end{cases}$$

En virtud del teorema 49,

$$\mu(l, m) = \begin{cases} 1, \text{ si } l = m \\ (-1)^s, \text{ si } \dfrac{m}{l} = p_1 p_2 \ldots p_s, \text{ donde } p_1, p_2, \ldots, p_s \text{ son} \\ \text{números primos distintos dos a dos;} \\ 0, \text{ en todos los demás casos.} \end{cases}$$

La forma clásica de la función de Moebius

$$\mu(d) = \begin{cases} 1, \text{ si } d = 1; \\ (-1)^s, \text{ si } d = p_1 p_2 \ldots p_s, \text{ donde } p_1, p_2, \ldots, \\ p_s \text{ son números enteros distintos dos a dos;} \\ 0, \text{ si } d = r^2 t, \ d \neq 1, \end{cases}$$

hallada por Moebius aproximadamente en 1832 y utilizada en la teoría de los números, está ligada con la función de Moebius de un conjunto parcialmente ordenado $D(n)$ del modo siguiente

$$\mu(l, m) = \mu\binom{m}{l}, \text{ donde } d = \frac{m}{l} \in N.$$

Esta relación explica el origen de la denominación de la función de Moebius.

Continuemos la exposición de los métodos que se emplean en el cálculo de las funciones de Moebius para conjuntos parcialmente ordenados arbitrarios. Sean P y L dos conjuntos parcialmente ordenados con las funciones de Moebius μ_P y μ_L, respectivamente, y sea $f: P \to L$ una aplicación del conjunto P en el L que conserva el orden. Veamos cómo se puede hallar μ_L con ayuda de las μ_P y f conocidas y discutamos dos tipos de aplicaciones: los operadores de clausura y la correspondencia de Galois.

Generalicemos la noción de operador de clausura, introducida para el booleano en el § 8.2, sobre el conjunto arbitrario parcialmente ordenado P.

La aplicación φ: $P \to P$ se llama operador de clausura sobre el conjunto P, si para cualesquiera elementos a, $b \in P$ se cumplen las siguientes condiciones:

a) $a \leqslant \varphi(a)$; b) si $a \leqslant b$, entonces $\varphi(a) \leqslant \varphi(b)$; c) $\varphi(\varphi(a)) = \varphi(a)$.

Los ejemplos de operadores de clausura son numerosos. Así, por ejemplo, en el retículo completo de los subespacios de un espacio topológico servirá de operador de clausura una aplicación que a todo subespacio le asigna su clausura. En un conjunto parcialmente ordenado P con la unidad 1, a título de operador de clausura interviene la aplicación $\varphi(x) = 1$ para todo $x \in P$.

Si φ es un operador de clausura, entonces $\varphi(x)$ se llamará *φ-clausura* del elemento x. Un elemento que coincide con su φ-clausura se denomina *φ-cerrado*.

Teorema 50. Si φ es el operador de clausura sobre un conjunto parcialmente ordenado P, el subconjunto $A \subseteq P$ se compone de elementos φ-cerrados y si $a = \inf A$ existe, entonces a será también un elemento φ-cerrado.

Demostración. Por cuanto $a \leqslant x$ para todo $x \in A$, entonces $\varphi(a) \leqslant \varphi(x) = x$ para todos los $x \in A$, y, por lo tanto, $\varphi(a) \leqslant a$. La desigualdad inversa se desprende de la definición de operador de clausura. El teorema queda demostrado.

Teorema 51. Si φ es un operador de clausura en un retículo completo P, entonces, un conjunto parcialmente ordenado Q de todos los elementos φ-cerrados, considerado como subconjunto del conjunto parcialmente ordenado P, es también un retículo completo. Además, para todo subconjunto no vacío A del conjunto Q tienen lugar las correlaciones:

$$\inf_Q A = \inf_P A \text{ y } \sup_Q A = \varphi(\sup_P A).$$

El conjunto Q recibe el nombre de *factor* del conjunto parcialmente ordenado con relación al operador de clausura φ.

Demostración. Sea 1 la unidad de un retículo completo P. Por cuanto $\varphi(1) \geqslant 1 \geqslant \varphi(1)$, entonces 1 pertenece a Q, y, obviamente, es la unidad de este conjunto parcialmente ordenado. Luego, si A es un subconjunto no vacío del conjunto Q, el elemento $a = \inf_P A$ es, con arreglo al teorema 50, φ-cerrado. Por supuesto, $a \leqslant x$ para todo $x \in A$. Si $v \in Q$ y $v \leqslant x$ para todo $x \in A$, entonces $v \leqslant a$. Así que, $a = \inf_Q A$, y, por consiguiente, Q es un retículo completo. Luego, sea $b = \sup_P A$ y sea $\bar{b} = \sup_Q A$. Está claro que $\bar{b} \in Q$, y $\bar{b} \geqslant b$, puesto que $\bar{b} \geqslant x$ para todo $x \leqslant A$. De aquí: $\bar{b} = \varphi(\bar{b}) \geqslant \varphi(b)$. La desigualdad $\bar{b} \leqslant \varphi(b)$ es lícita, ya que $\varphi(b) \geqslant \varphi(x) = x$ para todo $x \in A$. Por eso, $b = \varphi(b)$, lo que se trataba de demostrar.

Sea φ el operador de clausura sobre P y sea Q el factor de un conjunto parcialmente ordenado con relación a φ. Consideremos álgebra de incidencia $A(Q)$ como subconjunto del álgebra $A(P)$, al definir adicionalmente pa-

ra toda $f \in A(Q)$:

$$f(x, y) = 0, \text{ si } x \notin Q \text{ ó } y \notin Q.$$

Denotemos con μ y μ_Q las funciones de Moebius para los conjuntos parcialmente ordenados P y Q, respectivamente. Definamos de un modo análogo también ζ, ζ_Q y δ, δ_Q.

Teorema 52 (de Rota). Sea P un conjunto parcialmente ordenado y localmente finito, y sea φ el operador de clausura sobre P con el factor Q. Entonces, para todos los $x, y \in P$ se verifica la correlación:

$$\sum_{z \in P; \varphi(z) = \varphi(y)} \mu(x, z) = \begin{cases} \mu_Q(\varphi(x), \varphi(y)), & \text{si } x = \varphi(x) \\ 0, & \text{si } x < \varphi(x). \end{cases}$$

Demostración.

$$\sum_{z \in P; \varphi(z) = \varphi(y)} \mu(x, z) = \sum_{z} \mu(x, z) \delta_Q(\varphi(z), \varphi(y)) =$$

$$= \sum_{\varphi(z), \varphi(w)} \mu(x, z) \zeta_Q(\varphi(z), \varphi(w)) \mu_Q(\varphi(w), \varphi(y)) =$$

$$= \sum_{z, \varphi(w)} \mu(x, z) \zeta(z, \varphi(w)) \mu_Q(\varphi(w), \varphi(y)) = \sum_{\varphi(w) \in Q} \delta(x, \varphi(w)) \mu_Q(\varphi(w), \varphi(y))$$

(aquí hemos aprovechado el hecho de que $z \leqslant \varphi(w)$ cuando y sólo cuando $\varphi(z) \leqslant \varphi(w)$. El teorema está demostrado.

Ejercicios.

5. Calcúlense las funciones de Moebius para los conjuntos parcialmente ordenados aducidos en los ejemplos 7, 8, 9 y 10 en § 8.1.

6. Sea μ una función de Moebius del retículo finito P, y supongamos que $x, y, z \in P$. Demuéstrense las siguientes afirmaciones:

a) (P. Hall). Si $x \leqslant y$ e y no es una unión de elementos que cubren x, entonces $\mu(x, y) = 0$.

b) (Weisner). Si $x \leqslant y \leqslant z$, entonces

$$\sum_{t; \forall t = y}{}' \mu(x, t) = \begin{cases} \mu(x, y), & \text{si } z = x; \\ 0, & \text{si } z \neq x. \end{cases}$$

7. Demuéstrese que la función de Moebius μ de un retículo distributivo finito P se define del modo siguiente:

$$\mu(x, y) = \begin{cases} 0, \text{ si } y \text{ no es una unión de elementos que cubren } x; \\ (-1)^n, \text{ si } y \text{ es igual a la unión de } n \text{ elementos distintos que cubren } x. \end{cases}$$

8. Sea μ una función de Moebius de un retículo geométrico finito P y supongamos que $x, y \in P$, $x \leqslant y$. Demuéstrese que $\mu(x, y) \neq 0$. Muéstrese, además, que el valor de $\mu(x, y)$ es positivo, si el número $r(y) - r(x)$ es par, y negativo, si es impar. Aquí r es la función de rango de P.

9. (Crapo). Sea P un retículo finito, $a \in P$ y $a^{\perp}$, un conjunto de complementos al elemento a en P. Demuéstrese que para todo $a \in P$:

$$\mu(0, 1) = \sum_{b, c \in a^{\perp}}{}' \mu(0, b) \zeta(b, c) \mu(c, 1).$$

10. Sea P un retículo finito. Demuéstrense las siguientes afirmaciones:

a) si P es un retículo sin complementos, entonces $\mu(0, 1) = 0$.

b) Si P es un retículo modular, entonces $\mu(0, 1) = \mu(0, a) \sum_{z \in a^{-1}} \mu(0, z)$ para todo $a \in P$.

c) Si P es un retículo semimodular, entonces $\mu(0, 1) = \mu(0, a) \sum'_{z \in a^{-1}} (0, z)$ para todos los elementos modulares $a \in P$.

Analicemos ahora la conexión de Galois. Sean P y L unos conjuntos parcialmente ordenados. Un par (σ, τ) de aplicaciones $\sigma: P \to L$ se denomina *correspondencia de Galois* entre P y L, si para todos los $x, y \in P$ y todos los $a, b \in L$ se cumplen las condiciones siguientes:

a) Si $x \leqslant y$ en P, entonces $\sigma(x) \geqslant \sigma(y)$ en L;

b) Si $a \leqslant b$ en L, entonces $\tau(a) \geqslant \tau(b)$ en P;

c) $x \leqslant \tau\sigma(x)$ para todo $x \in P$ y $a \leqslant \sigma\tau(a)$ para todo $a \in L$.

No es difícil comprobar que $\tau\sigma$ y $\sigma\tau$ son operadores de clausura en los conjuntos P y L, respectivamente.

El concepto citado tiene por origen la teoría de Galois para las ecuaciones algebraicas, donde se examina la correspondencia de Galois entre los subcampos de la ampliación algebraica K del campo dado K_0 y los subgrupos de los grupos de todos aquellos automorfismos de la ampliación K que dejan K_0 fijo por elementos. Rota y sus discípulos contribuyeron considerablemente (utilizando la correspondencia de Galois) al avance de la teoría de las funciones de Moebius (véase, por ejemplo, [1]).

Demos a conocer sin demostración un resultado muy importante que se debe a Rota.

Teorema 53. Supongamos que (σ, τ) es una correspondencia entre los conjuntos parcialmente ordenados y localmente finitos P y L, y sea Q el factor del conjunto P con relación al operador de clausura $\tau\sigma$. Entonces, para todos los $x \in P$, $y \in L$:

$$\sum_{z \in P : \sigma(z) = y} \mu_P(x, z) = \sum_{u \in L : \tau(u) = x} \mu_L(y, u) = \mu_Q(x, \tau y).$$

La ventaja principal del concepto de correspondencia de Galois consiste en que se puede calcular la función de Moebius μ_L de un retículo L, analizando un subconjunto arbitrario P y un álgebra de Boole $\mathscr{B}(P)$ generada por el subconjunto P.

Veamos ahora algunos problemas combinatorios en cuya resolución se emplean funciones de Moebius. Comencemos por exponer la inversión de Moebius. La inversión de las series finitas es uno de los instrumentos más útiles en el análisis combinatorio y en la teoría de las probabilidades. Su caso particular es el principio clásico de inclusiones-exclusiones (véase § 3.1). Aunque varios problemas de inversión pueden expresarse en términos de inclusiones-exclusiones, tal procedimiento parece, a menudo, artificial. Comunmente resulta posible cierta ordenación «natural» de los objetos en consideración. Esto constituye la base para la técnica de inversión de Moebius.

Teorema 54 (1ª fórmula de inversión de Moebius). Sean g y f las funciones definidas en un conjunto finito parcialmente ordenado P con valores sobre el conjunto de números reales, y

$$g(x) = \sum_{y:y \leq x} f(y) \text{ para todo } x \in P.$$

Entonces

$$f(x) = \sum_{y:y \leq x} g(y)\mu(y, x) \text{ para todo } x \in P.$$

Demostración. Fijemos x y estudiemos una suma

$$S = \sum_{y:y \leq x} g(y)\mu(y, x) = \sum_{y:y \leq x} \left(\sum_{z:z \leq y} f(z) \right) \mu(y, x).$$

Aquí en lugar de $g(y)$ hemos sustituido su valor expresado en términos de $f(z)$. Cambiemos ahora el orden de la sumación y obtengamos

$$S = \sum_{z:z \leq y} f(z) \sum_{y:y \leq x} \mu(y, x) = \sum_{z} f(z)\zeta(z, y) \sum_{y:y \leq x} \mu(y, x) =$$

$$= \sum_{z} f(z) \sum_{y:z \leq y \leq x} \zeta(z, y)\mu(y, x) = \sum_{z} f(z)\delta(z, x) = f(x),$$

es decir, el teorema queda demostrado.

Observación 1. La suposición de que las funciones g y f son reales en la formulación del teorema 54 puede omitirse, exigiendo, en vez de esto, que tomen valores en un campo de característica 0.

Observación 2. El teorema 54 es lícito también para los conjuntos parcialmente ordenados y localmente finitos. En este caso, para garantizar el carácter finito de las sumas se exige que exista un elemento $m \in P$, tal que $g(y) = 0$ para cualquier $y \not\geq m$. En este caso la función g está correctamente definida. En efecto,

$$g(x) = \sum_{y:y \leq x} f(y) = \sum_{y:m \leq y \leq x} f(y),$$

donde el número de sumandos es finito para todo conjunto parcialmente ordenado y localmente finito.

Observación 3. Por ahora no se han establecido las condiciones, bajo las cuales serían admisibles las sumas infinitas.

Teorema 55 (2ª fórmula de inversión de Moebius). Sean g y f las funciones definidas en un conjunto parcialmente ordenado local finito P con valores sobre un conjunto de números reales, y

$$g(x) = \sum_{y:y \geq x} f(y) \text{ para todo } x \in P.$$

Entonces

$$f(x) = \sum_{y:y \geq x} \mu(x, y)g(y) \text{ para todo } x \in P.$$

La demostración es plenamente análoga a la del teorema 54 y por eso se omite aquí.

Veamos unos cuantos ejemplos.

EJEMPLO 5. Sea f una función definida sobre el conjunto de números positivos enteros de orden ordinario, y

$$g(n) = \sum_{m:m\le n} f(m).$$

Entonces, en virtud del teorema 54 y del ejemplo 2, tenemos

$$f(n) = g(n) - g(n-1).$$

EJEMPLO 6. Sea $\mathscr{P}(S_n)$ un booleano, $g(B) = \sum_{A:A\subseteq B} f(A)$, y $h(B) = \sum_{A:A\supseteq B} f(A)$, donde $B\in\mathscr{P}(S_n)$. Entonces, en virtud de los teoremas 54 y 55 y del ejemplo 3, tenemos

$$f(B) = \sum_{A:A\subseteq B} (-1)^{|B|-|A|} g(A)$$

y

$$f(B) = \sum_{A:A\supseteq B} (-1)^{|B|-|A|} h(A)$$

Suponiendo $|B| = n$ y sumando separadamente en el segundo miembro de la igualdad

$$f(B) = \sum_{A:A\subseteq B} (-1)^{|B|-|A|} g(A)$$

los sumandos con $|A| = n, n-1, \ldots, 1, 0$, obtenemos:

$$f(B) = g(B) - \sum_{A:A\subset B;\,|A|=n-1} g(A) + \sum_{A:A\subset B;\,|A|=n-2} g(A) - \ldots +$$
$$+ \sum_{A:A\subset B;\,|A|=n-k} (-1)^k g(A) + \ldots + (-1)^n \sum_{A:A\subset B;\,|A|=0} g(A).$$

De la última fórmula pueden obtenerse diferentes variantes del método de inclusiones-exclusiones. Estas variantes utilizan la noción de conjunto finito. Sobre un conjunto finito S_n definamos una función ponderante $\omega(x)$, $x\in S_n$, que toma valores de cierto anillo conmutativo K. Haciendo uso de esta función $\omega(x)$, definamos la función de medida sobre el booleano $\mathscr{P}(S_n)$, la cual se denotará también con ω. Para cualquier $A\in\mathscr{P}(S_n)$ pongamos

$$\omega(A) = \begin{cases} 0, \text{ si } A = \varnothing; \\ \sum_{x\in A} w(x), \text{ si } A \neq \varnothing. \end{cases}$$

Sea K el conjunto de números reales. Entonces, si $\omega(x) = 1$ para todo $x\in S_n$, tendremos $\omega(A) = |A|$, $A\in\mathscr{P}(S_n)$, es decir, la medida coincide con la potencia del conjunto. Si $\omega(x)\ge 0$ para todo $x\in S_n$ y $\sum_{x\in S_n}\omega(x) = 1$, la

medida se denominará distribución probabilística. En este caso los elementos de $\mathcal{P}(S_n)$ se llaman sucesos y se tiene: $\omega(A) + \omega(\bar{A}) = \omega(S_n)$, donde $\bar{A} = S_n \setminus A$, $A \in \mathcal{P}(S_n)$.

Haciendo uso de las leyes de Morgan, obtenemos

$$\omega(\overline{A \cup B}) = \omega(\bar{A} \cap \bar{B});$$
$$\omega(\overline{A \cap B}) = \omega(\bar{A} \cup \bar{B}).$$

Sea ahora un conjunto $S_n = \{x_1, \ldots, x_n\}$ cuyos elementos pueden poseer o no poseer cada una de las propiedades $E_1, E_2, \ldots, E_t$. En el booleano $\mathcal{P}(S_n)$ está definida cierta medida ω. Convengamos en considerar que un elemento $x_i \in S_n$ posee la Q-propiedad, si posee las propiedades cuyos índices pertenecen al conjunto $Q \subseteq N = \{1, 2, \ldots, t\}$. Sea $Q \cup \bar{Q} = N$, $Q \cap \bar{Q} = \emptyset$, y $f(Q)$ la medida del subconjunto de elementos de S_n que poseen la Q-propiedad, y sea $g(Q)$ la medida del conjunto de elementos de S_n que poseen la $\bar{Q}$-propiedad y, quizás, otras propiedades cuyos números pertenecen a Q. En este caso es evidente la igualdad

$$g(Q) = \sum_{B:\, B \subseteq Q} f(B).$$

Aplicando las fórmulas de inversión, obtenemos para $Q = N$:

$$f(N) = \sum_{B:\, B \subseteq N} (-1)^{|Q| - |B|} g(B) = \omega(S_n) - \sum_{B:\, B \subset N;\, |B| = t-1} g(B) + \ldots +$$
$$+ (-1)^k \sum_{B:\, B \subset N,\, |B| = t-k} g(B) + \ldots + (-1)^t \sum_{B:\, B \subset N;\, |B| = 0} g(B).$$

Observemos que $f(N)$ es la medida del conjunto de elementos de S_n que no poseen ninguna de las propiedades $E_1, E_2, \ldots, E_N$; $g(B)$ es la medida del conjunto de elementos que poseen todas las propiedades con los números de $N \setminus B$, y, quizás, algunas de las propiedades con los números de B; $g(N) = \omega(S_n)$.

Es cómodo designar con la misma letra E_i, $i = 1, 2, \ldots, t$, el conjunto de elementos de S_n que poseen la propiedad E_i. En tal caso podemos escribir

$$f(N) = \omega\left(\bigcap_{i \in N} \bar{E}_i\right),$$
$$g(B) = \begin{cases} \omega(S_n), & \text{si } B = N; \\ \omega\left(\bigcap_{i \in N \setminus B} E_i\right), & \text{si } B \neq N. \end{cases}$$

Entonces,

$$\omega\left(\bigcap_{i \in N} \bar{E}_i\right) = \sum_{B:\, B \subseteq N} (-1)^{|N| - |B|} \omega\left(\bigcap_{i \in N \setminus B} E_i\right).$$

De aquí proviene que

$$\omega\left(\bigcap_{i \in N} \bar{E}_i\right) = \sum_{B:\, B \subseteq N} (-1)^{|B|} \omega\left(\bigcap_{i \in B} E_i\right).$$

Suponiendo $M(0) = \omega\left(\bigcap_{i\in N}\overline{E_i}\right)$, $A_0 = \omega(S_n)$,

$$A_k = \sum_{B:B\subseteq N;|B|=k} \omega\left(\bigcap_{i\in B} E_i\right), \text{ donde } k = 1, 2, \ldots, t,$$

obtenemos la *fórmula de Sylvester*

$$M(0) = \sum_{k=0}^{t} (-)^k A_k,$$

que representa una de las fórmulas del método de inclusiones-exclusiones.

La medida del conjunto de elementos de S_n, que poseen al menos una de la propiedades $E_1, E_2, \ldots, E_t$, se escribirá en este caso así:

$$M(1) = \omega\left(\bigcup_{i\in N} E_i\right).$$

En virtud de la igualdad evidente $M(1) = \omega(S_n) - M(0)$ y de la fórmula de Sylvester, obtenemos

$$M(1) = \sum_{k=1}^{t} (-1)^{k-1} A_k,$$

$$\omega\left(\bigcup_{i\in N} E_i\right) = \sum_{B:B\subseteq N, B\neq\varnothing} (-1)^{|B|-1}\omega\left(\bigcap_{i\in B} E_i\right)$$

Aplicando a la última relación la fórmula de inversión, obtenemos

$$\omega\left(\bigcap_{i\in N} E_i\right) = \sum_{B:B\subseteq N, B\neq\varnothing} (-1)^{|B|-1}\omega\left(\bigcup_{i\in B} E_i\right).$$

Al aprovechar las designaciones

$$A[k] = \sum_{B:B\subseteq N;|B|=k} \omega\left(\bigcup_{i\in B} E_i\right), \text{ donde } k = 1, 2, \ldots, t,$$

obtenemos

$$\omega\left(\bigcap_{i\in N} E_i\right) = \sum_{k=1}^{t} (-1)^{k-1} A[k].$$

Denotemos ahora con $M(r)$ la medida del conjunto de elementos de S_n que poseen exactamente r propiedades de la totalidad $E_1, E_2, \ldots, E_t$. Haciendo uso de la designación E_i como conjunto de elementos que poseen la propiedad E_i, podemos escribir

$$M(r) = \sum_{C:C\subseteq N;|C|=r} \omega\left(\bigcap_{i\in C} E_i \bigcap_{j\in\overline{C}} \overline{E_j}\right),$$

donde $r = 0, 1, \ldots, t$, y $\overline{C} = N \setminus C$.

Suponiendo $S_n = \bigcap_{i\in C} E_i$, de la fórmula obtenida más arriba.

$$\omega\left(\bigcap_{i\in N} \overline{E_i}\right) = \sum_{B\ B\subseteq N} (-1)^{|B|}\omega\left(\bigcap_{i\in B} E_i\right)$$

llegamos a que

$$\omega\left(\bigcap_{i\in C} E_i \bigcap_{i\in C} \overline{E_j}\right) = \sum_{B:B\subseteq C} (-1)^{|B|}\omega\left(\bigcap_{i\in C} E_i \bigcap_{j\in B} E_j\right).$$

De aquí se deduce que

$$\omega\left(\bigcap_{i\in C} E_i\right) \bigcap_{j\in C} E_j\Big) = \sum_{D:D\subseteq N;D\supseteq C} (-1)^{|D|-|C|}\omega\left(\bigcap_{i\in D} E_i\right).$$

De las últimas tres fórmulas tenemos

$$M(r) = \sum_{C:C\subseteq N;|C|=r} \quad \sum_{D:D\subseteq N;D\supseteq G} (-1)^{|D|-r}\omega\left(\bigcap_{i\in D} E_i\right).$$

Cambiemos el orden de la sumación en el segundo miembro de la última igualdad y obtengamos

$$M(r) = \sum_{D:D\subseteq N;|D|\geq r} (-1)^{|D|-r}\omega\left(\bigcap_{i\in P} E_i\right) \sum_{C:C\subseteq D;|C|=r} 1.$$

De aquí se deduce

$$M(r) = \sum_{D:D\subseteq N;|D|\geq r} (-1)^{|D|-r}\binom{|D|}{r}\omega\left(\bigcap_{i\in D} E_i\right).$$

Haciendo $|D| = k$ y usando las mismas designaciones que figuran en la fórmula de Sylvester, obtenemos en definitiva

$$M(r) = \sum_{k=r}^{l} (-1)^{k-r}\binom{k}{r} A_k,$$

donde $r = 0, 1, \ldots, l$.

EJEMPLO 7. Sea $D(n)$ un conjunto de todos los divisores de un número natural n, ordenados respecto de la divisibilidad, y

$$g(n) = \sum_{k:k|n} f(k),$$

donde $k \mid n$ significa que k divide a n. En virtud del teorema 54 y del ejemplo 4,

$$f(n) = \sum_{k:k|n} \mu(k, n)g(k) = \sum_{k:k|n} \mu\left(\frac{n}{k}\right) g(k),$$

es decir, obtenemos la fórmula de inversión de Moebius bien conocida de la teoría de los números.

Veamos algunas aplicaciones de la fórmula obtenida.

Función de Euler. La función de Euler $\varphi(n)$ se define como un número de números enteros positivos, inferiores a n y recíprocamente primos con él. Si la descomposición canónica de n tiene la forma: $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, entonces

$$\varphi(n) = (n)\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right).$$

Obtengamos esta fórmula por el método de inclusiones-exclusiones. A título de elementos tomemos los números 0, 1, 2, . . ., $n-1$. Diremos que un elemento posee la propiedad E_i, si se divide por el número p_i, $i = 1, 2, \ldots, r$. Es obvio que $\varphi(n)$ es igual al número de elementos que no poseen ninguna de las propiedades $E_1, E_2, \ldots, E_r$. El número de elementos que poseen las propiedades dadas $E_{j_1}, E_{j_2}, \ldots, E_{j_k}$, $1 \leqslant j_1 < \ldots < j_k \leqslant r$, es igual a

$$M(E_{j_1}, E_{j_2}, \ldots, E_{j_k}) = \frac{n}{p_{j_1} p_{j_2} \cdots p_{j_k}}.$$

Aplicando la fórmula de Sylvester, obtenemos

$$\varphi(n) = n + \sum_{k=1}^{r} (-1)^k \sum_{1 \leq j_1 < \ldots < j_k \leq r} \frac{n}{p_{j_1} p_{j_2} \cdots p_{j_k}} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

De aquí se desprende el carácter multiplicativo de la función $\varphi(n)$, a saber: si m y n son recíprocamente primos, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.

Denotemos con $\varphi_d(n)$ el número de números enteros positivos que son inferiores a n y que tienen con n el máximo común divisor igual a d. Entonces es obvio que $\varphi_1(n) = \varphi(n)$.

Supongamos que $d_1, d_2, \ldots, d_k$ son todos los divisores del número n, y sean $d_1', d_2', \ldots, d_k'$ sus divisores complementarios, es decir, tales que $d_i d_i' = n$, $i = 1, 2, \ldots, k$. Entonces,

$$\varphi(d_i') = \varphi\left(\frac{n}{d}\right) = \varphi_{d_i}(n).$$

Evidentemente,

$$\sum_{i=1}^{k} \varphi(d_i') = \sum_{i=1}^{k} \varphi_{d_i}(n) = n.$$

De aquí obtenemos la *fórmula de Gauss:*

$$n = \sum_{d \mid n} \varphi(d).$$

Aplicando la fórmula de inversión de Moebius, obtenemos

$$\varphi(n) = \sum_{d \mid n} \mu(d, n) d = \sum_{d \mid n} d\mu\left(\frac{n}{d}\right).$$

Cálculo de los collares. Supongamos que se tiene una reserva ilimitada de cuentas (abalorias) de k diferentes colores. ¿Cuántos son los collares compuestos de n cuentas? Convengamos en considerar iguales aquellos collares que se obtienen uno del otro por el desplazamiento cíclico de las cuentas.

Al desplazar todas las n cuentas «en círculo», descubriremos que, realizado un número determinado de desplazamientos, digamos, tras d desplazamientos, la «configuración de colores» inicial se repitirá y, además, d será

el divisor del número n. Llamaremos período a un número mínimo de desplazamientos que conducen a la configuración inicial. Así, por ejemplo,

$$bckbck \to kbckbc \to ckbckb \to bckbck,$$

es decir, el período de esta cadena es igual a 3. Supongamos que tenemos una cadena de longitud n y período d. Al realizar los desplazamientos, obtenemos d diferentes cadenas, incluida la inicial. Uniendo los extremos de cada una de dichas cadenas, tenemos un mismo collar. Más aún, solamente tales cadenas nos dan este collar. De aquí, si designamos con $M(n)$ el número de collares de longitud n y con $m(d)$, el número de cadenas de período d, llegamos a que

$$M(n) = \sum_{d:d|n} \frac{1}{d}\, m(d).$$

Por cuanto se usan las cuentas de k diferentes colores, el número de todas las cadenas de longitud n es igual a k^n y, por consiguiente,

$$k^n = \sum_{d:d|n} \frac{1}{d}\, m(d).$$

Haciendo uso de la inversión de Moebius, obtenemos

$$m(d) = \sum_{x:x|d} \mu\left(\frac{d}{x}\right) k^x.$$

De aquí encontramos que

$$M(n) = \sum_{d:d|n} \frac{1}{d} \sum_{x:x|d} \mu\left(\frac{d}{x}\right) k^x = \frac{1}{n} \sum_{d:d|n} \varphi\left(\frac{n}{d}\right) k^d,$$

donde $\varphi\left(\frac{n}{d}\right)$ es la función de Euler.

EJEMPLO 8. Coloración de los mapas. El mapa es una totalidad finita de dominios conexos en un plano, limitados con curvas suaves. Dos países, separados por cierta curva (por más de un punto), se llaman contiguos (limítrofes). Si los países están pintados de un modo tal que no haya dos países limítrofes pintados de un mismo color, la coloración se considera correcta. Sea G un mapa y $M_G(\lambda)$ el número de sus coloraciones correctas en λ colores. Un submapa G' del mapa G se obtiene de G, borrando ciertas fronteras entre los países. Cualquier mapa puede ser colorado empleando $\lambda^{|G|}$ métodos, donde $|G|$ es el número de países en el mapa G. Cada cual de estas coloraciones es correcta para un solo submapa. (Hace falta borrar las fronteras entre los países pintados de un mismo color). La relación «G' es un submapa de G» convierte el conjunto de todos los submapas del mapa G en un conjunto parcialmente ordenado y

$$\lambda^{(G)} = \sum_{G':G' \subseteq G} M_{G'}(\lambda).$$

Aplicando la inversion de Moebius, llegamos a la fórmula

$$M_G(\lambda) = \sum_{G' \cdot G' \subseteq G} \lambda^{|G'|} \mu(G', G).$$

Por razones evidentes, $M_G(\lambda)$ se denomina *polinomio cromático* del mapa G. Si no disponemos de un método sencillo para calcular los valores de μ, la búsqueda del polinomio $M_G(\lambda)$ se hace un problema bastante difícil. Los polinomios cromáticos fueron introducidos por Birkhoff al analizar el problema de cuatro colores.

Sea P un conjunto finito parcialmente ordenado con cero 0, uno 1 y una función de rango r. El polinomio

$$\chi(P; x) = \sum_{a \in P} \mu(0, a) x^{r(1) - r(a)}$$

se llama *polinomio característico del conjunto parcialmente ordenado P*. Es evidente, que él es una generalización del polinomio cromático para un conjunto parcialmente ordenado. Directamente del teorema 49 puede deducirse el siguiente resultado:

Teorema 56. Sea P un conjunto finito parcialmente ordenado con 0 y 1, que posee una función de rango. Si $P = P_1 \times P_2$, entonces

$$\chi(P; x) = \chi(P_1; x)\chi(P_2; x).$$

Ejercicios. 11. Compruébese que el polinomio característico $\chi(\mathcal{P}(S_n); x)$ del booleano $\mathcal{P}(S_n)$ es igual a $(x - 1)^n$.

12. Hállense los polinomios característicos para los conjuntos parcialmente ordenados mencionados en los ejemplos 7, 8 y 9 del § 8.1.

Al utilizar la inversión de Moebius como un medio principal, Crapo y Rota mostraron que el problema de cuatro colores y el estudio del los polinomios característicos y cromáticos son casos particulares de un problema más general, a saber, del problema crítico para geometrías combinatorias. El problema citado que consiste en la búsqueda de los conjuntos mínimos de los hiperplanos separadores para un conjunto de puntos en los espacios proyectivos finitos incluye, como casos particulares, algunos problemas de la teoría de codificación y los resultados de Segre, relacionados con la caracterización de los conjuntos independientes en un espacio proyectivo. Además, quedan establecidas las relaciones entre las álgebras de incidencia y las funciones generatrices que permiten pasar de la resolución de ciertos problemas mencionados a la búsqueda de determinadas funciones de incidencia.

Sea $S(P)$ un álgebra estándar de incidencia del conjunto parcialmente ordenado P. La relación de equivalencia $\sim$, definida en los segmentos del conjunto finito parcialmente local P, se denomina compatible, si de la condición $f(x, y) = f(u, v)$; $g(x, y) = g(u, v)$ para todos los pares de segmentos, tales que $[x, y] \sim [u, v]$, $f, g \in S(P)$, se deduce que $(f*g)(x, y) = (f*g)(u, v)$. Por ejemplo, para cualquier conjunto parcialmente ordenado P la relación

de isomorfismo es, desde luego, compatible. Precisamente esta afirmación se demuestra en el corolario 9.

Fijemos una relación de equivalencia compatible. Las clases de equivalencia de los segmentos se llamarán tipos. Examinemos un conjunto de funciones definidas en un conjunto de los tipos $\alpha, \beta, \gamma, \ldots$, con la particularidad de que la multiplicación de las funciones $f*g = h$ las definimos del modo siguiente:

$$h(\alpha) = \sum_{\beta,\ \gamma} \begin{bmatrix} \alpha \\ \beta,\ \gamma \end{bmatrix} f(\beta)g(\gamma).$$

La sumación se realiza respecto de todos los pares de tipos. El símbolo $\begin{bmatrix} \alpha \\ \beta,\ \gamma \end{bmatrix}$ es igual al número de diferentes elementos z del segmento $[x, y]$ del tipo α, tales que $[x, z]$ es un segmento del tipo β y $[z, y]$, del tipo γ. Este símbolo recibe el nombre de coeficiente de incidencia. Sea $h_\delta \in S(P)$ y

$$h_\delta(x, y) = \begin{cases} 1, \text{ si } [x, y] \text{ es del tipo } \delta; \\ 0, \text{ en el caso contrario;} \end{cases}$$

entonces,

$$(h_\beta * h_\gamma)(u, v) = \begin{bmatrix} \alpha \\ \beta,\ \gamma \end{bmatrix}.$$

Por cuanto $\sim$ es una relación compatible, el primer miembro de la última igualdad no depende de la elección concreta del intervalo $[u, v]$ del tipo α.

Un conjunto de todas las funciones definidas en los tipos forma un *álgebra reducida de incidencia* $R(P)$, la cual es isomorfa al álgebra de series de potencias formales.

En efecto, un elemento de $R(P)$ se define de un modo único por la sucesión $[a_n]$ de números reales, si ponemos $f(i, j) = a_{j-i}$, $i \leqslant j$.

El producto de elementos se define por la igualdad:

$$h(i, j) = \sum_{k:\, i \leqslant k \leqslant j} f(i, k)g(k, j) = \sum_{k:\, i \leqslant k \leqslant j} a_{k-i} b_{j-k}.$$

Al hacer $r = k - i$, $n = j - i$, obtenemos

$$h(i, j) = \sum_{r=0}^{n} a_r b_{n-r} = c_n.$$

De aquí se deduce que la aplicación del conjunto de series de potencias en $R(P)$, definida del modo siguiente:

$$F(t) = \sum_{n=0}^{\infty} a_n t^n \to f(i, j) = a_{j-i},\ j \geqslant i,$$

es un isomorfismo.

Nos hemos detenido muy brevemente en las principales direcciones

combinatorias del desarrollo de las álgebras de incidencia. Para el estudio ulterior de ellas se recomiendan las obras [1, 3, 12 y 93].

8.4. MATROIDES

La teoría de los matroides tuvo su inicio en los años 30 de nuestro siglo. En 1930 B.L. Van der Waerden examinó en su libro «Algebra moderna» una dependencia algebraica, a la par con la dependencia lineal. En 1935 H.Whitney introdujo por primera vez, deseando generalizar el concepto de grafo dual, una noción abstracta de matroide. En 1936 M. Mac Lane dió una interpretación del matroide en términos de la geometría proyectiva, lo que sirvió de base para que los matroides se denominen geometrías combinatorias, y G. Birkhoff introdujo el concepto de M-estructura (retículo matroidal) y notó que las geometrías proyectivas constituyen precisamente M-estructuras (cada elemento es una unión de puntos).

En 1942 R. Rado generalizó el teorema de P.Hall sobre el sistema de representantes distintos y mostró que los problemas combinatorios extremales pueden expresarse en términos de una estructura abstracta de independencia. En 1965 Edmonds y Fulkerson descubrieron que para el sistema dado de subconjuntos de un conjunto finito, la totalidad de todas las transversales parciales es una totalidad de subconjuntos independientes de cierto matroide que se denominó matroide transversal. Tal conexión despertó gran atención hacia los sistemas de representantes, pues muy pronto se puso de manifiesto que varios espacios de independencia, que se estudiaban con gran esmero, pueden ser representados en forma de espacios transversales.

Estos resultados, como también los obtenidos más tarde, aclararon una vinculación estrecha entre la teoría de los matroides y la teoría algebraica de retículos, con lo que se hizo posible trasladar a la teoría de los matroides los conceptos e imágenes de la geometría proyectiva, en particular, el concepto de dimensión de un espacio lineal. Merced a esta circunstancia se reveló una semejanza, bastante inesperada, entre los resultados de las diferentes ramas de la matemática discreta (teoría de los grafos, teoría de las transversales, teoría de codificación, etc.).

Los matroides, como retículos geométricos, ya se han considerado en el § 8.2. Por eso, nos limitamos aquí a recordar algunas definiciones del matroide y del retículo que le corresponde.

Se llama *pregeometría* (o *matroide*) G a un conjunto finito S con operador de clausura $(-)$ que satisface la propiedad de sustitución: para cualesquiera elementos $p, q \in S$ y para todo subconjunto $A \subseteq S$, de $p \in \overline{A \cup \{q\}}$, $p \notin \overline{A}$ se deduce $q \in \overline{A \cup \{p\}}$. Una pregeometría se llama *geometría*, si el conjunto vacío y todos los subconjuntos de un solo elemento son cerrados.

En la definición de la pregeometría G la condición de finitud del conjunto S se sustituye, a menudo, por la condición de base finita: para todo $A \subseteq S$ existe un subconjunto finito $A_f \subseteq A$ tal que $\overline{A_f} = \overline{A}$.

Los subconjuntos cerrados de una geometría se denominan *superficies*. Un conjunto de todas las superficies de la geometría, ordenado por inclusión (en el sentido teórico-conjuntista), forma un retículo geométrico, el cual define la geometría G con una exactitud de hasta un isomorfismo (véase teorema 36).

Sea $L(G)$ un retículo de la geometría $G = (S, \bar{\ })$. Se llama *rango* r de la superficie $\overline{A}$ a la longitud de la cadena máxima desde el elemento nulo hasta $\overline{A}$ en $L(G)$ (véase teorema 30) y se llama rango del conjunto A al rango de su clausura en $L(G)$, es decir, $r(A) = r(\overline{A})$ para todo $A \subseteq S$. Por consiguiente, en virtud del teorema 31, para la función de rango r queda cumplida la propiedad principal

$$r(A \cup B) + r(A \cap B) \leqslant r(A) + r(B),$$

cualesquiera que sean A, $B \subseteq S$. Dicha propiedad generaliza la propiedad correspondiente de la función de dimensión de los subespacios lineales de un espacio proyectivo (donde tiene lugar la igualdad). Además, $r(\varnothing) = 0$ y $r(A) \leqslant r(A \cup \{p\}) \leqslant r(A) + 1$, cualesquiera que sean $A \subseteq S$ y $p \subseteq S$. Si $r(A) = |A|$, donde $|A|$ es la potencia del subconjunto $A \subseteq S$, A será independiente (véase teorema 35). De lo contrario, $r(A) < |A|$, y A es dependiente. El conjunto $A \subseteq S$ se denomina *generador* para la geometría G, si $\overline{A} = S$. Los conjuntos generadores independientes de una geometría se denominan *base*. Los conjuntos dependientes mínimos (por inclusión) de una geometría se llaman *ciclos*.

Los términos «conjuntos dependientes e independientes», «bases» y «conjuntos generadores» son bien conocidos del álgebra lineal. La denominación «ciclo» se ha tomado de la teoría de los grafos, en cuyos márgenes, según veremos, los ciclos de un matroide corresponden plenamente a los del grafo.

Demos ahora una serie de otras definiciones del matroide a través del rango, conjuntos independientes, bases y ciclos, respectivamente, y luego demostremos la equivalencia de ellos.

Sea S un conjunto finito y sea r una función de números enteros sobre el conjunto $\mathfrak{P}(S)$. Un *par* (S, r) *se llama matroide* $M'(S, r)$, y $r(A)$, rango de $A \subseteq S$, si para todos los A, $B \subseteq S$ se cumplen las siguientes condiciones:

$R1)$ $0 \leqslant r(A) \leqslant |A|$;

$R2)$, si $A \subseteq B$, entonces $r(A) \leqslant r(B)$ (monotonía);

$R3)$ $r(A \cup B) + r(A \cap B) \leqslant r(A) + r(B)$ (semimodularidad).

Sea S un conjunto finito y r, una función de números enteros sobre el conjunto $\mathfrak{P}(S)$. Un *par* (S, r) *se llama matroide* $M'(S, r)$, y $r(A)$, rango de $A \subseteq S$, si para cualesquiera $A \subseteq S$ y a, $b \in S$ son lícitas las siguientes condiciones:

$R4)$ $r(\varnothing) = 0$;

$R5)$ $r(A) \leqslant r(A \cup \{a\}) \leqslant r(A) + 1$;

$R6)$ si $r(A) = r(A \cup \{a\}) = r(A \cup \{b\})$, entonces $r(A \cup \{a, b\}) = r(A)$

Sea (S, r) un matroide $M(S, r)$ y $S' = \{a \in S \mid r(\{a\}) = 0\}$. Entonces, $r(A) = r(A \setminus S')$ para todo $A \subseteq S$, y, por lo tanto, $(S \setminus S', r)$ es un matroide que tiene, de hecho, la misma construcción que (S, r). Para $a, b \in S$ supongamos $a \equiv b$, cuando y sólo cuando $r(\{a, b\}) = 1$. En tal caso, $\equiv$ es la relación de equivalencia, y si $[a_1], \ldots, [a_n]$ son clases contiguas, entonces $r([a_1] \cup \ldots \cup [a_n]) = r(\{a_1, \ldots, a_n\})$ no depende de cómo se eligen los representantes. Por consiguiente, podemos identificar los elementos correspondientes sin perder la generalidad de nuestros razonamientos. Suponiendo hecha tal identificación, pongamos para cualquier $A \subseteq S$:

$$\overline{A} = \{a \in S \mid r(A \cup \{a\}) = r(A)\}.$$

Obtenemos una geometría, con la particularidad de que su rango se determina por la definición de él sobre los conjuntos cerrados. Quiere decir que la construcción de un matroide puede determinarse partiendo del retículo de las superficies de la geometría asociada con el matroide citado.

Sea S un conjunto finito y sea F una familia no vacía de subconjuntos del conjunto S. Entonces, el *par* (S, F) *se llama matroide* $M(S, F)$, y los elementos de la familia F, conjuntos independientes $M(S, F)$, si se cumplen las siguientes condiciones:

$F1)$ $\varnothing \in F$;

$F2)$ si $A \subseteq B$, $B \in F$, entonces $A \in F$;

$F3)$ si A_1 y A_2 son subconjuntos independientes máximos del conjunto A, entonces $|A_1| = |A_2|$.

Cabe notar que el axioma $F1)$ se deduce, de hecho, de $F2)$.

Sea S un conjunto finito y sea C, una familia de sus subconjuntos (ciclos) no vacíos. Entonces el *par* (S, C) se denomina matroide $M(S, C)$, si se cumplen las siguientes condiciones:

$C1)$ ninguno de los ciclos es un subconjunto propio de otro ciclo;

$C2)$ si C_1 y C_2 son ciclos diferentes, y $a \in C_1 \cap C_2$, existe un ciclo $C_3 \in C$, tal que $C_3 \subseteq (C_1 \cup C_2) \setminus \{a\}$.

Sea S un conjunto finito y sea B una familia de sus subconjuntos (bases) no vacíos. Entonces el *par* (S, B) *se denomina matroide* $M(S, B)$, si se cumplen las siguientes condiciones:

$B1)$ para todos los A, $B_1 \subseteq S$, si $A \subseteq B_1$, $A \neq B_1$ y $B_1 \in B$, entonces $A \notin B$;

$B2)$ para cualesquiera bases B_1 y B_2 y para todo $a \in B_1$ existe $b \in B_2$, tal que $(B_1) \setminus \{a\} \cup \{b\} \in B$.

Dos matroides, $(S_1, \bar{\ })$ y $(S_2, \bar{\ })$ se llaman *isomorfos*, si existe tal aplicación biunívoca φ: $S_1 \to S_2$, que $a \in A$ cuando y sólo cuando $\varphi(a) \in \overline{\varphi(A)}$, donde $A \subseteq S_1$.

Teorema 57. Supongamos que $(S, \bar{\ })$ es un matroide sobre el conjunto finito S; r, una función de rango; y F, C, B, familias de conjuntos independientes, de ciclos y de bases del matroide $(S, \bar{\ })$, respectivamente. Entonces, en $(S, \bar{\ })$ se cumplen:

a) las condiciones $R1)$—$R6)$ de los matroides $M(S, r)$ y $M'(S, r)$;

b) las condiciones $F1$)—$F3$) del matroide $M(S, F)$;

c) las condiciones $C1$) y $C2$) del matroide $M(S, C)$;

d) las condiciones $B1$ y $B2$) del matroide $M(S, B)$;

o bien, lo que es equivalente, cada matroide $(S, \bar{\ })$ es matroide $M(S, r)$, $M'(S, r)$, $M(S, F)$, $M(S, C)$ y $M(S, B)$ simultáneamente.

Demostración. La validez de las condiciones $R3$), $R4$) y $R5$) en $(S, \bar{\ })$ ya quedó comprobada. Obtengamos las demás condiciones de las tres mencionadas, mediante una cadena de afirmaciones más sencillas.

1. Las condiciones $R4$) y $R5$) traen consigo $R1$) y $R2$). Demostremos primero la siguiente afirmación.

Lema 13. Para todos los A, $B \subseteq S$, si $A \subseteq B$, entonces

$$0 \leqslant r(B) - r(A) \leqslant |B \setminus A|.$$

Demostración del lema. Si $A = B$, la afirmación del lema es evidente. Sea $A \neq B$ y $B \setminus A = \{a_1, \ldots, a_k\}$. Entonces, en virtud de la propiedad $R5$), tenemos:

$$0 \leqslant r(A \cup \{a_1\}) - r(A) \leqslant 1;$$
$$0 \leqslant r(A \cup \{a_1, a_2\}) - r(A \cup \{a_1\}) \leqslant 1;$$
$$0 \leqslant r(A \cup \{a_1, a_2, a_3\}) - r(A \cup \{a_1, a_2\}) \leqslant 1;$$
$$0 \leqslant r(B) - r(B \setminus \{a_k\}) \leqslant 1.$$

Sumemos todas estas desigualdades y obtengamos la desigualdad requerida: $0 \leqslant r(B) - r(A) \leqslant |B \setminus A|$. El lema está demostrado.

Directamente del lema se desprende la validez de la condición $R2$) y de la $R1$), pero en el último caso es necesario sustituir en la desigualdad $A = \varnothing$ y hacer uso de la propiedad $R4$).

2. Las condiciones $R2$) y $R3$) traen consigo $R6$). Sea $r(A) = r(A \cup \{a\}) = r(A \cup \{b\})$, donde $A \subseteq S$; $a, b \in S$. Se pide demostrar que $r(A \cup \{a, b\}) = r(A)$. Si $a = b$, *la afirmación es evidente. Si* $a \neq b$, entonces, en virtud de la condición de semimodularidad $R3$), podemos escribir

$$2r(A) = r(A \cup \{a\}) + r(A \cup \{b\}) \geqslant r(A \cup \{a, b\}) + r(A),$$

de donde tenemos: $r(A \cup \{a, b\}) \leqslant r(A)$. Pero, $A \subseteq A \cup \{a, b\}$, y, en virtud de $R2$): $r(A) \leqslant r(A \cup \{a, b\})$. Quiere decir que $r(A \cup \{a, b\}) = r(A)$. La implicación está demostrada y, de este modo, la comprobación de las condiciones del punto a) se da por terminado.

Comprobemos la validez en $(S, \bar{\ })$ de las condiciones $F1$)—$F3$). Evidentemente, la condición $R4$) trae consigo $F1$)

3. La condición $R5$) trae consigo $F2$). Demostrémoslo por reducción al absurdo. Sea $A \subseteq B$ y $B \in F$, pero A es dependiente. Entonces, $r(A) < |A|$. En virtud del lema 13, tenemos

$$r(B) \leqslant r(A) + |B \setminus A| < |A| + |B \setminus A| = |B|.$$

Por consiguiente, B es dependiente y, por lo tanto, $B \notin F$. Hemos llegado a una contradicción. Por eso, $A \in F$, lo que se trataba de demostrar.

4. La condición $R6$) trae consigo la condición $F3$). Sea $A, B \subseteq S$. Directamente de $R6$) se desprende que si $r(A \cup \{a\}) = r(A)$ para todo $a \in B$, entonces $r(A \cup B) = r(A)$. Aprovechemos este hecho para demostrar nuestra implicación. Sean A_1 y A_2 los subconjuntos independientes máximos del conjunto A. Es evidente que $A_1 \nsubseteq A_2$, es decir, $A_1 \setminus A_2 \neq \varnothing$. Más aún, para todo $a \in (A_1 \setminus A_2)$ queda válida la igualdad $r(A_2 \cup \{a\}) = r(A_2)$. Por consiguiente,

$$r(A_1 \cup A_2) = r(A_2 \cup (A_1 \setminus A_2)) = r(A_2).$$

Análogamente, $r(A_1 \cup A_2) = r(A_1)$. De aquí, $r(A_1) = r(A_2)$, es decir, $|A_1| = |A_2|$ y la validez de la condición $F3$) y, junto con ella, del punto b) queda establecida.

5. Las condiciones $R1$)—$R3$) traen las condiciones $C1$) y $C2$). Directamente de la definición del ciclo y de la condición de monotonía $R2$) obtenemos que un subconjunto $A \subseteq S$ es un ciclo cuando y sólo cuando para todo elemento $a \in A$ se verifica la igualdad

$$r(A \setminus \{a\}) = |A| - 1.$$

De aquí se deduce la validez de la condición $C1$), a saber, ningún ciclo es subconjunto propio de otro ciclo.

Luego, sean C_1 y C_2 unos ciclos arbitrarios de un matroide, tales que $C_1 \neq C_2$ y $a \in (C_1 \cap C_2)$. Entonces, $C_1 \cap C_2 \neq C_1$, y por consiguiente, $(C_1 \cap C_2) \in F$. En virtud de las condiciones de monotonía $R2$) y de semimodularidad $R3$), obtenemos

$$\begin{aligned} r((C_1 \cup C_2) \setminus \{a\}) \leqslant r(C_1 \cup C_2) \leqslant r(C_1) + r(C_2) - r(C_1 \cap C_2) = \\ = (|C_1| - 1) + (|C_2| - 1) - |C_1 \cup C_2| = \\ = |C_1 \cup C_2| - 2 \leqslant |(C_1 \cup C_2) \setminus \{a\}|. \end{aligned}$$

Por consiguiente, $((C_1 \cup C_2) \setminus \{a\}) \notin F$. Por eso, existe tal ciclo C_3 que $C_3 \subseteq ((C_1 \cup C_2) \setminus \{a\})$. La validez de la condición $C2$) queda establecida.

6. Las condiciones $F2$) y $F3$) traen las condiciones $B1$) y $B2$). Sean B_1 y B_2 las bases de un matroide. Está claro que B_1 y $B_2 \in F$. Sea $B_1 \subseteq B_2$, pero $B_1 \neq B_2$. Entonces, en virtud de la condición $F3$), en B_2 existe un elemento $a \notin B_1$, tal que $B_1 \cup \{a\} \in F$. Esto contradice el hecho de que B_1 es una base del matroide. Quiere decir que $B_2 \notin B$, y la validez de la condición $B1$)queda establecida.

Sea ahora $a \in B_1$. Es evidente que $(B_1 \setminus \{a\}) \in F$. Se sabe que $|B_1| = |B_2|$. De aquí, $|B_2| = |B_1 \setminus \{a\}| + 1$. Debido a la condición $F3$), en B_2 existe un elemento $b \in (B_1 \setminus \{a\})$, tal que $((B_1 \setminus \{a\}) \cup \{b\}) \in F$. Pero, por cuanto $|(B_1 \setminus \{a\}) \cup \{b\}| = |B_1| = |B_2|$, entonces $((B_1 \setminus \{a\} \cup \cup \{b\}) \in B$, y, por tanto, la condición $B2$) se cumple. El teorema está demostrado.

Demostrando el teorema 57, hemos establecido, de hecho, la validez de las siguientes afirmaciones.

Corolario 11. Cada matroide $M(S, r)$ es a la vez un matroide $M(S, C)$.

Cada matroide $M'(S, r)$ es a la vez un matroide $M(S, F)$ y un matroide $M(S, B)$. Cada matroide $M(S, F)$ es un matroide $M(S, B)$.

Seguimos demostrando la equivalencia de las definiciones del matroide.

Proposición 4. Cada matroide $M(S, r)$ es un matroide $M'(S, r)$.

Demostración. Ya hemos demostrado que las condiciones $R2$) y $R3$) traen consigo $R6$). La condición $R4$) se deduce obviamente de $R1$). Comprobemos que las condiciones $R2$) y $R3$) traen consigo $R5$) y, de este modo, tendremos demostrada la sugestión. En efecto, si $a \in A$, entonces $r(A \cup \{a\}) = r(A)$. Si, en cambio, $a \in (S \setminus A)$, entonces, en virtud de las condiciones $R2$) y $R3$),

$$r(A) + 1 \geqslant r(A) + r(\{a\}) \geqslant r(A \cup \{a\}) + r(\varnothing) = r(A \cup \{a\}) \geqslant r(A).$$

Por consiguiente, $r(A) \leqslant r(A \cup \{a\}) \leqslant r(A) + 1$ para todo $A \subseteq S$ y todo $a \in S$, lo que se trataba de demostrar.

Teorema 58. Cada matroide $M(S, F)$ es también un matroide $(S, \bar{\ })$ con la familia F de conjuntos independientes.

Demostración. Sea una familia F de conjuntos independientes que satisfacen los axiomas $F1$)—$F3$). Llamemos rango de A a la potencia total de los subconjuntos independientes máximos del conjunto A y denotémoslo con $r(A)$. Definamos la aplicación $A \to \overline{A}$, al poner $a \in \overline{A}$ cuando y sólo cuando $a \in A$, o bien cuando existe un subconjunto $B \subseteq A$, tal que $B \in F$ y $(B \cup \{a\}) \notin F$. Demostremos que la aplicación $A \to \overline{A}$, definida de este modo, es un operador de clausura con la propiedad de sustitución.

Las propiedades «$A \subseteq \overline{A}$» y «si $A \subseteq B$, entonces $\overline{A} \subseteq \overline{B}$» se cumplen evidentemente. Con el fin de demostrar la propiedad de idempotencia $\overline{\overline{A}} = \overline{A}$, mostremos al principio que $r(\overline{A}) = r(A)$ para todo $A \subseteq S$. Supongamos lo contrario. Sea que existen los conjuntos $A_1, A_2 \in F$, tales que $A_1 \subseteq A$, $A_2 \subseteq \overline{A}$, y $|A_1| = r(A) < r(\overline{A}) = |A_2|$. Entonces, en virtud de la condición F3), existe un elemento $a \in A_2$ que satisface la condición $A_1 \cup \{a\} \in F$, con la particularidad de que $a \in (\overline{A} \setminus A)$ porque el conjunto A_1 es máximo. Elijamos un subconjunto máximo $A' \subseteq A$, tal que $A' \in F$ y $(A' \cup \{a\}) \notin F$. En este caso, $r(A) = |A'| < |A_1 \cup \{a\}|$, de donde, en virtud de $F3$), $(A' \cup \{a\}) \in F$, lo que es imposible. Por consiguiente, $r(\overline{A}) = r(A)$ para todo $A \subseteq S$.

Ahora, sea $\overline{\overline{A}} \neq \overline{A}$, o bien, lo que es equivalente, $b \in (\overline{\overline{A}} \setminus \overline{A})$. En este caso, $(A_1 \cup \{b\}) \in F$ para todos los $A_1 \in F$, $A_1 \subseteq A$, y obtenemos

$$r(\overline{\overline{A}}) \geqslant \max_{A_1 \in F, A_1 \subseteq A} |A_1 \cup \{b\}| = r(A) + 1 = r(\overline{A}) + 1,$$

lo que contradice el hecho que acabamos de demostrar. Así pues, $\overline{\overline{A}} \setminus \overline{A} = \varnothing$, y la idempotencia está establecida.

Nos resta mostrar que la aplicación $A \to \overline{A}$ satisface la propiedad de sustitución. Supongamos que $a, b \in S$, $A \subseteq S$ y $a \notin \overline{A}$, $a \in (\overline{A \cup \{b\}})$. De la definición de clausura se deduce la existencia de tal conjunto $A_1 \in F$, $A_1 \subseteq (A \cup \{b\})$, que $(A_1 \cup \{a\}) \notin F$. Por cuando $a \notin \overline{A}$, tenemos $b \in A_1$ y $A_2 = ((A_1 \setminus \{b\}) \cup \{a\}) \in F$. De aquí,

$$A_2 \cup \{b\} = ((A_1 \setminus \{b\}) \cup \{a\}) \cup \{b\} = (A_1 \cup \{a\}) \notin F.$$

Por consiguiente, con arreglo a la definición de aplicación $A \to \overline{A}$, tenemos $b \in \overline{A \cup \{a\}}$. De este modo, el axioma de sustitución queda demostrado.

Por fin, es obvio que $A \in F$ cuando y sólo cuando $a \notin \overline{A \setminus \{a\}}$ para todo $a \in A$, es decir, el matroide $(S, \overline{\ })$ cuenta con una totalidad de conjuntos independientes, tal que coincide exactamente con la familia F del matroide $M(S, F)$. El teorema está demostrado.

Sea $M(S, C)$ un matroide. Un subconjunto $A \subseteq S$ se llama independiente, si no contiene ciclos. Denotemos con F una familia de conjuntos independientes del matroide $M(S, C)$. Está claro que $C_1 \in C$ cuando y sólo cuando $C_1 \notin F$ y si de $A \subseteq C_1$ y $A \neq C_1$ se deduce que $A \in F$.

Proposición 5. Supongamos que $A \subseteq S$ y $a \in S$. Entonces, si $A \in F$ y $(A \cup \{a\}) \notin F$, existe el único ciclo C_1 del matroide, tal que $C_1 \subseteq (A \cup \{a\})$. Además, es obvio que $a \in C_1$.

Demostración. Supongamos que existen dos ciclos C_1 y C_2 tales que $C_1 \neq C_2$, $a \in C_1 \subseteq (A \cup \{a\})$ y $a \in C_2 \subseteq (A \cup \{a\})$. Entonces, en virtud de la condición $C2$), existe un ciclo C_3, donde $C_3 \subseteq ((C_1 \cup C_2) \setminus \{a\}) \subseteq A \in F$, lo que es imposible. Por consiguiente, no existen tales dos ciclos y la proposición queda demostrada.

Teorema 59. El matroide $M(S, C)$ es a la vez matroide $M(S, F)$.

Demostración. Es evidente que las condiciones $F1$) y $F2$) se cumplen. Comprobemos la condición $F3$). Sean A_1 y A_2 subconjuntos independientes máximos diferentes de A. Entonces, $A_1 \setminus A_2 = \varnothing$, y $A_2 \setminus A_1 = \varnothing$. Supongamos $a \in (A_2 \setminus A_1)$. Entonces, $(A_1 \cup \{a\}) \notin F$, y, por lo tanto, existe un ciclo C_1 tal que $a \in C_1 \subseteq (A_1 \cup \{a\})$. Más aún, $C_1 \cap (A_1 \setminus A_2) \neq \varnothing$, de lo contrario $C_1 \subseteq A_2$. Supongamos que $b \in (C_1 \cap (A_1 \setminus A_2))$ y $A_3 = (A_1 \setminus \{b\}) \cup \{a\}$. Observemos que $|A_3| = |A_1|$.

Demostremos ahora que $A_3 \in F$. Efectivamente, es obvio que $(A_1 \setminus \{b\}) \in F$. Supongamos que $A_3 \notin F$. En este caso existe un ciclo C_2, tal que $a \in C_2 \subseteq A_3 \subseteq (A_1 \cup \{a\})$. Además, $C_2 \neq C_1$, puesto que $b \notin C_2$. Hemos llegado a la contradicción con la condición. Quiere decir que $A_3 \in F$.

El conjunto A_3 es un subconjunto independiente máximo del conjunto A. Demostrémoslo. Supongamos que A' es un subconjunto independiente máximo del conjunto A, tal que $A_3 \subseteq A'$, y $|A_1| < |A'|$. El elemento $b \notin A'$, pues de lo contrario sería $A_1 \subseteq A'$ y $|A_1| < |A'|$. Entonces, $(A' \cup \{b\}) \notin F$. Por consiguiente, existe un ciclo C' tal que $b \in C' \subseteq (A' \cup \{b\})$ y, más aún, $C' \cap (A' \setminus A_1) \neq \varnothing$, puesto que de lo contrario $C' \subseteq A_1$. Sea $c \in (C' \cap (A' \setminus A_1))$. Entonces, $((A' \setminus \{c\}) \cup \{b\}) \in F$. Esto se establece por reducción al absurdo, al igual que hemos demostrado que $A_3 \in F$. Pero, $A_1 \subseteq ((A' \setminus \{c\}) \cup \{b\})$ y $|A_1| < |(A' \setminus \{c\}) \cup \{b\}| = |A'|$; hemos llegado a una contradicción. Por consiguiente, A_3 es un subconjunto independiente máximo del conjunto A.

Así pues, A_3 y A_2 son subconjuntos independientes máximos del con-

junto A. Si $A_3 = A_2$, entonces $|A_1| = |A_2|$. Si $A_3 \neq A_2$, observaremos que $|A_3 \Delta A_2| < |A_1 \Delta A_2|$, donde $A \Delta B$ es la diferencia simétrica de los conjuntos.

Al repetir de manera análoga a A_3 el proceso de construcción de los conjuntos independientes $A_n (|A_n| = |A_1|)$, $(A_n \Delta A_2| < |A_{n-1} \Delta A_2|$; $n = 4, 5, \ldots)$, llegaremos, tras un número finito de pasos, a un subconjunto independiente máximo A_n del conjunto A, tal que $A_n = A_2$, y, por consiguiente, demostremos que $|A_1| = |A_2|$. El teorema está demostrado.

Sea $M(S, B)$ un matroide. Un subconjunto $A \subseteq S$ se llama *independiente*, si existe una base B_1, tal que $A \subseteq B_1$. Denotemos con F una familia de conjuntos independientes del matroide $M(S, B)$. Es evidente que las bases del matroide $M(S, B)$ son conjuntos independientes máximos del matroide $M(S, B)$.

Proposición 6. Para cualesquiera bases B_1 y B_2 del matroide $M(S, B)$ se verifica la igualdad $|B_1| = |B_2|$.

Demostración. Supongamos que $B_1 \neq B_2$. En tal caso $B_1 \setminus B_2 \neq \varnothing$, y $B_2 \setminus B_1 \neq \varnothing$, en virtud del axioma $B1$). Sea $a \in (B_1 \setminus B_2)$. Entonces, según el axioma $B2$), existe un elemento $b \in (B_2 \setminus B_1)$, tal que $B_3 = ((B_1 \setminus \{a\}) \cup \{b\}) \in B$. Observemos que $|B_3| = |B_1|$. Si $B_3 \subseteq B_2$, entonces $B_3 = B_2$ respecto del axioma $B1$). Si $B_3 \not\subseteq B_2$, observaremos $|B_3 \Delta B_2| < |B_1 \Delta B_2|$. Repitiendo el proceso de construcción de las bases, igual que se hizo más arriba, llegaremos, tras un número finito de pasos, a una base B_n, tal que $B_n \subseteq B_2$, es decir, $B_n = B_2$, y, por consiguiente, obtendremos $|B_1| = |B_2|$.

Teorema 60. Cada matroide $M(S, B)$ es un matroide $M(S, F)$.

Demostración. Es evidente que las condiciones $F1$) y $F2$) se cumplen. Demostremos la validez de la condición $F3$). Sean A_1 y A_2 subconjuntos independientes máximos diferentes del conjunto A. Entonces, existe una base B_i tal que $A_i = B_i \cap A$, donde $i = 1, 2$. Supongamos que $|A_1| < |A_2|$. Observemos que $(B_1 \setminus B_2) \setminus A = \varnothing$. En efecto, supongamos que esto no es así y $B_1 \subseteq A \cup B_2$. Entonces, $|A_2 \setminus A_1| = |(B_2 \setminus B_1) \cap A| \leqslant |B_2 \setminus B_1| = |B_1 \setminus B_2|$ = (en virtud de la proposición 6) = $|(B_1 \setminus B_2) \cap A| = |A_1 \setminus A_2|$, lo que contradice la suposición de que $|A_1| < |A_2|$. Quiere decir que $(B_1 \setminus B_2) \setminus A = \varnothing$. Ahora hagamos uso de la condición B2), sustituyendo por turno cada elemento de $(B_1 \setminus B_2) \setminus A$ por los elementos de $B_2 \setminus B_1$, y, de este modo, determinando la base B', donde $A_1 \subseteq B' \cap A$, y, $B' \cap (A_2 \setminus A_1) \neq \varnothing$. Si $|A_1| < |A_2|$, entonces $|(B_1 \setminus B_2) \cap A| = |A_1 \setminus A_2| < |A_2 \setminus A_1| = |(B_2 \setminus B_1) \cap A|$, de donde obtenemos: $|(B_1 \setminus B_2) \setminus A| > |(B_2 \setminus B_1) \setminus A|$. Por consiguiente, $A_1 \neq B' \cap A$. Pero, esto contradice el hecho de que A_1 es un conjunto independiente máximo del conjunto A. Por consiguiente, $|A_1| = |A_2|$, y el teorema está demostrado.

Con el teorema 60 se finaliza la demostración de equivalencia de las definiciones del matroide.

Fig.8.33.

En el § 6.3 se han aducido ejemplos de los matroides como sistemas de conjuntos sobre los cuales se resuelven correctamente, con ayuda del algoritmo «avido», los problemas de optimización combinatoria. Veamos otros ejemplos de los matroides. La comprobación del cumplimiento de los axiomas del matroide se omitirá a menudo en la exposición que sigue, quedándose ello a cargo del lector.

Ejemplos de los matroides. 1. *Matroides libres.* Un matroide sin ciclos sobre el n-conjunto S se denomina *libre* y se denota F_n. Es obvio que el matroide libre es un matroide en el cual cada conjunto está cerrado. Es fácil ver que el retículo de superficies del matroide libre F_n es isomorfo al retículo de todos los subconjuntos del n-conjunto. En la fig. 8.33 están expuestos los matroides libres F_1, F_2, F_3 y F_4.

2. *Matroides homogéneos.* Un matroide sobre el n-conjunto S, de cuyas bases sirven todos los k-subconjuntos y de ciclos, todos los $(k+1)$-subconjuntos, recibe el nombre de matroide *homogéneo* y se designa $U_k(n)$.

3. *n-particiones del conjunto.* Llamemos *n-partición* tal recubrimiento de un conjunto, donde cada subconjunto de n elementos está contenido en uno y sólo un subconjunto que integra el recubrimiento. A toda n-partición le corresponde un matroide, en el cual serán conjuntos cerrados:

a) todos los subconjuntos que se componenen no menos que de n elementos;

b) todos los miembros del recubrimiento;

c) el propio conjunto.

Para un subconjunto arbitrario $A \subseteq S$ la clausura $\overline{A}$ se define aquí del modo siguiente:

$$\overline{A} = \begin{cases} A, \text{ si } A \text{ contiene menos de } n \text{ elementos;} \\ B, \text{ si } A \text{ contiene no menos de } n \text{ elementos, y } A \text{ está} \\ \quad \text{contenido en el miembro del recubrimiento } B; \\ S, \text{ en el caso contrario.} \end{cases}$$

4. *Geometría de Wille de orden n.* Supongamos que un conjunto de puntos S satisface, junto con los conjuntos de los subconjuntos K y F (de curvas y de superficies, respectivamente) las condiciones:

a) cualesquiera $n+1$ puntos distintos yacen en la única curva, y cada curva contiene no menos de $n+1$ puntos distintos;

b) cualesquiera $n+2$ puntos distintos, que no están situados en una misma curva, yacen en la única superficie, y cada superficie contiene por lo menos $n+2$ puntos distintos que no están en una misma curva;

c) junto con cualesquiera $n + 1$ puntos distintos pertenece también a la superficie toda la curva definida por los puntos;

d) si dos superficies están situadas en la clausura de un sobconjunto S de $(n + 3)$ elementos, la intersección de dichas superficies contiene por lo menos n + 1 puntos distintos.

La geometría dada se denomina *geometría de Wille* de orden n. El subconjunto $A \subseteq S$ está cerrado en esta geometría, si y sólo si contiene todas las curvas y todas las superficies que pasan por sus puntos. La relación de clausura sobre S en esta geometría se define como $A \rightarrow \overline{A}$, donde $\overline{A}$ es la intersección de todos los subconjuntos cerrados que contienen A.

Si $n = 1$, la geometría de Wille representa la geometría proyectiva clásica.

5. *Matroides lineales.* Sea S un subconjunto finito del espacio vectorial V. Supongamos que el conjunto de vectores $A = \{a_1, \ldots, a_k\} \subseteq S$ pertenece a F cuando y sólo cuando los vectores $a_1, \ldots, a_k$ son linealmente independientes en V. En este caso se comprueba con facilidad que F es una familia de conjuntos independientes de cierto matroide M. La función de rango r de este matroide coincide con la dimensión del subespacio tendido sobre dichos vectores. Todo matroide isomorfo al matroide descrito M se denomina *lineal*.

6. *Matroides algebraicos.* Sea F un campo, y K, su ampliación. Diremos que el conjunto $\{a_1, a_2, \ldots, a_k\}$ de elementos de K es algebraicamente dependiente, si los elementos $a_1, a_2, \ldots, a_k$ satisfacen la ecuación polinomial de la forma $f(a_1, a_2, \ldots, a_k) = 0$, donde los coeficientes de f son elementos del campo F. En el caso contrario, $a_1, a_2, \ldots, a_k$ son algebraicamente independientes sobre el campo F.

Proposición 7. Sea S un subconjunto finito de ampliación del campo F; el subconjunto $A \subseteq S$ pertenece a F cuando y sólo cuando los elementos del conjunto A son algebraicamente independientes sobre el campo F. En este caso F es una familia de conjuntos independientes de cierto matroide sobre el conjunto S.

La demostración de este resultado no ofrece grandes dificultades, por lo cual se omite aquí.

7. *Matroides cíclicos de los grafos.* Sea $G = (X, S)$ un grafo no orientado sin lazos, con un conjunto de vértices X y un conjunto de aristas S. Definamos ahora sobre el conjunto S un matroide $M(G)$ llamado de *arista* (*poligonal* o *cíclico*) del grafo G)) del modo siguiente. Si $a, b \in X$ y $A \subseteq S$, entonces la arista $(a, b) \in A$, si y sólo si los vértices a y b son A-conexos, es decir, si existe tal sucesión de aristas $(a_0, a_1), (a_1, a_2), \ldots, (a_{n-1}, a_n)$ del conjunto A, que $a_0 = a$, y $a_n = b$.

Teorema 61. El par $(S, \bar{\ })$, donde S es un conjunto de aristas del grafo $G = (X, S)$, es un matroide.

Demostración. Todas las propiedades del matroide son evidentes, salvo, quizás, la de sustitución. Supongamos que los vértices a y b son A-conexos.

Entonces, existe una sucesión conexiva de aristas $(a_0, a_1), \ldots, (a_{n-1}, a_n)$, para la cual el número n es mínimo. Afirmamos que no hay arista que se encuentre dos veces en esta sucesión. En efecto, sea $0 \leqslant i < j \leqslant n-1$, y $(a_i, a_{i+1}) = (a_j, a_{j+1})$. Ahora, si $a_i = a_j$, y $a_{j+1} = a_j$, entonces, suprimiendo las aristas $(a_{i+1}, a_{i+2}), \ldots, (a_j, a_{j+1})$ en la sucesión, obtenemos una sucesión conexiva más corta. Si $a_i = a_{j+1}$, y $a_{j+1} = a_j$, podemos suprimir todas las aristas $(a_i, a_{i+1}), \ldots, (a_j, a_{j+1})$. Demostremos ahora la propiedad de sustitución para el operador de clausura. Sea $p \in \overline{A \cup \{q\}}$, donde $p = (a, b)$ y $q = (c, d)$. Supongamos que $s_0, \ldots, s_{n-1} \in (A \cup \{q\})$ es la sucesión más corta de aristas que une a y b. Por cuanto $p \notin A$, entonces, una de las aristas $s_0, \ldots, s_{n-1}$ ha de coincidir con q. De conformidad con la observación hecha más arriba, sólo una de las aristas $s_0, s_1, \ldots, s_{n-1}$, digamos, s_i, es igual a la arista q. Mas, en este caso, la sucesión $s_{i+1}, \ldots, s_{n-1}, q, s_0, \ldots, s_{i-1}$ unirá los vértices c y d. De aquí, $q \in \overline{A \cup \{p\}}$. El teorema está demostrado.

Un matroide M sobre el conjunto S se llama *gráfico*, si es isomorfo al matroide cíclico de algún grafo.

Proposición 8. Sea $M(G)$ un matroide cíclico del grafo $G = (X, S)$. Resultan válidas las suguientes afirmaciones:

a) el subconjunto de aristas $A \subseteq S$ es un conjunto independiente del matroide $M(G)$ cuando y sólo cuando el subgrafo de esqueleto $G = (X, A)$ es un bosque;

b) el subconjunto $B \subseteq S$ es una base del matroide $M(G)$ cuando, y sólo cuando el subgrafo de esqueleto $G = (X, A)$ es un bosque con el mismo número del componente conexo que tiene el grafo $G = (X, S)$;

c) el subconjunto $C \subseteq S$ es un ciclo del matroide $M(G)$ cuando y sólo cuando C es un conjunto de aristas del ciclo simple en el grafo $G = (X, S)$;

d) $r(A) = |X| - k(A)$, donde $k(A)$ es el número de componente conexo en el grafo de esqueleto $G = (X, A)$.

Demostración. El conjunto de aristas A de cualquier bosque es un conjunto independiente en $M(G)$, puesto que la supresión de cualquier arista $s \in A$ divide el componente conexo, que contiene s, en dos partes, es decir, $s \in \overline{A \setminus \{s\}}$. Por otro lado, si el subgrafo $G = (X, A)$ contiene un ciclo $\{s_0, s_1, \ldots, s_k\}$, entonces, por definición de la clausura, $s_0 \in \{s_1, \ldots, s_k\}$; de aquí se deduce que A es el conjunto dependiente. Esto demuestra las afirmaciones a), b) y c). Más aún, este hecho demuestra que el rango del conjunto A es igual al número de aristas en el bosque de esqueleto del subgrafo $G = (X, A)$, con el número del componente conexo igual al número del componente conexo del subgrafo $G = (X, A)$. En cada bosque el número de aristas es en una unidad inferior al número de vértices. Por consiguiente, si $X_1, \ldots, X_{k(A)}$ es un conjunto de vértices del componente conexo del subgrafo $G = (X, A)$, entonces

$$r(A) = \sum_{i=1}^{k(A)} (|X_i| - 1) = |X| - k(A).$$

La demostración de la proposición queda establecida.

8. *Grupos abelianos sin torsión.* Recordemos que si todos los elementos del grupo A, salvo el cero, tienen un orden infinito, A se denomina *grupo sin torsión.* Sea A un grupo abeliano sin torsión. Diremos que un elemento $a \in A$ es dependiente en el conjunto $B \subseteq A$, si a pertenece a un subgrupo del grupo A generado por el conjunto B. Un subconjunto $C \subseteq A$ es independiente, si ningún elemento a de C es dependiente sobre $C \setminus \{a\}$. Entonces, si B es un subconjunto finito del grupo abeliano A sin torsión, los subconjuntos independientes del conjunto B forman un matroide M. Los conjuntos cerrados del matroide M son todos los subgrupos H del grupo A, para los cuales el factor-grupo A/H es un grupo sin torsión.

9. *Matroides transversales.* Sean los conjuntos $A_1, A_2, \ldots, A_m$. Recordemos que un subconjunto $A \subseteq S = A_1 \cup A_2 \cup \ldots \cup A_m$ se llama transversal parcial, si existe una aplicación biunívoca $\varphi: A \to \{1, 2, \ldots, m\}$ tal que $a \in A_{\varphi(a)}$ para todo $a \in A$. Sea F una familia de todas las transversales parciales del conjunto S. Entonces, el par (S, F) forma un matroide sobre el conjunto S. De aquí se deduce directamente, por ejemplo, que todas las transversales parciales máximas son de igual potencia.

Introducidos los entes matemáticos, se despierta interés, comúnmente, por los métodos constructivos, es decir, cómo se pueden construir entes nuevos sobre los dados. Pasemos a la exposición de las principales construcciones de este tipo.

Sea $(S, \bar{\ })$ un matroide sobre un conjunto finito S y A, $B \subseteq S$. Definamos para todo $C \subseteq B \setminus A$ una aplicación

$$I_{[A,B]}: C \to (\overline{C \cup A} \cap B) \setminus A.$$

Proposición 9. La aplicación $I_{[A,B]}$ es un operador de clausura sobre el conjunto $B \setminus A$.

Demostración. Es evidente que $C \subseteq I_{[A,B]}(C)$ y que de $C \subseteq D$ proviene $I_{[A,B]}(C) \subseteq I_{[A,B]}(D)$ para todos los C, $D \subseteq (B \setminus A)$. Queda por demostrar la idempotencia: $I_{[A,B]}(I_{[A,B]}(C)) = I_{[A,B]}(C)$ para cualquier $C \subseteq (B \setminus A)$. Efectivamente,

$$I_{[A,B]}I_{[A,B]}(C) = [\overline{\overline{(C \cup A} \cap B) \setminus A] \cup A} \cap B] \setminus A =$$

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

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

De la relación $\overline{C \cup A} \cap (B \cup A) \subseteq \overline{C \cup A}$ se desprende que

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

De aquí, $\overline{\overline{C \cup A} \cap (B \cup A)} \cap B \subseteq \overline{C \cup A} \cap B$. Por consiguiente,

$$\overline{(\overline{C \cup A} \cap (B \cup A)} \cap B) \setminus A \subseteq (\overline{C \cup A} \cap B) \setminus A = I_{[A,B]}(C),$$

es decir, tenemos: $I_{[A,B]}(I_{[A,B]}(C)) \subseteq I_{[A,B]}(C)$. Pero, $I_{[A,B]}(I_{[A,B]}(C)) \supseteq I_{[A,B]}(C)$. De aquí, $I_{[A,B]}(I_{[A,B]}(C)) = I_{[A,B]}(C)$, lo que se trataba de demostrar.

Proposición 10. Sea $M = (S, \bar{\ })$ un matroide sobre el conjunto finito S y supongamos que $B \subseteq S$. Entonces, el conjunto B forma, junto con la aplicación I_B: $C \to \bar{C} \cap B$ definida para todo $C \subseteq B$, el matroide (B, I_B).

Demostración. Si en el operador de clausura $I_{[A,B]}(C)$ de la proposición 9 ponemos $A = \varnothing$, obtendremos: $I_B(C) = I_{[\varnothing,B]}(C) = \bar{C} \cap B$. Quiere decir que la aplicación $C \to I_B(C)$ es el operador de clausura. Evidentemente, la propiedad de sustitución también tiene lugar. En efecto, sea $a \in I_B(C \cup \cup \{b\})$, $a \notin I_B(C)$. En este caso, $a \in (\overline{C \cup \{b\}} \cap B)$, pero $a \notin (\bar{C} \cap B)$. Por consiguiente, $a \in \overline{C \cup \{b\}}$, pero $a \notin \bar{C}$. De aquí, por la propiedad de sustitución para el matroide M tenemos: $b \in \overline{C \cup \{a\}}$. Por lo tanto, $b \in \overline{C \cup \{a\}} \cap B$, puesto que a, $b \in B$. La proposición está demostrada

Denotemos con $M \mid B$ el matroide (B, I_B) y llamémoslo submatroide del matroide M. Evidentemente, si F es una familia de todos los conjuntos independientes del matroide M, entonces $\{A \mid A \subseteq B, A \in F\}$ es una familia de conjuntos independientes del submatroide $M \mid B$. Además, el retículo $L(B)$ de superficies del submatroide $M \mid B$ del matroide M se obtiene a partir del retículo $L(S)$ de superficies del matroide M, al formar en el interior de $L(S)$ los supremos de todos los subconjuntos del conjunto B que se considera como conjunto de átomos en $L(S)$. En este caso, los supremos en $L(B)$ y en $L(S)$ coinciden, lo que no siempre tiene lugar para los ínfimos. En particular, si B es una superficie del matroide M, el retículo $L(B)$ es isomorfo al intervalo $[0, B]$ en $L(S)$.

Proposición 11. Sea $M = (S, \bar{\ })$ un matroide y sea que $A \subseteq S$. El conjunto $S \setminus A$, dotado para todo $C \subseteq S \setminus A$ de una aplicación

$$I_{M/A}: C \to (\overline{C \cup A} \setminus A,$$

forma el matroide $(S \setminus A, I_{M/A})$.

Demostración. Si en el operador de clausura $I_{[A,B]}(C)$ de proposición ponemos $B = S$, obtendremos: $I_{M/A}(C) = I_{[A,S]}(C) = \overline{C \cup A} \setminus A$. Quiere decir que $C \to I_{M/A}(C)$ es un operador de clausura. Queda por comprobar la propiedad de sustitución, es decir, que para cualesquiera a, $b \in (S \setminus A)$ y para todo $C \subseteq (S \setminus A)$ de $a \in I_{M/A}(C \cup \{b\})$, $a \notin I_{M/A}(C)$ se deduce: $b \in I_{M/A}(C \cup \{a\})$. En efecto, sea $a \in (\overline{C \cup \{b\}} \cup A \setminus A)$, $a \notin (\overline{C \cup A} \setminus A)$. Es evidente que a, $b \notin A$. De aquí, $a \in \overline{C \cup A \cup \{b\}}$, $a \notin \overline{C \cup A}$. En virtud de la propiedad de sustitución, para el matroide M tenemos: $b \in \overline{C \cup A \cup \{a\}}$. Pero, $b \notin A$. Por consiguiente, $b \in (\overline{C \cup A \cup \{a\}} \setminus A) = I_{M/A}(C \cup \{a\})$, lo que se trataba de demostrar.

Denotemos con M/A el matroide $(S \setminus A, I_{M/A})$ y llamémoslo contracción del matroide M por medio del matroide A. Observemos que si $L(S \setminus A)$ es un retículo de superficies del matroide M/A, entonces él será isomorfo al intervalo $[\bar{A}, 1]$ en el retículo de superficies del matroide $M = (S, \bar{\ })$.

Designemos con $M.A$ la contracción del matroide $M = (S, \bar{\ })$ por medio del conjunto $S \setminus A$. Está claro que si F es una familia de conjuntos inde-

pendients del matroide M, entonces la familia de subconjuntos $B \subseteq A$, para los cuales en M existen subconjuntos independientes máximos C de $S \setminus A$, donde $(B \cup C) \in F$, es exactamente la familia de conjuntos independientes de contracción $M.A$.

Proponemos que el lector demuestre, a título de ejercicios no complejos, las siguientes dos proposiciones.

Proposición 12. Sea M un matroide sobre el conjunto finito S; $M \mid B$, su submatroide, y r, r_B, las funciones de rango para M y $M \mid B$, respectivamente. Entonces, para todo $A \subseteq B$ serán lícitas las siguientes afirmaciones:

a) A es independiente en $M \mid B$, cuando y sólo cuando A es independiente en M;

b) A es una base del matroide $M \mid B$, si y sólo si A es un subconjunto independiente máximo del conjunto B en M;

c) A es un ciclo en $M \mid B$, si y sólo si A es un ciclo en M;

d) $r_B = r(A)$.

Proposición 13. Sea M un matroide sobre el conjunto finito S; M/A, su contracción por medio del conjunto A, y r, $r_{S \setminus A}$, funciones de rango para M y M/A, respectivamente. En este caso para todos los $B \subseteq S \setminus A$ son lícitas las siguientes afirmaciones:

a) B es independiente en M/A, si y sólo si $B \cup C$ es independiente en M para todos los subconjuntos independientes $C \subseteq A$;

b) B es una base del matroide M/A, si y sólo si $B \cup C$ es la base del matroide $M = (S, \bar{\ })$ para todos los subconjuntos independientes máximos C del conjunto A;

c) B es un ciclo en M/A, si y sólo si $B = C \setminus A = \varnothing$, donde C es un ciclo en M, y B es un conjunto mínimo con tal propiedad;

d) $r_{S \setminus A}(B) = r(B \cup A) - r(A)$.

Supongamos que $(S, \bar{\ })$ es un matroide y A, $B \in S$. El par $(S, I_{[A,B]})$ se denomina *menor del matroide* $(S, \bar{\ })$. El fácil ver que cada menor del matroide es, a su vez, un matroide, puesto que puede obtenerse como submatroide de contracción del matroide, o bien, lo que es equivalente, como contracción de un submatroide del matroide.

Sea $M = (S, \bar{\ })$ un matroide. El submatroide $M \mid (S \setminus \{a\})$, donde $a \in S$, se denota a menudo, para la comodidad con $M - a$, y se dice que dicho submatroide se ha obtenido a partir del matroide M por exclusión del elemento a. Por analogía, un submatroide $M \mid (S \setminus A)$ del matroide $M = (S, \bar{\ })$ se denota con $M - A$. Es natural, en este caso, llamar menor del matroide a una sucesión arbitraria de contracciones y exclusiones del matroide.

Proposición 14. Sea $(S, \bar{\ })$ un matroide en el conjunto finito S, y A, $B \subseteq S$. Si A es un subconjunto independiente máximo del conjunto B, entonces, $\overline{A} = \overline{B}$.

Demostración. Si $A = B$, la afirmación es obvia. Supongamos que $A \neq B$, es decir, que $A \subset B$. En virtud de las propiedades del operador de clausura, $\overline{A} \subseteq \overline{B}$. Sea, ahora, $a \in (B \setminus A)$. Entonces, $(A \cup \{a\}) \notin F$. Por consi-

guiente, existe un elemento $b \in (A \cup \{a\})$, tal que $b \in \overline{A \cup \{a\} \setminus \{b\}}$. Si $a = b$, tenemos $a \in \overline{A}$. En cambio, si $a \neq b$, entonces $b \in A$ y $b \notin A \setminus \{b\}$, puesto que $A \in F$. Por eso, $b \notin A \setminus \{b\}$ y $b \in (A \cup \{a\} \setminus \{b\})$. De aquí, conforme a la propiedad de sustitución, tenemos otra vez $a \in \overline{A}$. De este modo, $B \subseteq \overline{A}$, y, por consiguiente, $\overline{B} \subseteq \overline{A}$. Quiere decir que $\overline{A} = \overline{B}$, y la proposición queda demostrada.

Inmediatamente de la proposición 14 se deduce que cada base de un matroide es, a la vez, un conjunto independiente máximo y un conjunto generador mínimo. Precisamente esta correlación sirvió de fuente para la introducción de la noción de matroide dual. La idea de dualidad es uno de los instrumentos más potentes en la teoría de los matroides y tiene importantes aplicaciones en muchas ramas del análisis combinatorio, en particular, en la teoría de los grafos.

Teorema 62. Supongamos que $M = (S, \bar{\ })$ es un matroide en el conjunto finito S, B es la familia de sus bases y $B^* = \{A_i \subseteq S \mid A_i = S \setminus B_i$, donde $B_i \in B\}$, es decir, B^* es una familia de complementos de las bases del matroide M en S. Entonces, un par (S, B^*) satisface los axiomas $B1$) y $B2$) y es, por lo tanto, el matroide $M^* = M(S, B^*)$.

El matroide M^* se llama *dual* respecto del matroide M, y los elementos de la familia B^* se denominan *cobases* del matroide M.

Demostración. En el matroide $M = (S, \bar{\ })$, para cualquier $A \subseteq S$ y para todo $B_1 \in B$ tiene lugar la siguiente implicación: si $B_1 \subseteq A$ y $B_1 \neq A$, entonces $A \notin B$, o bien, lo que es equivalente, para cualquier $A_1 \subseteq S$ y para todo $A_2 \in B^*$, si $A_1 \subseteq A_2$ y $A_1 \neq A_2$, tenemos: $A_1 \notin B^*$. Así pues, el par (S, B^*) satisface el axioma $B1$).

Supongamos ahora que $A_1, A_2 \in B^*$, $A_1 \neq A_2$, y $a \in (A_1 \setminus A_2)$. Demostremos que en este caso existe un elemento $b \in A_2$, tal que $((A_1 \setminus \{a\}) \cup \{b\}) \in B^*$. De este modo se establecerá la validez del axioma $B2$). Por cuanto $a \notin (S \setminus A_1) \in B$ y $a \in (A_1 \setminus A_2)$, entonces, en virtud de la sugestión 5, existe el único ciclo C_1 del matroide M, tal que $a \in C_1 \subseteq ((S \setminus A_1) \cup \{a\})$. Es evidente que $C_1 \subseteq (S \setminus A_2)$, puesto que $(S \setminus A_2) \in B$. Elijamos $b \in (C_1 \setminus (S \setminus A_2))$, entonces, evidentemente, $b \in (A_2 \cap (S \setminus A_1))$. Comprobemos que $D = ((S \setminus A_1) \setminus \{b\}) \cup \{a\}$ es la base del matroide M. En efecto, sea D dependiente. Existe, pues, un ciclo C_2 tal que $C_2 \subseteq D$ y $a \in C_2$. En virtud de la proposición 5, tenemos $C_1 = C_2$. Mas, esto es imposible, puesto que $b \in C_1$ y $b \notin C_2$. Esto significa que el conjunto D es independiente. Además, $|D| = |S \setminus A_1|$, y $(S \setminus A_1) \in B$. Por consiguiente, $D \in B$. De aquí, $(S \setminus D) \in B^*$. Pero, $S \setminus D = (A_1 \setminus \{a\}) \cup \{b\}$, lo que se trataba de demostrar.

Teorema 63. Sea M un matroide en el conjunto finito S, $A \subseteq S$, y sea M^* un matroide dual respecto de M. Resultan válidas las siguientes afirmaciones:

a) A es un conjunto independiente del matroide M^* cuando y sólo cuando $S \setminus A$ es un conjunto generador del matroide M;

b) $r^*(A) = |A| - r(S) + r(S \setminus A)$, donde r^* es una función de rango del matroide M^*; en particular, $r(S) + r^*(S) = |S|$;

c) $M^{**} = M$.

Demostración. a) En virtud del teorema 62, el conjunto A es independiente en M^* cuando y sólo cuando, A contiene la base del matroide M^*, o bien, lo que es equivalente, cuando y sólo cuando $S \setminus A$ contiene la base del matroide M, o bien, cuando y sólo cuando $S \setminus A$ genera el matroide M. Así pues, si F^* es una familia de conjuntos independientes del matroide M^*, entonces, $F^* = \{A \subseteq S \mid S \setminus A$ es un conjunto generador en $M\} = \{A \subseteq S \mid$ y existe una base $B_1 \in B$, tal que $B_1 \subseteq S \setminus A\} = \{A \subseteq S \mid r(S \setminus A) = r(S)\}$.

b) Para todos los $A \subseteq S$: $r^*(A) = \max\{|A \cap A'| \mid A' \in F^*\}$. Elijamos $A' \in F^*$, entonces, en virtud de a), existe tal base B_1 del matroide M que $B_1 \subseteq S \setminus A'$, es decir, $A' \subseteq S \setminus B_1$. De este modo, $|A \cap A'| \leqslant |A \cap (S \setminus (S \setminus B_1))| = |A| - |A \cap B_1|$. Pero, $r(S \setminus A) \geqslant r((S \setminus A) \cap B_1) = |(S \setminus A) \cap B_1| = |B_1| - |A \cap B_1|$. Por consiguiente, $|A \cap A'| \leqslant |A| - |B_1| + r(S \setminus A) = |A| - r(S) + r(S \setminus A)$. Así pues, $r^*(A) \leqslant |A| - r(S) + r(S \setminus A)$. Por otra parte, existe una base B_2 del matroide M, tal que $r(S \setminus A) = |(S \setminus A) \cap B_2| = |B_2 \setminus A|$, y, por lo tanto, $(S \setminus B_2) \in F^*$. Por consiguiente, $r^*(A) \geqslant |A \cap (S \setminus B_2)| = |A| - |A \cap B_2| = |A - (|B_2| - |B_2 \setminus A|) = |A| - r(S) + r(S \setminus A)$. Quiere decir que $r^*(A) = |A| - r(S) + r(S \setminus A)$.

c) Se deduce obviamente de la definición del matroide M^*. La demostración queda establecida.

Sea $G(X, S)$ un grafo no orientado sin lazos con el conjunto de vértices X y el conjunto de aristas S, y sea $M(G)$ un matroide cíclico del grafo G. Un matroide $M^*(G)$, dual respecto de $M(G)$, se denomina matroide *cocíclico* del grafo G. Un matroide se llama *cográfico*, si es isomorfo al matroide cocíclico de cierto grafo.

Para ilustrar las aplicaciones de la dualidad demos a conocer sin demostración el siguiente resultado conocido.

Teorema 64 (de Whitney). Un grafo es planario cuando, y sólo cuando, su matroide cíclico es cográfico, o bien, lo que es equivalente, cuando su matroide cocíclico es gráfico.

Teniendo presente el teorema 64, se llama frecuentemente planario un matroide que es a la vez tanto gráfico, como cográfico.

Sean $M_i = (S_i, I_i)$ los matroides con operadores de clausura I_i, $i = 1, 2, \ldots, n$, tales que $S_i \cap S_j = \varnothing$ para $i \neq j$. Entonces, un par (S, I), donde $S = \bigcup_{i=1}^{n} S_i$ y $I(A) = \bigcup_{i=1}^{n} (A \cap S_i)$ para cualesquiera $A \subseteq S$, forma, evidentemente un matroide llamado *producto* de los matroides M_i ($i = 1, 2, \ldots, n$) y denotado con $\prod_{i=1}^{n} M_i$.

Teorema 65. Para todo $A \subseteq S$ son válidas las siguientes afirmaciones:

a) A es un conjunto independiente del matroide $\prod_{i=1}^{n} M_i$ cuando y sólo cuando $(A \cap S_i)$ sea un conjunto independiente del matroide M_i para cualquier i;

b) A es una base del matroide $\prod_{i=1}^{n} M_i$, cuando y sólo cuando $(A \cap S_i)$ es la base del matroide M_i para cualquier i;

c) A es un ciclo del matroide $\prod_{i=1}^{n} M_i$ cuando y sólo cuando existe un índice i, tal que $(A \cap S_i) = A$, y $(A \cap S_j) = \varnothing$, para cualquier $j \neq i$;

d) $r(A) = \sum_{i=1}^{n} r_i(A \cap S_i)$, donde r_i es una función de rango del matroide M_i.

La demostración del teorema es obvia, por eso proponemos que el mismo lector la restablezca.

Los matroides M_i en $M = \prod_{i=1}^{n} M_i$ se denominan *factores* del matroide M. Un matroide que no puede ser descompuesto en un producto de matroides menores se llama *conexo*.

Proposición 15. Sea f una función semimodular de números enteros y monótona creciente, definida sobre un conjunto $\mathcal{P}(S)$ de todos los subconjuntos del conjunto finito S; además, $f(\varnothing) = 0$ y $F = \{A \subseteq S \mid \forall B \subseteq A: \mid B \mid \leqslant f(B)\}$. Entonces, el par (S, F) es un matroide, y su función de rango r para un subconjunto arbitrario $A \subseteq S$ se calcula por la fórmula

$$r(A) = \min_{B \subseteq A} \{f(B) + \mid A \setminus B \mid\}.$$

Demostración. Veamos una familia $K = \{A \subseteq S \mid f(A) < \mid A \mid\}$ y demostremos que sus elementos mínimos son ciclos de cierto matroide, es decir, satisfacen las condiciones $C1$) y $C2$). La condición $C1$) se cumple, evidentemente, por construcción.

Supongamos que $C_1 \neq C_2$ son conjuntos mínimos de la familia K, y que $a \in (C_1 \cap C_2)$. Entonces $\mid C_1 \mid \geqslant 2$, y, por consiguiente, $\mid C_1 \mid - 1 = \mid C_1 \setminus \{a\} \mid \leqslant f(C_1 \setminus \{a\}) \leqslant f(C_1) < (C_1)$, es decir, $f(C_1) = \mid C_1 \mid - 1$, y $f(B) \geqslant \mid B \mid$ para todo $B \subset C_1$. De un modo análogo llegamos a que $f(C_2) = \mid C_2 \mid - 1$. En particular, tenemos $\mid C_1 \cap C_2 \mid \leqslant f(C_1 \cap C_2)$ y, de este modo, por ser la función f monótona y semimodular, obtenemos

$$f((C_1 \cup C_2) \setminus \{a\}) \leqslant f(C_1 \cup C_2) \leqslant f(C_1) + f(C_2) - f(C_1 \cap C_2) \leqslant \mid C_1 \mid - \\ - 1 + \mid C_2 \mid - 1 - \mid C_1 \cap C_2 \mid \leqslant \mid C_1 \cup C_2 \mid - 2 \leqslant \mid (C_1 \cup C_2) \setminus \{a\} \mid.$$

El conjunto $(C_1 \cup C_2) \setminus \{a\}$ pertenece a la familia K y, por lo tanto, contiene su conjunto mínimo. La condición $C2$) está comprobada.

Así pues, la familia F define el matroide M. Resta por demostrar que

la función

$$r(A) = \min_{B \subseteq A} \{f(B) + |A \setminus B|\},$$

definida para todos los $A \subseteq S$, es la función de rango del matroide M. Con este fin es suficiente comprobar que r satisface las condiciones $R1$)—$R3$). Directamente de la definición de r se deduce que $0 \leqslant r(A) \leqslant |A|$ para todo $A \subseteq S$, y que $r(A) \leqslant r(B)$ para $A \subseteq B$, es decir, las condiciones $R1$) y $R2$) se cumplen. Ahora, para todos los subconjuntos $A_1 \subseteq A$ y $B_1 \subseteq B$ se verifica la igualdad

$$|A \setminus A_1| + |B \setminus B_1| = |(A \cup B) \setminus (A_1 \cup B_1)| + |(A \cap B) \setminus (A_1 \cap B_1)|.$$

Por consiguiente, por ser la función f semimodular, tenemos

$$(f(A_1) + |A \setminus A_1|) + (f(B_1) + |B \setminus B_1|) \geqslant f(A_1 \cup B_1) + \\ + |(A \cup B) \setminus (A_1 \cup B_1)| + f(A_1 \cap B_1) + |(A \cap B) \setminus (A_1 \cap B_1)|.$$

De este modo,

$$r(A) + r(B) = \min_{\substack{A_1 \subseteq A \\ B_1 \subseteq B}} \{f(A_1) + |A \setminus A_1| + f(B_1) + |B \setminus B_1|\} \geqslant$$

$$\geqslant \min_{\substack{C_1 \subseteq A \cup B \\ C_2 \subseteq A \cap B}} \{f(C_1) + |(A \cup B) \setminus C_1| + f(C_2) + |(A \cap B) \setminus C_2|\} =$$

$$= r(A \cup B) + r(A \cap B).$$

De este modo queda establecida la validez de $R3$), y la proposición queda demostrada.

Teorema 66. Supongamos que $M_i = (S, r_i)$ es un matroide en el conjunto finito S; r_i, una función de rango, y $F(M_i)$, una familia de conjuntos independientes del matroide M_i ($i = 1, 2, \ldots, n$). Entonces, el par (S, F), donde

$$F = \{A \subseteq S \mid A = A_1 \cup A_2 \cup \ldots \cup A_n;\ A_i \in F(M_i)\},$$

es un matroide cuya función de rango r se define por la correlación

$$r(A) = \min_{B \subseteq A} \left\{ \sum_{i=1}^{n} r_i(B) + |A \setminus B| \right\}.$$

Demostración. Sea $f(A) = \sum_{i=1}^{n} r_i(A)$ para todo $A \subseteq B$. En este caso f es una función semimodular monótona creciente de números enteros, ya que tales son las funciones de rango r_i de los matroides M_i. Por consiguiente, en virtud de la proposición 15, la familia

$$F^* = \{A \subseteq S \mid \forall B \subseteq A: |B| \leqslant f(B)\}$$

define el matroide $M(S, r)$, donde

$$r(A) = \min_{B \subseteq A} \{f(B) + |A \setminus B|\} = \min_{B \subseteq A} \left\{ \sum_{i=1}^{n} r_i(B) + |A \setminus B| \right\}.$$

Luego, sea $B \subseteq A$, $A \in F$, y $B = \bigcup_{i=1}^{n} B_i$, donde $B_i \subseteq A_i$ para todo $i = 1, 2, \ldots, n$. Entonces,

$$|B| = \left| \bigcup_{i=1}^{n} B_i \right| \leqslant \sum_{i=1}^{n} |B_i| = \sum_{i=1}^{n} r(B_i) \leqslant \sum_{i=1}^{n} r_i(B),$$

puesto que $B_i \in F(M_i)$ para todo $i = 1, 2, \ldots, n$. Por consiguiente, $A \in F^*$. Es evidente que la afirmación recíproca es también cierta, a saber, si $A \in F^*$, entonces $A \in F$. Quiere decir que $F = F^*$, y el teorema queda demostrado.

El matroide (S, F), citado en la formulación del teorema 66, recibe el nombre de *unión de los matroides* $M_1, \ldots, M_n$ y se denota $\bigcup_{i=1}^{n} M_i$.

Se denomina *extensión unipuntual* del matroide $M = (S, \bar{\ })$ mediante un punto $p \notin S$ a tal matroide $M = (S \cup \{p\}, -)$, donde $r(M') = r(M)$, y $M = M' - p$.

Proposición 16. Cada matroide cuenta con una extensión unipuntual.

Demostración. Sea $M = (S, \bar{\ })$ un matroide. Construyamos su extensión unipuntual $M' = (S \cup \{p\}, I)$, tomando por operador de clausura la aplicación $A \to I(A)$, donde

$$I(A) = \begin{cases} \overline{A}, \text{ si } p \notin A \text{ y } \overline{A} \neq S; \\ \overline{A \setminus \{p\} \cup \{p\}}, \text{ si } p \in A \text{ y } r(A \setminus \{p\}) = r(S) - 1; \\ S \cup \{p\}, \text{ si } \overline{A} = S, \text{ o bien } p \in A \text{ y } r(A \setminus \{p\}) = r(S) - 1. \end{cases}$$

Comprobemos la propiedad de sustitución. Sea $a \in I(A \cup \{b\})$; $a, b \notin I(A)$. Entonces son posibles dos casos: $a = p \in I(A \cup \{b\})$ y $a \neq p$, $a \in I(A \cup \{b\})$. En el primer caso tenemos o bien $b = p$, o bien $r(A) = r(S) - 1$. De aquí, $b \in I(A \cup \{a\})$. En el segundo caso, si $p \notin A$, entonces $b \in I(A \cup \{a\})$; si, en cambio, $p \in A$, entonces $a \in I(A \cup \{b\}) = \overline{(A \setminus \{p\}) \cup \{b\} \cup \{p\}}$, de donde $a \in \overline{(A \setminus \{p\}) \cup \{b\}}$, y, por consiguiente, en virtud de la propiedad de sustitución, para el matroide M tenemos $b \in \overline{(A \setminus \{p\}) \cup \{a\}}$. La igualdad $r(M') = r(M)$ se cumple por construcción. La proposición está demostrada.

Se dice que dos conjuntos $A, B \subseteq S$ del matroide $M = (S, \bar{\ })$ forman un *par modular*, si

$$r(A \cap B) + r(A \cup B) = r(A) + r(B).$$

Se llama *filtro modular* del matroide $M = (S, \bar{\ })$ a una familia Φ de subconjuntos del conjunto S, tal que

a) si $A \in \Phi$ y $A \subseteq B$, entonces $B \in \Phi$;

b) si $A, B \in \Phi$, y (A, B) es un par modular, entonces $A \cap B = \Phi$.

Proposición 17. Sea $M = (S \cup \{p\}, I)$ un matroide sobre el conjunto $S \cup \{p\}$, $p \notin S$, con operador de clausura I y función de rango r. Entonces, el conjunto $\Phi = \{A \subseteq S \mid p \in I(A)\}$ es un filtro modular del matroide $M - p$.

Demostración. Es evidente que Φ es un filtro. La condición $A \in \Phi$ es equivalente a la igualdad $r(A \cup \{p\}) = r(A)$. Por consiguiente, si $A, B \in \Phi$, y

(A, B) es un par modular en $M - p$, entonces, $r((A\cap B)\cup\{p\})\leqslant r(A\cup\{p\})+$ $+ r(B\cup\{p\}) - r(A\cup B\cup\{p\}) = r(A) + r(B) - r(A\cup B) = r(A\cap B)$. De este modo, $A\cap B\in\Phi$. La proposición está demostrada.

Proposición 18. Sea Φ un filtro modular del matroide $M = (S, \bar{\ })$. Entonces existe una única extensión unipuntual $M' = (S\cup\{p\}, I)$ del matroide M, tal que $\Phi = \{A\subseteq S \mid p\in\bar{A}\}$.

Demostración. Sea r la función de rango del matroide M. Definamos una función de valores enteros r^* para todos los subconjuntos $A\subseteq S\cup\{p\}$ del modo siguiente:

$$r^*(A) = r(A), \text{ si } A\subseteq S;$$
$$r^*(A\cup\{p\}) = r(A) + 1, \text{ si } A\subseteq S \text{ y } A\notin\Phi;$$
$$r^*(A\cup\{p\}) = r(A), \text{ si } A\subseteq S \text{ y } A\in\Phi.$$

Comprobemos que r^* es la función de rango de cierto matroide. Con este fin mostremos que ella satisface los axiomas $R1$)—$R3$), con lo cual establezcamos también la unicidad de la extensión.

Está claro que r^* satisface los axiomas $R1$) y $R2$). Para comprobar $R3$), hace falta examinar dos casos: un par $A\cup\{p\}$, B, y otro par $A\cup\{p\}$, $B\cup\{p\}$, donde A, $B\subseteq S$, $p\notin S$. En el primer caso, para cualesquiera A, $B\subseteq S$ tenemos $r^*(A\cup B\cup\{p\}) - r^*(A\cup B)\leqslant(A\cup\{p\}) - r^*(A)$. Observemos que el primer miembro de la desigualdad es siempre inferior o igual a 1, además es igual a 1 sólo cuando $\overline{A\cup B}\notin\Phi$. De este modo, $\bar{A}\notin\Phi$, puesto que en tal caso $r^*(A\cup\{p\}) - r^*(A)$ también debe ser igual a 1. De aquí se deduce que $r^*(A\cup B\cup\{p\}) - r^*(A\cup\{p\})\leqslant r^*(A\cup B) - r^*(A) = r(A\cup B) - r(A\leqslant r(B -$ $- r(A\cap B) = r^*(B) - r^*(A\cap B)$, con lo cual queda establecido en el caso dado el carácter semimodular de la función. En el segundo caso mostremos que $r^*((A\cap B)\cup\{p\}) + r^*(A\cup B\cup\{p\})\leqslant r^*(A\cup\{p\}) + r^*(B\cup\{p\})$. Si $\overline{A\cup B}\notin\Phi$, entonces $\bar{A}$, $\bar{B}$ y $\overline{A\cap B}$ tampoco se disponen en Φ y, por consiguiente, $r^*(X\cup\{p\}) = r(X) + 1$, cuando $X = A$, B, $A\cup B$ y $A\cap B$. Así pues, nuestra desigualdad se verifica, puesto que coincide en este caso con la condición de semimodularidad para la función de rango r del matroide M. En cambio, si $\overline{A\cup B}\in\Phi$, esto puede tener lugar sólo cuando $\bar{A}\in\Phi$ y $\bar{B}\in\Phi$. Además, (A, B) es un par modular en M. Es fácil probar que en este caso $(\bar{A}, \bar{B})$ es también un par modular y, por lo tanto, $\overline{A\cap B} = (\bar{A}\cap\bar{B})\in\Phi$. De aquí, $r^*(X\cup$ $\cup\{p\}) = r(X)$ cuando $X = A$, B, $A\cup B$ y $A\cap B$. De este modo, la desigualdad está demostrada, puesto que en este caso también ella coincide exactamente con la condición de semimodularidad para r. La sugestión queda demostrada.

Directamente de la proposición 18 se deduce el siguiente resultado que se debe a Crapo:

Corolario 12. Sea Φ un filtro modular del matroide $M = (S, \bar{\ })$ y sea $M' = (S\cup\{p\}, I)$ la extensión del matroide M construida con ayuda de Φ. Entonces son superficies en M' todos los subconjuntos $S\cup\{p\}$ de los tipos siguientes:

a) $A \cup \{p\}$, si A es una superficie del matroide M y $A \in \Phi$;

b) A, si A es una superficie del matroide M y $A \notin \Phi$;

c) $A \cup \{p\}$, si A es una superficie del matroide M; A no se dispone en Φ y no se cubre en M por ninguna superficie de Φ. No hay otras superficies en M'.

Cabe notar, además, que las extensiones unipuntuales del matroide $M = (S, \bar{\ })$, ordenadas por inclusión de sus filtros modulares en M, forman un retículo.

Definamos dos construcciones más: acortamiento e incremento.

Teorema 67. Sean M un matroide sobre el conjunto finito S; F, una familia de sus conjuntos independientes; r, la función de rango; k, un número positivo entero tal que $k \leqslant r(S)$. Entonces, la familia

$$F_k = \{A \subseteq S \mid A \in F, \text{ y } |A| \leqslant k\}$$

es una familia de conjuntos independientes del matroide M_k sobre el conjunto S con la función de rango $r_k(A) = \min\{k, r(A)\}$. El retículo de superficies del matroide M_k se obtiene del retículo $L(M)$ de superficies del matroide M, eliminando todas las superficies de rango $\geqslant k$ sustituyéndolas por un nuevo elemento maximal del retículo.

La demostración del teorema no es difícil y se recomienda al lector a título de ejercicio.

El matroide M_k citado en la formulación del teorema 67 se denomina *k-acortamiento* del matroide M.

Si el matroide M sobre el conjunto S es isomorfo al $(r-1)$-acortamiento del matroide H sobre el conjunto S, suele decirse que el matroide H es un incremento del matroide M. Sin restringir la generalidad de nuestros razonamientos, podemos considerar que el retículo del matroide H se obtiene a partir del retículo del matroide M por inclusión del nivel de nuevos coátomos, el cual yace más arriba que los coátomos iniciales y debajo del elemento unidad del retículo.

No nos detendremos detalladamente en la construcción del incremento, sino que daremos a conocer sin demostración algunos resultados.

Teorema 68 (de Crapo). Una familia H de subconjuntos no vacíos del conjunto S es un conjunto de coátomos en el retículo de incremento del matroide $M = (S, \bar{\ })$ cuando y sólo cuando se cumplen las siguientes tres condiciones:

a) H es una anticadena en el booleano $\mathcal{P}(S)$;

b) para todo $A \in H$, si $B \subseteq A$ y $|B| = r - 1$, entonces $\bar{B} \subseteq A$;

c) para toda base B_i existe el único elemento $A_i \in H$, tal que $B_i \subseteq A_i$.

Sean H y T dos anticadenas pertenecientes al booleano $\mathcal{P}(S)$; se dice que la anticadena H es inferior a la anticadena T, si para todo $A \in H$ existe un elemento $B \in T$ tal que $A \subseteq B$. En caso de que tal elemento $B \in T$ sea único, suele decirse que T *rompe* la anticadena H. Toda clase de incrementos (más exactamente, las familias de coátomos en el retículo del incremento) del

matroide M sobre el conjunto finito S, ordenados como anticadenas del booleano $\mathscr{P}(S)$, forman el retículo completo, en el que el elemento minimal se denomina incremento libre del matroide M. Si el incremento libre del matroide M se conoce, todos los demás incrementos de dicho matroide pueden obtenerse por partición del incremento libre.

La demostración de las afirmaciones aducidas y de otras, referentes a las extensiones e incrementos de los matroides se da en las obras [94, 95].

La construcción del incremento libre se expone en [96, 97].

Ejercicios. 1. Sea $M = (S, \bar{\ })$ un matroide, $B \subseteq A \subseteq S$. ¿Se verificarán las igualdades siguientes:

a) $(M \mid A) \mid B = M \mid B$;

b) $M.B = (M.A).B$;

c) $(M \mid A).B = (M.(S \setminus (A \setminus B))) \mid B$;

d) $(M.A) \mid B = (M \mid (S \setminus (A \setminus B))).B$;

e) $(M \mid A)^* = M^*/(S \setminus A)$;

f) $(M/A)^* = M^* \mid (S \setminus A)$?

2. Cerciórese de la validez de las siguientes afirmaciones:

a) todo menor de un matroide gráfico es gráfico;

b) todo submatroide de un matroide transversal es transversal;

c) la suma de los matroides transversales es un matroide transversal.

3. ¿Podrá contar un matroide gráfico M con incrementos y k-acortamientos no gráficos? Si puede, dénse ejemplos.

Se llama aplicación *débil* de un retículo geométrico P en el retículo geométrico L a la aplicación σ: $P \to L$, para la cual

a) $\sigma(x) = \sup\{\sigma(a) \mid x \geqslant a,\ a \geqslant 0\}$;

b) $r(\sigma(x)) \leqslant r(x)$.

Se llama aplicación *fuerte* del retículo geométrico P en el retículo geométrico L a la aplicación σ: $P \to L$, para la cual

a) $\sigma(\sup A) = \sup\{\sigma(x) \mid x \in A\}$ para todos los $A \subseteq P$;

b) de $y \geqslant x$ en P se deduce que $\sigma(y) \geqslant \sigma(x)$ en L.

Se llama *aplicación fuerte* (*débil*, respectivamente) de la geometría $G = (S, \bar{\ })$ en la geometría $H = (T, \bar{\ })$ a la función inyectiva

$$f : S \cup \{O\} \to T \cup \{O\},$$

donde O es un conjunto vacío, tal que $f(O) = 0$, y la preimagen de un subconjunto cerrado independiente, (respectivamente arbitrario) de la geometría H es cerrada (independiente respectivamente) en G. Cada aplicación fuerte es débil, lo recíproco no es cierto.

Ni las aplicaciones fuertes ni tampoco las débiles, forman por separado categorías bastante buenas, para que puedan emplearse en plena medida las ideas de la teoría de categorías. Sin embargo, siendo analizadas en conjunto, se obtienen ciertos resultados del tipo canónico, por cuanto los entes en la categoría de matroides y las aplicaciones fuertes tienden a ser canónicos con respecto a los entes de la categoría de matroides y las aplicaciones débiles. La razón de esto radica, por lo visto, en que las aplicaciones fuertes que conservan el rango son isomorfismos, no obstante se encuentran, a menu-

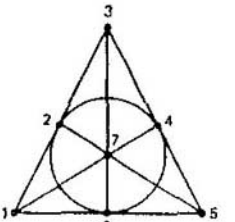

Fig.8.34.

do, varios matroides de un mismo rango que satisfacen cierto diagrama prefijado de las aplicaciones fuertes ligadas entre sí precisamente por las aplicaciones débiles.

Para ponerse en contacto con los resultados principales de las aplicaciones débiles y fuertes de los matroides recomendamos las obras [98—102 y 138—140].

Como conclusión de nuestra breve introducción a la teoría de los matroides, discutamos algunos problemas. Uno de los problemas más antiguos de la teoría de matroides, que hasta el momento no ha sido resuelto totalmente, es el problema de representación del matroide dado mediante los vectores con coordenadas de un campo (problema de coordenatización).

Un matroide $M = (S; \bar{})$ se llama *representable* sobre el campo F, si existe un espacio lineal V sobre F y una aplicación $\varphi: S \to V$, para la cual $A \subseteq S$ es independiente en M cuando y sólo cuando φ es biunívoca en A, y $\varphi(A)$ es linealmente independiente en V.

Es obvio que un matroide representable sobre F se describe por una matriz de dimensión $r \times n$, de cuyas columnas sirven las imágenes de los elementos de S, al realizarse la aplicación φ (si $|S| = n$ y $r(S) = r$). El problema de representación consiste en determinar si es representable o no el matroide dado M sobre el campo (cuerpo) dado F.

Por ejemplo, los matroides, representables sobre el campo $G(F(2)$, se denominan *binarios*.

He aquí los resultados más característicos concernientes a la representación de los matroides:

a) un matroide $M = (S, \bar{})$ es binario cuando y sólo cuando no tiene un menor que sea isomorfo al matroide homogéneo $U_2(4)$, o bien, lo que es equivalente, cuando y sólo cuando la diferencia simétrica entre dos cualesquiera ciclos distintos del matroide M es una unión de los ciclos disjuntos;

b) un matroide M es ternario, es decir, representable sobre el campo $GF(3)$, si y sólo si no tiene menores isomorfos al matroide homogéneo $U_2(5)$, al de Fano (fig. 8.34) o a los matroides duales respecto de los mencionados;

c) si un matroide M sin lazos y puentes es representable sobre el campo $GF(2)$ y sobre algún otro campo, cuya característica es distinta de 2, enton-

ces, M es representable sobre todos los campos a la vez, con ayuda de una matriz bien unimodular (es decir, de una matriz cuyos menores son todos iguales a 0, ± 1).

Los matroides representables sobre cualquier campo se llaman *regulares*. Un matroide $M = (a, \ )$ se denomina *lazo*, si $r(a) = 0$, y *puente*, si $r^*(a) = 0$.

Teorema 69. Si un matroide M en el conjunto S es representable sobre cierto campo F, el matroide M^*, dual de M, es también representable sobre F.

Demostración. Sea M un matroide de rango r en el conjunto S, $|S| = n$, y sea A una matriz de orden $r \times n$ que representa el matroide M sobre el campo F. Supongamos que X es el conjunto de todos los vectores columnas x, para los cuales $Ax = 0$. El conjunto x es un subespacio de dimensión $n - r$. Elijamos en X una familia de $n - r$ vectores columnas linealmente independientes y formemos, a base de dichos vectores (empleándolos como columnas) una matriz B de orden $n \times (n - r)$. Observemos que $AB = 0$.

Mostremos que la matriz B^T, transpuesta a B, es una representación sobre el campo F del matroide dual M^*. Con este fin demostremos que r columnas arbitrarias de la matriz A son linealmente independientes, cuando y sólo cuando el conjunto complementador de $n - r$ columnas es B^T-linealmente independiente. Sin restringir la generalidad, se pueden tomar las primeras r columnas de la matriz A.

Las primeras r columnas de la matriz A son linealmente dependientes cuando y sólo cuando existe un vector columna no nulo x, $x^T = (x_1, x_2, \ldots, x_2, 0, \ldots, 0)$ perteneciente a X. Tal vector $x \in X$ existe, a su vez, cuando y sólo cuando existe un vector columna no nulo y de dimensión $n - r$ tal que $x = By$. Representemos ahora la matriz B en la forma $\begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$, donde B_1 es una submatriz de orden $r \times (n - r)$, y B_2, una submatriz de orden $(n - r) \times (n - r)$. Entonces, es fácil ver que $B_2 y = 0$. Por cuanto $y \neq 0$, llegamos a que B_2 es una matriz regular. De este modo, las filas de la matriz B_2 y, por consiguiente, las últimas $n - r$ columnas de la matriz B^T son dependientes. El teorema queda demostrado.

Supongamos que $A_1, A_2, \ldots, A_n \in \mathcal{P}(S)$, donde $\mathcal{P}(S)$ es el conjunto de todos los subconjuntos del conjunto S. Definamos la *suma* $\sum_{i=1}^{n} A_i$ *según el módulo* 2, como un conjunto $|x \in S|\ x$ que se contiene en el número impar de sumandos $A_i|$. En particular, $A_1 + A_2$ es, según el módulo 2, $A_1 \Delta A_2$, o sea, la diferencia simétrica de los conjuntos A_1 y A_2.

Ejercicio 4. Sea M un matroide. Demuéstrese que son equivalentes las siguientes afirmaciones:

a) para cualesquiera ciclos C y un cociclo C^* del matroide M es cierto que $|C \cap C^*|$ es par;

b) Una suma según el módulo 2 de cualquier familia de ciclos del matroide M es igual a la unión de los ciclos disjuntos del mismo matroide;

c) para una base B y un ciclo C arbitrarios del matroide M tenemos: $C=\sum_{e_i\in C\setminus B} C(e_i)$ según el módulo 2, donde $C(e_i)$ es un ciclo del matroide M, tal que $C(e_i)\subseteq B\cup\{e_i\}$.

d) M es un matroide binario.

A la par con el problema de representación, un gran interés práctico despiertan los problemas de descripción de las clases de matroides: binarios, gráficos, cográficos, regulares, transversales y otros;

d) un matroide M es gráfico, si y sólo si es binario y no contiene menores isomorfos a los matroides cocíclicos de los grafos de Kuratowski $K_{3,3}$ y K_5, al matroide de Fano y al dual de este último.

e) un matroide M es cográfico, si y sólo si es binario y no contiene menores isomorfos a los matroides cíclicos de los grafos de Kuratowski $K_{3,3}$ y K_5, al matroide de Fano y al dual de este último;

f) un matroide binario es regular, si y sólo si no contiene menores isomorfos al matroide de Fano y al dual de este último.

Para ilustrar la importancia de los problemas de caracterización, diremos que casi todos los métodos conocidos de la síntesis topológica de circuitos eléctricos y de esquemas combinatorios de conmutación están basados en el empleo de las propiedades que poseen los matroides cíclico y cocíclico del grafo del esquema y también en la siguiente propiedad notable: la matriz de incidencia de un matroide cocíclico del grafo del esquema (la matriz de cortes de un esquema eléctrico) puede ser reducida mediante las opeaciones de filas elementales a una matriz de incidencia A del esquema eléctrico (dicho de otro modo, el matroide, correspondiente a la matriz de incidencia A sobre $GF(2)$, es isomorfo al matroide de cortes del grafo del esquema). Cada matroide gráfico, al igual que cada matroide cográfico, es binario, pero no cada matroide binario es gráfico. Por ejemplo, el matroide de Fano es binario, mas no es gráfico; más aún, su matriz de representación sobre $GF(2)$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

no puede ser reducida, mediante las transformaciones elementales de filas, a las matriz de incidencia de ningún grafo del esquema. Por eso, desempeñan un papel de importancia excepcional en la síntesis topológica de los esquemas eléctricos las caracterizaciones mencionadas más arriba de los matroides gráficos y cográficos, como también las siguientes circunstancias:

- al orientar la arista de un grafo, el matroide cíclico del grafo se hace también orientado;

- del carácter orientado de un matroide se desprende el carácter orientado del matroide dual;

- un matroide orientado tiene representación lineal sobre todos los campos, es decir, es regular y representable por una matriz modular.

Entre las caracterizaciones aducidas están ausentes prácticamente las constructivas, por cuanto seleccionar todos los menores del matroide y, con mayor razón, establecer su isomorfismo respecto de otros matroides resulta difícil incluso para los matroides «pequeños». Tanto más valiosa es la caracterización constructiva de los matroides regulares recién obtenida por Seymour [103]. Demos a conocer sin demostración su resultado.

Sean $M_1 = (S_1, -)$ y $M_2 = (S_2, -)$ los matroides binarios, con la particularidad de que S_1 y S_2 pueden intersecarse. En tal caso el matroide $M_1 \Delta M_2$ sobre el conjunto $S_1 \Delta S_2 = (S_1 \setminus S_2) \cup (S_2 \setminus S_1)$, los ciclos de los cuales son los subconjuntos del conjunto $S_1 \Delta S_2$ del tipo $C_1 \Delta C_2$ (donde C_i son ciclos del matroide M_i, $i = 1, 2$), es binario. Supongamos que $|S_1|$, $|S_2| < |S_1 \Delta S_2|$. Entonces, el matroide $M_1 \Delta M_2$ lleva el nombre de 1-suma (2-suma y 3-suma, respectivamente) de los matroides M_1 y M_2, si $S_1 \cap S_2 = \varnothing$ ($|S_1 \cap S_2| = 1$, y $S_1 \cap S_2 = \{z\}$, respectivamente, donde z no es ni lazo ni colazo de los matroides M_1 y M_2; $|S_1 \cap S_2| = 3$ y $S_1 \cap S_2 = Z$, donde Z es un ciclo que no contiene ningún cociclo de los matroides M_1 y M_2).

En 1975 Brilavski demostró que las 1-suma, 2-suma y 3-suma de dos matroides regulares son regulares.

Sea dada una matriz

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

Denotemos con R_{10} el matroide, que tiene como elementos las columnas de la matriz y como bases sus conjuntos linealmente independientes máximos en un espacio lineal sobre $GF(2)$.

Teorema 70 (de Seymour). Cada matroide regular M puede ser construido mediante las 1-suma, 2-suma y 3-suma de matroides, cada uno de los cuales es isomorfo a los menores del matroide M y es o bien gráfico, o bien cografico, o isomorfo al matroide R_{10}.

Detengámos también en otras aplicaciones de los matroides. Se denomina *coloración correcta* de un grafo G tal atribución de los colores a sus vértices que ningún par de vértices adyacentes está pintado de igual color. Se denomina *k-coloración* del grafo G una coloración correcta del grafo G en la que se usan k colores o menos. Dos k-coloraciones del grafo G se considerarán diferentes, si atribuyen diferentes colores por lo menos a un vértice. El *número cromático* $\chi(G)$ del grafo G se define como el menor k, para el cual el grafo G tiene k-coloración. Es fácil determinar el número cromático

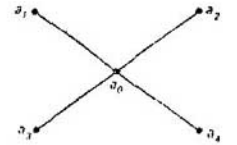

Fig.8.35.

para ciertos grafos conocidos, por ejemplo: $\chi(K_n) = n$; $\chi(K_{m,n}) = 2$, y $\chi(T) = 2$ para cualquier árbol no trivial T.

Sea $P(G; \lambda)$ el número de diferentes λ-coloraciones del grafo G. Si $\lambda \leqslant \chi(G)$, entonces, naturalmente, $P(G; \lambda) = 0$. El menor de los número naturales λ, para el cual $P(G; \lambda) > 0$, será, evidentemente, el número cromático del grafo. La hipótesis bien sabida de cuatro colores (cuya validez fue demostrada no hace mucho tiempo) afirma que si G es un grafo planario, entonces $P(G; 4) > 0$.

Es evidente que para todo grafo completo K_n tenemos

$$P(K_n; \lambda) = \lambda(\lambda - 1) \ldots (\lambda - n + 1),$$

puesto que cualquier vértice dado del grafo completo K_n puede ser pintado por λ métodos; para el segundo vértice puede utilizarse cualquiera de $(\lambda - 1)$ colores restantes, etc. Por fin, el último vértice se pinta empleando $(\lambda - n + 1)$ métodos. El vértice central a_0 del grafo $K_{1,4}$ (fig. 8.35) puede ser pintado de λ modos, mientras que cualquiera de los vértices pendientes, de $\lambda - 1$ modos. Por eso, $P(K_{1,4}; \lambda) = \lambda(\lambda - 1)^4$.

Teorema 71. Supongamos que G es un grafo sin lazos y aristas paralelas (múltiples) y sea a una arista del grafo G. Entonces

$$P(G; \lambda) = P(G - a; \lambda) - P(G/a; \lambda),$$

donde $G - a$ y G/a son los grafos obtenidos de G por eliminación o contracción, respectivamente, de la arista a.

Demostración. La igualdad requerida se desprende directamente del hecho de que el conjunto de λ-coloraciones correctas del grafo $G - a$ puede partirse en dos subconjuntos: coloraciones, en las que los vértices extremos de la arista a están pintados de colores distintos, y aquéllas, en las que los vértices citados están pintados de un mismo color. La potencia del primer subconjunto es igual, obviamente, al número de λ-coloraciones del grafo G, es decir, a $P(G, \lambda)$, y la potencia del segundo subconjunto, al número de λ-coloraciones del grafo G/a, es decir, a $P(G/a; \lambda)$. El teorema queda demostrado.

En todos los ejemplos aducidos $P(G; \lambda)$ es un polinomio de la variable λ. Esto es siempre así, de lo que nos convencemos ahora mismo.

Sea G un grafo incompleto arbitrario sobre n vértices. Es evidente que este grafo puede obtenerse a partir del grafo K_n eliminando sucesivamente las aristas que no pertenecen al grafo G. Designemos estas aristas, para concretar, mediante $a_1, \ldots, a_k$. Introduzcamos las siguientes designaciones:

Fig.8.36.

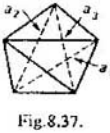

Fig.8.37.

Fig.8.38.

Fig.8.39.

$G_1 = K_n - a_1$; $G_2 = G_1 - a_2$; . . ., $G_k = G_{k-1} - a_k$, $G^1 = K_n/a_1$; $G^2 = G_1/a_2$, . . ., $G^k = G_{k-1}/a_k$. Entonces, en virtud del teorema 71, tenemos: $P(K_n; \lambda) = P(G_k; \lambda) - \sum_{i=1}^{k} P(G^i, \lambda)$, pero $G_k = G$. Por consiguiente,

$$P(G; \lambda) = P(K_n; \lambda) + \sum_{i=1}^{k} P(G^i; \lambda).$$

Cada uno de los grafos G^i, donde $i = 1, \ldots, k$, contiene $(n - 1)$ vértices y la función del grafo, $P(G^i; \lambda)$, puede ser expresada a través de las funciones del grafo completo sobre $(n - 1)$ vértices y de los grafos sobre $(n - 2)$ vértices. Por consiguiente, $P(G; \lambda)$ puede representarse en forma de la suma $P(K_i, \lambda)$, puesto que, contrayendo las aristas, siempre podemos llegar a los grafos completos, por ejemplo, K_1. Pero, $P(K_i; \lambda) = \lambda \ldots (\lambda - i + 1)$ son polinomios. Por lo tanto, $P(G; \lambda)$ es un polinomio de la variable λ para cualquier grafo G.

La función $P(G; \lambda)$ se llama por esta razón polinomio cromático del grafo G (véase el ejemplo 8 del § 8.3).

Ilustremos lo dicho con un ejemplo y hallemos el polinomio cromático del grafo G expuesto en la fig. 8.36. Denotemos con a_1, a_2 y a_3 las aristas del grafo completo K_5 que no pertenecen al grafo G (véase fig. 8.37). En tal caso, $G^1 = K_4$; $G^2 = K_4$, y el grafo G^3, representado en la fig. 8.38, se obtiene a partir del grafo completo K_4, eliminando en él la arista b (véase fig. 8.39). Además, $K_4/b = K_3$. De aquí,

$$P(K_5; \lambda) = P(G; \lambda) - 2P(K_4; \lambda) - P(G^3; \lambda);$$
$$P(K_4; \lambda) = P(G^3; \lambda) - P(K_3; \lambda).$$

Por consiguiente, $P(G; \lambda) = P(K_5; \lambda) + 3P(K_4; \lambda) + P(K_3; \lambda) = \lambda(\lambda - 1)(\lambda - 2)(\lambda - 3)(\lambda - 4) + \lambda(\lambda - 1)(\lambda - 2)(\lambda - 3) + \lambda(\lambda - 1)(\lambda - 2) = \lambda^5 - 7\lambda^4 + 18\lambda^3 - 20\lambda^2 + 8\lambda$. En particular, el grafo G puede ser pintado de tres colores, por cuanto

$$P(G; 3) = 6 > 0.$$

He aquí algunas propiedades del polinomio cromático $P(G; \lambda)$ que se desprenden directamente del teorema 71.

Teorema 72. Sea $G = (X, S)$ un grafo sin lazos y aristas paralelas (múltiples) con un conjunto de vértices X, un conjunto de aristas S y con k componentes de conexión $G_1, G_2, \ldots, G_k$. Entonces:

a) $P(G; \lambda)$ es un polinomio de la variable λ de grado $|X|$;

b) el coeficiente de $\lambda^{|X|}$ en $P(G; \lambda)$ es igual a 1;

c) el coeficiente de $\lambda^{|X|-1}$ en $P(G; \lambda)$ es igual a $-|S|$;

d) el término independiente del polinomio $P(G, \lambda)$ es igual a 0;

e) $P(G; \lambda) = \prod_{i=1}^{n} P(C_i; \lambda)$;

f) el índice mínimo en las potencias de la variable λ que figuran en $P(G, \lambda)$ con coeficientes no nulos es igual a k.

Teorema 73. El grafo G con n vértices es un árbol cuando y sólo cuando $P(G; \lambda) = \lambda(\lambda - 1)^{n-1}$.

Demostración. Probemos, por inducción respecto del número de vértices, que el polinomio cromático de cualquier árbol marcado con n vértices es igual a $\lambda(\lambda - 1)^{n-1}$. Cuando $n = 1$ y $n = 2$, el resultado es evidente. Supongamos que el polinomio cromático de todos los árboles con $n - 1$ vértices tiene la forma $\lambda(\lambda - 1)^{n-2}$. Sea x un vértice pendiente del árbol T, y sea a su arista incidente con relación al vértice x. Por hipótesis de inducción, el polinomio cromático del árbol $T - a$ es $\lambda(\lambda - 1)^{n-2}$. El vértice x puede ser pintado de cualquier color distinto del color de otro vértice terminal de la arista a, de modo que x puede pintarse empleando $\lambda - 1$ métodos. Así pues, $P(T; \lambda) = (\lambda - 1) \times P(T - a; \lambda) = \lambda(\lambda - 1)^{n-1}$.

Viceversa, sea G un grafo, en el que $P(G; \lambda) = \lambda(\lambda - 1)^{n-1}$. Por cuanto el coeficiente de λ en $P(G; \lambda)$ no es igual a 0, y el de λ^{n-1} es igual a $(n - 1)$, entonces, en virtud del teorema 72, el grafo G es conexo y tiene $(n - 1)$ aristas, es decir, tiene en una unidad menos aristas que vértices. Por consiguiente, G es un árbol. El teorema está demostrado.

Aduzcamos sin demostración algunos resultados más sobre los polinomios cromáticos.

Teorema 74. Sea $P(G; \lambda) = \sum_{i=1}^{|X|} a_i \lambda^i$ un polinomio cromático del grafo $G = (X, S)$. En este caso:

a) la sucesión $a_1, a_2, \ldots, a_{n-1}, a_n = 1$ es de signo alternativo;

b) si G es un grafo conexo, entonces

$$|a_i| \geqslant \binom{|X| - 1}{i - 1};$$

c) $a_k = \sum_{j=0}^{|S|} (-1)^j m_{kj}$, donde m_{kj} es el número de subgrafos generados del grafo G con k componentes de conexión y j aristas.

Entre los problemas referentes a los polinomios cromáticos quedan no resueltos los de descripción de los grafos que tienen un mismo polinomio cromático y el problema de hallar las condiciones necesarias y suficientes para que un polinomio sea cromático.

Sea G un grafo sin lazos y aristas paralelas (múltiples) y sea L un retículo geométrico definido por el matroide cíclico $M(G)$ del grafo. Para cualquier coloración α de las vértices del grafo G, denotemos con $A(\alpha)$ el con-

junto de aquellas aristas del grafo que tienen ambos vértices terminales igualmente pintados en α.

Proposición 19. Para cualquier coloración α, el conjunto de aristas $A(\alpha)$ es una superficie en $M(G)$.

Demostración. Supongamos que esto no es así. Sea $b \in \overline{A(\alpha)} \setminus A(\alpha)$. Entonces, existe un ciclo $\{b, a_1, \ldots, a_k\}$ del grafo C, tal que $\{a_1, \ldots, a_k\} \subseteq A(\alpha)$, y $b \notin A(\alpha)$. Pero, esto es imposible. Quiere decir que dos vértices terminales de la arista b están igualmente pintados para α, y, por lo tanto, $b \in A(\alpha)$. De aquí, $\overline{A(\alpha)} \setminus A(\alpha) = \varnothing$, y $\overline{A(\alpha)} = A(\alpha)$. La proposición está demostrada.

Para un número positivo entero arbitrario λ y para cualquier superficie A de un matroide cíclico $M(G)$ del grafo G, denotemos con $Q(\lambda; A)$ y $F(\lambda; A)$, respectivamente, el número de coloraciones α de λ colores del grafo G, tales que $A(\alpha) = A$ y $A(\alpha) \supseteq A$, respectivamente. Entonces

$$F(\lambda; A) = \sum_{B: B \geq A \text{ en } L} Q(\lambda; B).$$

De acuerdo con la fórmula de inversión de Moebius (véase teorema 55), tenemos

$$Q(\lambda; A) = \sum_{B: B \geq A \text{ en } L} \mu(A, B) F(\lambda; B).$$

En particular, cuando $A = \varnothing$:

$$Q(\lambda; \varnothing) = \sum_{B: B \geq 0 \text{ en } L} \mu(0, B) F(\lambda; B),$$

donde B son las superficies del matroide cíclico $M(G)$. Pero, $Q(\lambda; \varnothing)$ coincide con el número de coloraciones correctas en λ colores, es decir, con el número de λ-coloraciones del grafo G el cual es igual a $P(G; \lambda)$. Por otra parte, para cualquier superficie $B \in L$, o más bien para un subgrafo del grafo G, definido por el conjunto de aristas B,

$$F(\lambda; B) = \lambda^{k(B)} \lambda^{|X| - m},$$

donde m es el número de vértices y $k(B)$, el número de componentes conexas en el subgrafo definido por B. Quiere decir que

$$F(\lambda; B) = \lambda^{|X| - m + k(B)} = \lambda^{|X| - r(B)},$$

donde r es la función de rango del matroide cíclico $M(G)$, puesto que, en virtud de la proposición 8, $r(B) = m - k(B)$.

De este modo queda demostrado el siguiente resultado:

Teorema 75. Para un grafo arbitrario $G = (X, S)$ con k componentes de conexión y para cualquier número positivo entero λ:

$$P(G; \lambda) = \lambda^{|X|} \sum_{B \in L} \lambda^{-r(B)} \mu(0, B) = \lambda^k \sum_{B \in L} \lambda^{r(S) - r(B)} \mu(0, B),$$

donde μ es la función de Moebius del retículo geométrico L del matroide cíclico $M(G)$ del grafo G, y la suma se toma respecto de todas las superficies B del matroide $M(G)$.

Sea $M = (S, \bar{\ })$ un matroide y r, su función de rango. Se llama polinomio característico $P(M; \lambda)$ del matroide M al polinomio característico del retículo de superficies L, es decir,

$$P(M; \lambda) = \sum_{A \in L} \mu(0, A) \lambda^{r(S) - r(A)}.$$

De este modo, si $G = (X, S)$ es un grafo sin lazos y aristas múltiples, entonces, en virtud del teorema 75,

$$\lambda^k P(M(G); \lambda) = P(G; \lambda),$$

donde $M(G)$ es el matroide cíclico del grafo G. El *número cromático* $\chi(M)$ del matroide M se define como λ natural mínimo, para el cual $P(M; \lambda) > 0$. Por cuanto $P(G; \lambda) > 0$ cuando y sólo cuando $P(M(G); \lambda) > 0$, entonces los números cromáticos del grafo G y de su matroide cíclico $M(G)$ son iguales. Más aún, de aquí proviene en seguida que si los grafos G_1 y G_2 tienen matroides cíclicos isomorfos, sus números cromáticos son iguales.

El polinomio característico $P(M; \lambda)$ del matroide $M = (S, \bar{\ })$ tiene muchas propiedades comúnes con el polinomio cromático del grafo G. Por ejemplo:

a) si a no es ni lazo ni puente, entonces

$$P(M; \lambda) = P(M - a, \lambda) - P(M/a); \lambda);$$

b) si M tiene lazos, entonces $P(M; \lambda) = 0$;

c) si M se descompone en las componentes $M_1, \ldots, M_k$, entonces

$$P(M, \lambda) = \prod_{i=1}^{k} P(M_i; \lambda);$$

d) la sucesión de los coeficientes de $P(M; \lambda)$ es de signo alternativo.

Sea K una clase de matroide cerrado respecto de las sumas directas (uniones) y la formación de menores. Veamos las funciones f, definidas sobre los elementos de la clase K con valores en un anillo conmutativo con la unidad, que toman valores iguales en los matroides isomorfos, tales que para todos los M, M_1 y $M_2 \in K$:

a) $f(M_1 + M_2) = f(M_1) f(M_2)$;

b) $f(M) = f(M - a) + f(M/a)$, si a no es ni lazo ni puente.

Las funciones f que poseen las propiedades citadas llevan el nombre de invariantes de Tutte—Grothendieck.

Sea K una clase de todos los matroides. Pongamos $f_1(M)$ y $f_2(M)$ iguales al número de bases y al número de conjuntos independientes, respectivamente, del matroide M. Es fácil ver que f_1 y f_2 son invariantes de Tutte—Grothendieck. Se puede mostrar también que si $P(M; \lambda)$ es el polinomio ca-

racterístico del matroide M, entonces $(-1)^{r(M)}P(M; \lambda)$ es también un invariante de Tutte—Grothendieck.

Se llama *función de rango generalizada* del matroide $M = (S, \bar{})$ a un polinomio

$$R(M, x, y) = \sum_{A \subseteq S} x^{r(S)-r(A)} y^{r^*(S)-r^*(S \setminus A)},$$

donde r y r^* son funciones de rango de los matroides M y M^*, respectivamente. Haciendo uso de las relaciones entre r y r^*, podemos escribir que

$$R(M; x, y) = \sum_{A \subseteq S} x^{r(S)-r(A)} y^{|A|-r(A)}.$$

Directamente de la definición obtenemos:

$$R(M; x, y) = R(M^*; y, x);$$
$$R(M; x, y) = 1 + y, \text{ si } M \text{ es un lazo;}$$
$$R(M; x, y) = 1 + x, \text{ si } M \text{ es un puente.}$$

Se propone que a título de ejercicio se demuestre el siguiente teorema:

Teorema 76. El polinomio $R(M; x, y)$ es un invariante de Tutte—Grothendieck para cualquier clase de matroides K.

El polinomio $T(M; x, y) = R(M; x - 1, y - 1)$ para matroides gráficos fue estudiado por Tutte y por eso lleva el nombre *polinomio de Tutte.*

Resultó que todos los invariantes de Tutte—Grothendieck de una clase arbitraria K podían ser obtenidos del polinomio de Tutte. Por ejemplo:

a) $T(M; 2, 2) = 2^{|S|}$;

b) $T(M; 1, 1)$ es igual al número de bases del matroide M;

c) $T(M; 2, 1)$ es igual al número de conjuntos independientes del matroide M;

d) $T(M; 1, 2)$ es igual al número de conjuntos generadores del matroide M;

e) $T(M; 0, 0) = 0$;

f) $T(M; 1, 0) = (-1)^{r(S)}\mu(0, 1)$, donde μ es la función de Moebius del retículo de superficies del matroide M.

Más aún, a través del polinomio de Tutte se expresa el polinomio característico $P(M; \lambda)$ del matroide M:

$$P(M; \lambda) = (-1)^{r(S)}T(M; 1 - \lambda, 0).$$

Sin embargo, incluso matroides no isomorfos pueden poseer un mismo polinomio de Tutte. Por ejemplo, los matroides M_1 y M_2 de rango 3 sobre el conjunto $S = \{1, 2, 3, 4, 5, 6, 7\}$, expuestos en la fig. 8.40, son precisamente de esta clase.

$$T(M_1; x, y) = T(M_2; x, y) = x^3 + 3x^2 + x^2y + 2y + 5xy + 2xy^2 + \\ + 2y + 4y^2 + 3y^3 + y^4.$$

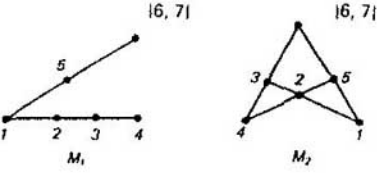

Fig.8.40.

No obstante, M_1 se diferencia de M_2 en una cantidad distinta de ciclos, superficies y coátomos.

Los matroides de Tutte realizan una conexión de los matroides con los códigos y empaques lineales, debido a lo cual toda una serie de problemas de la teoría de codificación se reduce a los problemas de la teoría de matroides. Veamos, por ejemplo, el problema de cálculo de la distribución de los pesos de un código.

Sea A una matriz de orden $k \times n$ con coeficientes de $GF(q)$. Vinculemos con cada tal matriz de rango k los siguientes dos objetos: U, que representa el código lineal sobre $GF(q)$, es decir, el espacio de filas de la matriz A; M, que es el matroide de las columnas de la matriz A. Sea $u \in U$. Se denomina peso $w(u)$ del vector u al número de sus componentes no nulas. Un polinomio

$$A(U, z) = \sum_{u \in U} z^{w(u)} = \sum_{i=1}^{n} A_i z^i,$$

donde A_i es el número de vectores $u \in U$ con $w(u) = i$ y lleva el nombre de *numerador ponderal* del código U.

Teorema 77. La función f, definida para todas las $(k \times n)$-matrices A sobre $GF(q)$ por medio de

$$f(A) = \frac{1}{(1-z)^k z^{n-k}} A(U; z),$$

es un invariante de Tutte—Grothendieck. Más aún,

$$f(A) = T\left(M; \frac{1 + (q-1)z}{1-z}, \frac{1}{z}\right),$$

donde $T(M, x, y)$ es el polinomio de Tutte.

A título de ilustración de la relación recíproca entre los códigos y matroides puede deducirse la fórmula de Mac Williams (que relaciona el numerador ponderal con el numerador ponderal del código que el es dual) basándose en la dualidad correspondiente del polinomio de Tutte.

Problema crítico. Sea $V(n, q)$ un espacio vectorial de dimensión n sobre el campo finito $GF(q)$, y sea S un subconjunto del espacio $V(n, q)$ que no contiene vector nulo. El subespacio de $V(n, q)$ de dimensión $n-1$ recibe el nombre de hiperplano. El problema crítico para el conjunto S consiste en la búsqueda de tal número positivo entero mínimo k, para el cual se en-

contrarán k hiperplanos $H_1, H_2, \ldots, H_k$ tales que $H_1 \cap H_2 \cap \ldots \cap H_k \cap S = \varnothing$; dicho de otro modo, para todo $p \in S$ existe por lo menos un solo hiperplano H_i, tal que $p \notin H_i$.

Por cuanto para cada hiperplano H_i del espacio $V(n, q)$ existe tal funcional lineal L_i sobre $V(n, q)$ con valores en $GF(q)$, tales que $H_i = L_i^{-1}(0)$, entonces el problema crítico puede enunciarse de otro modo. Diremos que una sucesión $(L_1, L_2, \ldots, L_k)$ de funcionales lineales *distingue* el conjunto S, si para todo $p \in S$ existe un índice $i (i = 1, 2, \ldots, k)$ tal que $L_i(p) \neq 0$. Un número positivo entero mínimo k, para el cual la sucesión $(L_1, L_2, \ldots, L_k)$ de funcionales lineales distingue el subconjunto S de $V(n, q)$, se denomina *exponente crítico* del conjunto S. Entonces el problema crítico consiste precisamente en la búsqueda del exponente crítico.

Si S consta de un solo vector nulo, su exponente crítico es igual a 1. En el caso cuando S consta de todos los vectores no nulos del espacio $V(n, q)$, su exponente crítico es igual, por lo visto, a n.

Teorema 78. Sea M un matroide lineal generado por un subconjunto S de $V(n, q)$ (véase el ejemplo 5 en el § 8.4) y sea $P(M; \lambda)$ su polinomio característico. Entonces, el número de sucesiones ordenadas $(L_1, \ldots, L_k)$ de funcionales lineales sobre $V(n, q)$, que distinguen el subconjunto S, es igual a $P(M, q^k)$.

Demostración. Supongamos que $A \subseteq S$ y que $g_k(A)$ es el número de sucesiones ordenadas $(L_1, L_2, \ldots, L_k)$ de funcionales lineales sobre $V(n, q)$ tales que $A \subseteq \bigcap_{i=1}^{k} L_i^{-1}(0)$. Sea $f_k(A)$ el número de sucesiones $(L_1, L_2, \ldots, L_k)$ para las cuales A es exactamente igual a la intersección de los núcleos, es decir, $A = \bigcap_{i=1}^{k} L_i^{-1}(0)$. Entonces, $g_k(A) = \sum_{B: A \subseteq B} f_k(B)$ y, en virtud de la fórmula de inversión de Moebius (véase teorema 55), tenemos

$$f_k(A) = \sum_{B: A \subseteq B} \mu(A, B) g_k(B).$$

Sea W_B una cápsula lineal de los vectores de B en $V(n, q)$. Entonces, W_B es un subespacio del espacio $V(n, q)$ y $\dim B = r(B)$, donde r es la función de rango del matroide M. Observemos que $g_k(B)$ es igual al número de sucesiones ordenadas $(L_1, L_2, \ldots, L_k)$ de funcionales lineales sobre el factor-espacio $V(n, q)/W_B$. Por cuanto $\dim V(n, q)/W_B = r(S) - r(B)$, entonces

$$g_k(B) = q^{(r(S) - r(B))k}.$$

Por consiguiente, $f_k(A) = \sum_{\substack{B: A \supseteq B \\ \subseteq B}} \mu(A, B)^{(r(S) - r(B))k}$. Al poner $A = \varnothing$, obtenemos

$$f_k(\varnothing) = \sum_{B: B \subseteq S} \mu(0, B) q^{(r(S) - r(B))k} = P(M; q^k),$$

donde $f_k(\varnothing)$ es precisamente el número de sucesiones ordenadas $(L_1, L_2, \ldots, L_k)$ de las funcionales lineales sobre $V(n, q)$ que distinguen S. El teorema está demostrado.

Corolario 13. Sea M un matroide generado por el subconjunto S de vectores no nulos del espacio $V(n, q)$ de dimensión n sobre el campo $GF(q)$. Entonces, el polinomio característico $P(M; \lambda)$ del matroide M posee la siguiente propiedad:

$$P(M; q^k) = 0 \text{ para } k = 0, 1, \ldots, c-1;$$
$$P(M; q^k) > 0 \text{ para } k \geqslant c,$$

donde c es la exponente crítica del conjunto S. Además, $c \leqslant n$ para todos los subconjuntos S de $V(n, q)$.

Crapo y Rota suponen que el problema crítico es «el problema central en la teoría combinatoria extremal» (véase [104]). En efecto, toda una serie de problemas combinatorios se enuncia adecuadamente en términos de esta teoría. Por ejemplo, la hipótesis de cuatro colores, mencionada más arriba, se enuncia así: si M es un matroide cíclico de un simple grafo planario, tendremos para las exponentes críticas: $c(M; 2) \leqslant 2$, y $c(M; 4) \leqslant 1$. Sin embargo, se han obtenido muy pocos resultados generales concernientes al problema crítico. Se ha demostrado, por ejemplo, que

a) la exponente crítica de una geometría lineal finita sobre $GF(q)$ es igual a 1, cuando y sólo cuando dicha geometría es isomorfa al submatroide de la geometría afín $AG(n, q)$;

b) las raíces del polinomio característico $P(G; \lambda)$ de una geometría superresoluble G son números positivos iguales a $|A_{i+1} \setminus A_i|$ (la geometría combinatoria $G = (S, \bar{})$ se denomina *superresoluble*, si existen superficies modulares $A_0 \subseteq A_1 \subseteq \ldots \subseteq A_n = S$, tales que $r(A_i) = i$. La superficie A de la geometría G se denomina *modular*, si forma un par modular con todas las demás superficies de la geometría G).

Ejercicios. 5. Sea S un conjunto finito y sea $\Pi = \{s_1, s_2, \ldots, s_n\}$ una partición del conjunto S. Diremos que un subconjunto $A \subseteq S$ es independiente, si ningún par de elementos de A yace en un mismo bloque de la partición Π, es decir, $|A \cap S_i| \leqslant 1$, $i = 1, 2, \ldots, n$. Muéstrese que el par $(S, \mathcal{F})$, donde $\mathcal{F}$ es una familia de todos los subconjuntos independientes del conjunto S, representa un matroide llamado *matroide de partición*.

6. Sea $G(V, E)$ un grafo orientado finito sin lazos, y S, $T \subseteq V$. Diremos que un subconjunto $A \subseteq S$ es independiente, si existe $|A|$ caminos que van de los vértices del conjunto A a los del conjunto T en el grafo G y que no se intersecan por los vértices. Muéstrese que el par $(S, \mathcal{F})$, donde $\mathcal{F}$ es una familia de todos los subconjuntos independientes del conjunto S, representa un matroide denominado *gammoide* (indicación: hágase uso del lema 6 del § 8.1)

7. Demuéstrese que cada matroide transversal es un gammoide. ¿Es cierta la afirmación inversa?

8. Muéstrese que un matroide es gammoide cuando y sólo cuando su contracción es un matroide transversal.

El resumen de los resultados referentes a los gammoides se da en [141].

Una peculiaridad de la estructura matroidal consiste en que cualquier conjunto independiente máximo por inclusión es también máximo por el

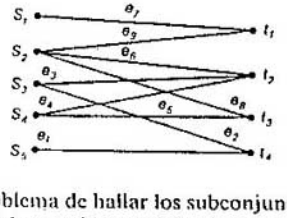

Fig.8.41.

número de elementos. El problema de hallar los subconjuntos independientes máximos por inclusión del matroide es trivial; basta añadir los elementos hasta que sea posible. En esto precisamente está basado el algoritmo «ávido» (véase § 6.3).

Ejercicio. 9. Muéstrese que si el algoritmo «ávido» elige k elementos, esos tienen un peso máximo entre todos los conjuntos independientes compuestos de k o menos elementos.

10. Supongamos que se tiene un conjunto de tareas cuyo cumplimiento con ayuda de un ordenador requiere un lapso de tiempo igual. Además, se conoce el plazo extremal de cumplimiento de cada tarea. Muéstrese que el juego de todos los subconjuntos de tareas, que pueden realizarse según un horario, forma el conjunto de todos los conjuntos independientes de cierto matroide.

11. Supongamos que en el ejercicio 10 se paga una multa por cada tarea no realizada. ¿En qué orden han de realizarse las tareas para que la multa total sea mínima?

12. Supongamos que a todos los elementos del matroide M les han sido asignados los pesos no negativos. Demuéstrese que

a) para todo x perteneciente a la base del matroide M, no existe un ciclo C, tal que $x \in C$ y x posea el menor peso entre todos los $y \in C$;

b) para cada elemento x de peso máximo, perteneciente a la base, existe por lo menos un cociclo c^*, tal que $x \in C^*$, y x tenga el mayor peso entre todos los elementos de C^*.

13. Sea M matroide sobre el conjunto S, a cuyos elementos les han sido asignados pesos no negativos, y sea B una familia de todas las bases, mientras que C^* es una familia de todos los cocicios del matroide M. Muéstrese que en este caso

$$\min_{A \in B} \max_{x \in B} w(x) = \max_{C^* \in C^*} \min_{x \in C^*} w(x).$$

Veamos un grafo bipartido $G(S \cup T, E)$ (fig. 8.41). Un subconjunto $\{e_2, e_4, e_9\} \subseteq E$ es una combinación de pares máxima por inclusión del grafo G, el cual no es máximo por el número de elementos. Por consiguiente, el par $(E, \mathscr{P})$, donde $\mathscr{P}$ es una familia de combinaciones de pares, no es matroide. Sin embargo, la familia de combinaciones de pares $\mathscr{P}$ del grafo posee una estructura bastante buena: es una intersección de dos matroides, es decir, pueden encontrarse dos tales matroides, $(E, \mathscr{S}_1)$ y $(E, \mathscr{S}_2)$ sobre el conjunto E de aristas del grafo con familias de conjuntos independientes $\mathscr{S}_1$ y $\mathscr{S}_2$, respectivamente, que $\mathscr{P} = \mathscr{S}_1 \cap \mathscr{S}_2$. Por ejemplo, definamos para el grafo expuesto en la fig. 8.41 dos matroides de partición $(E, \mathscr{S}_1)$ y $(E, \mathscr{S}_2)$ (véase ejercicio 5), poniendo $\Pi_1 = \{\{e_7\}, \{e_6, e_8, e_9\}, \{e_2, e_3\}, \{e_4, e_5\}, \{e_1\}\}$, y $\pi_2 = \{\{e_9, e_7\}, \{e_3, e_4, e_6\}, \{e_8, e_5\}, \{e_2, e_1\}\}$. No es difícil notar que el subconjunto $A \subseteq E$ es una combinación de pares en el grafo $G(S \cup T, E)$ cuando y sólo cuando A es independiente tanto en el matroide $(E, \mathscr{S}_1)$ (ningún par de aristas de A tiene vértice común en S), como también en el matroide $(E,$

$\mathcal{S}_2$) (ningún par de aristas de A tiene vértice común en T). Por consiguiente, $\mathcal{S} = \mathcal{S}_1 \cap \mathcal{S}_2$. De este modo, el problema sobre una combinación de pares en un grafo bipartido puede considerarse como un problema de búsqueda del subconjunto máximo del conjunto E que sea independiente en dos matroides a la vez.

Ejercicio 14. Sea S un conjunto finito y $\mathcal{F} = \{S_1, \ldots, S_n\}$ una familia de subconjuntos del conjunto S. Se pregunta si existe o no tal subconjunto $H \subseteq S$ que $|H| = n$ y $|H \cap S_i| = 1$ para $i = 1, \ldots, n$. Enúnciese este problema como un problema de intersección de un matroide transversal (ejemplo 9) y de un matroide de partición (véase ejercicio 5).

Sean dos matroides, $M_1(S, \mathcal{S}_1)$ y $M_2 = (S, \mathcal{S}_2)$ sobre el conjunto S, a cada elemento del cual le está asignado el peso $w(s)$, donde $s \in S$. Se requiere encontrar un subconjunto $I \in \mathcal{S}_1 \cap \mathcal{S}_2$ tal que la suma $\sum_{s \in I} w(s)$ sea máxima.

Teorema 79 (de Edmonds). El problema de intersección ponderada de los matroides es equivalente al problema de programación lineal

$$\text{máx} \left(\sum_{s \in S} w(s) \cdot x(s) \right)$$

a condición de que para todo $A \subseteq S$

$$\sum_{s \in A} x(s) \leqslant r_{M_1}(A) \text{ y } \sum_{s \in A} x(s) \leqslant r_{M_2}(A),$$

donde r_{M_i} es la función de rango del matroide r_{M_i}, $i = 1, 2$; $x(s)$ es una función binaria sobre el conjunto S.

La relación existente entre la teoría de los matroides y la optimización combinatoria fue revelada por primera vez en [142]. En la misma obra Edmonds anunció la solución polinomial del problema sobre la intersección de matroides, cuyo algoritmo de resolución puede encontrarse en [143, 144]. Los algoritmos y su argumentación para los problemas de optimización combinatoria de estructura matroidal están bien descritos en [145].

Solamente hemos hecho un breve resumen de las tendencias principales de la teoría de los matroides. Para el estudio ulterior del problema se recomiendan las obras [1, 34, 104...109, 138 y 145].

BIBLIOGRAFÍA

1. **M. Aigner**, Combinatorial Theory. Heidelberg. 1979.
2. **A. Kaufmann**, Introduction a la combinatorique en vue des application, Dunon, Paris, 1968.
3. **В. Н. Сачков**, Введение в комбинаторные методы дискретной математики. М., Наука, 1982. (V. N. Sachkov, Introducción a los métodos combinatorios de las matemáticas discretas.)
4. **M. Hall**, Combinatorial Theory, Toronto, 1967.
5. **С. В. Яблонский**, Введение в дискретную математику. М., Наука, 1979. (S. V. Yablonski, Introducción a las matemáticas discretas.)
6. **Г. П. Гаврилов, А. А. Сапоженко**, Сборник задач по дискретной математике. М., Наука, 1977. (G. P. Gavrilov, A. A. Sapojenko, Problemas de las matématicas discretas.)
7. Комбинаторный анализ. Задачи и упражения (под ред. Рыбникова К. А.). М., Наука, 1982. (Análisis combinatorio. Problemas y ejercicios, dirigido por Rybnikov K. A.)
8. **L. Lovasz**, Combinatorial problems and Exercises. Budapest. Akademiai Kiado, 1979.
9. **G. Birkhoff, T. Bartee**, Modern applied algebra. New-York, 1970.
10. Applied Combinatorial Mathematics. Ed. by E. Beckenbach. New-York, 1964.
11. **Г. П. Егорычев**, Интегральные представления и вычисление комбинаторных сумм. — Новосибирск: Наука, 1977. (G. P. Egórychev, Representaciones integrales y cálculo de las sumas combinatorias.)
12. Перечислительные задачи комбинаторного анализа/ Под редакцией Г. П. Гаврилова. — М.: Мир, 1979. (Problemas enumerativos del análisis combinatorio.)
13. **М. Л. Платонов**, Комбинаторные числа класса отображений и их приложения. М. Наука, 1979. (M. I. Platónov, Números combinatorios de la clase de aplicaciones y su empleo.)
14. **J. Riordan**, An Introduction to Combinatorial Analysis. New-York, 1958.
15. **R. Graham**, Rudiments of Ramsey Theory, American Math. Soc., Providence, 1981.
16. **G. Endrews**, Theory of partitions, Reding, Mass. 1976.
17. **M. Marcus, H. Minc**, Survey of matriz theory and matrix inequalities, 1964.
18. **H. Minc**, Permanents. Reding. Mass. USA, 1978.
19. **В. А. Носов, В. Н. Сачков, В. Е. Тараканов**, Комбинаторный анализ. Итоги науки и техники, 1981, т. 18, с. 53—93. (V. A. Nósov, V. N. Sachkov, V. E. Tarakánov, Análisis combinatorio.)
20. **J. Dénes, A. D. Keedwell**, Latin squares and their applications. Budapest. Akadémiai Kiadó, 1974.
21. **F. Kárteszi**, Introduction to finite geometry, Akademiai Kiado, Budapest, 1976.
22. **P. Cameron, J. van Lint**, Graph theory, coding theory and block-designes. Cambridge Univ., 1975.
23. **R. Busucker, Th. Saaty**, Finite Graphs and networks. Mc Graw Hill Book Co.
24. **N. Christofides**, Graph theory. An algorithmic approach. London, 1975.
25. **O. Ore**, Theory of graphs. Amer. Math. Soc., 1962.
26. **В. К. Леонтьев**, Дискретные экстремальные задачи. Итоги науки и техники, 1979, т. 16, с. 39—101. (Leóntiev V. K. Problemas extremales discretos.)
27. **H. Saaty**, Optimization in Integers and Related Extremal Problems.) New-York, 1970.

28. **L. Ford, D. Fulkerson.** Flows in Nerworks. Princeton, 1962.
29. **В. Н. Сачков,** Вероятностные методы в комбинаторном анализе. М. Наука, 1978. (**V. N. Sachkov,** Métodos probabilísticos en el análisis combinatorio.)
30. **P. Erdös, J. Spencer,** Probabilistic methods in combinatorics. Budapest, 1974.
31. **G. Birkhoff,** Lattice Theory. Providence, 1967.
32. **G. Grätzer,** General Lattice Theory. Berlin, 1978.
33. *Скорняков Л. А.* Элементы теории структур. — М.: Мир, 1982 (**L. Skorniakov,** Elementos de la teoría de las estructuras.)
34. **Welsh D. J. A.** Matroid theory. London: Academic Press, 1976.
35. **R. L. Graham,** Partitions of a finite set. J. Combinatorial Theory, 1966, v. 1, N 2, p. 215—223.
36. **A. Renyi,** On a problem of information theory. Publ. Math. Inst. Hungar. Acad. Sci., 1961, v. 6, p. 505—516.
37. **G. Katona G.** On separating systems of a finite set. J. Combinatorial Theory, 1966, v. 1, N 2, p. 174—194.
38. П. Эрдеш, Д. Клейтман, Экспериментальные задачи о подмножествах конечного множества — М.: Мир, 1976, с. 115—130. (**P. Erdos, J. Spencer,** Probabilistic Methods in combinatorics.)
39. **P. Erdös, Ko Chao, R. Rado,** Intersection theorems for systems of finite sets. Quart. J. Math., ser. 2, 1961, v. 12, n 48, p. 313—320.
40. **P. Turan,** Egy gratelmeleti szélsoértekfeladatrol. Mat. és Fiz. Lapok, 1941, vol. 48, N 3, p. 436—453.
41. А. Ф. Сидоренко, О проблеме Турана для 3-графов. В кн.: Комбинаторный анализ. Вып. 6. М. Изд-во МГУ, 1983, с. 51—57. (**A. F. Sidorenko,** Sobre el problema de Turan para 3-grafos.)
42. **В. И. Больщаков,** (A_1, . . ., A_n)-перманенты и их приложения. Вестн. Моск. ун-та, сер. матем., мех. 1985, № 3, с. 18—22. (**V. I. Bolshakov,** (A_1, . . ., A_n)-permanentes y sus aplicaciones.)
43. **R. Mullin, G. C. Rota,** On the foundations of combinatorial theory III: theory of binomial enumeration. — In: Graph theory and its applications, N. Y.: Academic Press, 1970. p. 167—213.
44. **A. P. Giunand,** The umbral method: a survey of elementary mnemonic and manipulative uses. — Amer. Math. Monthly, 1979, v. 86, N 3, p. 187—195.
45. **F. P. Ramsey,** On a problem of formal logic. — Proc. London Math. Soc., Ser. 2, 1929, v. 30, N 4, p. 264—286.
46. **D. Konig.** Uber Graphen und ihre Anwendungen auf Determinantentheorie und Mengenlehre. — Math. Ann., 1916, v. 77, N 4, p. 453—465.
47. **A. Hedayat, W. D. Wallis,** Hadamard matrices and their applications. — Ann. Statist., 1978, v. 6, N 6, p. 1184—1238.
48. **J. Riordan,** Three-line Lanin rectangles. — Amer. Math. Monthly, 1944, v. 51, p. 450—452.
49. **М. Н. Добровольский,** О четырехстрочных латинских прямоугольниках. — В кн.: Материалы межвузовской научной конференции педагогических институтов центральной зоны. Тула, 1968, с. 72—75. (**M. N. Dobrovolski.** Sobre los rectángulos latinos de cuatro filas.)
50. **K. Yamamoto,** On the asymtotic number of Latin rectangles. Jap. J. of Math., 1951, v. 21, p. 113—119.
51. **G. Tarry,** Le probleme des 36 officiers. — C.—R. Assoc. Fr. Acad. Sci., 1900, v. 1, p. 122—123; 1901, v. 2, p. 170—203.
52. **H. B. Mann,** The construction of orthogonal Latin squares. — Ann. Math. Statistics, 1942, v. 13, N 4, p. 418—423.
53. **R. C. Bose, S. S. Shrikhande, E. T. Parker,** Further results on the construction of mutual-

ly orthogonal Latin squares and the falsity of Euler' s conjecture. — Canadian J. of Math., 1960, v. 12, N 2, p. 189—203.
54. J. Steiner, Combinatorische Aufgabe. — J. Reine und Angew. Math., 1953, v. 45, p. 181—182.
55. M. Reiss, Uber eine Steinersche combinatorische Aufgabe welche in 45-sten Bande dieses Journal, setie 181, gestellet worden ist. — J. Reine und Angew. Math., 1859, v. 56, p. 326—344.
56. T. R. Kirkman, On a problem in combination. — Cambridge and Dublin Math. J., 1847, v. 2, p. 191—204.
57. T. R. Kirkman, Note on an unanswered prize question. — Cambridge and Dublin Math. J., 1850, v. 5, p. 255—262.
58. R. Wilson, Nonosomorphic Steiner triple systems. — Math. Z., 1974, v. 135, p. 303—313.
59. E. H. Moore, Concerning triple systems. — Math. Ann., 1893, v. 43, p. 271—285.
60. E. Netto, Lehrbuch der Combinatorik. — Oslo: 1927, p. 234.
61. C. C. Lindner, A. Rosa, Steiner quadruple systems. — Discrete Math., 1978, v. 21, p. 147—181.
62. G. J. Ryser, Combinatorial Mathematics. New-York, 1963.
63. J. P. M. Binet, Mémoire sur un système de formules analytiques, et leur application á des considérations geometriques. — J. Ec. Polyt., 1812, v. 9, cah. 16, p. 280—302.
64. A. L. Cauchy, Mémoire sur les functions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment. — J. Ec. Polyt., 1812, v. 10, cah. 17, p. 29—112, Oeuvres (2)i.
65. T. Muir, On a class of permanent symmetric functions. — Proc. Roy. Soc., Edinburgh, 1882, v. 11, p. 409—418.
66. T. Muir, A relation between permanents and determinants. — Proc. Roy Soc., Edinburgh, 1897, v. 22, p. 134—136.
67. Г. П. Егорычев, Решение проблемы Ван дер Вардена для перманентов — Институт физики им. Л. В. Киренского СО АН СССР, Препринт ИФСО—13М. Красноярск, 1980. (G. P. Egórychev, Solución del problema de Van der Waerden para los permanentes.)
68. Д. И. Фалимман, Доказательство гипотезы Ван дер Вардена о перманенте дважды стохастической матрицы. — Матем. заметки, 1981, т. 29, № 6, с. 931—938. (D. I. Falikman, Demostración de la hipótesis de Van der Waerden sobre el permanente de una matriz dos veces estocástica.)
69. А. И. Кострикин, Ю. И.Манин, Линейная алгебра и геометрия. — М.: Изд-во МГУ, 1980. (Kostrikin A. I., Munin Yu. I. Algebra lineal y geometría.)
70. А. А. Панов, О сигнатуре и ядре билинейной формы, связанной с перманентом. — Успехи матем. наук, 1984, т. 39, № 6, с. 201—202. (A. A. Panov, Sobre la signatura y el núcleo de una forma bilineal asociada con un permanente.)
71. B. L. Waerden, van der. Aufgabe 45. — Iber Deutsch. Math. Verein., 1926, v. 35, p. 117.
72. P. A. Mac Mahon, Researches in the theory of determinants. Trans. Cambridge Philos. Soc., *(24, v. 23, N 5, p. 89—135).
73. Л. М. Брэгман, Некоторые свойства неотрицательных матриц и их перманентов. Докл. АН СССР, 1973, т. 211, № 1, с. 27—30. (L. M. Bregman, Algunas propiedades de las matrices no negativas y de sus permanentes.)
74. A. A. Schrijver, A short proof of Mine s conjecture. — J. Combinatorial theory, ser. A, 1978, v. 25, N 1, p. 80—83
75. J. M. Hammersley, An improved lower bound for the multidimensional dimer problem. — Proc. Cambridge Philos. Soc., 1968, v. 64, N 2, p. 455—463.
76. Л. А. Скорняков, Проективные плоскости. — Успехи матем. наук, 1951, т. 6, вып. 6, с. 112—153. (L. A. Skornjakov, Planos proyectivos.)
77. R. Hartshorne, Foundations of Projective Geometry. New-York, 1967.
78. C. Berge, Théorie des graphes et ses applications. Paris. 1958.
79. N. L. Biggs, E. K. Lloyd, R. J. Wilson, Graph Theory. 1736—1936. — Oxford: Clarendon Press, 1977.

80. **V. Klee,** Combinatorial optimization: what is the state of the art? — Math. Oper. Research, 1980, v. 5, N 1, p. 1—26.
81. **В. Е. Бурков, С. Е. Ловецкий,** Методы решения экстремальных комбинаторных задач. — Изв. АН СССР, сер. техническая кибернетика, 1968, № 4, с. 82—93. (**V. E. Burkov, S. E. Lovétski,** Métodos de resolución de los problemas combinatorios extremales.)
82. **W. Feller,** An Introduction to Probability Theory and Its Applications. Vol 1. New-York, 1966.
83. **R. C. Bose, S. Chowla,** Theorems in additive theory of numbers. — Comment. Math Helv., 1962, v. 37, N 2, p. 141—147.
84. **А. Г. Дьячков, В. В. Рыков** Об одной модели кодирования для суммирующего канала с множественным доступом. — Проблемы передачи информации, 1981, т. 17, № 2, с. 26—39. (**A. G. Djachkóv, V. V. Rykov,** Sobre un modelo de codificación para el canal de sumación con acceso multiplicativo.)
85. **B. Lindström,** On B_2-sequences of vectors — J of Number Theory, 1972, v. 4, N 3, p. 261—265.
86. **Л. Д. Мешалкин,** К обоснованию метода случайного баланса. Заводская лаборатория, 1970, т. 36, № 3, с. 18—27. (**L. D. Meshalkin,** Para la argumentación del método de equilibrio aleatorio.)
87. **М. Б. Малютов, М. С. Пинскер,** Замечания о простейшей модели метода случайного баланса. — В кн.: Вероятностные методы исследования. — М.: Изд-во МГУ, 1974. (**M. B. Malútov, M. S. Pinsker,** Notas sobre un modelo más simple del método de equilibrio aleatorio.)
88. **L. Wegener,** On separating systems whose elements are sets of at most k elements — Discrete Math., 1979, v. 28, p. 219-222.
89. **В. Н. Лузгин,** Разделяющие системы разбиений конечного множества. — В кн.: Комбинаторный анализ. Вып. 5. — М.: Изд-во МГУ, 1980, с. 39—45. (**V. N. Luzguín,** Sistemas separadores de particiones de un conjunto finito.)
90. **А. Г. Курош,** Лекции по общей алгебре. — М.: Наука, 1973. (**A. G. Kurosh,** Conferencias del álgebra general)
91. Дж. Л. Келли, Общая топология. — М.: Наука. (**J. L. Cayley,** Topologia general.)
92. **R. P. Dilworth,** A decomposition theorem for partially ordered sets. — Ann. af Math., ser. 2, 1950, v. 51, N 1, p. 161—166.
93. **Б. С. Стечкин,** Теоремы вложения для мебиус-функций. — Докл. АН СССР, 1980, т. 260, № 1, с. 40—43. (**B. S. Stechkin,** Teoremas de encaje para las funciones de Moebius.)
95. **H. H. Crapo,** Erecting geometries. — Ann. New-York Acad. Sci., 1970, v. 175, p. 89—92.
94. **H. H. Crapo,** Single-element extention of matroids. — J. Res. Nat. Bur. Standards, 1969, v 69B, p. 55—65.
96. **А. М. Ревякин,** О наращениях комбинаторных геометрий. — Вестн. Моск. ун-та, сер мат., мех., 1976, № 4, с. 59—62. (**A. M. Revjakin,** Sobre alargamientos de las geometrías combinatorias.)
97. **H. Q. Nguen,** Constructing the free erection of a geometry. J. Combinatorial Theory, ser B, 1979, v. 27, N 2, p. 216—224.
98. **T. Brilawsky,** Modular construction for combinatorial geometries. — Trans. Amer. Math. Soc., 1975, v. 203, p. 1—44.
99. **D. Higgs,** Strong maps of geometries. — J. Combin. Theory, 1968, v. 5, N 2, p. 185—191.
100. **D. Higgs,** Maps of geometries. — J. London Math. Soc., 1966, v. 41, N 4, p. 612—618.
101. **H. Q. Nguen,** Functors of the category of combinatorial geometry and strong maps. — Discrete Math., 1977, v. 20, N 2, p. 143—158.
102. **D. Lucas,** Weak maps of combinatorial geometries. — Trans. Amer. Math. Soc., 1975, v. 206, p. 247—279.
103. **P. D. Seymour,** Decomposition of regular matroids. — J. Combinatorial Theory, ser. B, 1980, v. 28, N 3, p. 305—359.

104. **H. H. Crapo, G. C. Rota,** On the foundations of Combinatorial theory II: Combinatorial geometries. — Cambridge Mass.: MIT Press, 1970.
105. **Дж. Х. Мейсон,** Изучение матроидов как геометрических конфигураций. — М.: Мир, 1980. (J. H. Mason, Estudio de los matroides como configuraciones geométricas.)
106. **B. Lindstrom,** Lectures on matroids. — Stock. Univ., 1974, N 7, p. 1—43.
107. **L. Mirsky,** Transversal theory. — N. Y.: Academic Press, 1971.
108. **R. Rundow,** Introduction to the theory of matroids. — Lect. Notes in Econ. and Math. Syst., 1975, v. 109, p. 1—110.
109. **W. T. Tutte,** Lectures on matroids — J. Res. Mat. Bur. of Standards, 1965, v. 69B, p. 1—47.
110. **D. J. A. Welsh,** Colouring, flows and projective geometry. — Nieuw. arch. wisk., 1980, v. 28, N 2, p. 159—176.
111. **В. М. Алексеев, В. М. Тихомиров, С. В. Фомин,** Оптимальное управление. — Наука, 1979. (V. M. Alexiéev, V. M. Tijomirzov, S. V. Fomín, Dirección optimal.)
112. **В. А. Носов, В. Н. Сачков, В. Е. Тараканов,** Комбинаторный анализ — Итоги науки и техники, 1983, т. 21, с. 120—178. (V. A. Nósov, V. N. Sachkov, V. E. Tarakanov, Análisis Combinatorio.)
113. **В. П. Козырев, С. В. Юшманов,** Теория графов (алгоритмические, алгебраические и метрические проблемы). — Итоги науки и техники, 1985, т. -3, с. 68—117. (V. P. Kózirev, S. V. Yushmánov, Teoría de los grafos (problemas algorítmicos, algebraicos y métricos.)
114. **J. Von Neumann,** Lectures on continuous geometries. Inst. of advanced Studies, Princeton, N. Y., 1936.
115. **G. Birkhoff,** Lattice Theory. First Edition, Amer. Math. Soc., 1940.
116. **F. Maeda, S. Maeda,** Theory of symmetric lattices. Springer-Verlag, N. Y., 1970.
117. **F. Maeda,** Lattice theoretic characterization of abstract geometries. J. Sci. Hirosima Univ., Ser. A, 15, 1951, 87—96.
118. **U. Sasaki, S. Fujiwara,** The decomposition of matroid lattices. J. Sci. Hirosima Univ., Ser. A., 15, 1952, 183—188.
119. **K. Menger,** Zur allgemeinen Kurventheorie. Fund. Math., 10, 1927, 96—115.
120. **L. Mirski,** Perfect H. Sistems of representatives. J. Math. Anal. Applic., 15, 1966, 520—568.
121. **J. T. Robacker,** On network theory. RAND Corporation Research Memorandum. RM—1498, 1955.
122. **F. Harary,** Graph Theory. Reding, Mass., 1969.
124. **В. А. Емеличев, М. М. Ковалев, М. К. Кравцов,** Многогранники, графы, оптимизация. М. Наука, 1981. (V. A. Emelichev, M. M. Kovalev, M. K. Kravtzov. Poliedros, grafos, optimización.)
125. **В. Е. Тараканов,** Комбинаторные задачи и (0, 1)-матрицы. Наука, 1985. (V. E. Tarakanov, Problemas combinatorios y (0, 1)-matrices.)
126. **Э. Майника,** Алгоритмы оптимизации на сетях и графах. — М.: Мир, 1981. (E. Minieka, Algoritmos de optimización en redes y grafos.)
127. **Ch. Papadimitrion, k. Steigitz,** Combinatorial Optimization: Algorithms and Complexity, USA, Prentice-Hall, 1982.
128. **M. Nakamura, M. Iri,** A structural theory for submodular functions, polimatroids and polymatroid intersection. Research Memorandum RM1 81—06, University of Tokyo, 1981.
129. **M. Iri,** A review of recent work in Japan on principal partitions of matroids and their application. Annals of New-York Academy of Sciences 319, 1979, 306—319.
130. **M. Iri, S. Fujishige,** Use of matroid theory in operations research, circiuts and systems theory. International Journal of Systems Science 12, 1981, 27—54.
131. **N. Tomizawa, S. Fujishige,** Historical survey of extensions of the concept of principal partition and their unifying generalization to hypermatriods. Systems Science Research Report N 5. Tokyo Institute of Technology, 1982.

132. **S. Fujishige,** Submodular systems and related topics. Math. Programming Study, 22, 1984, 113—131.
133. **L. Mirski,** Transversal theory. Academic Press, N. Y., 1971.
134. **P. Elias, A. Feinstein, C. E. Shannon,** A note on the maximum flow through a network. IRE Trans. Inform. Theory, 2, n 4, 1956, 117—119.
135. **А. А. Зыков,** Теория конечных графов. Н. Наука, 1969. (**A. A. Zykov,** Teoria de los grafos finitos)
136. **M. Iri,** Application of matroid theory to engineering systems problems. Proc. of the 6 Conference on Probability Theory. September 1—15, 1976, Brasov, Romania, Bucureşti, 1981, 107—127.
137. **I. Herstein,** Noncommutative Rings, New-York, 1968.
138. Theory of matroids (edited by N. White). Cambridge e.a. 1986.
139. **А. М. Ревякин,** Об одной конструкции в категориях комбинаторных геометрий и отображений. ДАН СССР, 1976, т. 229, № 5, 1055—1058. (**A. M. Reviakin,** Sobre una construcción en las categorías de las geometrías y aplicaciones combinatorias).
140. **А. М. Ревякин,** Некоторые свойства и конструкции категории комбинаторных геометрий и отображений. В кн.: Комбинаторный анализ. Вып. 6. М. Изд-во МГУ, 1983, 4—12. (**A. M. Reviakin,** Propiedades y construcciones de la categoría de las geometrías y aplicaciones combinatorias.)
141. **A. W. Ingleton,** Transversal matroids and related structures. Higher Combinatorics (Aigner, ed.), Dordrecht: Reidel 1977
142. **J. Edmonds,** Matroids and the greedy algorithm. Math. Prog., 1971, 1, 127—136.
143. **E. L. Lawler,** Matroid intersection algorithms. Math. Prog., 1975, 9, 31—56.
144. **J. Edmonds,** Minimum partition of a matroid into independent subsets. J. Res. NBS, 1965, 69B, 67—77.
145. **E. L. Lawler,** Combinatorial optimization: networks and matroids. New York, 1976.

Índice alfabético de materias