CAPITULO XII

POLINOMIOS DE COEFICIENTES RACIONALES

§ 56. Reducibilidad de los polinomios sobre el campo de los números racionales

El tercer campo numérico que, junto con los campos de números reales y de números complejos tiene para nosotros un interés especial, es el *campo de los números racionales*; éste lo designaremos mediante R. Entre todos los campos numéricos éste es el más pequeño, pues, como se demostró en el § 43, el campo R está contenido totalmente en cualquier campo numérico. Ahora nos va a interesar el problema de la reducibilidad de los polinomios sobre el campo de *números racionales* y, *en el siguiente párrafo*, el problema de las raíces racionales (enteras o fraccionarias) de los polinomios de coeficientes racionales. Subrayemos una vez más, que éstos son dos problemas distintos; por ejemplo, el polinomio

$$x^4 + 2x^2 + 1 = (x^2 + 1)^2$$

es reducible sobre el campo de números racionales, a pesar de que no tiene ninguna raíz racional.

¿Qué se puede decir de la reducibilidad de los polinomios sobre el campo R? Ante todo, obsérvese que, dado un polinomio $f(x)$ *de coeficientes racionales que no sean todos enteros, entonces*, reduciendo éstos a un común denominador y multiplicando $f(x)$ por este denominador, igual, por ejemplo, a k, resulta un polinomio $kf(x)$ cuyos coeficientes son ya números enteros. Es evidente, que los polinomios $f(x)$ y $kf(x)$ tienen raíces iguales; por otra parte, *éstos son a la vez reducibles o irreducibles sobre el campo* R.

Mas, por ahora, no tenemos derecho de limitarnos a estudiar en adelante los polinomios de coeficientes enteros. En efecto, supongamos que el polinomio $g(x)$ de coeficientes enteros es reducible sobre el campo de los números racionales, o sea, que se descompone *en factores de menor grado de coeficientes racionales (en general*, fraccionarios). ¿Se deduce de esto que $g(x)$ se descompone en factores de coeficientes enteros? En otras palabras, ¿puede ocurrir que un polinomio de coeficientes enteros sea reducible sobre el campo de números racionales y sea irreducible sobre el anillo de *los números enteros*?

La respuesta a estas preguntas se puede obtener haciendo un exámen análogo al que se hizo en el § 51. Llamemos *primitivo* al polinomio $f(x)$ de coeficientes enteros, si sus coeficientes son primos entre sí, o sea, si no tienen divisores comunes distintos de 1 y -1. Cualquier polinomio $\varphi(x)$ de coeficientes racionales se puede representar de un modo único en forma de un producto de una fracción irreducible por un polinomio primitivo:

$$\varphi(x) = \frac{a}{b} f(x); \tag{1}$$

para esto hay que sacar fuera de paréntesis el común denominador de todos los coeficientes del polinomio $\varphi(x)$, y después, los factores comunes de los numeradores de estos coeficientes; obsérvese que el grado de $f(x)$ es igual al grado de $\varphi(x)$. La unicidad (salvo el signo) de la representación (1) se demuestra del modo siguiente. Sea

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x),$$

donde $g(x)$ es de nuevo un polinomio primitivo. Entonces,

$$adf(x) = bcg(x).$$

Por lo tanto, ad y bc se han obtenido sacando todos los factores comunes de los coeficientes de un mismo polinomio de coeficientes enteros, por lo cual, pueden diferenciarse entre sí solamente en el signo. De aquí se deduce, que los polinomios primitivos $f(x)$ y $g(x)$ también pueden diferenciarse entre sí solamente en el signo.

Para los polinomios primitivos de coeficientes enteros conserva su valor el **lema de Gauss:**

El producto de dos polinomios primitivos de coeficientes enteros es un polinomio primitivo.

En efecto, sean dados los polinomios primitivos de coeficientes enteros

$$f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_ix^{k-i} + \ldots + a_k,$$

$$g(x) = b_0x^l + b_1x^{l-1} + \ldots + b_jx^{l-j} + \ldots + b_l$$

y sea

$$f(x)\,g(x) = c_0x^{k+l} + c_1x^{k+l-1} + \ldots + c_{i+j}x^{(k+l)-(i+j)} + \ldots + c_{k+l}.$$

Si *este producto no es primitivo, existe un número* **primo** p *que* es común divisor de todos los coeficientes $c_0, c_1, \ldots, c_{k+l}$. Como no todos los coeficientes del polinomio primitivo $f(x)$ pueden dividirse por p, habrá uno, sea éste a_i, que será el primero que no se divide por p; del mismo modo, sea b_j el primer coeficiente del polinomio $g(x)$ que no se divide por p. Multiplicando término a término $f(x)$ por $g(x)$ y reuniendo los términos que contienen a $x^{(k+l)-(i+j)}$,

resulta:

$$c_{i+j} = a_i b_j + a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \ldots + a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots$$

El primer miembro de esta igualdad se divide por p. Por éste se dividen también todos los términos del segundo miembro, menos el primero; en efecto, en virtud de las condiciones impuestas a la elección de i y j, todos los coeficientes a_{i-1}, a_{i-2}, . . ., y también b_{j-1}, b_{j-2}, . . ., se dividen por p. De esto se deduce, que el producto $a_i b_j$ también se divide por p y, por esto, como p es un número primo, tiene que dividirse por p por lo menos uno de los coeficientes a_i, b_j, lo cual, sin embargo, no es cierto. Con esto queda terminada la demostración del lema.

Pasemos a responder a las preguntas que se hicieron más arriba. Supongamos que el polinomio $g(x)$ de grado n, de coeficientes enteros, es reducible sobre el campo de números racionales:

$$g(x) = \varphi_1(x)\, \varphi_2(x),$$

donde $\varphi_1(x)$ y $\varphi_2(x)$ son polinomios de coeficientes racionales de grado menor que n. Entonces,

$$\varphi_i(x) = \frac{a_i}{b_i} f_i(x), \quad i = 1, 2,$$

donde $\frac{a_i}{b_i}$ es una fracción irreducible, $f_i(x)$ es un polinomio primitivo. Por lo tanto,

$$g(x) = \frac{a_1 a_2}{b_1 b_2} [f_1(x)\, f_2(x)].$$

El primer miembro de esta igualdad es un polinomio de coeficientes enteros, por esto, el denominador $b_1 b_2$ del segundo miembro tiene que simplificarse. Mas, por el lema de Gauss, el polinomio que figura entre corchetes es primitivo, por lo tanto, cualquier factor primo de $b_1 b_2$ puede simplificarse solamente con cierto factor primo de $a_1 a_2$, y como a_i y b_i son primos entre sí, $i = 1, 2$, el número a_2 tiene que dividirse por b_1 y el número a_1, por b_2:

$$a_2 = b_1 a_2', \quad a_1 = b_2 a_1'.$$

De aquí que

$$g(x) = a_1' a_2' f_1(x)\, f_2(x).$$

Uniendo el coeficiente $a_1' a_2'$ a cualquiera de los factores $f_1(x)$, $f_2(x)$, obtenemos la descomposición del polinomio $g(x)$ en factores de menor grado de coeficientes enteros. Con esto, queda demostrado el siguiente **teorema**:

Un polinomio de coeficientes enteros que es irreducible sobre el anillo de los números enteros, es irreducible también sobre el campo de los números racionales.

Por fin, hemos obtenido ahora el derecho de limitarnos a estudiar las descomposiciones de los polinomios de coeficientes enteros en factores cuyos coeficientes también sean enteros, en las cuestiones relacionadas con la irreducibilidad de los polinomios sobre el campo de números racionales.

Ya sabemos que sobre el campo de los números complejos, es reducible todo polinomio cuyo grado sea mayor que la unidad, y sobre el campo de los números reales, todo polinomio (de coeficientes reales) cuyo grado sea mayor que dos. Otra cosa ocurre en el caso del campo de los números racionales: *para cualquier n se puede indicar un polinomio de n-ésimo grado de coeficientes racionales (e incluso enteros) que es irreducible sobre el campo de los números racionales.* La demostración de esta afirmación se basa en el siguiente criterio suficiente de irreducibilidad de un polinomio sobre el campo R, denominado **criterio de Eisenstein:**

Sea dado un polinomio

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$

de coeficientes enteros. Si, al menos de un modo, se puede elegir un número primo p que satisfaga a las condiciones siguientes:

1) *el coeficiente superior a_0 no es divisible por p,*

2) *todos los demás coeficientes son divisibles por p,*

3) *el término independiente, siendo divisible por p, no es divisible por p^2, entonces el polinomio $f(x)$ es irreducible sobre el campo de los números racionales.*

En efecto, si el polinomio $f(x)$ es reducible sobre el campo R, entonces se descompone en dos factores de menor grado de coeficientes enteros:

$$f(x) = (b_0x^k + b_1x^{k-1} + \ldots + b_k)(c_0x^l + c_1x^{l-1} + \ldots + c_l),$$

donde $k<n$, $l<n$, $k+l=n$. Identificando los coeficientes de ambos miembros de esta igualdad, obtenemos:

$$\left.\begin{aligned} a_n &= b_kc_l, \\ a_{n-1} &= b_kc_{l-1} + b_{k-1}c_l, \\ a_{n-2} &= b_kc_{l-2} + b_{k-1}c_{l-1} + b_{k-2}c_l, \\ &\cdots\cdots\cdots\cdots\cdots \\ a_0 &= b_0c_0. \end{aligned}\right\} \qquad (2)$$

De la primera de las igualdades (2) se deduce que, como a_n es divisible por p y el número p es primo, uno de los factores b_k, c_l tiene que ser divisible por p. Ambos no pueden ser divisibles por p, puesto que, por la hipótesis, a_n no es divisible por p^2. Supongamos, por ejemplo, que b_k es divisible por p y, por lo tanto, c_l es primo

con p. Examinemos ahora la segunda de las igualdades (2). Su primer miembro, y también el primer término del segundo miembro, son divisibles por p, por lo cual, el producto $b_{k-1}c_l$ también es divisible por p; pero como c_l no es divisible por p, tiene que ser divisible por p el número b_{k-1}. De un modo semejante, de la tercera de las igualdades (2), resulta que b_{k-2} es divisible por p, etc. Por fin, de la $(k+1)$-ésima igualdad resultará que b_0 es divisible por p; pero entonces, de la última de las igualdades (2) se deduce que a_0 es divisible por p, lo cual contradice a la hipótesis.

Para cualquier n es muy fácil escribir polinomios de coeficientes enteros de n-ésimo grado que satisfagan a las condiciones del criterio de Eisenstein y, por lo tanto, que sean irreducibles sobre el campo de los números racionales. Tal es, por ejemplo, el polinomio $x^n - 2$; a éste es aplicable el criterio de Eisenstein para $p = 2$.

El criterio de Eisenstein es solamente una condición suficiente de irreducibilidad sobre el campo R, pero no es una condición necesaria: puede ocurrir que, para un polinomio dado $f(x)$, no se pueda elegir un número primo p, de modo que se cumplan las condiciones del criterio de Eisenstein, siendo el polinomio reducible como, por ejemplo, $x^2 - 5x + 6$, o irreducible, como $x^2 + 1$. Además del criterio de Eisenstein existen muchos más criterios suficientes distintos de irreducibilidad de los polinomios sobre el campo R que, por cierto, son menos importantes. Existe también un método que pertenece a Kronecker, que permite responder para cualquier polinomio de coeficientes enteros si éste es reducible o no lo es sobre el campo R. Mas, este método es muy complicado y casi no tiene aplicación práctica.

Ejemplo. Examinemos el polinomio

$$f_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

donde p es un número primo. Son raíces de este polinomio las raíces p-ésimas de la unidad, distintas de la unidad misma; como estas raíces, junto con la unidad, dividen al círculo unidad del campo complejo en p partes iguales, el polinomio $f_p(x)$ se llama *polinomio de división del círculo*.

A este polinomio no se le puede aplicar directamente el criterio de Eisenstein. Mas, hagamos una sustitución de la indeterminada, poniendo $x = y + 1$. Resulta:

$$g(y) = f_p(y+1) = \frac{(y+1)^p - 1}{(y+1) - 1} =$$

$$= \frac{1}{y}\left[y^p + py^{p-1} + \frac{p(p-1)}{2!}y^{p-2} + \ldots + py\right] =$$

$$= y^{p-1} + py^{p-2} + \frac{p(p-1)}{2!}y^{p-3} + \ldots + p.$$

Los coeficientes de polinomio $g(y)$ son los números binomiales y, por esto, todos, menos el superior, son divisibles por p; el término independiente no es divisible

por p^2. Por lo tanto, según el criterio de Eisenstein el polinomio $g(y)$ es irreducible sobre el campo R. De aquí se deduce la *irreducibilidad sobre el campo R del polinomio de división del círculo* $f_p(x)$. En efecto, si

$$f_p(x) = \varphi(x)\,\psi(x),$$

entonces

$$g(y) = \varphi(y+1)\,\psi(y+1).$$

§ 57. Raíces racionales de los polinomios de coeficientes enteros

Más arriba se señaló, que el problema de la descomposición de un polinomio dado en factores irreducibles sobre el campo de los números racionales no tiene prácticamente una solución más o menos satisfactoria. Pero un caso particular de este problema, referente a la separación de los factores lineales de un polinomio de coeficientes racionales, o sea, a la averiguación de sus raíces racionales, es muy elemental y se resuelve sin recurrir a cálculos complicados. Es comprensible que, con el problema de la averiguación de las raíces racionales de los polinomios de coeficientes racionales no se agota de ningún modo el problema general de las raíces reales de estos polinomios, es decir, que los métodos y resultados expuestos en el capítulo noveno conservan también enteramente su valor para los polinomios de coeficientes racionales.

Empezando a resolver el problema de la averiguación de las raíces racionales de los polinomios de coeficientes racionales, señalemos que, como se había indicado en el párrafo anterior, podemos limitarnos a estudiar solamente los polinomios de coeficientes enteros; además, se van a examinar por separado los casos de raíces enteras y de raíces fraccionarias.

Si el número entero α *es raíz del polinomio* $f(x)$ *de coeficientes enteros,* α *es divisor del término independiente de este polinomio.*

En efecto, sea

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n.$$

Dividamos $f(x)$ por $x-\alpha$:

$$f(x) = (x-\alpha)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}).$$

Efectuando la división por el método de Horner, expuesto en el § 22, obtenemos que *todos los coeficientes del cociente, incluyendo también* b_{n-1}, *son números enteros*, y como

$$a_n = -\alpha b_{n-1} = \alpha(-b_{n-1}),$$

nuestra proposición queda demostrada *.

* Sería erróneo demostrar este teorema alegando al hecho de que el término independiente a_n es el producto (salvo el signo) de todas las raíces del polinomio $f(x)$, pues, entre éstas puede haber también fraccionarias, irracionales y complejas, debido a lo cual, no se puede afirmar por anticipado que el producto de todas estas raíces, a excepción de α, es un número entero.

Por lo tanto, si un polinomio $f(x)$ de coeficientes enteros tiene raíces enteras, éstas se hallan entre los divisores del término independiente. Por consiguiente, se deben ensayar todos los divisores posibles del término independiente, tanto los positivos como los negativos; si ninguno de éstos es raíz del polinomio, este último carece en general de raíces.

Puede ocurrir que el ensayo de todos los divisores del término independiente sea muy engorroso, incluso cuando los valores del polinomio se calculen por el método de Horner en vez de sustituir directamente cada uno de los divisores en lugar de la indeterminada. Las observaciones que se hacen a continuación permiten simplificar un poco estos cálculos. Como 1 y -1 siempre son divisores del término independiente, se calculan en primer lugar $f(1)$ y $f(-1)$, lo cual no ofrece dificultad alguna. Si, luego, el número entero α es raíz de $f(x)$:

$$f(x) = (x-\alpha)\,q(x),$$

como se indicó más arriba, todos los coeficientes del cociente $q(x)$ son números enteros y, por esto, los cocientes

$$\frac{f(1)}{\alpha-1} = -q(1), \quad \frac{f(-1)}{\alpha+1} = -q(-1)$$

tienen que ser números enteros. Por lo tanto, *solamente tienen que ensayarse los divisores α del término independiente (distintos de 1 y -1) para los cuales cada uno de los cocientes $\frac{f(1)}{\alpha-1}$, $\frac{f(-1)}{\alpha+1}$ es un número entero.*

Ejmplos. 1. Hallar las raíces enteras del polinomio

$$f(x) = x^3 - 2x^2 - x - 6.$$

Los divisores del término independiente son: ± 1, ± 2, ± 3, ± 6. Como $f(1) = -8$, $f(-1) = -8$, los números 1 y -1 no son raíces. Por otra parte, los números

$$\frac{-8}{2+1}, \quad \frac{-8}{-2-1}, \quad \frac{-8}{6-1}, \quad \frac{-8}{-6-1}$$

son fraccionarios, por lo cual, los divisores 2, -2, 6, -6 tienen que ser desechados, mientras que los números

$$\frac{-8}{3-1}, \quad \frac{-8}{3+1}, \quad \frac{-8}{-3-1}, \quad \frac{-8}{-3+1}$$

son enteros, y por esto, los divisores 3 y -3 tienen que ser ensayados. Apliquemos el método de Horner:

$$\begin{array}{r|rrrr} -3 & 1 & -2 & -1 & -6 \\ \hline & 1 & -5 & 14 & -48 \end{array},$$

o sea, $f(-3) = -48$ y, por esto, -3 no es raíz de $f(x)$. Finalmente,

$$\begin{array}{r|rrrr} 3 & 1 & -2 & -1 & -6 \\ \hline & 1 & 1 & 2 & 0 \end{array},$$

o sea, $f(3)=0$: el número 3 es raíz de $f(x)$. A la vez, hemos hallado los coeficientes del cociente de la división de $f(x)$ por $x-3$;

$$f(x)=(x-3)(x^2+x+2).$$

Fácilmente se observa que el número 3 no es raíz del cociente x^2+x+2, o sea, este número no es raíz múltiple de $f(x)$.

2. Hallar las raíces enteras del polinomio

$$f(x)=3x^4+x^3-5x^2-2x+2.$$

Aquí, los divisores del término independiente son: ± 1 y ± 2. Por otra parte, $f(1)=-1$, $f(-1)=1$, o sea, 1 y -1 no son raíces. Finalmente, como los números

$$\frac{1}{2+1} \quad \text{y} \quad \frac{-1}{-2-1}$$

son fraccionarios, los números 2 y -2 tampoco serán raíces, por lo cual, el polinomio $f(x)$ carece de raíces enteras.

Examinemos el problema de las raíces fraccionarias.

Si un polinomio de coeficientes enteros, cuyo coeficiente superior es igual a la unidad, tiene una raíz racional, ésta es un número entero.

En efecto, supongamos que la fracción irreducible $\frac{b}{c}$ es raíz del polinomio

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n$$

de coeficientes enteros, o sea, que

$$\frac{b^n}{c^n}+a_1\frac{b^{n-1}}{c^{n-1}}+a_2\frac{b^{n-2}}{c^{n-2}}+\ldots+a_n=0.$$

De aquí, resulta la igualdad

$$\frac{b^n}{c}=-a_1b^{n-1}-a_0b^{n-2}c-\ldots-a_nc^{n-1},$$

es decir, que una fracción irreducible es igual a un número entero, lo cual es imposible.

Para obtener todas las raíces racionales (enteras o fraccionarias) de un polinomio de coeficientes enteros

$$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n$$

hay que hallar todas las raíces enteras del polinomio

$$\varphi(y)=y^n+a_1y^{n-1}+a_0a_2y^{n-2}+\ldots+a_0^{n-2}a_{n-1}y+a_0^{n-1}a_n$$

y dividirlas por a_0.

En efecto, multipliquemos $f(x)$ por a_0^{n-1}, y hagamos después la sustitución de la indeterminada poniendo $y=a_0x$. Evidentemente,

$$\varphi(y)=\varphi(a_0x)=a_0^{n-1}f(x).$$

De aquí se deduce, que las raíces del polinomio $f(x)$ son iguales a las raíces del polinomio $\varphi(y)$, divididas por a_0. En particular,

a las raíces racionales de $f(x)$ corresponderán raíces racionales de $\varphi(y)$; pero, como el coeficiente superior de $\varphi(y)$ es igual a la unidad, estas raíces sólo pueden ser enteras, y ya tenemos un método para buscarlas.

Ejemplo. Hallar las raíses racionales del polinomio

$$f(x) = 3x^4 + 5x^3 + x^2 + 5x - 2.$$

Multiplicando $f(x)$ por 3^3 y poniendo $y = 3x$, obtenemos:

$$\varphi(y) = y^4 + 5y^3 + 3y^2 + 45y - 54.$$

Buscamos las raíces enteras del polinomio $\varphi(y)$.

Por el método de Horner, hallamos $\varphi(1)$:

$$1 \left| \begin{array}{cccc} 1 & 5 & 3 & 45 & -54 \\ \hline 1 & 6 & 9 & 54 & 0 \end{array} \right. .$$

Por lo tanto, $\varphi(1) = 0$, o sea, 1 es una raíz de $\varphi(y)$, siendo

$$\varphi(y) = (y-1)\, q(y),$$

donde

$$q(y) = y^3 + 6y^2 + 9y + 54.$$

Hallemos las raíces enteras del polinomio $q(y)$. Los divisores del término independiente son: ± 1, ± 2, ± 3, ± 6, ± 9, ± 18, ± 27, ± 54. Aquí

$$q(1) = 70, \quad q(-1) = 50.$$

Calculando $\dfrac{q(1)}{\alpha - 1}$ y $\dfrac{q(-1)}{\alpha + 1}$ para cada divisor de α, se observa, que se tienen que desechar todos los divisores menos $\alpha = -6$. Ensayamos este divisor:

$$-6 \left| \begin{array}{cccc} 1 & 6 & 9 & 54 \\ \hline 1 & 0 & 9 & 0 \end{array} \right. .$$

Por lo tanto, $q(-6) = 0$, o sea, -6 es raíz de $q(y)$ y, por esto, de $\varphi(y)$.

Por consiguiente, el polinomio $\varphi(y)$ tiene las raíces enteras 1 y -6. Así, las raíces racionales del polinomio $f(x)$ son los números $\dfrac{1}{3}$ y -2, y sólo éstos.

Es menester subrayar una vez más, que los métodos expuestos anteriormente **solamente** se pueden aplicar a los polinomios de coeficientes enteros y **sólo** para hallar sus raíces racionales.

§ 58. Los números algebraicos

Todo polinomio de grado n de coeficientes racionales tiene n raíces en el campo de los números complejos, algunas de las cuales (e incluso todas) pueden estar fuera del campo de los números racionales. Mas, no cualquier número real o complejo es raíz de algún polinomio de coeficientes racionales. Los números complejos (y, en particular, los números reales) que son raíces de tales polinomios, se llaman números *algebraicos*, en contraposición a los números *trascendentes*. Entre los números algebraicos figuran los números

racionales, como raíces de los polinomios de primer grado de coeficientes racionales, y también cualquier radical de la forma $\sqrt[n]{a}$, siendo el subradical a un número racional, pues es raíz del binomio $x^n - a$. Por otra parte, en los cursos completos de análisis matemático se demuestra que es trascendente el número e, base del sistema de los logaritmos naturales, y también el número π, bien conocido en la geometría elemental.

Si el número α es algebraico, éste será incluso raíz de un polinomio de coeficientes enteros y, por esto, será raíz de uno de los divisores irreducibles de este polinomio, que también es de coeficientes enteros. *El polinomio irreducible de coeficientes enteros que tiene por raíz al número α se determina unívocamente, salvo un factor constante, o sea, de un modo único en absoluto, si se exige que los coeficientes de este polinomio sean primos entre sí* (es decir, que el polinomio sea primitivo). En efecto, si α es una raíz de dos polinomios irreducibles $f(x)$ y $g(x)$, el máximo común divisor de éstos tiene que ser distinto de la unidad, por lo cual, en virtud de su irreducibilidad, estos polinomios pueden diferenciarse entre sí solamente en un factor de grado cero.

Los números algebraicos que son raíces de un mismo polinomio irreducible (sobre el campo R), se llaman *conjugados entre sí**. Por consiguiente, todo el conjunto de números algebraicos se descompone en clases finitas disjuntas de números conjugados entre sí. Todo número racional, como raíz de un polinomio de primer grado, no tiene números conjugados distintos de sí mismo, siendo ésta una característica de los números racionales. En efecto, todo número algebraico que no sea racional será raíz de un polinomio irreducible de grado mayor que la unidad, por lo cual, tendrá algún conjugado distinto de sí mismo.

El conjunto de todos los números algebraicos es un subcampo del campo de los números complejos. En otras palabras, la suma, diferencia, producto y cociente de números algebraicos son también números algebraicos.

En efecto, supongamos que se han dado los números algebraicos α y β. Designemos mediante $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, todos los números conjugados con α; mediante $\beta_1 = \beta, \beta_2, \ldots, \beta_s$, todos los números conjugados con β; mediante $f(x)$ y $g(x)$, los polinomios irreducibles de coeficientes racionales que tienen por raíces los números α y β, respectivamente. Escribamos un polinomio cuyas raíces sean todas las sumas posibles $\alpha_i + \beta_j$; éste es

$$\varphi(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} [x - (\alpha_i + \beta_j)].$$

* No se debe confundir este concepto con el de números complejos conjugados.

Evidentemente, los coeficientes de este polinomio no varían al permutar entre sí todas las α_i, y también al permutar entre sí todas las β_j. Por consiguiente, según el teorema de los polinomios que son simétricos con respecto a dos sistemas de indeterminadas (véase el final del § 53), estos coeficientes son polinomios en los coeficientes de los polinomios $f(x)$ y $g(x)$. En otras palabras, resulta que los coeficientes del polinomio $\varphi(x)$ son números racionales, por lo cual, el número $\alpha + \beta = \alpha_1 + \beta_1$, al ser una de sus raíces, es un número algebraico.

Del mismo modo, mediante los polinomios

$$\psi(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} [x - (\alpha_i - \beta_j)]$$

y

$$\chi(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} (x - \alpha_i \beta_j)$$

se demuestra que los números $\alpha - \beta$ y $\alpha\beta$ son algebraicos.

Para demostrar que el cociente de dos números algebraicos es un número algebraico, es suficiente demostrar que, si el número α es algebraico y distinto de cero, entonces, el número α^{-1} también lo es. Sea α raíz del polinomio

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

de coeficientes racionales. Entonces, evidentemente, el polinomio

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

que también es de coeficientes racionales, tiene la raíz α^{-1}, como se quería demostrar.

Del teorema que acabamos de demostrar se deduce, que cualquier suma de un número racional y un radical, por ejemplo, $1 + \sqrt[3]{2}$, y también cualquier suma de radicales, por ejemplo, $\sqrt{3} + \sqrt[3]{5}$, son números algebraicos. Mas, por ahora, no podemos afirmar que son algebraicos los números que se escriben en forma de radicales «de dos pisos», por ejemplo, $\sqrt{1 + \sqrt{2}}$. Esto se va a deducir solamente del siguiente **teorema**:

Si el número ω *es raíz del polinomio*

$$\varphi(x) = x^n + \alpha x^{n-1} + \beta x^{n-2} + \ldots + \lambda x + \mu,$$

cuyos coeficientes son números algebraicos, entonces, ω *es también un número algebraico.*

Supongamos que α_i, β_j, ..., λ_s, μ_t toman todos los valores conjugados con los números α, β, ..., λ, μ, siendo $\alpha_1 = \alpha$, $\beta_1 = \beta$, ..., $\lambda_1 = \lambda$, $\mu_1 = \mu$. Consideremos todos los polinomios posibles

de la forma:

$$\varphi_{i,j,\ldots,s,t}(x) = x^n + \alpha_i x^{n-1} + \beta_j x^{n-2} + \ldots + \lambda_s x + \mu_t,$$

de modo que $\varphi_{1,1,\ldots,1,1}(x) = \varphi(x)$, y tomemos el producto de todos estos polinomios:

$$F(x) = \prod_{i,j,\ldots,s,t} \varphi_{i,j,\ldots,s,t}(x).$$

Evidentemente, los coeficientes del polinomio $F(x)$ son simétricos con respecto a cada uno de los sistemas α_i, β_j, . . ., λ_s, μ_t, por lo cual, (de nuevo en virtud del teorema del § 53), éstos son polinomios en los coeficientes de aquellos polinomios irreducibles (de *coeficientes racionales*) *cuyas raíces son* α, β, . . ., λ, μ, *respectivamente*, o sea, ellos mismos son números racionales. Por consiguiente, el número ω, siendo raíz de $\varphi(x)$, es también raíz del polinomio $F(x)$ de coeficientes racionales, es decir, es un número algebraico.

Apliquemos este teorema al número $\omega = \sqrt{1+\sqrt{2}}$. En virtud del teorema anterior, el número $\alpha = 1 + \sqrt{2}$ es algebraico y, por esto, el número ω es raíz del polinomio $x^2 - \alpha$, de coeficientes algebraicos, o sea, el mismo es algebraico. En general, reiterando los dos teoremas que acabamos de demostrar, el lector obtendrá sin dificultad alguna el siguiente resultado:

Todo número que se expresa por radicales sobre el campo de números racionales (*es decir, que se expresa por una combinación de radicales, lo más complicada que sea, y en el caso general, por radicales «de muchos pisos»*), *es un número algebraico.*

Evidentemente, los números algebraicos que se expresan por radicales forman un campo. Pero hay que tener presente que, como *esto se deduce de la observación que se hizo (sin demostración)* al final del § 38, éste es solamente una parte del campo de todos los números algebraicos.

Antes ya se había señalado que los números e y π son trascendentes. Pero, en la realidad, hay una infinidad de números trascendentes. Además, aplicando los conceptos y métodos de la teoría de los conjuntos, demostraremos que, en cierto sentido, hay más números trascendentes que algebraicos; el significado exacto de esta expresión quedará claro a continuación.

Un conjunto infinito M se llama *numerable*, si éste puede ponerse en correspondencia biunívoca con el conjunto de los números naturales, o sea, si sus elementos se pueden numerar mediante los números naturales, y *no numerable*, en caso contrario.

Lema 1. *Todo conjunto infinito M contiene un subconjunto numerable.*

En efecto, tomemos en M un elemento arbitrario a_1. Elijamos después un elemento a_2, distinto de a_1. En general, supongamos que ya se han elegido n elementos distintos en M: $a_1, a_2, \ldots a_n$. Como el conjunto M es infinito, éste no puede agotarse con los elementos elegidos, por lo cual, se puede indicar otro elemento a_{n+1}, distinto de éstos. Continuando este proceso, hallaremos en M un

subconjunto infinito formado por los elementos

$$a_1, a_2, \ldots, a_n, \ldots;$$

es evidente que este subconjunto es numerable.

Lema 2. *Todo subconjunto infinito B de un conjunto numerable A, es numerable.*

Como el conjunto A es numerable, éste se puede escribir en la forma:

$$a_1, a_2, \ldots, a_n, \ldots \tag{1}$$

Sea a_{k_1} el primer elemento de la sucesión (1) perteneciente a B; sea a_{k_2} el segundo elemento que tiene la misma propiedad, etc. Poniendo $a_{k_n} = b_n$, $n = 1, 2, \ldots$, obtenemos que los elementos del subconjunto B forman una sucesión,

$$b_1, b_2, \ldots, b_n, \ldots,$$

o sea, este subconjunto es numerable.

Lema 3. *La unión de un conjunto numerable de conjuntos finitos que no tienen elementos comunes, es un conjunto numerable.*

En efecto, sean dados los conjuntos finitos

$$A_1, A_2, \ldots, A_n, \ldots$$

y sea B la unión de ellos. Está claro que quedan numerados todos los elementos del conjunto B, si de un modo arbitrario se numeran los elementos del conjunto finito A_1, y después se continúa esta numeración pasando a considerar los elementos del conjunto A_2, etc.

Lema 4. *La unión de dos conjuntos numerables que no tienen elementos comunes, es un conjunto numerable.*

Sean dados los conjuntos numerables A con los elementos

$$a_1, a_2, \ldots, a_n, \ldots$$

y B con los elementos

$$b_1, b_2, \ldots, b_n, \ldots$$

y sea C la unión de estos conjuntos. Si se pone

$$a_n = c_{2n-1}, \quad b_n = c_{2n}, \qquad n = 1, 2, \ldots,$$

todos los elementos del conjunto C quedarán representados en forma de la sucesión

$$c_1, c_2, \ldots, c_{2n-1}, c_{2n}, \ldots,$$

lo que demuestra que este conjunto es numerable.

Demostremos ahora el siguiente **teorema:**

El conjunto de todos los números algebraicos es numerable.

Demostremos previamente que *es numerable el conjunto de todos los polinomios en una indeterminada de coeficientes enteros.* Si

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

es un polinomio de éstos, distinto de cero, llamaremos *altura* del polinomio al número natural

$$h_f = n + |a_0| + |a_1| + \ldots + |a_{n-1}| + |a_n|.$$

Es evidente, que existe solamente un número finito de polinomios de coeficientes enteros de una altura dada h; designemos este conjunto mediante M_h. Designemos también con M_0 el conjunto formado por el cero solamente. El conjunto de todos los polinomios de coeficientes enteros es la unión del conjunto numerable de los conjuntos finitos $M_0, M_1, M_2, \ldots, M_h, \ldots$, o sea, en virtud del lema 3, es numerable.

De aquí, por el lema 2, se deduce que *el conjunto de todos los polinomios primitivos irreducibles de coeficientes enteros también es numerable.* Por otra parte, ya sabemos que todo número algebraico es raíz de un polinomio primitivo irreducible de coeficientes enteros y solamente de uno. Por consiguiente, reuniendo las raíces de todos los polinomios de este tipo, o sea, tomando la unión de un conjunto numerable de conjuntos finitos, obtenemos el conjunto de todos los números algebraicos; por lo tanto, en virtud del lema 3, este conjunto es numerable.

Finalmente, demostremos el **teorema**:

El conjunto de todos los números trascendentes no es numerable.

Examinemos primero el conjunto F de todos los números reales x, situados entre el cero y la unidad, $0 < x < 1$, y demostremos que *este conjunto no es numerable. Es sabido, que cada uno de los números indicados x se puede expresar* en forma de una fracción decimal propia infinita

$$x = 0,\ \alpha_1\alpha_2 \ldots \alpha_n \ldots$$

y que esta expresión es única, si no se permiten fracciones en las que, para todos los n, empezando desde cierto $n = N$, todos los $\alpha_n = 9$; recíprocamente, cualquier fracción de la forma indicada es igual a cierto número x de este conjunto F. Supongamos ahora que el conjunto F es numerable, o sea, que **todos** los números x se pueden escribir en forma de una sucesión

$$x_1,\ x_2,\ \ldots,\ x_k,\ \ldots \tag{2}$$

Sea

$$x_k = 0,\ \alpha_{k_1}\alpha_{k_2} \ldots \alpha_{k_n} \ldots$$

la expresión del número x_k en forma de fracción decimal infinita. Escribamos ahora una fracción decimal infinita

$$0,\ \beta_1\beta_2 \ldots \beta_n \ldots, \tag{3}$$

de modo que la cifra β_1 sea distinta de la primera cifra decimal de la fracción x_1, o sea, $\beta_1 \neq \alpha_{11}$, que la cifra β_2 sea distinta de la segunda cifra decimal de la fracción x_2, o sea, $\beta_2 \neq \alpha_{22}$, y, en general, que $\beta_n \neq \alpha_{nn}$. Supongamos además que entre las cifras β_n hay una infinidad de ellas, distintas de la cifra 9. Está claro que existe una fracción (3) que satisface a todas estas condiciones. Por consiguiente, ésta es un número del conjunto F y, por la construcción misma, es distinta de todos los números de la sucesión (2). Esta contradicción muestra que el conjunto F no es numerable.

De aquí se deduce, que *el conjunto de todos los números complejos no es numerable*, pues, en caso contrario, en virtud del lema 2, éste no podría contener el subconjunto no numerable F. En virtud del lema 4, es evidente ahora que no es numerable el conjunto de todos los números trascendentes, pues, la unión de este conjunto con el conjunto numerable de todos los números algebraicos es el conjunto de todos los números complejos, o sea, no es numerable.

En virtud del lema 1, los dos teoremas que hemos demostrado muestran que, en la realidad, el conjunto de los números trascendentes es más rico en elementos, o sea, es más «potente» que el conjunto de los números algebraicos.

CAPITULO XIII

FORMA NORMAL DE UNA MATRIZ

§ 59. Equivalencia de las λ-matrices

Aquí volvemos a examinar otra vez algunas cuestiones relacionadas con el álgebra lineal. Al estudiar el capítulo 7, el lector ya se *habrá convencido del papel importante que desempeña el concepto* de semejanza de las matrices. Precisando, dos matrices cuadradas de orden n son semejantes cuando, y sólo cuando, determinan (en bases diversas) una misma transformación lineal del espacio lineal de n dimensiones. Sin embargo, por ahora, no sabemos contestar a la pregunta, si son semejantes o no dos matrices determinadas. Por otra parte, no sabemos hallar, por ahora, entre todas las matrices semejantes a la matriz dada A, la que, en tal o cual sentido, tiene la forma más simple; incluso la cuestión sobre las condiciones para que una matriz A sea semejante a una matriz diagonal, fue estudiada en el § 33 solamente para un caso particular. Precisamente estas cuestiones se van a estudiar en el presente capítulo, y además, para el caso de un campo fundamental P arbitrario.

Ocupémonos primero del estudio de las matrices cuadradas de orden n, cuyos elementos son polinomios de grados arbitrarios en una indeterminada λ con coeficientes del campo P. Tales matrices se llaman *matrices polinomiales* o, abreviadamente, *λ-matrices*. Es un ejemplo de λ-matriz la matriz característica $A - \lambda E$ de una matriz cuadrada arbitraria A con elementos del campo P; en la diagonal principal de esta matriz figuran polinomios de primer grado; fuera de la diagonal principal, polinomios de grado cero o ceros. Cualquier matriz con elementos del campo P (para abreviar, a tales *matrices* las llamaremos *numéricas*) también será un caso particular de las λ-matrices: sus elementos son polinomios de grado cero, o son iguales a cero.

Sea dada una λ-matriz

$$A(\lambda) = \begin{pmatrix} a_{11}(\lambda) & \dots & a_{1n}(\lambda) \\ \dots & \dots & \dots \\ a_{n1}(\lambda) & \dots & a_{nn}(\lambda) \end{pmatrix}.$$

Llamemos *transformaciones elementales* de esta matriz a las transformaciones de los cuatro tipos siguientes:

1) multiplicación de cualquier fila de la matriz $A(\lambda)$ por cualquier número α del campo P, distinto de cero;

2) *multiplicación de cualquier columna* de la matriz $A(\lambda)$ por cualquier número α del campo P, distinto de cero;

3) agregación a cualquier i-ésima fila de la matriz $A(\lambda)$ una j-ésima fila cualquiera, $j \neq i$, y además, multiplicada por cualquier polinomio $\varphi(\lambda)$ del anillo $P[\lambda]$;

4) agregación a cualquier i-ésima columna de la matriz $A(\lambda)$ una j-ésima columna cualquiera, $j \neq i$, y además, multiplicada por cualquier polinomio $\varphi(\lambda)$ del anillo $P[\lambda]$.

Fácilmente se observa que, *para cada una de las transformaciones elementales de una λ-matriz, existe la transformación inversa, que también es elemental.* Así, pues, para la transformación 1), la inversa es la transformación elemental que consiste en multiplicar la misma fila por el número α^{-1}, que existe en virtud de la condición $\alpha \neq 0$; para la transformación 3), la inversa es la transformación que consiste en agregar a la i-ésima fila la j-ésima fila, multiplicada por $-\varphi(\lambda)$.

Efectuando unas cuantas transformaciones elementales en una matriz $A(\lambda)$, se pueden permutar dos filas o dos columnas cualesquiera.

Supongamos, por ejemplo, que se necesita permutar la i-ésima y la j-ésima filas de la matriz $A(\lambda)$. Como muestra el esquema que sigue, esto se realiza efectuando cuatro transformaciones elementales:

$$\begin{pmatrix} i \\ j \end{pmatrix} \to \begin{pmatrix} i+j \\ j \end{pmatrix} \to \begin{pmatrix} i+j \\ -i \end{pmatrix} \to \begin{pmatrix} j \\ -i \end{pmatrix} \to \begin{pmatrix} j \\ i \end{pmatrix}.$$

Aquí se ejecutaron las siguientes transformaciones: a) a la i-ésima fila se le agregó la j-ésima; b) de la j-ésima fila se restó la nueva i-ésima; c) a la nueva i-ésima fila se le agregó la nueva j-ésima; d) la nueva j-ésima fila se multiplicó por -1.

Diremos que las λ-matrices $A(\lambda)$ y $B(\lambda)$ son equivalentes, lo cual escribiremos con la notación $A(\lambda) \sim B(\lambda)$, si se puede pasar de la matriz $A(\lambda)$ a la matriz $B(\lambda)$ efectuando un número finito de transformaciones elementales. Es evidente que esta relación de equivalencia es reflexiva, transitiva y también simétrica, en virtud de la existencia de la transformación elemental inversa para cualquier transformación elemental. En otras palabras, *todas las λ-matrices cuadradas de orden n sobre el campo P se descomponen en clases disjuntas de matrices equivalentes.*

Nuestro objetivo próximo consiste en buscar, entre todas las λ-matrices equivalentes a una matriz dada $A(\lambda)$, una matriz que sea

lo más simple posible. Para esto, introduciremos el concepto siguiente. Se llama *λ-matriz canónica* a una λ-matriz que posea las tres propiedades siguientes:

a) esta matriz es diagonal, o sea, tiene la forma siguiente

$$\begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix} \tag{1}$$

b) cualquier polinomio $e_i(\lambda)$, $i = 2, 3, \ldots, n$, es divisible por el polinomio $e_{i-1}(\lambda)$;

c) el coeficiente superior de cada polinomio $e_i(\lambda)$, $i = 1, 2, \ldots, n$, es igual a la unidad, si el polinomio es distinto de cero.

Obsérvese que, si entre los polinomios $e_i(\lambda)$ que figuran en la diagonal principal de la λ-matriz canónica (1), hay algunos iguales a cero, entonces, en virtud de la propiedad b), éstos inevitablemente ocupan los últimos sitios en la diagonal principal. Por otra parte, si entre los polinomios $e_i(\lambda)$ hay algunos de grado cero, entonces, según la propiedad c), éstos son todos iguales a 1 y, en virtud de la propiedad b), ocupan los primeros sitios en la diagonal principal de la matriz (1).

En particular, algunas matrices numéricas, como la matriz unidad y la matriz cero, son también λ-matrices canónicas.

Toda λ-matriz es equivalente a una λ-matriz canónica, o sea, en otras palabras, mediante transformaciones elementales se reduce a la forma canónica.

Demostraremos este teorema por inducción sobre el orden n de las λ-matrices consideradas. En efecto, para $n = 1$, se tiene:

$$A(\lambda) = (a(\lambda)).$$

Si $a(\lambda) = 0$, nuestra matriz ya es canónica. Si $a(\lambda) \neq 0$, es suficiente dividir el polinomio $a(\lambda)$ por su coeficiente superior —esto es una transformación elemental de la matriz— y obtenemos una matriz canónica.

Supongamos que el teorema ya está demostrado para las λ-matrices de orden $n - 1$. Examinemos una λ-matriz arbitraria $A(\lambda)$ de orden n. Si ésta es igual a cero, entonces ya es canónica y no hay nada que demostrar. Por esto, supondremos que entre los elementos de la matriz $A(\lambda)$ hay algunos distintos de cero.

Cambiando las filas de la matriz $A(\lambda)$ por columnas, si esto fuese necesario, se puede trasladar al ángulo superior de la izquierda uno de sus elementos distinto de cero. Por lo tanto, entre las λ-matri-

ces que son equivalentes a la matriz $A(\lambda)$, hay algunas en cuyos ángulos superiores de la izquierda figuran polinomios distintos de cero. Consideremos todas estas matrices. Los polinomios que figuran en el ángulo superior de la izquierda de estas matrices pueden tener grado distinto. Pero el grado de un polinomio es un número natural, y en cualquier conjunto de números naturales, no vacío, existe el número menor. Por consiguiente, entre todas las λ-matrices que son equivalentes a la matriz $A(\lambda)$ y que tienen en el ángulo superior de la izquierda un elemento distinto de cero, se puede hallar una tal, que el polinomio que figure en dicho ángulo tenga el menor grado posible. Finalmente, dividiendo la primera fila de esta matriz por el coeficiente superior del polinomio indicado, obtenemos una λ-matriz equivalente a la matriz $A(\lambda)$,

$$A(\lambda) \sim \begin{pmatrix} e_1(\lambda) & b_{12}(\lambda) & \dots & b_{1n}(\lambda) \\ b_{21}(\lambda) & b_{22}(\lambda) & \dots & b_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ b_{n1}(\lambda) & b_{n2}(\lambda) & \dots & b_{nn}(\lambda) \end{pmatrix},$$

en la que $e_1(\lambda) \neq 0$, el coeficiente superior de este polinomio es igual a 1 y **con ninguna combinación de transformaciones elementales se puede pasar de la matriz obtenida a una matriz en cuyo ángulo superior de la izquierda figure un polinomio de grado menor, distinto de cero.**

Demostremos que *todos los elementos de la primera fila y de la primera columna de la matriz obtenida son divisibles por* $e_1(\lambda)$. Supongamos, por ejemplo, que, para $2 \leqslant j \leqslant n$,

$$b_{1j}(\lambda) = e_1(\lambda)\, q(\lambda) + r(\lambda),$$

donde el grado de $r(\lambda)$ es menor que el grado de $e_1(\lambda)$, si $r(\lambda)$ es diferente de cero. Entonces, restando de la j-ésima columna de nuestra matriz su primera columna, multiplicada por $q(\lambda)$, y permutando después la primera y j-ésima columnas, llegaremos a obtener una matriz equivalente a la matriz $A(\lambda)$, en cuyo ángulo superior de la izquierda figurará el polinomio $r(\lambda)$, o sea, un polinomio de grado menor que $e_1(\lambda)$, lo cual contradice a la elección de este polinomio. De aquí se deduce que $r(\lambda) = 0$, como se quería demostrar.

Restando ahora de la j-ésima columna de nuestra matriz su primera columna multiplicada por $q(\lambda)$, se sustituye el elemento $b_{1j}(\lambda)$ por cero. Realizando tales transformaciones para $j = 2, 3, \dots, n$, se sustituyen por ceros todos los elementos $b_{1j}(\lambda)$. De un modo análogo, se sustituyen también por ceros todos los elementos $b_{i1}(\lambda)$, $i = 2, 3, \dots, n$. *Por consiguiente, obtendremos una matriz equivalente* $A(\lambda)$ *en cuyo ángulo superior de la izquierda figurará*

el polinomio $e_1(\lambda)$ *y en la que todos los demás elementos de la primera fila y de la primera columna serán iguales a cero*:

$$A(\lambda) \sim \begin{pmatrix} e_1(\lambda) & 0 & \dots & 0 \\ 0 & c_{22}(\lambda) & \dots & c_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ 0 & c_{n2}(\lambda) & \dots & c_{nn}(\lambda) \end{pmatrix}. \tag{2}$$

Por la hipótesis de inducción, la matriz de $(n-1)$-ésimo orden que figura en el ángulo inferior de la derecha de la matriz obtenida (2), mediante transformaciones elementales se reduce a la forma canónica:

$$\begin{pmatrix} c_{22}(\lambda) & \dots & c_{2n}(\lambda) \\ \dots & \dots & \dots \\ c_{n2}(\lambda) & \dots & c_{nn}(\lambda) \end{pmatrix} \sim \begin{pmatrix} e_2(\lambda) & & 0 \\ & \ddots & \\ 0 & & e_n(\lambda) \end{pmatrix}.$$

Efectuando las mismas transformaciones con las filas y columnas correspondientes de la matriz (2) —evidentemente, en este caso la primera fila y la primera columna de esta matriz se quedan invariables —, obtenemos que

$$A(\lambda) \sim \begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix}. \tag{3}$$

Para demostrar que la matriz (3) es canónica no queda más que demostrar que $e_2(\lambda)$ es divisible por $e_1(\lambda)$. Supongamos que

$$e_2(\lambda) = e_1(\lambda)\, q(\lambda) + r(\lambda),$$

donde $r(\lambda) \neq 0$ *y el grado de* $r(\lambda)$ *es menor que el de* $e_1(\lambda)$. Pero, agregando a la segunda columna de la matriz (3) su primera columna multiplicada por $q(\lambda)$ y restando después de la segunda fila la primera, *se sustituye el elemento* $e_2(\lambda)$ *por el elemento* $r(\lambda)$. Permutando luego las primeras dos filas y las primeras dos columnas, conseguiremos trasladar el polinomio $r(\lambda)$ al ángulo superior de la izquierda de la matriz, lo cual, sin embargo, contradice a la elección del polinomio $e_1(\lambda)$.

El teorema de la reducción de una λ-matriz a la forma canónica queda demostrado. Este teorema se puede completar con el siguiente **teorema de unicidad:**

Toda λ-matriz es equivalente solamente a una matriz canónica. En efecto, sea dada una λ-matriz arbitraria $A(\lambda)$ de orden n. Fijemos algún número natural k, $1 \leqslant k \leqslant n$, y consideremos todos los menores de k-ésimo orden de la matriz $A(\lambda)$. Calculando estos menores obtenemos un sistema finito de polinomios en λ; designemos con $d_k(\lambda)$ el máximo común divisor de este sistema de polinomios, tomado con el coeficiente superior 1.

Por consiguiente, tenemos los polinomios

$$d_1(\lambda),\ d_2(\lambda),\ \ldots,\ d_n(\lambda), \tag{4}$$

determinados unívocamente por la misma matriz $A(\lambda)$. Aquí, $d_1(\lambda)$ es el máximo común divisor de todos los elementos de la matriz $A(\lambda)$, tomado con el coeficiente superior 1, y $d_n(\lambda)$ es igual al determinante de la matriz $A(\lambda)$, dividido por su coeficiente superior. Obsérvese también, que si la matriz $A(\lambda)$ tiene rango r, entonces

$$d_{r+1}(\lambda) = \ldots = d_n(\lambda) = 0,$$

mientras que todos los demás polinomios del sistema (4) son distintos de cero.

El máximo común divisor $d_k(\lambda)$ *de todos los menores de k-ésimo orden de una λ-matriz* $A(\lambda)$, $k = 1, 2, \ldots, n$, *no varía al realizar transformaciones elementales en la matriz* $A(\lambda)$.

Esta proposición es casi evidente, si se efectúan transformaciones elementales del tipo 1) y 2) en la matriz $A(\lambda)$. Así, por ejemplo, si la i-ésima fila de la matriz se multiplica por un número α del campo P, $\alpha \neq 0$, todos los menores de k-ésimo orden, por los que pasa la i-ésima fila, se multiplicarán por α, mientras que los demás menores de k-ésimo orden se quedarán invariables. Mas, al buscar el máximo común divisor de unos cuantos polinomios, cualesquiera de éstos se pueden multiplicar por números del campo P distintos de cero.

Examinemos ahora las transformaciones elementales del tipo 3) y 4). Supongamos, por ejemplo, que a la i-ésima fila de la matriz $A(\lambda)$ se le agrega su j-ésima fila, $j \neq i$, multiplicada por el polinomio $\varphi(\lambda)$; designemos con $\overline{A}(\lambda)$ la matriz que resulta después de esta transformación y con $\overline{d}_k(\lambda)$, el máximo común divisor de todos sus menores de k-ésimo orden, tomado con el coeficiente superior 1. Veamos lo que ocurre con los menores de k-ésimo orden de la matriz $A(\lambda)$ al hacer esta transformación.

Está claro que no varían los menores por los que no pasa la i-ésima fila. Tampoco varían los menores por los que pasan la i-ésima y la j-ésima filas, pues el determinante no varía al sumar a una de sus filas un múltiplo de otra fila. Por fin, tomemos cualquiera de los menores de k-ésimo orden por los que pasa la i-ésima

fila, pero no pasa la j-ésima; designémoslo mediante M. Evidentemente, el menor correspondiente de la matriz $\overline{A}(\lambda)$ se puede representar en forma de una suma del menor M y de un menor M', multiplicado por $\varphi(\lambda)$, donde este último es el menor de la matriz $A(\lambda)$ que se obtiene del menor M al sustituir los elementos de la i-ésima fila de la matriz $A(\lambda)$ por sus elementos correspondientes de la j-ésima fila. Como M y M' son divisibles por $d_k(\lambda)$, también será divisible por $d_k(\lambda)$ la suma $M + \varphi(\lambda) M'$.

De lo dicho se deduce, que todos los menores de k-ésimo orden de la matriz $\overline{A}(\lambda)$ son divisibles por $d_k(\lambda)$, por lo cual, $\overline{d}_k(\lambda)$ también es divisible por $d_k(\lambda)$. Pero, como para la transformación elemental considerada existe una transformación elemental inversa del mismo tipo, $d_k(\lambda)$ también es disvisible por $\overline{d}_k(\lambda)$. Si se tiene en cuenta que los coeficientes superiores de estos polinomios son iguales a 1, se tiene $\overline{d}_k(\lambda) = d_k(\lambda)$, como se quería demostrar.

Por lo tanto, *a todas las λ-matrices equivalentes a la matriz* $A(\lambda)$ *corresponde una misma colección de polinomios* (4). En particular, esto mismo se refiere a cualquier (si hay varias) matriz canónica equivalente a $A(\lambda)$. Supongamos que (3) es una de estas matrices.

Calculemos el polinomio $d_k(\lambda)$, $k = 1, 2, \ldots, n$, utilizando la matriz (3). Está claro, que el menor de k-ésimo orden que figura *en el ángulo superior de la izquierda de esta matriz, es igual al* producto

$$e_1(\lambda)\, e_2(\lambda) \ldots e_k(\lambda). \tag{5}$$

Si, luego, se toma en la matriz (3) el menor de k-ésimo orden que figura en las filas cuyos índices son $i_1, i_2, \ldots, i_k$, donde $i_1 < i_2 < \ldots < i_k$, y en las columnas *que tienen los mismos índices de ordenación*, resulta que este menor es igual al producto $e_{i_1}(\lambda)\, e_{i_2}(\lambda) \ldots e_{i_k}(\lambda)$, el cual es divisible por (5). En efecto, $1 \leqslant i_1$, y, por esto, $e_{i_1}(\lambda)$ es divisible por $e_1(\lambda)$; $2 \leqslant i_2$, y por esto, $e_{i_2}(\lambda)$ es divisible por $e_2(\lambda)$, etc. Finalmente, si en la matriz (3) *se toma el menor de k-ésimo orden por el que pasa, al menos para* una i, la i-ésima fila de esta matriz, pero no pasa su i-ésima columna, resulta que este menor contiene una fila nula, por lo cual, es igual a cero.

De lo expuesto se deduce, que el producto (5) es el máximo común divisor de todos los menores de k-ésimo orden de la matriz (3) y, por consiguiente, de la matriz inicial $A(\lambda)$,

$$d_k(\lambda) = e_1(\lambda)\, e_2(\lambda) \ldots e_k(\lambda), \qquad k = 1, 2, \ldots, n. \tag{6}$$

Ahora es fácil demostrar que *los polinomios* $e_k(\lambda)$, $k = 1, 2, \ldots, n$, *se determinan univocamente por la misma matriz* $A(\lambda)$. **Supongamos que el rango de esta matriz es** r. Entonces, como ya sabemos,

$d_r(\lambda) \neq 0$, pero $d_{r+1}(\lambda) = 0$, y por esto, en virtud de (6), $e_{r+1}(\lambda) = 0$. De aquí, en virtud de las propiedades de la matriz canónica, se deduce, en general, que **si el rango r de la matriz $A(\lambda)$ es menor que n, entonces,**

$$e_{r+1}(\lambda) = e_{r+2}(\lambda) = \ldots = e_n(\lambda) = 0. \tag{7}$$

Por otra parte, para $k \leqslant r$, como $d_{k-1}(\lambda) \neq 0$, de (6) resulta que

$$e_k(\lambda) = \frac{d_k(\lambda)}{d_{k-1}(\lambda)}. \tag{8}$$

Con esto se termina la demostración de la unicidad de la forma canónica de una λ-matriz.

Al mismo tiempo hemos obtenido un método para hallar directamente los polinomios $e_k(\lambda)$ llamados *factores invariantes* de la matriz $A(\lambda)$.

Ejemplo. Reducir a la forma canónica la λ-matriz

$$A(\lambda) = \begin{pmatrix} \lambda^3 - \lambda & 2\lambda^2 \\ \lambda^2 + 5\lambda & 3\lambda \end{pmatrix}.$$

Efectuando una cadena de transformaciones elementales, obtenemos:

$$A(\lambda) \sim \begin{pmatrix} \lambda^3 - \lambda & \frac{2}{3}\lambda^2 \\ \lambda^2 + 5\lambda & \lambda \end{pmatrix} \sim \begin{pmatrix} \frac{1}{3}\lambda^3 - \frac{10}{3}\lambda^2 - \lambda & 0 \\ \lambda^2 + 5\lambda & \lambda \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} \frac{1}{3}\lambda^3 - \frac{10}{3}\lambda^2 - \lambda & 0 \\ 0 & \lambda \end{pmatrix} \sim \begin{pmatrix} \lambda^3 - 10\lambda^2 - 3\lambda & 0 \\ 0 & \lambda \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^3 - 10\lambda^2 - 3\lambda \end{pmatrix}.$$

Pero se podrían calcular directamente los factores invariantes de la matriz $A(\lambda)$. Precisamente, calculando el máximo común divisor de los elementos de esta matriz, obtenemos:

$$d_1(\lambda) = e_1(\lambda) = \lambda.$$

Calculando el determinante de la matriz $A(\lambda)$ y observando que su coeficiente superior es igual a 1, resulta:

$$d_2(\lambda) = \lambda^4 - 10\lambda^3 - 3\lambda^2,$$

y, *por esto*,

$$e_2(\lambda) = \frac{d_2(\lambda)}{d_1(\lambda)} = \lambda^3 - 10\lambda^2 - 3\lambda.$$

§ 60. λ-matrices unimodulares. Relación entre la semejanza de las matrices numéricas y la equivalencia de sus matrices características

De los resultados del párrafo precedente se desprende un criterio de equivalencia de las λ-matrices, que se puede formular de los siguientes dos modos, que son casi idénticos:

Dos λ-matrices son equivalentes si, y sólo si, éstas se reducen a una misma forma canónica.

Dos λ-matrices son equivalentes si, y sólo si, éstas tienen factores invariantes iguales.

Deduzcamos otro criterio de carácter distinto.

Ya sabemos que al conjunto de las λ-matrices canónicas pertenece la matriz unidad E. Llamemos a una λ-matriz $U(\lambda)$ *unimodular*, si su forma canónica coincide con la matriz unidad E, o sea, si todos sus factores invariantes son iguales a la unidad.

Una λ-matriz $U(\lambda)$ es unimodular si, y sólo si, su determinante es distinto de cero, pero no depende de λ, o sea, si es un número del campo fundamental P, distinto de cero.

En efecto, si $U(\lambda) \sim E$, a estas dos matrices les corresponde un mismo polinomio $d_n(\lambda)$. Pero, para la matriz unidad, $d_n(\lambda) = 1$. De aquí se deduce que el determinante de la matriz $U(\lambda)$, que se diferencia de $d_n(\lambda)$ solamente en un factor numérico distinto de cero, es un número del campo P, distinto de cero. Recíprocamente, si el determinante de la matriz $U(\lambda)$ es diferente de cero y no depende de λ, entonces, para esta matriz, el polinomio $d_n(\lambda)$ será igual a 1, por lo cual, según (6) del párrafo anterior, todos los factores invariantes $e_i(\lambda)$ de la matriz $U(\lambda)$, $i = 1, 2, \ldots, n$, son iguales a la unidad.

De aquí se deduce que, *toda matriz numérica no degenerada es una λ-matriz unimodular*. Pero, una λ-matriz unimodular puede ser de forma complicada. Así, pues, la λ-matriz

$$\begin{pmatrix} \lambda & \lambda^3+5 \\ \lambda^2-\lambda-4 & \lambda^4-\lambda^3-4\lambda^2+5\lambda-5 \end{pmatrix}$$

es unimodular, pues su determinante es igual a 20, o sea, es distinto de cero y no depende de λ.

Del teorema demostrado anteriormente se deduce que, *el producto de λ-matrices unimodulares es unimodular*, pues, es suficiente recordar que, al multiplicar matrices, sus determinantes se multiplican.

Una λ-matriz $U(\lambda)$ es unimodular si, y sólo si, existe la matriz inversa y ésta es una λ-matriz.

En efecto, dada una λ-matriz no degenerada, buscando de un modo ordinario la matriz inversa, tendremos que dividir los complementos algebraicos de los elementos de la matriz dada por el determinante de ésta, o sea, por un polinomio en λ. Por esto, en el caso general, los elementos de la matriz inversa serán fracciones racionales en λ, pero no polinomios en λ, o sea, **esta matriz no será una λ-matriz.** Si se da una matriz unimodular, habrá que dividir los complementos algebraicos solamente por un número del campo P, distinto de cero, o sea, los elementos de la matriz inversa serán polinomios en λ, por lo cual, la misma matriz inversa será una λ-matriz. Recíproca-

mente, si una λ-matriz $U(\lambda)$ tiene λ-matriz inversa $U^{-1}(\lambda)$, los determinantes de ambas matrices serán polinomios en λ, su producto será igual a 1, por lo cual, ambos determinantes tendrán que ser polinomios de grado cero.

De la última observación, se deduce el siguiente complemento del teorema que acabamos de demostrar:

Una λ-matriz que es inversa a una λ-matriz unimodular, es también unimodular.

El concepto de matriz unimodular se emplea en el enunciado siguiente del nuevo **criterio de equivalencia de las λ-matrices:**

Dos λ-matrices $A(\lambda)$ y $B(\lambda)$ de orden n son equivalentes si, y sólo si, existen unas λ-matrices unimodulares $U(\lambda)$ y $V(\lambda)$ del mismo orden n, tales que

$$B(\lambda) = U(\lambda)\, A(\lambda)\, V(\lambda). \tag{1}$$

Introduzcamos primero el siguiente concepto, que se emplea en la demostración de este criterio. Llamemos *matriz elemental* a la matriz numérica (que, por lo tanto, es una λ-matriz):

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 1 \\ & \cdots\cdots & \alpha & \cdots\cdots & \\ & & & 1 & \\ & & & & \ddots \\ 0 & & & & \\ & & & & 1 \end{pmatrix} (i), \tag{2}$$

que se diferencia de la matriz unidad solamente en que, en cierto i-ésimo lugar de la diagonal principal, $1 \leqslant i \leqslant n$, figura un número arbitrario α del campo P, **distinto de cero.** Por otra parte, llamemos **también** *matriz elemental* a la λ-matriz

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & \cdots 1 \cdots & \varphi(\lambda) & \cdots\cdots & \\ & & & & 1 \\ & & & & \ddots \\ & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ (i), \\ \\ \\ \\ \\ \\ \\ (j) \end{matrix} \tag{3}$$

que se diferencia de la matriz unidad solamente en que, en la intersección de la i-ésima fila y la j-ésima columna, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, siendo $i \neq j$, figura un polinomio arbitrario $\varphi(\lambda)$ del anillo $P[\lambda]$.

Toda matriz elemental es unimodular. En efecto, el determinante de la matriz (2) es igual a α, pero, por la condición, $\alpha \neq 0$; por otra parte, el determinante de la matriz (3) es igual a 1.

La ejecución en una λ-matriz $A(\lambda)$ de cualquier transformación elemental es equivalente a la multiplicación de esta matriz a la izquierda o a la derecha por una matriz elemental.

En efecto, el lector comprobará sin dificultad la justeza de las cuatro proposiciones siguientes: 1) multiplicar la matriz $A(\lambda)$ a la izquierda por la matriz (2) equivale a multiplicar la i-ésima de la matriz $A(\lambda)$ por el número α; 2) multiplicar la matriz $A(\lambda)$ a la derecha por la matriz (2) equivale a multiplicar la i-ésima columna de la matriz (2) por el número α; 3) multiplicar la matriz $A(\lambda)$ a la izquierda por la matriz (3) equivale a sumar a la i-ésima fila de la matriz $A(\lambda)$ su j-ésima fila, multiplicada por $\varphi(\lambda)$; 4) multiplicar la matriz $A(\lambda)$ a la derecha por la matriz (3) equivale a sumar a la j-ésima columna de la matriz $A(\lambda)$ su i-ésima columna, multiplicada por $\varphi(\lambda)$.

Pasemos a demostrar ahora nuestro **criterio de equivalencia de las λ-matrices.** Si $A(\lambda) \sim B(\lambda)$, de la matriz $A(\lambda)$ se puede pasar a la matriz $B(\lambda)$ realizando un número finito de transformaciones elementales. Sustituyendo cada una de estas transformaciones por la multiplicación a la izquierda o a la derecha, por una matriz elemental, llegaremos a la siguiente igualdad:

$$B(\lambda) = U_1(\lambda) \ldots U_k(\lambda) A(\lambda) V_1(\lambda) \ldots V_l(\lambda), \tag{4}$$

donde todas las matrices $U_1(\lambda), \ldots, U_k(\lambda), V_1(\lambda) \ldots, V_l(\lambda)$ son elementales y, por consiguiente, unimodulares. Por esto, serán también unimodulares las matrices

$$U(\lambda) = U_1(\lambda) \ldots U_k(\lambda), \quad V(\lambda) = V_1(\lambda) \ldots V_l(\lambda), \tag{5}$$

que son productos de matrices unimodulares, y la igualdad (4) se escribirá de la forma (1). Obsérvese que si, por ejemplo, $k = 0$, o sea, que se efectuaron transformaciones elementales solamente sobre las columnas, entonces, ponemos simplemente $U(\lambda) = E$.

La parte ya demostrada permite a la vez enunciar la siguiente proposición:

Una λ-matriz es unimodular si, y sólo si, ésta se representa en forma de un producto de matrices elementales.

En efecto, ya hemos empleado el hecho de que el producto de matrices elementales es unimodular. Recíprocamente, una matriz unimodular arbitraria $W(\lambda)$ es equivalente a la matriz unidad E.

Aplicando a las matrices E y $W(\lambda)$ la demostración que se llevó a cabo con las matrices $A(\lambda)$ y $B(\lambda)$, de (4) obtenemos la igualdad

$$W(\lambda) = U_1(\lambda) \ldots U_k(\lambda) V_1(\lambda) \ldots V_l(\lambda),$$

o sea, la matriz $W(\lambda)$ ha quedado representada en forma de un producto de matrices elementales.

Ahora es fácil demostrar **la proposición recíproca de nuestro criterio.** Supongamos que para las matrices $A(\lambda)$ y $B(\lambda)$ existen unas matrices unimodulares $U(\lambda)$ y $V(\lambda)$ tales, que se verifica la igualdad (1). Por lo demostrado, las matrices $U(\lambda)$ y $V(\lambda)$ se pueden representar en forma de productos de matrices elementales; supongamos que (5) son las representaciones dichas. La igualdad (1) se escribirá ahora en la forma (4) y, sustituyendo cada multiplicación por una matriz elemental por su transformación elemental correspondiente, obtenemos, por fin, que $A(\lambda) \sim B(\lambda)$.

Polinomios matriciales. El concepto de λ-matriz se puede interpretar de otro modo. Llamemos *λ-polinomio matricial de orden n sobre el campo P* a un polinomio en λ cuyos coeficientes son matrices cuadradas de un mismo orden n, con elementos del mismo campo P; su forma general es:

$$A_0\lambda^k + A_1\lambda^{k-1} + \ldots + A_{k-1}\lambda + A_k. \tag{6}$$

Entendiendo el producto de la matriz A_i por λ^{k-i}, $i = 0, 1, \ldots, k$, en correspondencia con el § 15, como el producto de todos los elementos de la matriz A_i por λ^{k-i}, y efectuando después la suma de las matrices de acuerdo con el mismo § 15, obtenemos que, *todo λ-polinomio matricial de orden n se puede expresar en forma de una λ-matriz de orden n.* Así, pues,

$$\begin{pmatrix} 4 & 0 \\ -1 & 1 \end{pmatrix}\lambda^3 + \begin{pmatrix} 0 & -3 \\ 0 & 1 \end{pmatrix}\lambda^2 + \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix}\lambda + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 4\lambda^3 + \lambda & -3\lambda^2 + 2\lambda + 1 \\ -\lambda^3 & \lambda^3 + \lambda^2 - 2\lambda \end{pmatrix}.$$

Recíprocamente, *toda λ-matriz de orden n se puede expresar en forma de un λ-polinomio matricial de orden n.* Así, pues,

$$\begin{pmatrix} 3\lambda^2 - 5 & \lambda + 1 \\ \lambda^4 + 2\lambda & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\lambda^4 + \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}\lambda^2 + \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\lambda + \begin{pmatrix} -5 & 1 \\ 0 & -3 \end{pmatrix}.$$

La correspondencia entre las λ-matrices y los λ-polinomios matriciales es biunívoca e isomorfa en el sentido del § 46. En efecto, la igualdad de los λ-polinomios de la forma (6) como matrices es equivalente a la igualdad de los coeficientes matriciales de potencias iguales de λ, y la multiplicación de una matriz por λ es equivalente

a su multiplicación por una matriz escalar con λ en la diagonal principal.

Sea dada una λ-matriz $A(\lambda)$, siendo

$$A(\lambda) = A_0\lambda^k + A_1\lambda^{k-1} + \ldots + A_{k-1}\lambda + A_k,$$

donde la matriz A_0 no es nula. Al número k lo llamaremos *grado* de la λ-matriz $A(\lambda)$; evidentemente, éste será el grado superior (respecto a λ) de los elementos de la matriz $A(\lambda)$.

La consideración de las λ-matrices como polinomios matriciales permite desarrollar para las λ-matrices una teoría de divisibilidad análoga a la teoría de divisibilidad de los polinomios numéricos, pero, naturalmente, más complicada porque el producto de las matrices no es conmutativo y por la existencia de divisores de cero. Nos limitaremos a estudiar el **algoritmo de la división con resto.**

Sean dadas sobre el campo P las λ-matrices de orden n:

$$A(\lambda) = A_0\lambda^k + A_1\lambda^{k-1} + \ldots + A_{k-1}\lambda + A_k,$$
$$B(\lambda) = B_0\lambda^l + B_1\lambda^{l-1} + \ldots + B_{l-1}\lambda + B_l;$$

supongamos que la matriz B_0 no es degenerada, o sea, que existe la matriz B_0^{-1}. Entonces, sobre el campo P se pueden hallar unas λ-matrices $Q_1(\lambda)$ y $R_1(\lambda)$ del mismo orden n, tales que

$$A(\lambda) = B(\lambda)\,Q_1(\lambda) + R_1(\lambda), \qquad (7)$$

donde el grado de $R_1(\lambda)$ es menor que el grado de $B(\lambda)$, o bien, $R_1(\lambda) \equiv 0$. Por otra parte, sobre el campo P se pueden hallar unas λ-matrices $Q_2(\lambda)$ y $R_2(\lambda)$ de orden n, tales que

$$A(\lambda) = Q_2(\lambda)\,B(\lambda) + R_2(\lambda), \qquad (8)$$

donde el grado de $R_2(\lambda)$ es menor que el grado de $B(\lambda)$, o bien, $R_2(\lambda) \equiv 0$. Las matrices $Q_1(\lambda)$ y $R_1(\lambda)$, y también $Q_2(\lambda)$ y $R_2(\lambda)$, que satisfacen a estas condiciones, se determinan unívocamente.

La demostración de este teorema se efectúa del mismo modo que la demostración del teorema correspondiente para los polinomios numéricos (véase el § 20). Supongamos, por ejemplo, que a la condición (7) satisfacen también las matrices $\overline{Q}_1(\lambda)$ y $\overline{R}_1(\lambda)$, donde el grado de $R_1(\lambda)$ es menor que el de $B(\lambda)$. Entonces,

$$B(\lambda)\,[Q_1(\lambda) - \overline{Q}_1(\lambda)] = \overline{R}_1(\lambda) - R_1(\lambda).$$

El grado del segundo miembro es menor que l, mientras que el grado del primer miembro es mayor o igual a l, si la expresión entre corchetes es diferente de cero, puesto que la matriz B_0 no es degenerada. De aquí se deduce la unicidad de las matrices $Q_1(\lambda)$ y $R_1(\lambda)$.

Para demostrar la existencia de estas matrices, observemos que, para $k \geqslant l$, el grado de la diferencia

$$A(\lambda) - B(\lambda) \cdot B_0^{-1} A_0 \lambda^{k-l}$$

es estrictamente menor que k; por esto, $B_0^{-1} A_0 \lambda^{k-l}$ será el término superior del λ-polinomio matricial $Q_1(\lambda)$. A continuación se obra igual que en el § 20. Por otra parte, el grado de la diferencia

$$A(\lambda) - A_0 B_0^{-1} \lambda^{k-l} \cdot B(\lambda)$$

también es estrictamente menor que k, o sea, $A_0 B_0^{-1} \lambda^{k-l}$ es el término superior del λ-polinomio matricial $Q_2(\lambda)$. Vemos, pues, que en el caso general, las λ-matrices $Q_1(\lambda)$ y $Q_2(\lambda)$ (y también $R_1(\lambda)$ y $R_2(\lambda)$), que satisfacen a las condiciones del teorema, verdaderamente, son distintas.

Teorema fundamental de la semejanza de las matrices. Como ya se señaló, todavía no conocemos un procedimiento para responder a la pregunta si unas matrices numéricas dadas A y B (o sea, matrices con elementos del campo fundamental P) son semejantes o no. Por otra parte, sus matrices características $A - \lambda E$ y $B - \lambda E$ son λ-matrices y el problema de la equivalencia de estas matrices se resuelve de un modo efectivo. Por esto, se comprende el valor tan grande que tiene el siguiente teorema:

Las matrices A y B, con elementos del campo P, son semejantes si, y sólo si, sus matrices características $A - \lambda E$ y $B - \lambda E$ son equivalentes.

En efecto, supongamos que las matrices A y B son semejantes, o sea, que sobre el campo P existe una matriz no degenerada C tal, que

$$B = C^{-1} A C.$$

Entonces

$$C^{-1}(A - \lambda E) C = C^{-1} A C - \lambda (C^{-1} E C) = B - \lambda E.$$

Pero las matrices numéricas no degeneradas C^{-1} y C son λ-matrices unimodulares. Vemos, pues, que la matriz $B - \lambda E$ se obtiene multiplicando la matriz $A - \lambda E$ a la izquierda y a la derecha por matrices unimodulares, o sea, $A - \lambda E \sim B - \lambda E$.

La demostración del teorema recíproco es más complicada. Supongamos que

$$A - \lambda E \sim B - \lambda E.$$

Entonces, existen unas matrices unimodulares $U(\lambda)$ y $V(\lambda)$, tales, que

$$U(\lambda)(A - \lambda E) V(\lambda) = B - \lambda E. \tag{9}$$

Teniendo en cuenta que para las matrices unimodulares existen las matrices inversas y éstas son λ-matrices, de (9) deducimos las

siguientes igualdades, que se emplean a continuación:

$$\left.\begin{aligned} U(\lambda)(A-\lambda E) &= (B-\lambda E)V^{-1}(\lambda), \\ (A-\lambda E)V(\lambda) &= U^{-1}(\lambda)(B-\lambda E). \end{aligned}\right\} \tag{10}$$

Como la λ-matriz $B-\lambda E$ es de grado 1 con respecto a λ, y además, el coeficiente superior del polinomio matricial correspondiente es la matriz no degenerada $-E$, a las matrices $U(\lambda)$ y $B-\lambda E$ se les puede aplicar el algoritmo de la división con resto, según el cual, existen unas matrices $Q_1(\lambda)$ y R_1 (esta última, si es distinta de cero, tiene que ser de grado 0 con respecto a λ, o sea, no depende de λ), tales, que

$$U(\lambda) = (B-\lambda E)Q_1(\lambda) + R_1. \tag{11}$$

De modo análogo,

$$V(\lambda) = Q_2(\lambda)(B-\lambda E) + R_2. \tag{12}$$

Aplicando (11) y (12), de (9) obtenemos:

$$R_1(A-\lambda E)R_2 = (B-\lambda E) - U(\lambda)(A-\lambda E)Q_2(\lambda)(B-\lambda E) -$$
$$-(B-\lambda E)Q_1(\lambda)(A-\lambda E)V(\lambda) + (B-\lambda E)Q_1(\lambda)(A-\lambda E)Q_2(B-\lambda E)$$

o, en virtud de (10),

$$R_1(A-\lambda E)R_2 = (B-\lambda E) - (B-\lambda E)V^{-1}(\lambda)Q_2(\lambda)(B-\lambda E) -$$
$$-(B-\lambda E)Q_1(\lambda)U^{-1}(\lambda)(B-\lambda E) +$$
$$+(B-\lambda E)Q_1(\lambda)(A-\lambda E)Q_2(\lambda)(B-\lambda E) = (B-\lambda E)\times$$
$$\times\{E - [V^{-1}(\lambda)Q_2(\lambda) + Q_1(\lambda)U^{-1}(\lambda) - Q_1(\lambda)(A-\lambda E)Q_2(\lambda)](B-\lambda E)\}$$

La expresión que figura entre corchetes en el segundo miembro, verdaderamente, es igual a cero. En caso contrario, ésta, siendo una λ-matriz, puesto que $V^{-1}(\lambda)$, así como $U^{-1}(\lambda)$, son λ-matrices, sería por lo menos de grado cero y, entonces, el grado de la expresión entre llaves sería no menor que 1 y, por consiguiente, el grado de todo el segundo miembro no sería menor que 2. Pero, esto es imposible, puesto que en el primer miembro figura una λ-matriz de grado 1.

Por lo tanto,

$$R_1(A-\lambda E)R_2 = B-\lambda E,$$

de donde, igualando los coeficientes matriciales de potencias iguales de λ, obtenemos:

$$R_1AR_2 = B, \tag{13}$$
$$R_1R_2 = E. \tag{14}$$

La igualdad (14) muestra que la matriz numérica R_2 no sólo es distinta de cero, sino incluso no degenerada, siendo

$$R_2^{-1} = R_1,$$

y entonces, la igualdad (13) toma la forma

$$R_2^{-1} A R_2 = B,$$

lo cual demuestra la semejanza de las matrices A y B.

A la vez, **hemos aprendido a hallar la matriz R_2 no degenerada que transforma la matriz A en la matriz B.** Precisando, si las matrices $A - \lambda E$ y $B - \lambda E$ son equivalentes, entonces con un número finito de transformaciones elementales se transforma la primera en la segunda. Tomemos las transformaciones de éstas que se relacionan a las columnas, y designemos mediante $V(\lambda)$ el producto de las matrices elementales correspondientes, tomadas en el mismo orden. Dividamos después $V(\lambda)$ por $B - \lambda E$, de modo que el cociente quede a la izquierda del divisor (véase (8)). El residuo de esta división será la matriz R_2.

En realidad, se puede prescindir de la división indicada, utilizando el siguiente lema que hallará también aplicación en el § 62:

Lema. *Sea*

$$V(\lambda) = V_0\lambda^s + V_1\lambda^{s-1} + \ldots + V_{s-1}\lambda + V_s, \quad V_0 \neq 0. \tag{15}$$

Si

$$V(\lambda) = (\lambda E - B) Q_1(\lambda) + R_1, \tag{16}$$

$$V(\lambda) = Q_2(\lambda)(\lambda E - B) + R_2,$$

se tiene

$$R_1 = B^s V_0 + B^{s-1} V_1 + \ldots + BV_{s-1} + V_s, \tag{17}$$

$$R_2 = V_0 B^s + V_1 B^{s-1} + \ldots + V_{s-1} B + V_s.$$

Es suficiente demostrar, por ejemplo, la primera de estas dos afirmaciones, pues la segunda se demuestra por analogía. La demostración consiste en la comprobación directa del cumplimiento de la igualdad (16); para esto el polinomio $V(\lambda)$ se sustituye por su expresión (15), en lugar de R_1 se pone (17) y en vez de $Q_1(\lambda)$ se toma el polinomio

$$Q_1(\lambda) = V_0\lambda^{s-1} + (BV_0 + V_1)\lambda^{s-2} + (B^2V_0 + BV_1 + V_2)\lambda^{s-3} + \ldots$$
$$\ldots + (B^{s-1}V_0 + B^{s-2}V_1 + \ldots + V_{s-1}).$$

La prueba de esto la dejamos a cuenta del lector.

Ejemplo. Sean dadas las matrices

$$A=\begin{pmatrix}-2 & 1\\ 0 & 3\end{pmatrix},\quad B=\begin{pmatrix}-10 & -4\\ 26 & 11\end{pmatrix}.$$

Sus matrices características son equivalentes, puesto que se reducen a una misma forma canónica

$$\begin{pmatrix}1 & 0\\ 0 & \lambda^2-\lambda-6\end{pmatrix},$$

por esto, las matrices A y B son semejantes.

Para hallar la matriz R_2 que transforma A en B, hallemos alguna cadena de transformaciones elementales que transforme $A-\lambda E$ en $B-\lambda E$. Así, pues,

$$A-\lambda E=\begin{pmatrix}-2-\lambda & 1\\ 0 & 3-\lambda\end{pmatrix}\sim\begin{pmatrix}-2-\lambda & 1\\ -16-8\lambda & 11-\lambda\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}8+4\lambda & -4\\ -16-8\lambda & 11-\lambda\end{pmatrix}\sim\begin{pmatrix}40+4\lambda & -4\\ -104 & 11-\lambda\end{pmatrix}\sim\begin{pmatrix}-10-\lambda & -4\\ 26 & 11-\lambda\end{pmatrix}=B-\lambda E.$$

Las dos últimas transformaciones se refieren a las columnas: a la primera columna se suma la segunda, multiplicada por -8, y después, la primera columna se multiplica por $-\frac{1}{4}$. El producto de las matrices elementales correspondientes es

$$V(\lambda)=\begin{pmatrix}1 & 0\\ -8 & 1\end{pmatrix}\begin{pmatrix}-\frac{1}{4} & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-\frac{1}{4} & 0\\ 2 & 1\end{pmatrix}.$$

Esta matriz no depende de λ, por lo cual, ésta será la matriz R_2 buscada.

Claro, la matriz que transforma A en B está muy lejos de determinarse unívocamente. Tal es también, por ejemplo, la matriz

$$\begin{pmatrix}3 & 1\\ 2 & 1\end{pmatrix}.$$

§ 61. Forma normal de Jordan

Ahora estudiaremos las matrices cuadradas de orden n con elementos del campo P. Se distinguirá un tipo especial de matrices de éstas, llamadas **matrices de Jordan**, y se demostrará que estas matrices sirven de forma normal para una clase de matrices muy amplia. Precisando, *las matrices cuyas raíces características pertenecen al campo fundamental P (y solamente tales matrices), son semejantes a ciertas matrices de Jordan, o, como suele decirse, se reducen a la forma normal de Jordan.* De aquí se deducirá que, si se toma por P el campo de los números complejos, *cualquier matriz con elementos complejos se reduce a la forma normal de Jordan en este campo.*

Introduzcamos las definiciones necesarias. Se llama *«malla» de Jordan* de orden k correspondiente al número λ_0, la matriz de orden

k, $1 \leqslant k \leqslant n$, que tiene la forma

$$\begin{pmatrix} \lambda_0 & 1 & & & 0 \\ & \lambda_0 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda_0 \end{pmatrix}; \tag{1}$$

en otras palabras, en su diagonal principal figura un mismo número λ_0 del campo P; la paralela, situada por encima de la diagonal principal y más próxima a ésta, está ocupada totalmente por el número 1; todos los demás elementos de la matriz son iguales a cero. Así, pues,

$$(\lambda_0), \quad \begin{pmatrix} \lambda_0 & 1 \\ 0 & \lambda_0 \end{pmatrix}, \quad \begin{pmatrix} \lambda_0 & 1 & 0 \\ 0 & \lambda_0 & 1 \\ 0 & 0 & \lambda_0 \end{pmatrix}$$

son mallas de Jordan de primero, segundo y tercer orden, respectivamente.

Se llama *matriz de Jordan* de orden n a la matriz de order n que tiene la forma

$$J = \begin{pmatrix} \boxed{J_1} & & & 0 \\ & \boxed{J_2} & & \\ & & \ddots & \\ 0 & & & \boxed{J_s} \end{pmatrix}; \tag{2}$$

aquí, a lo largo de la diagonal principal figuran las mallas de Jordan $J_1, J_2, \ldots, J_s$ de ciertos órdenes, que necesariamente no son distintas, y que corresponden a ciertos números del campo P, tampoco necesariamente distintos; todos los lugares fuera de estas mallas están ocupados por ceros. Aquí, $s \geqslant 1$, o sea, una malla de Jordan de orden n pertenece al conjunto de las matrices de Jordan de este mismo orden y, naturalmente, $s \leqslant n$.

Obsérvese, a pesar de que esto no se va a aplicar a continuación, que se podría haber descrito la estructura de la matriz de Jordan sin recurrir al concepto de célula de Jordan. Así, pues, es evidente que una matriz es de Jordan si, y sólo si, ésta tiene la forma

$$\begin{pmatrix} \lambda_1 & \varepsilon_1 & & & 0 \\ & \lambda_2 & \varepsilon_2 & & \\ & & \ddots & \ddots & \\ & & & \ddots & \varepsilon_{n-1} \\ 0 & & & & \lambda_n \end{pmatrix},$$

donde λ_i, $i = 1, 2, \ldots, n$, son números arbitrarios del campo P, y cada ε_j, $j = 1, 2, \ldots, n-1$, es igual a la unidad o a cero, siendo $\lambda_j = \lambda_{j+1}$ cuando $\varepsilon_j = 1$.

Las matrices diagonales son casos particulares de las matrices de Jordan; éstas son precisamente las matrices de Jordan cuyas mallas son de orden 1.

Nuestro objetivo próximo consiste en **hallar la forma canónica para la matriz característica $J - \lambda E$ de una matriz arbitraria de Jordan J, de orden n.** Hallemos primero la forma canónica para la matriz característica

$$\begin{pmatrix} \lambda_0 - \lambda & 1 & & & 0 \\ & \lambda_0 - \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda_0 - \lambda \end{pmatrix} \tag{3}$$

de una malla de Jordan (1), de orden k. Calculando el determinante de esta matriz y recordando que el coeficiente superior del polinomio $d_k(\lambda)$ tiene que ser igual a 1, obtenemos,

$$d_k(\lambda) = (\lambda - \lambda_0)^k.$$

Por otra parte, entre los menores de $(k-1)$-ésimo orden de la matriz (3) hay uno que es igual a la unidad, precisamente, el que resulta después de haber suprimido la primera columna y la última fila de esta matriz. Por esto,

$$d_{k-1}(\lambda) = 1.$$

De aquí se deduce que *la forma canónica de la matriz* (3) *es la siguiente* λ*-matriz de orden* k:

$$\begin{pmatrix} 1 & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & 1 \\ 0 & & & (\lambda-\lambda_0)^k \end{pmatrix}. \tag{4}$$

Demostremos ahora el **lema** que sigue:

Si los polinomios $\varphi_1(\lambda)$, $\varphi_2(\lambda)$, ..., $\varphi_t(\lambda)$ *del anillo* $P[\lambda]$ *son primos entre sí dos a dos, se verifica la siguiente equivalencia*:

$$\begin{pmatrix} \varphi_1(\lambda) & & & 0 \\ & \varphi_2(\lambda) & & \\ & & \cdot & \\ 0 & & & \varphi_t(\lambda) \end{pmatrix} \sim \begin{pmatrix} 1 & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & 1 & \\ 0 & & & \prod_{i=1}^{t} \varphi_i(\lambda) \end{pmatrix}.$$

Evidentemente, es suficiente considerar el caso $t = 2$. Como los polinomios $\varphi_1(\lambda)$ y $\varphi_2(\lambda)$ son primos entre sí, en el anillo $P[\lambda]$ existen unos polinomios $u_1(\lambda)$ y $u_2(\lambda)$, tales que

$$\varphi_1(\lambda)\,u_1(\lambda) + \varphi_2(\lambda)\,u_2(\lambda) = 1.$$

Por esto,

$$\begin{pmatrix} \varphi_1(\lambda) & 0 \\ 0 & \varphi_2(\lambda) \end{pmatrix} \sim \begin{pmatrix} \varphi_1(\lambda) & \varphi_1(\lambda)\,u_1(\lambda) \\ 0 & \varphi_2(\lambda) \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} \varphi_1(\lambda) & \varphi_1(\lambda)\,u_1(\lambda) + \varphi_2(\lambda)\,u_2(\lambda) \\ 0 & \varphi_2(\lambda) \end{pmatrix} = \begin{pmatrix} \varphi_1(\lambda) & 1 \\ 0 & \varphi_2(\lambda) \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & \varphi_1(\lambda) \\ \varphi_2(\lambda) & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & \varphi_1(\lambda) \\ 0 & -\varphi_1(\lambda)\,\varphi_2(\lambda) \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 \\ 0 & -\varphi_1(\lambda)\,\varphi_2(\lambda) \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & \varphi_1(\lambda)\,\varphi_2(\lambda) \end{pmatrix},$$

como se quería demostrar.

Consideremos ahora la matriz característica

$$J - \lambda E = \begin{pmatrix} \boxed{J_1 - \lambda E_1} & & & 0 \\ & \boxed{J_2 - \lambda E_2} & & \\ & & \cdot & \\ 0 & & & \boxed{J_s - \lambda E_s} \end{pmatrix} \tag{5}$$

de la matriz de Jordan J de la forma (2); aquí, E_i, $i = 1, 2, \ldots, s$, es la matriz unidad del mismo orden que la malla J_i. Supongamos que las mallas de Jordan de la matriz J corresponden a los siguientes números **distintos**: $\lambda_1, \lambda_2, \ldots, \lambda_t$, donde $t \leqslant s$. Supongamos también que al número λ_i, $i = 1, 2, \ldots, t$, corresponden q_i mallas de Jordan, $q_i \geqslant 1$, y sean los órdenes de éstas, colocados en orden no creciente, los números

$$k_{i1} \geqslant k_{i2} \geqslant \ldots \geqslant k_{iq_i}. \tag{6}$$

Obsérvese, a pesar de que no vamos a utilizar esto, que

$$\sum_{i=1}^{t} q_i = s,$$

$$\sum_{i=1}^{t} \sum_{j=1}^{q_i} k_{ij} = n.$$

Aplicando transformaciones elementales a las filas y columnas de la matriz (5) que pasan por la malla $J_i - \lambda E_i$ de esta matriz, no se tocan, evidentemente, las otras mallas diagonales. De aquí se deduce que en la matriz (5), mediante transformaciones elementales, se puede sustituir cada malla $J_i - \lambda E_i$, $i = 1, 2, \ldots, s$, por la malla correspondiente de la forma (4). En otras palabras, *la matriz $J - \lambda E$ es equivalente a una matriz diagonal, en cuya diagonal, además de ciertas unidades, figuran también los siguientes polinomios, que corresponden a todas las mallas de Jordan de la matriz J;*

$$\left.\begin{array}{l} (\lambda-\lambda_1)^{k_{11}},\ (\lambda-\lambda_1)^{k_{12}},\ \ldots,\ (\lambda-\lambda_1)^{k_{1q_1}}, \\ (\lambda-\lambda_2)^{k_{21}},\ (\lambda-\lambda_2)^{k_{22}},\ \ldots,\ (\lambda-\lambda_2)^{k_{2q_2}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (\lambda-\lambda_t)^{k_{t1}},\ (\lambda-\lambda_t)^{k_{t2}},\ \ldots,\ (\lambda-\lambda_t)^{k_{tq_t}}. \end{array}\right\} \tag{7}$$

En este caso, no indicamos los lugares en la diagonal donde figuran los polinomios (7), puesto que en cualquier λ-matriz diagonal, los elementos diagonales se pueden cambiar de sitio arbitrariamente permutando las filas y las columnas homólogas. Esta observación se debe tener en cuenta a continuación.

Sea q el máximo entre los números q_i, $i = 1, 2, \ldots, t$. Designemos con $e_{n-j+1}(\lambda)$ el producto de los polinomios que figuran en la j-ésima columna de la tabla (7), $j = 1, 2, \ldots, q$, o sea,

$$e_{n-j+1}(\lambda) = \prod_{i=1}^{t} (\lambda-\lambda_i)^{k_{ij}}; \tag{8}$$

si en este caso en la j-ésima columna hay sitios vacíos (para algunos i puede ocurrir que $q_i < j$), suponemos que los factores correspon-

dientes en (8) son iguales a la unidad. Como, por la condición, los números $\lambda_1, \lambda_2, \ldots, \lambda_t$ son distintos, los grados de los binomios lineales que figuran en la j-ésima columna de la tabla (7) son primos entre sí dos a dos. Por esto, según el lema demostrado anteriormente, mediante transformaciones elementales, estos binomios se pueden sustituir en la matriz diagonal considerada por su producto $e_{n-j+1}(\lambda)$ y cierta cantidad de unidades. Haciendo esto para $j = 1, 2, \ldots, q$, obtenemos que

$$J-\lambda E \sim \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & e_{n-q+1}(\lambda) & \\ & & & & \ddots \\ & & & & & e_{n-1}(\lambda) \\ 0 & & & & & & e_n(\lambda) \end{pmatrix}. \tag{9}$$

Esta es la forma canónica buscada de la matriz $J - \lambda E$. En efecto, los coeficientes superiores de todos los polinomios que figuran en (9) en la diagonal principal, son iguales a la unidad, y, en virtud de la condición (6), cada uno de estos polinomios es divisible por el precedente.

Ejemplo. Sea

$$J = \begin{pmatrix} \boxed{\begin{matrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{matrix}} & & & & 0 \\ & \boxed{2} & & & \\ & & \boxed{\begin{matrix} 5 & 1 \\ 0 & 5 \end{matrix}} & & \\ & & & \boxed{\begin{matrix} 5 & 1 \\ 0 & 5 \end{matrix}} & \\ 0 & & & & \boxed{2} \end{pmatrix}$$

Para esta matriz de Jordan de noveno orden, la tabla de polinomios (7) es de la forma

$$(\lambda-2)^3,\ \lambda-2,\ \lambda-2,$$
$$(\lambda-5)^2,\ (\lambda-5)^2.$$

Por esto, los factores invariantes de la matriz J son:

$$e_9(\lambda) = (\lambda-2)^3(\lambda-5)^2,$$
$$e_8(\lambda) = (\lambda-2)(\lambda-5)^2,$$
$$e_7(\lambda) = \lambda-2,$$

mientras que $e_6(\lambda) = \ldots = e_1(\lambda) = 1$.

Ahora que hemos aprendido a escribir inmediatamente la forma canónica de su matriz característica, partiendo de la forma dada de Jordan J, se puede demostrar el siguiente **teorema:**

Dos matrices de Jordan son semejantes si, y sólo si, éstas constan de unas mismas mallas de Jordan, o sea, que solamente pueden diferenciarse en el orden de colocación de estas mallas a lo largo de la diagonal principal.

En efecto, la tabla de polinomios (7) se determinaba completamente por el conjunto de las mallas de Jordan de la matriz de Jordan J, y en ella de ningún modo se reflejaba la colocación de las mallas de Jordan a lo largo de la diagonal principal de esta matriz. De aquí se deduce que, si las matrices de Jordan J y J' poseen una misma colección de mallas de Jordan, a éstas corresponde una misma tabla de polinomios (7), y por esto, unos mismos polinomios (8). Por lo tanto, las matrices características $J - \lambda E$ y $J' - \lambda E$ tienen unos mismos factores invariantes, o sea, son equivalentes, y por lo tanto, las matrices J y J' son semejantes.

Recíprocamente, si las matrices de Jordan son semejantes, sus matrices características tienen iguales factores invariantes. Supongamos que los polinomios (8) para $j = 1, 2, \ldots, q$, son los factores invariantes de éstos, que son distintos de la unidad. Pero, con los polinomios (8) se restablece la tabla de los polinomios (7). Más exactamente, los polinomios (8) se descomponen en productos de potencias de factores lineales, puesto que, como ya se ha demostrado, para cualquier matriz de Jordan los factores invariantes de la matriz característica poseen esta misma propiedad. Precisamente, la tabla (7) consta de las potencias máximas de los factores lineales en que se descomponen los polinomios (8). Finalmente, con la tabla (7) se restablecen las mallas de Jordan de las matrices iniciales de Jordan, pues, a cada polinomio $(\lambda - \lambda_i)^{k_{ij}}$ en la tabla (7) corresponde una malla de Jordan de orden k_{ij}, correspondiente al número λ_i. Con esto, queda demostrado que las matrices J y J' constan de unas mismas mallas de Jordan y que se pueden diferenciar solamente por la colocación de éstas.

En particular, de este teorema se deduce que, *una matriz de Jordan que es semejante a una matriz diagonal, es también diagonal, y que dos matrices diagonales son semejantes si, y sólo si, se diferencian*

entre sí en una permutación de los números que figuran en la diagonal principal.

Reducción de una matriz a la forma normal de Jordan. Si una matriz A con elementos del campo P *se reduce a la forma normal de Jordan*, o sea, es semejante a una matriz de Jordan, entonces, como esto se deduce del teorema demostrado más arriba, *la forma normal de Jordan se determina por la matriz A unívocamente, salvo el orden de colocación de las mallas en la diagonal principal.* La condición para que la matriz A permita tal reducción se indica en el siguiente teorema, cuya demostración nos proporciona a la vez un método práctico para hallar la matriz de Jordan que es semejante a la matriz A, si tal matriz de Jordan existe. Obsérvese en este caso, que **la reducción en el campo** P significa que todos los elementos de la matriz con la que se efectúa la transformación pertenecen al campo P.

Una matriz A con elementos del campo P se reduce en este campo a la forma normal de Jordan cuando, y sólo cuando, todas las raíces características de la matriz A pertenecen al mismo campo fundamental P.

En efecto, si la matriz A es semejante a una matriz de Jordan J, entonces, estas dos matrices tienen unas mismas raíces características. Pero las raíces características de la matriz J se hallan sin dificultad alguna; como el determinante de la matriz $J - \lambda E$ es igual al producto de sus elementos que están en la diagonal principal, el polinomio $|J - \lambda E|$ se descompone sobre el campo P en factores lineales y los números que están en la diagonal principal de la matriz J, y sólo éstos, son sus raíces.

Recíprocamente, supongamos que todas las raíces características de la matriz A pertenecen al mismo campo P. Si

$$e_{n-q+1}(\lambda),\ \ldots,\ e_{n-1}(\lambda),\ e_n(\lambda), \tag{10}$$

son los factores invariantes de la matriz $A - \lambda E$ distintos de 1, entonces,

$$|A - \lambda E| = (-1)^n e_{n-q+1}(\lambda) \ldots e_{n-1}(\lambda) e_n(\lambda).$$

En efecto, los determinantes de la matriz $A - \lambda E$ y de su matriz canónica sólo pueden diferenciarse entre sí en un factor constante que, en realidad, es igual a $(-1)^n$, puesto que así es el coeficiente superior del polinomio característico $|A - \lambda E|$. Por lo tanto, entre los polinomios (10) no hay iguales a cero, la suma de los grados de estos polinomios es igual a n y todos ellos se descomponen sobre el campo P en factores lineales; esto último es debido a que, por la condición, el polinomio $|A - \lambda E|$ tiene tal descomposición.

Sean (8) las descomposiciones de los polinomios (10) en productos de potencias de factores lineales. Llamemos *divisores elementales del polinomio* e_{n-j+1}, $j = 1, 2, \ldots, q$, a las potencias de distintos binomios lineales, diferentes de la unidad, que figuran en su descom-

posición (8), o sea,

$$(\lambda-\lambda_1)^{k_{11}},\ (\lambda-\lambda_2)^{k_{21}},\ \ldots,\ (\lambda-\lambda_t)^{k_{t1}}.$$

A los divisores elementales de todos los polinomios (10) los llamaremos *divisores elementales de la matriz A* y los escribiremos en forma de la tabla (7).

Tomemos ahora una matriz de Jordan J de orden n, formada por mallas de Jordan, definidas del modo siguiente: **a cada divisor elemental $(\lambda-\lambda_i)^{k_{ij}}$ de la matriz A ponemos en correspondencia la malla de Jordan de orden k_{ij} que corresponde al número λ_i.** Es evidente, que los polinomios (10), y sólo éstos, son los factores invariantes de la matriz $J-\lambda E$ distintos de la unidad. Por esto, las matrices $A-\lambda E$ y $J-\lambda E$ son equivalentes y, por consiguiente, la matriz A es semejante a la matriz de Jordan J.

Ejemplo. Sea dada la matriz

$$A=\begin{pmatrix} -16 & -17 & 87 & -108 \\ 8 & 9 & -42 & 54 \\ -3 & -3 & 16 & -18 \\ -1 & -1 & 6 & -8 \end{pmatrix}.$$

Reduciendo la matriz $A-\lambda E$ de un modo ordinario a la forma canónica, obtenemos que los factores invariantes de esta matriz, distintos de la unidad, son los polinomios

$$e_4(\lambda)=(\lambda-1)^2(\lambda+2),$$
$$e_3(\lambda)=\lambda-1.$$

Vemos, pues, que la matriz A se reduce a la forma normal de Jordan incluso en el campo de los números racionales. Sus divisores elementales son los polinomios $(\lambda-1)^2$, $\lambda-1$ y $\lambda+2$, por lo cual, la matriz

$$J=\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}$$

es la forma normal de Jordan de la matriz A.

Si quisiéramos hallar la matriz no degenerada que transforma la matriz A en la matriz J, tendríamos que valernos de las indicaciones hechas al fin al del párrafo precedente.

Finalmente, basándose en los resultados anteriores, se puede demostrar la siguiente **condición necesaria y suficiente de reducción de una matriz a la forma diagonal**, condición de la que inmediatamente se desprende el criterio suficiente de reducción a la forma diagonal, demostrado en el § 33.

Una matriz A de orden n con elementos del campo P, se reduce a la forma diagonal si, y sólo si, todas las raíces del último factor invariante $e_n(\lambda)$ de su matriz característica pertenecen al campo P, no teniendo que haber múltiples entre ellas.

En efecto, la reducción de una matriz a la forma diagonal es equivalente a la reducción a una forma de Jordan, en la que las mallas de Jordan sean de orden 1. En otras palabras, todos los divisores elementales de la matriz A tienen que ser polinomios de primer grado. Pero, como todos los factores invariantes de la matriz $A - \lambda E$ son divisores del polinomio $e_n(\lambda)$, esta última condición equivale a que todos los divisores elementales del polinomio $e_n(\lambda)$ sean de grado 1, como se quería demostrar.

§ 62. Polinomio mínimo

Sea dada una matriz cuadrada A de orden n con elementos del campo P. Si

$$f(\lambda) = \alpha_0\lambda^k + \alpha_1\lambda^{k-1} + \ldots + \alpha_{k-1}\lambda + \alpha_k$$

es un polinomio del anillo $P[\lambda]$, la matriz

$$f(A) = \alpha_0 A^k + \alpha_1 A^{k-1} + \ldots + \alpha_{k-1}A + \alpha_k E$$

se llama *valor* del polinomio $f(\lambda)$ para $\lambda = A$; advirtamos que, en este caso, el término independiente del polinomio $f(\lambda)$ se multiplica por la potencia cero de la matriz A, o sea, por la matriz unidad E.

Fácilmente se comprueba que, si

$$f(\lambda) = \varphi(\lambda) + \psi(\lambda),$$

o si

$$f(\lambda) = u(\lambda)\, v(\lambda),$$

entonces,

$$f(A) = \varphi(A) + \psi(A)$$

o, respectivamente,

$$f(A) = u(A)\, v(A).$$

Si la matriz A anula al polinomio $f(\lambda)$, o sea, si

$$f(A) = 0,$$

la matriz A se llamará *raíz matricial*, o bien, cuando esto no dé lugar a confusiones, se llamará simplemente *raíz* del polinomio $f(\lambda)$.

Toda matriz A es raíz de un polinomio no nulo.

En efecto, sabemos que todas las matrices cuadradas de orden n forman sobre el campo P un espacio vectorial de n^2 dimensiones.

De aquí se deduce, que el sistema de $n^2 + 1$ matrices

$$A^{n^2},\ A^{n^2-1},\ \ldots,\ A,\ E,$$

es linealmente dependiente sobre el campo P, o sea, en P existen unos elementos $\alpha_0, \alpha_1, \ldots, \alpha_{n^2}, \alpha_{n^2+1}$, no simultáneamente iguales a cero, tales, que

$$\alpha_0 A^{n^2} + \alpha_1 A^{n^2-1} + \ldots + \alpha_{n^2} A + \alpha_{n^2+1} E = 0.$$

Por lo tanto, resulta que la matriz A es raíz del polinomio no nulo

$$\varphi(\lambda) = \alpha_0 \lambda^{n^2} + \alpha_1 \lambda^{n^2-1} + \ldots + \alpha_{n^2} \lambda + \alpha_{n^2+1},$$

cuyo grado no es superior a n^2.

La matriz A también es raíz de algunos polinomios cuyos coeficientes superiores son iguales a la unidad: es suficiente tomar cualquier polinomio distinto de cero que se anule por la matriz A, y dividirlo por su coeficiente superior. El polinomio de menor grado con el coeficiente superior igual a 1 que se anula por la matriz A, se llama *polinomio mínimo de la matriz A*. Obsérvese, que *el polinomio mínimo de la matriz A se determina unívocamente*, puesto que la diferencia de dos polinomios de éstos sería de menor grado que cada uno de los mismos y se anularía también por la matriz A.

Todo polinomio $f(\lambda)$ que se anula por la matriz A, es divisible por el polinomio mínimo $m(\lambda)$ de esta matriz.

En efecto, si

$$f(\lambda) = m(\lambda)\, q(\lambda) + r(\lambda),$$

donde el grado de $r(\lambda)$ es menor que el grado de $m(\lambda)$, se tiene

$$f(A) = m(A)\, q(A) + r(A)$$

y como $f(A) = m(A) = 0$, resulta, $r(A) = 0$, lo cual contradice a la definición del polinomio mínimo.

Demostremos ahora el siguiente **teorema**:

El polinomio mínimo de una matriz A coincide con el último factor invariante $e_n(\lambda)$ de la matriz característica $A - \lambda E$.

Demostración. Conservando las notaciones y aplicando los resultados del § 59, se puede escribir la igualdad

$$(-1)^n |A - \lambda E| = d_{n-1}(\lambda)\, e_n(\lambda). \qquad (1)$$

En particular, de aquí se deduce que los polinomios $e_n(\lambda)$ y $d_{n-1}(\lambda)$ no son nulos. Designemos ahora con $B(\lambda)$ la matriz adjunta a la matriz $A - \lambda E$ (véase el § 14),

$$B(\lambda) = (A - \lambda E)^*.$$

Como se deduce del § 14 (igualdad (3)), se cumple la igualdad

$$(A - \lambda E)\, B(\lambda) = |A - \lambda E|\, E. \qquad (2)$$

Por otra parte, como los menores de $(n-1)$*-ésimo orden de la* matriz $A - \lambda E$, tomados con los signos más o menos, y sólo éstos, son elementos de la matriz $B(\lambda)$, y el polinomio $d_{n-1}(\lambda)$ es el máximo común divisor de todos estos menores, se tiene:

$$B(\lambda) = d_{n-1}(\lambda)\, C(\lambda), \qquad (3)$$

en donde **el máximo común divisor de los elementos de la matriz** $C(\lambda)$ **es igual a 1.**

Pero, de las igualdades (2), (3) y (1), se deduce la igualdad

$$(A - \lambda E)\, d_{n-1}(\lambda)\, C(\lambda) = (-1)^n\, d_{n-1}(\lambda)\, e_n(\lambda)\, E.$$

Esta igualdad se puede simplificar por el factor no nulo $d_{n-1}(\lambda)$, lo cual se deduce de la siguiente observación general: si $\varphi(\lambda)$ es un polinomio no nulo, y $D(\lambda) = (d_{ij}(\lambda))$ es una λ-matriz no nula, donde suponemos que $d_{st}(\lambda) \not\equiv 0$, entonces, en la matriz $\varphi(\lambda)\, D(\lambda)$, en el lugar (s, t) figurará el elemento $\varphi(\lambda)\, d_{st}(\lambda)$, distinto de cero. Por lo tanto,

$$(A - \lambda E)\, C(\lambda) = (-1)^n\, e_n(\lambda)\, E,$$

de donde

$$e_n(\lambda)\, E = (\lambda E - A)\, [(-1)^{n+1}\, C(\lambda)] \qquad (4)$$

Esta igualdad muestra que el residuo de la división «a la izquierda» de la λ-matriz que figura en el primer miembro por el binomio $\lambda E - A$, es igual a cero. Sin embargo, del lema demostrado al final del § 60 se deduce que este residuo es igual a la matriz $e_n(A)\, E = e_n(A)$. En efecto, la matriz $e_n(\lambda)\, E$ se puede escribir en forma de un λ-polinomio matricial cuyos coeficientes son matrices escalares, o sea, son conmutables con la matriz A. Por lo tanto,

$$e_n(A) = 0,$$

o sea, **el polinomio** $e_n(\lambda)$ **verdaderamente se anula por la matriz** A.

De aquí se deduce, que el polinomio $e_n(\lambda)$ es divisible por el polinomio mínimo $m(\lambda)$ de la matriz A,

$$e_n(\lambda) = m(\lambda)\, q(\lambda). \qquad (5)$$

Está claro, que **el coeficiente superior del polinomio** $q(\lambda)$ **es igual a la unidad.**

Como $m(A) = 0$, de nuevo, en virtud del mismo lema del § 60, el residuo de la división «a la izquierda» de la λ-matriz $m(\lambda)\, E$ por el binomio $\lambda E - A$, es igual a cero, o sea,

$$m(\lambda)\, E = (\lambda E - A)\, Q(\lambda) \qquad (6)$$

Las igualdades (5), (4) y (6) nos llevan a la igualdad

$$(\lambda E - A)\,[(-1)^{n+1} C(\lambda)] = (\lambda E - A)\,[Q(\lambda)\, q(\lambda)].$$

Ambos miembros de esta igualdad se pueden simplificar por el factor común $\lambda E - A$, pues, el coeficiente superior E de este λ-polinomio matricial es una matriz no degenerada. Por lo tanto,

$$C(\lambda) = (-1)^{n+1} Q(\lambda)\, q(\lambda).$$

Recordemos, sin embargo, que el máximo común divisor de los elementos de la matriz $C(\lambda)$ es igual a 1. Por esto, el polinomio $q(\lambda)$ tiene que ser de grado cero, y como su coeficiente superior es igual a 1, resulta, $q(\lambda) = 1$. Por lo tanto, en virtud de (5),

$$e_n(\lambda) = m(\lambda),$$

que es lo que se quería demostrar.

Como, en virtud de (1), el polinomio característico de la matriz A es divisible por el polinomio $e_n(\lambda)$, del teorema que acabamos de demostrar se desprende el siguiente

Teorema de Hamilton-Cayley. *Toda matriz es raíz de su polinomio característico.*

Polinomio mínimo de una transformación lineal. Demostremos primero la siguiente proposición:

Si las matrices A y B son semejantes y la matriz A anula al polinomio $f(\lambda)$, entonces, la matriz B también anula al mismo.

En efecto, sea

$$B = C^{-1}AC.$$

Si

$$f(\lambda) = \alpha_0\lambda^k + \alpha_1\lambda^{k-1} + \ldots + \alpha_{k-1}\lambda + \alpha_k,$$

se tiene

$$\alpha_0 A^k + \alpha_1 A^{k-1} + \ldots + \alpha_{k-1}A + \alpha_k E = 0.$$

Transformando ambos miembros de esta igualdad con la matriz C, obtenemos:

$$C^{-1}(\alpha_0 A^k + \alpha_1 A^{k-1} + \ldots + \alpha_{k-1}A + \alpha_k E)\,C =$$
$$= \alpha_0 (C^{-1}AC)^k + \alpha_1 (C^{-1}AC)^{k-1} + \ldots + \alpha_{k-1}(C^{-1}AC) + \alpha_k E =$$
$$= \alpha_0 B^k + \alpha_1 B^{k-1} + \ldots + \alpha_{k-1}B + \alpha_k E = 0,$$

o sea, $f(B) = 0$.

De aquí se deduce, que *las matrices semejantes poseen un mismo polinomio mínimo.*

Supongamos ahora que φ es una transformación lineal del espacio lineal de n dimensiones sobre el campo P. Las matrices que determinan esta transformación en distintas bases del espacio, son seme-

jantes entre sí. El polinomio mínimo común de estas matrices se llama *polinomio mínimo de la transformación lineal* φ.

Aplicando las operaciones sobre las transformaciones lineales, introducidas en el § 32, se puede introducir el concepto de *valor* de un polinomio

$$f(\lambda) = \alpha_0\lambda^k + \alpha_1\lambda^{k-1} + \ldots + \alpha_{k-1}\lambda + \alpha_k$$

del anillo $P[\lambda]$ para λ, igual a una transformación lineal φ: este valor será la transformación lineal

$$f(\varphi) = \alpha_0\varphi^k + \alpha_1\varphi^{k-1} + \ldots + \alpha_{k-1}\varphi + \alpha_k\varepsilon,$$

donde ε es la transformación idéntica.

Diremos luego que la transformación lineal φ *anula* al polinomio $F(\lambda)$, si

$$f(\varphi) = \omega,$$

donde ω es la transformación nula.

Teniendo en cuenta la relación existente entre las operaciones sobre las transformaciones lineales y sobre las matrices, el lector demostrará sin dificultad alguna, que *el polinomio mínimo de una transformación lineal* φ *es el polinomio de menor grado con el coeficiente superior* 1, *determinado unívocamente, que se anula por la transformación* φ. Después de esto, los resultados obtenidos anteriormente y, en particular, el teorema de Hamilton-Cayley, se pueden enunciar de nuevo en términos de transformaciones lineales.

CAPITULO XIV

GRUPOS

§ 63. Definición y ejemplos de grupos

Los anillos y los cuerpos, que desempeñaron un papel tan grande en los capítulos anteriores, son sistemas algebraicos de dos operaciones independientes: adición y multiplicación. Sin embargo, en diversas ramas de las matemáticas y en sus aplicaciones, frecuentemente se encuentran tales sistemas algebraicos, en los que está definida una sola operación algebraica. Así, pues, limitándonos por ahora a los ejemplos que ya aparecieron en nuestro libro, señalemos, que en el conjunto de las sustituciones de grado n (véase el § 3), solamente habíamos definido una operación: la multiplicación. Por otra parte, en la definición del espacio vectorial (§ 8) está incluida la suma de vectores, mientras que el producto de vectores no había sido definido (señalemos, que el producto de un vector por un número no satisface a la definición de operación algebraica dada en el § 44).

Un tipo importante de sistemas algebraicos con una operación son los grupos. Este concepto posee un campo extraordinariamente amplio de aplicaciones y representa el objeto de una gran ciencia independiente, de la teoría de los grupos. El capítulo presente puede considerarse como introducción a la teoría de los grupos: en él se expondrán las nociones elementales sobre los grupos, cuyo conocimiento es necesario para cada matemático; el capítulo se terminará con la exposición de un teorema menos elemental.

De acuerdo a la teoría general de los grupos, convengamos en llamar *multiplicación* a la operación algebraica considerada y en emplear los símbolos correspondientes. Recordemos (véase el § 44), que **se supone que siempre es posible la operación algebraica, y que ésta es univalente:** para cualquier par de elementos a y b del conjunto considerado, existe el producto ab y representa un elemento unívocamente determinado de este conjunto.

Se llama *grupo* a un conjunto G con una operación algebraica, que es asociativa (aunque no necesariamente conmutativa), y para la que existe además la operación inversa.

Como la operación en el grupo puede ser no conmutativa, la existencia de la operación inversa significa lo siguiente: para cualquier par de elementos a y b de G, existe en G un elemento x y un elemento y, **unívocamente determinados**, tales que

$$ax = b, \quad ya = b.$$

Si el grupo G se compone de un número finito de elementos, se denomina *grupo finito*, y el número de sus elementos, se llama *orden* del grupo. Si la operación definida en el grupo es conmutativa, G se denomina grupo *conmutativo* o *abeliano*.

Señalemos las consecuencias elementales de la definición de grupo. Basándose en los razonamientos expuestos ya en el § 44, se puede afirmar que la ley asociativa nos permite hablar de un modo unívoco del *producto de un número finito cualquiera de elementos del grupo*, dados en un orden determinado (ya que la operación en el grupo puede ser no conmutativa).

Veamos las consecuencias de la existencia de la operación inversa.

Supongamos que en el grupo G se ha dado un elemento arbitrario a. De la definición del grupo se deduce la existencia en G de un elemento e_a, unívocamente determinado, tal que $ae_a = a$; por consiguiente, este elemento desempeña el papel de la unidad al multiplicar el elemento a por él a la derecha. Si b es otro elemento cualquiera del grupo G, y si y es el elemento del grupo que satisface a la igualdad $ya = b$, cuya existencia se deduce de la definición del grupo, se tiene:

$$b = ya = y(ae_a) = (ya)\,e_a = be_a.$$

Por lo tanto, el elemento e_a desempeña el papel de unidad a la derecha con respecto a todos los elementos del grupo G y no sólo con respecto al elemento inicial a; por eso, lo designaremos mediante e'. De la unicidad, que forma parte de la definición de la operación inversa, se deduce la unicidad de este elemento.

De este mismo modo se puede demostrar la existencia en G y la unicidad de un elemento e'' que satisfaga a la condición $e''a = a$ para todos los elementos a de G. En realidad, los elementos e' y e'' coinciden, puesto que de las igualdades $e''e' = e''$ y $e''e' = e'$ se deduce que $e'' = e'$. De esta manera, queda demostrado que *en cada grupo G existe un elemento e, unívocamente determinado, que satisface a la condición:*

$$ae = ea = a$$

para todos los elementos a de G. Este elemento se llama *unidad* del grupo G y se designa ordinariamente con el símbolo 1.

Para cada elemento dado a, de la definición del grupo se deduce, la existencia y unicidad de unos elementos a' y a'' tales, que

$$aa' = 1, \quad a''a = 1.$$

En la realidad, los elementos a' y a'' coinciden: de las igualdades

$$a''aa' = a''(aa') = a'' \cdot 1 = a'',$$
$$a''aa' = (a''a)\,a' = 1 \cdot a' = a',$$

se deduce que $a'' = a'$. Este elemento se llama *inverso* del elemento a y se designa con la notación a^{-1}, de modo que

$$aa^{-1} = a^{-1}a = 1.$$

Por lo tanto, *cada elemento del grupo posee un elemento inverso, unívocamente determinado.*

De las últimas igualdades se deduce, que el mismo elemento a sirve de inverso para el elemento a^{-1}. Es fácil observar también, que el inverso del producto de unos cuantos elementos es el producto de los elementos inversos de los factores y, además, tomados en orden inverso:

$$(a_1a_2 \ldots a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \cdots a_2^{-1}a_1^{-1}.$$

Por fin, el elemento inverso de la unidad es la unidad misma.

La prueba para averiguar si un conjunto dado con una operación es grupo o no, se facilita sumamente por el hecho de que en la definición de grupo la demanda del cumplimiento de la operación inversa se puede sustituir por la suposición de la existencia de la unidad y de los elementos inversos y, además, sólo por un lado (por ejemplo, por la derecha) y sin suponer la unicidad de ellos. Esto se deduce del siguiente **teorema:**

Un conjunto G con una operación asociativa es grupo, si en él existe por lo menos un elemento e que posee la propiedad:

$$ae = a \text{ para todos los elementos } a \text{ de } G,$$

y si entre todos los elementos unidades a la derecha existe por lo menos un elemento e_0 tal, que con respecto a él cada elemento a de G posee por lo menos un elemento inverso a la derecha a^{-1}:

$$aa^{-1} = e_0.$$

Demostración. Sea a^{-1} uno de los elementos inversos a la derecha de a. Entonces,

$$aa^{-1} = e_0 = e_0e_0 = e_0aa^{-1},$$

o sea, $aa^{-1} = e_0aa^{-1}$. Multiplicando a la derecha ambos miembros de esta igualdad por uno de los elementos que son inversos a la derecha de a^{-1}, obtenemos, $ae_0 = e_0\,ae_0$, de donde $a = e_0a$, puesto que e_0 es una unidad a la derecha de G. Por lo tanto, resulta que el elemento e_0 es también una unidad a la izquierda de G. Si ahora e_1 es una unidad a la derecha arbitraria y e_2 es una unidad a la izquierda

arbitraria, de las igualdades

$$e_2 e_1 = e_1 \text{ y } e_2 e_1 = e_2$$

se deduce que $e_1 = e_2$, o sea, que cualquier unidad a la derecha es igual a cualquier unidad a la izquierda. Queda, pues, demostrada la existencia y unicidad en el conjunto G del elemento unidad, que lo indicaremos, como anteriormente, mediante 1.

Luego,

$$a^{-1} = a^{-1} \cdot 1 = a^{-1} a a^{-1},$$

es decir, $a^{-1} = a^{-1} a a^{-1}$, donde a^{-1} es uno de los elementos inversos a la derecha de a. Multiplicando a la derecha ambos miembros de la *última igualdad por uno de los elementos inversos a la derecha* de a^{-1}, obtenemos, $1 = a^{-1} a$, o sea, que el elemento a^{-1} sirve también de elemento inverso a la izquierda de a. Si ahora a_1^{-1} es un elemento inverso a la derecha arbitrario de a, y a_2^{-1} es un elemento inverso a la izquierda arbitrario del mismo, de las igualdades

$$a_2^{-1} a a_1^{-1} = (a_2^{-1} a)\, a_1^{-1} = a_1^{-1},$$
$$a_2^{-1} a a_1^{-1} = a_2^{-1} (a a_1^{-1}) = a_2^{-1}$$

se deduce que $a_1^{-1} = a_2^{-1}$, es decir, se deduce la existencia y la unicidad, para cada elemento a de G, del elemento inverso a^{-1}.

Ahora es fácil mostrar que el conjunto G es grupo. En efecto, como bien se obverva, las ecuaciones $ax = b$, $ya = b$ se satisfacen con los elementos

$$x = a^{-1} b, \quad y = b a^{-1}.$$

La unicidad de estas soluciones se deduce de que si, por ejemplo, $ax_1 = ax_2$, multiplicando a la izquierda ambos miembros de esta igualdad por a^{-1}, obtenemos $x_1 = x_2$. El teorema queda demostrado.

Ya nos hemos encontrado unas cuantas veces con el concepto de isomorfismo: para los anillos, para los espacios lineales, para los espacios euclídeos. Este concepto puede ser definido también para los grupos y desempeña en la teoría de los mismos un papel tan importante como en la teoría de los anillos. Se dice que los grupos G y G' son *isomorfos*, si se puede establecer entre ellos una correspondencia biunívoca tal, que para cualquier par de elementos a y b de G y para sus correspondientes elementos a' y b' de G', al producto ab corresponde el producto $a'b'$. Del mismo modo que en el § 46 (para el cero y para el elemento opuesto del anillo), se puede demostrar que, en la correspondencia isomorfa de los grupos G y G', a la unidad del grupo G corresponde la unidad del grupo G', y si al elemento a de G le corresponde el elemento a' de G', al elemento a^{-1} le corresponderá el elemento a'^{-1}.

Pasando a examinar **ejemplos de grupos,** señalemos que, si la operación en el grupo se llamase *suma*, la unidad del grupo se llamaría *cero* y se indicaría con la notación 0, y en lugar de elemento inverso diríamos *elemento opuesto* y lo indicaríamos mediante $-a$.

Como primer ejemplo de grupo, anotemos que, *respecto a la suma, cualquier anillo* (*y, en particular, un cuerpo*) *representa un grupo, y además, abeliano*; éste es el llamado *grupo aditivo del anillo*. Esta observación proporciona inmediatamente una gran cantidad de ejemplos concretos de grupos, y entre ellos: el grupo aditivo de números enteros, el grupo aditivo de números pares, los grupos aditivos de números racionales, de números reales, de números complejos, etc, etc. Señalemos, que *los grupos aditivos de números enteros y de números pares son isomorfos entre sí*, a pesar de que el segundo forma sólo una parte del primero: la transformación que pone en correspondencia a cada número entero k el número par $2k$, es biunívoca y, como fácilmente se puede comprobar, representa una transformación isomorfa del primero de los grupos nombrados sobre el segundo.

Ningún anillo es grupo respecto a la multiplicación, puesto que no siempre se cumple la operación inversa, que es la división. No cambia el asunto al pasar de un anillo arbitrario a un cuerpo, puesto que en éste se mantiene sin cumplir la división por cero. Examinemos, sin embargo, el conjunto de todos los elementos del cuerpo diferentes de cero. Como el campo no contiene divisores de cero, es decir, que el producto de dos elementos diferentes de cero también es diferente de cero, la multiplicación representa una operación algebraica para el conjunto considerado, que es asociativa y conmutativa, siendo posible ya la división sin salir fuera de los límites de este conjunto. Por lo tanto, *el conjunto de todos los elementos diferentes de cero de cualquier campo representa un grupo abeliano*; éste se llama *grupo multiplicativo* del campo. Ejemplos concernientes a esto son: los grupos multiplicativos de números racionales, de números reales, de números complejos.

Es evidente que, respecto a la multiplicación, todos los números reales positivos forman grupo. *Este grupo es isomorfo al grupo aditivo de todos los números reales*: poniendo en correspondencia a cada número positivo a el número real $\ln a$, obtenemos una aplicación biyectiva del primero de los grupos sobre el segundo, que representa un isomorfismo en vista de la igualdad,

$$\ln (ab) = \ln a + \ln b.$$

Tomemos, ahora, en el campo de los números complejos, el conjunto de las raíces n-ésimas de la unidad. En el § 19 se había demostrado que el producto de dos raíces n-ésimas de la unidad, así como el número recíproco de la raíz n-ésima de la unidad, pertenecen al mismo conjunto considerado de números. Como la unidad también

pertenece, naturalmente, a este conjunto, y como la multiplicación de cualesquiera números complejos es asociativa y conmutativa, obtenemos que *las raíces n-ésimas de la unidad forman un grupo abeliano respecto a la multiplicación; este grupo es finito y de orden n. Por lo tanto, para cualquier número natural n, existen grupos finitos de orden n.*

El grupo (respecto a la multiplicación) de las raíces n-ésimas de la unidad es isomorfo al grupo aditivo del anillo Z_n construido en el § 45. En efecto, si ε es una raíz primitiva de orden n de la unidad, todos los elementos del primero de los grupos considerados tienen la forma ε^k, $k = 0, 1, \ldots, n-1$. Si ponemos en correspondencia a cada número ε^k el elemento C_k del anillo Z_n, o sea, la clase de números enteros cuyos residuos, al dividirlos por n, son iguales a k, obtenemos una correspondencia de isomorfismo entre los grupos considerados: si $0 \leqslant k \leqslant n-1$, $0 \leqslant l \leqslant n-1$ y si $k+l = nq + r$, donde $0 \leqslant r \leqslant n-1$, y q es igual a 0 ó a 1, entonces, $\varepsilon^k \cdot \varepsilon^l = \varepsilon^r$ y, a la vez, $C_k + C_l = C_r$.

Es oportuno señalar ahora unos cuantos ejemplos de conjuntos numéricos que no forman grupo. Así, el conjunto de todos los números enteros no forma grupo respecto a la multiplicación, el conjunto de todos los números reales positivos no forma grupo respecto a la suma, el conjunto de todos los números impares no forma grupo respecto a la suma, el conjunto de todos los números reales negativos no forma grupo respecto a la multiplicación. No representa dificultad alguna la comprobación de todas estas afirmaciones.

Naturalmente, todos los grupos numéricos examinados anteriormente son abelianos. Los espacios lineales sirven de ejemplos de grupos abelianos que no están formados por números: como se deduce de su definición (véase los §§ 29, 47), *todo espacio lineal sobre un cuerpo arbitrario P es grupo abeliano respecto a la operación de la suma.*

Veamos algunos ***ejemplos de grupos no conmutativos.***

El conjunto de todas las matrices de orden n sobre un campo P no representa grupo respecto a la operación de multiplicar, ya que no se cumple la condición de existencia del elemento inverso. Sin embargo, *si nos limitamos sólo a las matrices que no son degeneradas*, se obtiene ya un grupo. En efecto, como sabemos, el producto de dos matrices no degeneradas es una matriz no degenerada, la matriz unidad tampoco es degenerada, toda matriz no degenerada *posee matriz inversa, que tampoco es degenerada*, y, *por fin*, la ley asociativa, cumpliéndose para todas las matrices, se cumple, particularmente, para las matrices no degeneradas. Por consiguiente, se puede hablar del *grupo de las matrices no degeneradas de orden n sobre* el cuerpo P, tomando por operación en el grupo el producto de las matrices; este grupo no es conmutativo para $n \geqslant 2$.

El producto de sustituciones, definido en el § 3, da lugar a ejemplos muy importantes de grupos finitos no conmutativos. Ya sabemos que, en el conjunto de todas las sustituciones de grado n, la multiplicación representa una operación algebraica, que es, además, asociativa, aunque para $n \geqslant 3$ no es conmutativa; también sabemos que la sustitución idéntica E sirve de unidad en esta multiplicación y que para cualquier sustitución existe la sustitución inversa. Por lo tanto, *el conjunto de las sustituciones de grado n forma grupo respecto a la multiplicación, que es además finito y de orden n!*. Este se llama *grupo simétrico de grado n*, y para $n \geqslant 3$ no es conmutativo.

En lugar de examinar el conjunto de sustituciones de grado n, consideremos ahora solamente el conjunto de las sustituciones **pares**, compuesto, como ya sabemos, de $\frac{1}{2}n!$ elementos. Aplicando el teorema demostrado en el § 3, según el cual la paridad de la sustitución coincide con la paridad del número de trasposiciones que forman parte en cualquiera de las descomposiciones de esta sustitución en producto de trasposiciones, se obtiene, que *el producto de dos sustituciones pares es una sustitución par*; en efecto, la descomposición de AB en forma de un producto de trasposiciones se obtiene yuxtaponiendo las descomposiciones correspondientes de A y B. Ya se sabe que es asociativa la multiplicación de sustituciones; es evidente, que la sustitución idéntica es par. Por fin, es par la sustitución A^{-1}, si es par la sustitución A; esto es debido aunque sólo sea al hecho de que las expresiones de estas sustituciones se pueden obtener una de otra permutando de sitio las filas superior e inferior, o sea, que ellas contienen igual número de inversiones. Por consiguiente, *el conjunto de las sustituciones pares de n grado representa un grupo finito respecto a la multiplicación, de orden* $\frac{1}{2}n!$. Este se llama *grupo alternado de grado n*; es fácil comprobar que este grupo no es conmutativo para $n \geqslant 4$, a pesar de que es conmutativo para $n = 3$.

Los grupos simétrico y alternado desempeñan un gran papel en la teoría de los grupos finitos y también en la teoría de Galois. Señalemos que, por analogía con los grupos alternados, sería imposible construir con las sustituciones impares un grupo respecto a la multiplicación, puesto que el producto de dos sustituciones impares siempre es una sustitución par.

Las diversas ramas de la geometría proporcionan numerosos ejemplos de grupos distintos. Indiquemos un ejemplo sencillo de este género: el conjunto de todas las rotaciones de una esfera alrededor de su centro representa un grupo, pero no conmutativo, si es que llamamos producto de dos rotaciones al resultado de su realización consecutiva.

§ 64. Subgrupos

Un subconjunto A de un grupo G se llama *subgrupo* de éste si él mismo representa un grupo respecto a la operación definida en el grupo G.

Para verificar que el subconjunto A del grupo G forma un subgrupo de este grupo, es suficiente comprobar: 1) si contiene A el producto de dos elementos cualesquiera de A; 2) si contiene A, junto con cada uno de sus elementos, el elemento inverso. En efecto, del cumplimiento de la ley asociativa en el grupo G se deduce su cumplimiento para los elementos de A, y la pertenencia de la unidad del grupo G a A es consecuencia de 2) y 1).

Muchos de los grupos señalados en el párrafo anterior representan subgrupos de otros grupos indicados allí mismo. Así, el grupo aditivo de los números pares representa un subgrupo del grupo aditivo de los números enteros, y este último a su vez es un subgrupo del grupo aditivo de los números racionales. Todos estos grupos, como en general los grupos aditivos de números representan subgrupos del grupo aditivo de los números complejos. El grupo multiplicativo de los números reales positivos representa un subgrupo del grupo multiplicativo de todos los números reales diferentes de cero. El grupo alternado de grado n es un subgrupo del grupo simétrico del mismo grado.

Subrayemos, que la condición que figura en la definición de subgrupo, de que **el subconjunto A del grupo G sea grupo respecto a la operación definida en el grupo G**, es esencial. Así, el grupo multiplicativo de los números reales positivos **no representa** un subgrupo del grupo aditivo de todos los números reales, a pesar de que el primer conjunto está contenido en el segundo como subconjunto.

Si en el grupo G se han tomado los subgrupos A y B, su intersección $A \cap B$, es decir, el conjunto de los elementos pertenecientes a A y a B, también es un subgrupo del grupo G.

En efecto, si los elementos x e y pertenecen a la intersección $A \cap B$, estos pertenecen al subgrupo A, y por eso, el producto xy y el elemento inverso x^{-1} también pertenecen a A. Por las mismas razones, los elementos xy y x^{-1} pertenecen también al subgrupo B, y por eso, éstos pertenecen también a $A \cap B$.

Como fácilmente se ve, el resultado obtenido no sólo es justo para dos grupos, sino que también lo es para un número cualquiera de subgrupos, finito e incluso infinito.

El subconjunto del grupo G formado por el solo elemento 1, representa, evidentemente, un subgrupo de este grupo; este subgrupo, que está contenido en cualquier otro subgrupo del grupo G, se llama *subgrupo unidad* del grupo G. Por otra parte, el mismo grupo G representa uno de sus subgrupos.

Los llamados **subgrupos cíclicos** sirven de ejemplos interesantes de subgrupos. Introduzcamos primero el concepto de **potencia** de un elemento a de un grupo G. Siendo n un número natural arbitrario, el producto de n elementos iguales al elemento a se llama *potencia* del elemento a de grado n y se indica mediante a^n. Las *potencias negativas* del elemento a se pueden determinar, bien como elementos del grupo G, inversos a las potencias positivas de este elemento, o bien como el producto de unos cuantos factores, iguales al elemento a^{-1}. En la realidad, estas definiciones coinciden:

$$(a^n)^{-1} = (a^{-1})^n, \quad n > 0. \tag{1}$$

Para la demostración, es suficiente tomar el producto de $2n$ factores, de los cuales, los n primeros sean iguales a a y los demás, a a^{-1}, y efectuar todas las simplificaciones. El elemento igual a ambos miembros de la igualdad (1), se indicará mediante a^{-n}. Convengamos, por fin, en entender por la *potencia cero* a^0 del elemento a, el elemento **1**.

Obsérvese, que si la operación en el grupo G se llama suma, en lugar de las potencias del elemento a se debe hablar de los *múltiplos* de este elemento, escribiéndolos mediante ka.

Fácilmente se comprueba que en cualquier grupo G, para las potencias de cualquier elemento a con cualesquiera exponentes m y n, positivos, negativos o ceros, se verifican las igualdades:

$$a^n \cdot a^m = a^m \cdot a^n = a^{n+m}, \tag{2}$$

$$(a^n)^m = a^{nm}. \tag{3}$$

Designemos con $\{a\}$ el subconjunto del grupo G formado por todas las potencias del elemento a; el mismo elemento a también está incluido en él, representando la primera potencia. *El subconjunto* $\{a\}$ *es un subgrupo del grupo* G: el producto de elementos de $\{a\}$ pertenece a $\{a\}$, en virtud de (2); el elemento 1, igual a a^0, pertenece a $\{a\}$ y, por fin, $\{a\}$ junto con cada elemento suyo contiene al elemento inverso, puesto que de (3) se deduce la igualdad

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

El subgrupo $\{a\}$ se llama *subgrupo cíclico del grupo* G, *engendrado por el elemento* a. Como muestra la igualdad (2), este subgrupo siempre es conmutativo, incluso cuando el mismo grupo G no sea conmutativo.

Señalemos, que anteriormente no se había afirmado nunca que todas las potencias del elemento a son diferentes elementos del grupo. Si esto es verdaderamente así, entonces a se llama *elemento de orden infinito*. Sin embargo, supongamos que entre las potencias del elemento a haya algunas iguales, por ejemplo, $a^k = a^l$ siendo $k \neq l$; esto siempre tiene lugar en el caso de grupos finitos, pero puede

ocurrir también en un grupo infinito. Si $k > l$, se tiene

$$a^{k-l} = 1,$$

es decir, existen potencias **positivas** del elemento a que son iguales a la unidad. Supongamos que n es la potencia positiva menor del elemento a, que es igual a la unidad, o sea, que

$$1)\ a^n = 1, \quad n > 0,$$

$$2)\ \text{si } a^k = 1, \quad k > 0, \text{ entonces } k \geqslant n.$$

En este caso, se dice que a es un *elemento de orden finito*, precisamente, *de orden n*.

Es fácil observar que, si el elemento a es de orden finito n, todos los elementos

$$1,\ a,\ a^2,\ \ldots,\ a^{n-1} \tag{4}$$

son diferentes. *Cualquiera otra potencia del elemento a, positiva o negativa, es igual a uno de los elementos* (4). En efecto, si k es un número entero arbitrario, dividiéndolo por n se obtiene:

$$k = nq + r, \quad 0 \leqslant r < n,$$

y, por eso, en virtud de (2) y (3),

$$a^k = (a^n)^q \cdot a^r = a^r. \tag{5}$$

De esto se deduce que, *si el elemento a es de orden finito n y* $a^k = 1$, *entonces k se divide por n*. Por otra parte, como

$$-1 = n(-1) + (n-1),$$

para el elemento a de orden finito n,

$$a^{-1} = a^{n-1}.$$

Como el sistema (4) contiene n elementos, de los resultados obtenidos anteriormente se deduce que, *para un elemento a que tiene orden finito, su orden n coincide con el orden (o sea, con el número de los elementos) del subgrupo cíclico* $\{a\}$.

Señalemos, por fin, que todo grupo posee un elemento único de primer orden: éste es el elemento 1. Es evidente, que el subgrupo cíclico $\{1\}$ coincide con el subgrupo unidad.

Grupos cíclicos. Un grupo G se llama *cíclico* si se compone de las potencias de uno de sus elementos a, es decir, que coincide con uno de sus subgrupos cíclicos $\{a\}$; en este caso, a se llama *elemento generador* del grupo G. Es evidente, que todo grupo cíclico es abeliano.

El grupo aditivo de los números enteros sirve de ejemplo de grupo cíclico infinito, pues todo número entero es múltiplo de 1, es decir, que este número es el elemento generador del grupo considerado; se podría tomar también como elemento generador el número —1.

El grupo multiplicativo de las raíces de grado n de la unidad sirve de ejemplo de grupo finito cíclico de orden n, pues, como se había mostrado en el § 19, todas estas raíces son potencias de una de ellas, que es, precisamente, la raíz primitiva.

El teorema que sigue muestra que, con estos ejemplos se agotan en la realidad todos los grupos cíclicos:

Todos los grupos cíclicos infinitos son isomorfos entre sí; son isomorfos entre sí también todos los grupos cíclicos finitos de un orden dado n.

En efecto, resulta una aplicación biyectiva del grupo cíclico infinito, con el elemento generador a, sobre el grupo aditivo de los números enteros, al hacer corresponder a cada elemento a^k del primer grupo el número k; esta aplicación representa un isomorfismo, puesto que de acuerdo a (2), al multiplicar las potencias del elemento a se suman los exponentes. Si se da un grupo cíclico finito G de orden n, con el elemento generador a, entonces designando con ε una raíz primitiva de grado n de la unidad asociamos a cada elemento a^k del grupo G el número ε^k, $0 \leqslant k < n$. Esto representa una aplicación biyectiva del grupo G sobre el grupo multiplicativo de las raíces de grado n de la unidad, cuyo isomorfismo se deduce de (2) y (5).

Este teorema da la posibilidad de hablar simplemente del *grupo cíclico infinito*, o bien del *grupo cíclico de orden n*.

Demostremos ahora el **teorema** siguiente:

Todo subgrupo de un grupo cíclico es cíclico.

En efecto, sea $G = \{a\}$ un grupo cíclico con el elemento generador a, finito o infinito, y sea A un subgrupo del grupo G. Se puede suponer que A es diferente del subgrupo unidad, pues, en caso contrario, no habría que demostrar nada. Supongamos que a^k es la potencia positiva mínima del elemento a, contenida en A; tal potencia existe, puesto que si A contiene el elemento a^{-s}, $s > 0$, diferente de 1, contiene también el elemento a^s, inverso de él. Supongamos que A contiene también al elemento a^l, $l \neq 0$, y que l no es divisible por k. Entonces, si $d = (k, l)$, $d > 0$, es el máximo común divisor de los números k y l, existen unos números enteros u y v tales, que

$$ku + lv = d,$$

y por eso, el subgrupo A tiene que contener al elemento

$$(a^k)^u \cdot (a^l)^v = a^d,$$

pero como por la hipótesis $d < k$, llegamos a una contradicción con la elección del elemento a^k. Con esto, queda demostrado que $A = \{a^k\}$.

Descomposición de un grupo en clases con relación a un subgrupo. Tomando en el grupo G los subconjuntos M y N, por *producto MN de ellos* se entiende el conjunto de los elementos del grupo G que se

pueden representar, aunque sólo sea de un modo, en forma de un producto de un elemento de M por un elemento de N. Del cumplimiento de la ley asociativa para la operación en el grupo se deduce *su cumplimiento para la multiplicación de los subconjuntos del grupo*:

$$(MN)P = M(NP).$$

Naturalmente, uno de los conjuntos M, N puede estar compuesto de un solo elemento a. En este caso, se obtiene *el producto aN del elemento por el conjunto o el producto Ma del conjunto por el elemento.*

Supongamos que en el grupo G se ha dado un subgrupo arbitrario A. Si x es un elemento cualquiera de G, el producto xA se llama *clase adjunta a la izquierda del subgrupo A en el grupo G, engendrada por el elemento x**. Es comprensible, que *el elemento x está contenido en la clase adjunta xA*, puesto que el subgrupo A contiene la unidad, y $x \cdot 1 = x$.

Toda clase adjunta a la izquierda es engendrada por cualquiera de sus elementos, es decir, que si el elemento y pertenece a la clase adjunta xA, entonces,

$$yA = xA. \tag{6}$$

En efecto, y se puede representar en la forma

$$y = xa,$$

donde a es un elemento del subgrupo A. Por eso, para cualesquiera elementos a' y a'' de A, se tiene

$$ya' = x(aa'),$$
$$xa'' = y(a^{-1}a''),$$

con lo que queda demostrada la igualdad (6).

De esto se deduce que *dos clases adjuntas a la izquierda cualesquiera del subgrupo A en el grupo G, o coinciden, o no tienen ningún elemento común*. En efecto, si las clases adjuntas xA e yA contienen un elemento común z, se tiene:

$$xA = zA = yA.$$

Por lo tanto, todo el grupo G se descompone en clases adjuntas a la izquierda, disjuntas respecto al subgrupo A. Esta descomposición se llama *descomposición del grupo G en clases a la izquierda respecto del subgrupo A*.

Adviértase que una de las clases adjuntas a la izquierda de esta descomposición coincide con el mismo subgrupo A; esta clase está

* A veces, se llama clase de restos, clase residual o simplemente clase y también cogrupo. Para evitar confusiones, advirtamos, que un cogrupo nunca es un subgrupo, a excepción del cogrupo engendrado por el elemento unidad (o por cualquier elemento del subgrupo A) que coincide con el mismo subgrupo A. (*Nota del T.*).

engendrada por el elemento 1, o, en general, por cualquier elemento a de A, puesto que

$$aA = A.$$

Es obvio, que llamando al producto Ax *clase adjunta a la derecha del subgrupo* A *en el grupo* G, *engendrada por el elemento* x, de modo análogo obtendríamos la *descomposición a la derecha del grupo* G *respecto del subgrupo* A. Naturalmente, para un grupo abeliano, ambas descomposiciones, a la izquierda o a la derecha, respecto de cualquier subgrupo coinciden, es decir, se puede hablar simplemente de la *descomposición del grupo respecto del subgrupo.*

Así, pues, la descomposición del grupo aditivo de los números enteros con respecto del subgrupo de los números que son múltiplos del número k, se compone de k clases residuales distintas, engendradas por los números 0, 1, 2, . . ., $k-1$, respectivamente. En este caso, en la clase residual, engendrada por el número l, $0 \leqslant l \leqslant k-1$, están comprendidos todos los números que al ser divididos por k dan el resto l.

Cuando el grupo no es conmutativo, sus descomposiciones respecto de un subgrupo pueden ser distintas.

Veamos, por ejemplo, el grupo simétrico de 3er grado S_3, donde, de acuerdo al § 3, se escribirán sus elementos mediante ciclos. Tomemos en calidad de subgrupo A el subgrupo cíclico engendrado por el elemento (12); este subgrupo consta de la sustitución idéntica y de la sustitución (12) misma. Las otras clases adjuntas a la izquierda son: la clase $(13)\cdot A$, que se compone de las sustituciones (13) y (132) y la clase $(23)\cdot A$, que se compone de las sustituciones (23) y (123). Por otra parte, las clases adjuntas a la derecha relativas al subgrupo A son: el mismo subgrupo A, la clase $A\cdot(13)$, compuesta de las sustituciones (13) y (123), y la clase $A\cdot(23)$, compuesta de las sustituciones (23) y (132). Vemos, pues, que en este caso, la descomposición en clases a la derecha se diferencia de la descomposición en clases a la izquierda.

En el caso de grupos finitos, la existencia de descomposiciones de un grupo en clases respecto de un subgrupo nos lleva al siguiente teorema importante:

Teorema de Lagrange. *En todo grupo finito, el orden de cualquier subgrupo es un divisor del orden del mismo grupo.*

En efecto, supongamos que en el grupo finito G de orden n se haya dado un subgrupo A de orden k. Consideremos la descomposición del grupo G en clases a la izquierda respecto del subgrupo A. Supongamos que ésta consta de j clases; el número j se llama *índice* del subgrupo A en el grupo G. Cada clase adjunta a la izquierda xA consta de k elementos, exactamente, puesto que si

$$xa_1 = xa_2,$$

donde a_1 y a_2 son elementos de A, entonces, $a_1 = a_2$. Por lo tanto,

$$n = kj, \tag{7}$$

que es lo que se quería demostrar.

Como el orden de un elemento coincide con el orden de su subgrupo cíclico, del teorema de Lagrange se deduce que *el orden de cada elemento de un grupo finito es divisor del orden del grupo.*

Del teorema de Lagrange se deduce también, que *todo grupo finito, cuyo orden es un número primo, es cíclico.* En efecto, este grupo tiene que coincidir con el subgrupo cíclico engendrado por cualquiera de sus elementos, diferente de la unidad. En virtud de la descripción obtenida anteriormente de los grupos cíclicos, resulta que, *para cualquier número primo p, existe solamente un grupo finito de orden p, salvo un isomorfismo.*

§ 65. Divisores normales, grupo cociente, homomorfismos

Un subgrupo A de un grupo G se llama *divisor normal* de este grupo (o *subgrupo invariante**), si la descomposición del grupo G en clases a la izquierda respecto del subgrupo A coincide con la descomposición correspondiente a la derecha.

Por lo tanto, todos los subgrupos de un grupo abeliano son divisores normales del mismo. Por otra parte, en cualquier grupo G, el subgrupo unidad y el grupo mismo son divisores normales: ambas descomposiciones del grupo G en clases respecto del subgrupo unidad coinciden con la descomposición del grupo en elementos separados, ambas descomposiciones del grupo G en clases con respecto de este mismo grupo constan de una sola clase G.

Señalemos unos ejemplos más interesantes de divisores normales en grupos no conmutativos. En el grupo simétrico de 3er grado S_3, el subgrupo cíclico del elemento (123), que consta de la sustitución idéntica y de las sustituciones (123) y (132), representa un divisor normal: en ambas descomposiciones del grupo S_3 en clases con respecto de este subgrupo, la segunda clase adjunta consta de las sustituciones (12), (13) y (23).

En general, en el grupo simétrico S_n de grado n, el grupo alternado A_n de grado n es un divisor normal. En efecto, el orden del grupo A_n es igual a $\frac{1}{2}n!$, por lo cual, cada clase adjunta del subgrupo A_n en el grupo S_n tiene que estar constituida de la misma cantidad de elementos y, por consiguiente, solamente existe una clase más de éstas, que es precisamente el conjunto de las sustituciones impares.

En el grupo multiplicativo de las matrices cuadradas no degeneradas de orden n, cuyos elementos pertenecen al cuerpo P, las matri-

* También se llama *subgrupo normal*, o *subgrupo distinguido*. (*Nota del T.*).

ces, cuyos determinantes son iguales a 1, forman, evidentemente, un subgrupo. Este es, incluso, un divisor normal, puesto que las clases adjuntas a la derecha y a la izquierda de este subgrupo, engendradas por la matriz M, representan, tanto una como otra, la clase de todas las matrices, cuyos determinantes son iguales al determinante de la matriz M: es suficiente recordar que al multiplicar las matrices se multiplican sus determinantes.

A la definición de divisor normal expuesta anteriormente se le puede dar la forma siguiente:

Un subgrupo A de un grupo G se llama divisor normal de este grupo, si para cada elemento x de G

$$xA = Ax, \tag{1}$$

es decir, que para cada elemento x de G y para cada elemento a de A, se pueden elegir en A unos elementos a' y a'' tales que

$$xa = a'x, \quad ax = xa''. \tag{2}$$

Se pueden indicar también otras definiciones de divisor normal, equivalentes a la inicial. Así, llamaremos *conjugados* a los elementos a y b del grupo G, si existe en G al menos un elemento x tal, que

$$b = x^{-1}ax; \tag{3}$$

suele decirse que b es el elemento *transformado* del elemento a mediante (o por) el elemento x. Es evidente, que de (3) se deduce la igualdad

$$a = xbx^{-1} = (x^{-1})^{-1}\, bx^{-1}.$$

Un subgrupo A del grupo G es un divisor normal de éste cuando, y sólo cuando, junto con cada uno de sus elementos a contiene también a todos los elementos conjugados del mismo en G.

En efecto, si A es un divisor normal en G, entonces, en virtud de (2), para un elemento elegido a de A y para cualquier elemento x de G, se puede hallar en A un elemento a'' tal, que

$$ax = xa''.$$

De aquí que

$$x^{-1}ax = a'',$$

es decir, que cada elemento conjugado con a pertenece a A. Recíprocamente, si el subgrupo A, junto con cada uno de sus elementos a, contiene también todos los elementos conjugados con él, entonces, A contiene, en particular, al elemento

$$x^{-1}ax = a'',$$

de donde se deduce la segunda de las igualdades (2). Por la misma causa, A contiene también al elemento

$$(x^{-1})^{-1}\, ax^{-1} = xax^{-1} = a',$$

de donde se deduce la primera de las igualdades (2).

Aplicando este resultado, es fácil demostrar que *la intersección de cualesquiera divisores normales del grupo G también es un divisor normal de este grupo.* En efecto, si A y B son divisores normales del grupo G, entonces, como se ha mostrado en el párrafo anterior, la intersección $A \cap B$ representa un subgrupo del grupo G. Sea c un elemento cualquiera de $A \cap B$ y sea x un elemento cualquiera del grupo G. Entonces, el elemento $x^{-1}cx$ tiene que pertenecer tanto a A como a B, puesto que ambos divisores normales contienen al elemento c. De aquí se deduce, que el elemento $x^{-1}cx$ pertenece a la intersección $A \cap B$.

Grupo cociente (o grupo factor) *. La importancia del concepto de divisor normal se debe a que, de un modo muy natural, con las clases adjuntas relativas a un divisor normal (en virtud de (1), se puede no hacer distinción entre las clases adjuntas a la izquierda y a la derecha), se puede formar un nuevo grupo.

Obsérvese primero, que si A es un subgrupo arbitrario de un grupo G, se tiene,

$$AA = A, \tag{4}$$

pues, el producto de dos elementos cualesquiera del subgrupo A pertenece a A y, por otra parte, multiplicando todos los elementos de A por la unidad, se obtiene ya todo el subgrupo A.

Supongamos ahora que A sea un divisor normal del grupo G. *En este caso, el producto de dos clases adjuntas cualesquiera, relativas al subgrupo A* (en el sentido de multiplicación de subconjuntos del grupo G), *representa también una clase adjunta respecto de A*. En efecto, aplicando la ley asociativa del producto de subconjuntos del grupo, la igualdad (4) y la igualdad

$$yA = Ay$$

(compárese con (1)), entonces, para cualesquiera elementos x e y del grupo G, obtenemos:

$$xA \cdot yA = xyAA = xyA. \tag{5}$$

La igualdad (5) muestra que, para hallar el producto de dos clases adjuntas dadas del divisor normal A en el grupo G, se deben elegir en estas clases sendos **representantes** de un modo arbitrario (recordemos, que toda clase adjunta es engendrada por uno cualquiera de sus elementos) y se debe tomar la clase que contenga al producto de estos representantes.

* A pesar de que el autor emplea solamente la denominación de grupo factor, sin embargo, a continuación, utilizaremos la denominación de grupo cociente, que es más corriente en castellano y que, por cierto, designa lo mismo. Véase la versión castellana de la obra de Birkhoff y MacLane «Algebra Moderna», traducida por R. Rodríguez Vidal, Editorial Teide, Barcelona, pág. 171. (*Nota del. T.*).

De este modo, en el conjunto de todas las clases adjuntas del divisor normal A en el grupo G, se ha definido una operación de multiplicar. Demostremos que, *en este caso, se cumplen todas las condiciones inherentes a la definición de grupo.* En efecto, la asociatividad de la multiplicación de las clases adjuntas se deduce de la asociatividad de la multiplicación de los subconjuntos del grupo. El papel de la unidad lo desempeña el mismo divisor normal A, que representa una clase adjunta en la descomposición de G respecto de A: precisamente, en virtud de (4) y (1), para cualquier x de G, se tiene:

$$xA \cdot A = xA, \quad A \cdot xA = xAA = xA.$$

Finalmente, el inverso para la clase adjunta xA es la clase adjunta $x^{-1}A$, pues,

$$xA \cdot x^{-1}A = 1 \cdot A = A.$$

El grupo que hemos formado se denomina *grupo cociente* del grupo G por el divisor normal A y se designa con la notación G/A.

Vemos, pues, que con cada grupo se asocia toda una serie de grupos nuevos: sus grupos cocientes por diversos divisores normales. Es comprensible que, en este caso, el grupo cociente del grupo G por el subgrupo unidad es isomorfo al mismo grupo G.

Todo grupo cociente G/A de un grupo abeliano G es también abeliano, puesto que de $xy = yx$ se deduce que

$$xA \cdot yA = xyA = yxA = yA \cdot xA.$$

Todo grupo cociente G/A de un grupo cíclico G es también cíclico, puesto que si G es engendrado por el elemento g, $G = \{g\}$, y si se ha dado una clase adjunta arbitraria xA, existe un número entero k tal, que

$$x = g^k$$

y por eso,

$$xA = (gA)^k.$$

El orden de cualquier grupo cociente G/A de un grupo finito G es un divisor del orden del grupo mismo. En efecto, el orden del grupo cociente G/A es igual al índice del divisor normal A en el grupo G y, por eso, se puede aplicar la igualdad (7) del párrafo anterior.

Veamos unos cuantos **ejemplos de grupos cocientes.** Como en el grupo aditivo de los números enteros, el subgrupo de los números que son múltiplos de un número natural k tiene el índice k (véase el párrafo anterior), el grupo cociente de nuestro grupo por este subgrupo es un grupo finito de orden k que, además, es cíclico, puesto que el mismo grupo considerado es cíclico.

El grupo cociente del grupo simétrico S_n de grado n por el grupo alternado A_n de grado n, es un grupo de 2^0 orden, que, como el número 2 es primo, representa un grupo cíclico (véase el final del párrafo precedente).

Anteriormente habían sido descritas las clases adjuntas en el grupo multiplicativo de las matrices no degeneradas de orden n, cuyos elementos pertenecen a un campo P, relativas al divisor normal formado por las matrices cuyos determinantes son iguales a 1. De esta descripción se deduce que el grupo cociente correspondiente es isomorfo al grupo multiplicativo de los números del campo P que son diferentes de cero.

Homomorfismos. Los conceptos de divisor normal y de grupo cociente están estrechamente ligados con la siguiente generalización del concepto de isomorfismo.

Una *aplicación* φ *de un grupo* G *sobre un grupo* G', que hace corresponder a cada elemento a de G un elemento unívocamente determinado $a' = a\varphi$ de G', se llama *homomorfismo de* G *sobre* G', si en esta aplicación cada elemento a' de G' sirve de imagen de cierto elemento a de G, $a' = a\varphi$, y si, para cualesquiera elementos a, b del grupo G,

$$(ab)\,\varphi = a\varphi \cdot b\varphi.$$

Es obvio, que si se requiriese además que la aplicación φ fuese biyectiva, obtendríamos la definición ya conocida de isomorfismo.

Si φ *es un homomorfismo del grupo* G *sobre el grupo* G' *y* 1 *y* a *son, respectivamente, la unidad y un elemento arbitrario del grupo* G, *siendo* $1'$ *la unidad del grupo* G', *se tiene*:

$$1\varphi = 1',$$

$$(a^{-1})\,\varphi = (a\varphi)^{-1}.$$

En efecto, si $1\varphi = e'$ y x' es un elemento arbitrario del grupo G', entonces existe en G un elemento x tal, que $x\varphi = x'$. De aquí que

$$x' = x\varphi = (x \cdot 1)\,\varphi = x\varphi \cdot 1\varphi = x' \cdot e'.$$

De un modo análogo

$$x' = e'x'$$

y, por consiguiente, $e' = 1'$.

Por otra parte, si $(a^{-1})\,\varphi = b'$, se tiene

$$1' = 1\varphi = (aa^{-1})\,\varphi = a\varphi \cdot (a^{-1})\,\varphi = a\varphi \cdot b'$$

y, de un modo análogo,

$$1' = b' \cdot a\varphi,$$

de donde $b' = (a\varphi)^{-1}$.

Llamemos *núcleo* del homomorfismo φ del grupo G sobre el grupo G' al conjunto de los elementos del grupo G, a los que en la aplicación φ corresponde la unidad $1'$ del grupo G'.

El núcleo de cualquier homomorfismo φ *del grupo* G *es un divisor normal del grupo* G.

En efecto, si los elementos a, b del grupo G pertenecen al núcleo del homomorfismo φ, o sea,

$$a\varphi = b\varphi = 1',$$

se tiene

$$(ab)\,\varphi = a\varphi \cdot b\varphi = 1' \cdot 1' = 1',$$

es decir, el producto ab también pertenece al núcleo del homomorfismo φ. Por otra parte, si $a\varphi = 1'$, se tiene

$$(a^{-1})\,\varphi = (a\varphi)^{-1} = 1'^{-1} = 1',$$

es decir, a^{-1} pertenece al núcleo del homomorfismo φ. Por fin, si $a\varphi = 1'$ y x es un elemento arbitrario del grupo G, entonces

$$(x^{-1}ax)\,\varphi = (x^{-1})\,\varphi \cdot a\varphi \cdot x\varphi = (x\varphi)^{-1} \cdot 1' \cdot x\varphi = 1'.$$

En resumen, tenemos que el núcleo del homomorfismo considerado representa un subgrupo del grupo G que, junto con cada uno de sus elementos, contiene también a los elementos conjugados; es, pues, un divisor normal.

Sea, ahora, A un divisor normal arbitrario del grupo G. Haciendo corresponder a cada elemento x del grupo G la clase adjunta xA, relativa al divisor normal A, a la que pertenece el mismo elemento, obtenemos una aplicación del grupo G sobre todo el grupo cociente G/A. De la definición de la multiplicación en el grupo G/A (véase (5)), se deduce que esta aplicación es un homomorfismo.

El homomorfismo obtenido se llama *homomorfismo natural* del grupo G sobre el grupo cociente G/A. Es evidente, que el mismo divisor normal A sirve de núcleo de este homomorfismo.

De aquí que *los divisores normales del grupo* G, *y sólo ellos, sirven de núcleos de homomorfismos de este grupo.* Este resultado se puede considerar como una definición más de divisor normal.

Resulta que con los grupos cocientes del grupo G se agotan todos los grupos sobre los que puede aplicarse el grupo G de un modo homomorfo, y con los homomorfismos naturales sobre sus grupos cocientes se agotan todos los homomorfismos del mismo. Precisando, se verifica el siguiente

Teorema de los homomorfismos. *Supongamos que se haya dado un homomorfismo* φ *del grupo* G *sobre el grupo* G' *y que* A *es el núcleo de este homomorfismo. Entonces, el grupo* G' *es isomorfo al grupo cociente* G/A, *y además, existe una aplicación isomorfa* σ *del primero de estos grupos sobre el segundo tal, que el resultado de la realización consecutiva de las aplicaciones* φ *y* σ *coincide con el homomorfismo natural del grupo* G *sobre el grupo cociente* G/A.

En efecto, sea x' un elemento arbitrario del grupo G', y x, un elemento tal del grupo G, que $x\varphi = x'$. Como para cualquier elemento a del núcleo A del homomorfismo φ se verifica la igualdad $a\varphi = 1'$, se tiene

$$(xa)\,\varphi = x\varphi \cdot a\varphi = x' \cdot 1' = x',$$

o sea, que todos los elementos de la clase adjunta xA se representan en φ por el elemento x'.

Por otra parte, si z es un elemento cualquiera del grupo G tal, que $z\varphi = x'$, se tiene

$$(x^{-1}z)\,\varphi = x^{-1}\varphi \cdot z\varphi = (x\varphi)^{-1} \cdot z\varphi = x'^{-1} \cdot x' = 1',$$

o sea, que $x^{-1}z$ pertenece al núcleo A del homomorfismo φ. Poniendo $x^{-1}z = a$, se tiene $z = xa$, o sea, el elemento z pertenece a la clase adjunta xA. Por consiguiente, reuniendo todos los elementos del grupo G que en el homomorfismo φ se transforman en un elemento fijado x' del grupo G', obtenemos exactamente la clase adjunta xA.

La correspondencia σ que asocia a cada elemento x' de G' la clase adjunta del grupo G relativa al divisor normal A, que consta de todos los elementos del grupo G, que en la aplicación φ tienen por imagen a x', es una aplicación biyectiva del grupo G' sobre el grupo G/A. Esta aplicación σ es un isomorfismo, puesto que si

$$x'\sigma = xA, \quad y'\sigma = yA,$$

o sea, si

$$x\varphi = x', \quad y\varphi = y',$$

entonces,

$$(xy)\,\varphi = x\varphi \cdot y\varphi = x'y',$$
$$(x'y')\,\sigma = xyA = xA \cdot yA = x'\sigma \cdot y'\sigma.$$

Finalmente, si x es un elemento arbitrario de G y $x\varphi = x'$, se tiene

$$(x\varphi)\,\sigma = x'\sigma = xA,$$

es decir, que en la realidad, la realización consecutiva del homomorfismo φ y del isomorfismo σ hace corresponder al elemento x la clase adjunta xA engendrada por él mismo. El teorema queda demostrado.

§ 66. Sumas directas de grupos abelianos

Queremos acabar este capítulo con un teorema de la teoría de los grupos más profundo que aquellas propiedades elementales de los grupos que se habían expuesto anteriormente. A saber, basándose en la descripción de los grupos cíclicos, ya conocida por el § 64,

obtendremos en el párrafo siguiente una *descripción completa de los grupos finitos abelianos.*

Como está convenido en la teoría de los grupos abelianos, para la operación en el grupo se empleará la forma de expresión aditiva: se hablará de la **suma** $a + b$ de los elementos a y b del grupo, del **subgrupo nulo** 0, de los **múltiplos** ka de cierto elemento a, etc, etc.

En este párrafo examinaremos una construcción, cuya exposición va a estar adaptada para los grupos abelianos, a pesar de que podría ser presentada a la vez para grupos cualesquiera (aunque no fuesen conmutativos). Esta construcción está dictada por los ejemplos que siguen. El plano, considerado como un espacio lineal real de dos dimensiones, representa un grupo abeliano respecto a la suma de vectores. En este plano, cualquier recta que pase por el origen de coordenadas es un subgrupo del grupo indicado. Si A_1 y A_2 son dos rectas de éstas, entonces, como se sabe, todo vector que parte del origen de coordenadas se representa unívocamente en forma de suma de sus proyecciones sobre las rectas A_1 y A_2. Análogamente, todo vector del espacio lineal de tres dimensiones se expresa unívocamente en forma de una suma de tres vectores que pertenecen a tres rectas dadas A_1, A_2, A_3, suponiendo que estas rectas no estén situadas en un plano.

Se dice que un grupo abeliano G es una *suma directa* de sus subgrupos $A_1, A_2, \ldots, A_k$,

$$G = A_1 + A_2 + \ldots + A_k, \tag{1}$$

si cada elemento x del grupo G se expresa, y además, **unívocamente**, en forma de una suma de elementos $a_1, a_2, \ldots, a_k$ tomados en los subgrupos $A_1, A_2, \ldots, A_k$, correspondientemente:

$$x = a_1 + a_2 + \ldots + a_k. \tag{2}$$

La expresión (1) se denomina *descomposición directa* del grupo G; los subgrupos A_i, $i = 1, 2, \ldots, k$, se llaman *sumandos directos* de esta descomposición, y el elemento a_i de (2), *componente* del elemento x en el sumando directo A_i de la descomposición (1), $i = 1, 2, \ldots, k$.

Si se ha dado una descomposición directa (1) *del grupo G, y si todos, o unos cuantos, sumandos directos* A_i *de esta descomposición están también descompuestos en una suma directa*

$$A_i = A_{i1} + A_{i2} + \ldots + A_{ik_i}, \quad k_i \geqslant 1, \tag{3}$$

entonces, el grupo G representa una suma directa de todos sus subgrupos

$$A_{ij}, \quad j = 1, 2, \ldots, k_i, \quad i = 1, 2, \ldots, k.$$

En efecto, para un elemento arbitrario x del grupo G existe una expresión (2) respecto a la descomposición directa (1), y para cada

En efecto, sea x' un elemento arbitrario del grupo G', y x, un elemento tal del grupo G, que $x\varphi = x'$. Como para cualquier elemento a del núcleo A del homomorfismo φ se verifica la igualdad $a\varphi = 1'$, se tiene

$$(xa)\,\varphi = x\varphi \cdot a\varphi = x' \cdot 1' = x',$$

o sea, que todos los elementos de la clase adjunta xA se representan en φ por el elemento x'.

Por otra parte, si z es un elemento cualquiera del grupo G tal, que $z\varphi = x'$, se tiene

$$(x^{-1}z)\,\varphi = x^{-1}\varphi \cdot z\varphi = (x\varphi)^{-1} \cdot z\varphi = x'^{-1} \cdot x' = 1',$$

o sea, que $x^{-1}z$ pertenece al núcleo A del homomorfismo φ. Poniendo $x^{-1}z = a$, se tiene $z = xa$, o sea, el elemento z pertenece a la clase adjunta xA. Por consiguiente, reuniendo todos los elementos del grupo G que en el homomorfismo φ se transforman en un elemento fijado x' del grupo G', obtenemos exactamente la clase adjunta xA.

La correspondencia σ que asocia a cada elemento x' de G' la clase adjunta del grupo G relativa al divisor normal A, que consta de todos los elementos del grupo G, que en la aplicación φ tienen por imagen a x', es una aplicación biyectiva del grupo G' sobre el grupo G/A. Esta aplicación σ es un isomorfismo, puesto que si

$$x'\sigma = xA, \quad y'\sigma = yA,$$

o sea, si

$$x\varphi = x', \quad y\varphi = y',$$

entonces,

$$(xy)\,\varphi = x\varphi \cdot y\varphi = x'y',$$

$$(x'y')\,\sigma = xyA = xA \cdot yA = x'\sigma \cdot y'\sigma.$$

Finalmente, si x es un elemento arbitrario de G y $x\varphi = x'$, se tiene

$$(x\varphi)\,\sigma = x'\sigma = xA,$$

es decir, que en la realidad, la realización consecutiva del homomorfismo φ y del isomorfismo σ hace corresponder al elemento x la clase adjunta xA engendrada por él mismo. El teorema queda demostrado.

§ 66. Sumas directas de grupos abelianos

Queremos acabar este capítulo con un teorema de la teoría de los grupos más profundo que aquellas propiedades elementales de los grupos que se habían expuesto anteriormente. A saber, basándose en la descripción de los grupos cíclicos, ya conocida por el § 64,

Un grupo abeliano G representa una suma directa de sus subgrupos $A_1, A_2, \ldots, A_k$ *cuando, y sólo cuando, el mismo es engendrado por estos subgrupos,*

$$G = \{A_1, A_2, \ldots, A_k\}, \tag{6}$$

y la intersección de cada subgrupo A_i, $i = 2, \ldots, k$, *con el subgrupo engendrado por todos los subgrupos anteriores* $A_1, A_2, \ldots, A_{i-1}$, *contiene solamente al cero,*

$$\{A_1, A_2, \ldots, A_{i-1}\} \cap A_i = 0, \quad i = 2, \ldots, k. \tag{7}$$

En efecto, si el grupo G posee una descomposición directa (1), entonces, **para cada elemento** x de G existe una expresión (2) y, por esto, se verifica la igualdad (6). El cumplimiento de la igualdad (7) es consecuencia de la **unicidad** de la expresión (2) para cualquier elemento x: si para cierto i, la intersección $\{A_1, A_2, \ldots, A_{i-1}\} \cap \cap A_i$ contuviese un elemento x no nulo, entonces, por una parte, x se podría expresar como un elemento a_i de A_i, o sea, $x = a_i$, y por eso,

$$x = 0 + \ldots + 0 + a_i + 0 + \ldots + 0; \tag{8}$$

por otra parte, x, como elemento del subgrupo $\{A_1, A_2, \ldots, A_{i-1}\}$ posee una expresión de la forma

$$x = a_1 + a_2 + \ldots + a_{i-1},$$

o sea,

$$x = a_1 + a_2 + \ldots + a_{i-1} + 0 + \ldots + 0. \tag{9}$$

Es evidente, que para el elemento x, (8) y (9) son dos expresiones distintas de la forma (2).

Recíprocamente, supongamos que se cumplen las igualdades (6) y (7). De (6) se deduce, que cualquier elemento x del grupo G posee por lo menos una expresión de la forma (2). Por otra parte, supongamos que para cierto elemento x existen dos expresiones distintas de la forma (2)

$$x = a_1 + a_2 + \ldots + a_k = a'_1 + a'_2 + \ldots + a'_k. \tag{10}$$

Entonces, se puede hallar tal i, $i \leqslant k$, que

$$a_k = a'_k, \quad a_{k-1} = a'_{k-1}, \ldots, a_{i+1} = a'_{i+1}, \tag{11}$$

pero

$$a_i \neq a'_i,$$

o sea,

$$a_i - a'_i \neq 0. \tag{12}$$

Sin embargo, de (9) y (11) se deduce la igualdad

$$a_i - a'_i = (a'_1 - a_1) + (a'_2 - a_2) + \ldots + (a'_{i-1} - a_{i-1}),$$

que, en virtud de (12), contradice a la igualdad (7). El teorema queda demostrado.

El concepto de suma directa se puede examinar de otro modo distinto. Sean dados k grupos abelianos arbitrarios $A_1, A_2, \ldots, A_k$, algunos de los cuales pueden ser isomorfos. Designemos con G el conjunto de todos los sistemas posibles de la forma

$$(a_1, a_2, \ldots, a_k), \tag{13}$$

formados por sendos elementos de los grupos $A_1, A_2, \ldots, A_k$. El conjunto G se convierte en un grupo abeliano, si la suma de los sistemas de la forma (13) se define por la regla:

$$(a_1, a_2, \ldots, a_k) + (a'_1, a'_2, \ldots, a'_k) = \\ = (a_1 + a'_1, a_2 + a'_2, \ldots, a_k + a'_k), \tag{14}$$

según la cual se suman los elementos de los grupos dados $A_1, A_2, \ldots, A_k$ por separado. En efecto, las leyes asociativa y conmutativa de esta suma se deducen del cumplimiento de estas leyes en cada uno de los grupos dados; el papel del cero lo desempeña el sistema

$$(0_1, 0_2, \ldots, 0_k),$$

donde mediante 0_i se señala el elemento nulo del grupo A_i, $i = 1, 2, \ldots, k$; el elemento opuesto para el sistema (13) es el sistema

$$(-a_1, -a_2, \ldots, -a_k).$$

El grupo abeliano G construido se llama *suma directa* de los grupos $A_1, A_2, \ldots, A_k$ y se designa, como anteriormente, mediante

$$G = A_1 + A_2 + \ldots + A_k.$$

La razón de esta denominación consiste en que *el grupo G, que representa una suma directa de los grupos $A_1, A_2, \ldots, A_k$ en el sentido que acabamos de definir, se puede descomponer en una suma directa de sus subgrupos $A'_1, A'_2, \ldots, A'_k$, que son isomorfos a los grupos $A_1, A_2, \ldots, A_k$, correspondientemente.*

Designemos, para esto, mediante A'_i, $i = 1, 2, \ldots, k$, el conjunto de los elementos del grupo G, o sea, de los sistemas de la forma (13), en los que en el lugar de i figura un elemento arbitrario a_i del grupo A_i, y en los demás lugares, los ceros de los grupos correspondientes; éstos son, por consiguiente, los sistemas de la forma

$$(0_1, \ldots, 0_{i-1}, a_i, 0_{i+1}, \ldots, 0_k). \tag{15}$$

La definición de la suma (14) muestra que el conjunto A'_i representa un subgrupo del grupo G; el isomorfismo de este subgrupo con el grupo A_i se obtiene haciendo corresponder a cada sistema (15) el elemento a_i del grupo A_i.

Queda por demostrar que el grupo G representa una suma directa de los subgrupos $A_1', A_2', \ldots, A_k'$. En efecto, cualquier elemento (13) del grupo G se puede representar en forma de una suma de elementos de los subgrupos indicados:

$$(a_1, a_2, \ldots, a_k) = (a_1, 0_2, \ldots, 0_k) + \\ + (0_1, a_2, 0_3, \ldots, 0_k) + \ldots + (0_1, 0_2, \ldots, 0_{k-1}, a_k).$$

La unicidad de esta representación se deduce de que diferentes sistemas de la forma (13) son **diferentes** elementos del grupo G.

Si se han dado dos sistemas de grupos abelianos, $A_1, A_2, \ldots, A_k$ y $B_1, B_2, \ldots, B_k$, y los grupos A_i y B_i, $i = 1, 2, \ldots, k$, son isomorfos, entonces los grupos

$$G = A_1 + A_2 + \ldots + A_k$$

y

$$H = B_1 + B_2 + \ldots + B_k$$

también son isomorfos.

En efecto, si para $i = 1, 2, \ldots, k$, se ha establecido un isomorfismo φ_i entre los grupos A_i y B_i que hace corresponder a cada elemento a_i de A_i el elemento $a_i\varphi_i$ de B_i, entonces es evidente, que la aplicación φ que a cada elemento $(a_1, a_2, \ldots, a_k)$ del grupo G asocia el elemento del grupo H determinado por la igualdad

$$(a_1, a_2, \ldots, a_k)\varphi = (a_1\varphi_1, a_2\varphi_2, \ldots, a_k\varphi_k),$$

es un isomorfismo que aplica al grupo G sobre el grupo H.

Si se han dado los grupos abelianos **finitos** $A_1, A_2, \ldots, A_k$, *cuyos órdenes correspondientes son $n_1, n_2, \ldots, n_k$, entonces la suma directa G de estos grupos es también un grupo finito y su orden n es igual al producto de los órdenes de los sumandos directos,*

$$n = n_1 n_2 \ldots n_k. \tag{16}$$

En efecto, el número de sistemas diversos de la forma (13), para cada uno de los cuales el elemento a_1 puede tomar n_1 valores distintos, el elemento a_2, toma n_2 valores distintos, etc. se determina por la igualdad (16).

Veamos unos cuantos **ejemplos.**

Si el orden n de un grupo cíclico finito $\{a\}$ se descompone en un producto de dos números naturales que son primos entre sí,

$$n = st, \ (s, t) = 1,$$

entonces, el grupo $\{a\}$ se descompone en una suma directa de dos grupos cíclicos, cuyos órdenes correspondientes son s y t.

Para el grupo $\{a\}$ emplearemos la expresión aditiva. Poniendo $b = ta$, se tiene

$$sb = (st)a = na = 0,$$

pero, para $0 < k < s$,

$$kb = (kt)\, a \neq 0,$$

es decir, el subgrupo cíclico $\{b\}$ tiene el orden s. Análogamente, el subgrupo cíclico $\{c\}$ del elemento $c = sa$ tiene el orden t. La intersección $\{b\} \cap \{c\}$ contiene sólo el cero, puesto que si $kb = lc$ para $0 < k < s$, $0 < l < t$, entonces

$$(kt)\, a = (ls)\, a,$$

y como los números kt y ls son menores que n, se tiene

$$kt = ls,$$

lo cual es imposible, ya que los números s y t son primos entre sí. Finalmente, existen unos números u y v tales, que

$$su + tv = 1,$$

y, por lo tanto,

$$a = v\,(ta) + u\,(sa) = vb + uc,$$

y, por consiguiente, cualquier elemento del grupo $\{a\}$ se puede representar como una suma de elementos de los subgrupos $\{b\}$ y $\{c\}$.

Llamaremos a un grupo abeliano G *indescomponible*, si no puede ser descompuesto en una suma directa de dos o de unos cuantos subgrupos, diferentes del subgrupo cero. Un grupo cíclico finito, cuyo orden es una potencia de un número primo p, se denomina grupo cíclico *primario* respecto al número primo p. Aplicando unas cuantas veces la proposición demostrada anteriormente, obtenemos, que *todo grupo cíclico finito se descompone en una suma directa de grupos cíclicos primarios, respecto a diversos números primos.* Más exactamente, *todo grupo cíclico de orden*

$$n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s},$$

donde $p_1, p_2, \dots, p_s$ *son números primos* **distintos**, *se descompone en una suma directa de s grupos cíclicos que tienen los órdenes* $p_1^{k_1}, p_2^{k_2}, \dots, p_s^{k_s}$, *respectivamente.*

Todo grupo cíclico primario es indescomponible.

En efecto, sea dado un grupo cíclico finito $\{a\}$ de orden p^k, donde p es un número primo. Si este grupo fuese descomponible, entonces, en virtud de (7), tendría subgrupos diferentes de cero, la intersección de los cuales sería igual a cero. Sin embargo, en la realidad, **todo subgrupo diferente de cero contiene el elemento diferente de cero**

$$b = p^{k-1} a.$$

Para la demostración, tomemos un elemento arbitrario x diferente de cero de nuestro grupo,

$$x = sa, \quad 0 < s < p^k.$$

El número s se puede escribir en la forma

$$s = p^l s', \quad 0 \leqslant l < k,$$

donde el número s' ya no es divisible por p y, por consiguiente, éstos son primos entre sí, debido a lo cual, existen unos números u y v tales, que

$$s'u + pv = 1.$$

Entonces,

$$(p^{k-l-1}u)\, x = (p^{k-l-1}us)\, a = (p^{k-1}us')\, a =$$
$$= p^{k-1}(1 - pv)\, a = (p^{k-1} - p^k v)\, a = p^{k-1}a - v(p^k a) = p^{k-1}a = b,$$

o sea, el elemento b pertenece al subgrupo cíclico $\{x\}$.

El grupo aditivo de los números enteros (o sea, el grupo cíclico infinito), y también el grupo aditivo de todos los números racionales, son grupos indescomponibles.

Esto se deduce de que en cada uno de estos grupos, para cualquier par de elementos diferentes de cero, existe un común múltiplo diferente de cero, es decir, dos subgrupos cíclicos cualesquiera, diferentes de cero, tienen una intersección diferente de cero.

Obsérvese que, si en el grupo abeliano G la operación se llama multiplicación, entonces, se debe hablar del *producto directo* y no de la suma directa.

El grupo multiplicativo de los números reales diferentes de cero se descompone en un producto directo del grupo multiplicativo de los números reales positivos y del grupo formado por los números 1 y -1, respecto a la multiplicación.

En efecto, a la intersección de los dos subgrupos indicados de nuestro grupo pertenece solamente el número 1, que es el elemento unidad de este grupo. Por otra parte, todo número positivo es igual al producto de sí mismo por el número 1, todo número negativo es igual al producto de su valor absoluto por el número -1.

§ 67. Grupos abelianos finitos

Tomando cualquier conjunto finito de grupos cíclicos primarios, algunos de los cuales pueden estar referidos a un mismo número primo, o incluso pueden tener un mismo orden, o sea, que pueden ser isomorfos, la suma directa de ellos representa un grupo abeliano finito. Resulta, que con esto se agotan todos los grupos abelianos finitos:

Teorema fundamental de los grupos abelianos finitos. *Todo grupo abeliano finito G que no es un grupo cero, se descompone en una suma directa de subgrupos cíclicos primarios.*

Comenzaremos la demostración de este teorema observando que *en el grupo G, indispensablemente, existen elementos diferentes de cero, cuyos órdenes son potencias de números primos.* En efecto, si un elemento x del grupo G, diferente de cero, tiene el orden l, $lx = 0$, y p^k, $k > 0$, es una potencia del número primero p tal, que el número l,

$$l = p^k m,$$

es divisible por ella, entonces, el elemento mx es diferente de cero y tiene el orden p^k.

Sean

$$p_1,\ p_2,\ \ldots,\ p_s \tag{1}$$

todos los números primos **diversos**, algunas de cuyas potencias sirven de órdenes de algunos elementos del grupo G. Designemos con p cualquiera de estos números, y con P, el conjunto de los elementos del grupo G, cuyos órdenes son potencias del número p.

El conjunto P representa un subgrupo del grupo G. En efecto, P contiene al elemento 0, ya que su orden es igual a $1 = p^0$. Por otra parte, si $p^k x = 0$, entonces, $p^k(-x) = 0$. Finalmente, si $p^k x = 0$, $p^l y = 0$, y si, por ejemplo, $k \geqslant l$, entonces,

$$p^k(x + y) = 0,$$

o sea, el orden del elemento $x + y$, o bien es el número p^k, o bien es un divisor de este número, es decir, es una potencia del número p.

Tomando, por p cada uno de los números (1), sucesivamente, obtenemos s subgrupos no nulos,

$$P_1,\ P_2,\ \ldots,\ P_s. \tag{2}$$

El grupo G es una suma directa de estos subgrupos,

$$G = P_1 + P_2 + \ldots + P_s \tag{3}$$

En efecto, si x es un elemento arbitrario del grupo G, su orden l sólo puede dividirse por ciertos números primos del sistema (1),

$$l = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s},$$

donde $k_i \geqslant 0$, $i = 1, 2, \ldots, s$. Por eso, como se había demostrado al final del párrafo anterior, el subgrupo cíclico $\{x\}$ se descompone en una suma directa de subgrupos cíclicos primarios que tienen los órdenes $p_1^{k_1}$, $p_2^{k_2}$, $\ldots$, $p_s^{k_s}$ respectivamente. Estos subgrupos cíclicos primarios pertenecen a los subgrupos (2) correspondientes y, por

consiguiente, el elemento x se representa en forma de una suma de elementos, tomados uno por uno en todos o en unos cuantos de los subgrupos (2). De este modo, queda demostrada la igualdad

$$G = \{P_1, P_2, \ldots, P_s\},$$

que es análoga a la igualdad (6) del párrafo anterior.

Para demostrar la igualdad, análoga a la igualdad (7) del mismo párrafo, tomemos cualquier i, $2 \leqslant i \leqslant s$. Entonces, cualquier elemento y del subgrupo $\{P_1, P_2, \ldots, P_{i-1}\}$ tiene la forma

$$y = a_1 + a_2 + \ldots + a_{i-1},$$

donde el elemento a_j, $j = 1, 2, \ldots, i-1$, pertenece al subgrupo P_j, es decir, tiene el orden $p_j^{k_j}$. Entonces,

$$(p_1^{k_1} p_2^{k_2} \ldots p_{i-1}^{k_{i-1}})\, y = 0,$$

o sea, el orden del elemento y es cierto divisor del número $p_1^{k_1} p_2^{k_2} \ldots p_{i-1}^{k_{i-1}}$ y, por consiguiente, el elemento y, si es diferente de cero, no puede pertenecer al subgrupo P_i. De este modo, queda demostrado, que

$$\{P_1, P_2, \ldots, P_{i-1}\} \cap P_i = 0,$$

que es lo que se quería demostrar.

Obsérvese que el grupo abeliano en el que los órdenes de todos los elementos son potencias de un mismo número primo p, se denomina *primario* respecto del número p. Los grupos cíclicos primarios son casos particulares de los grupos primarios. Por lo tanto, los subgrupos (2) son primarios. Estos se llaman *componentes primarios* del grupo G, y la descomposición directa (3), *descomposición de este grupo en componentes primarios*. Como los subgrupos (2) están determinados unívocamente en el grupo G, *la descomposición del grupo G en componentes primarios se determina unívocamente*.

Es comprensible, que la descomposición de todo grupo abeliano finito en una suma directa de grupos primarios **reduce la demostración del teorema fundamental al caso de un grupo abeliano finito primario P, respecto de cierto número primo p.** Examinemos este caso.

Sea a_1 uno de los elementos del grupo P que tienen en éste el orden máximo. Si, luego, existen en el grupo P elementos, diferentes de cero, las intersecciones de cuyos subgrupos cíclicos con el subgrupo cíclico $\{a_1\}$ son iguales a cero, entonces, mediante a_2 indicamos uno de los elementos de orden máximo entre los elementos que poseen esta propiedad; por lo tanto,

$$\{a_1\} \cap \{a_2\} = 0.$$

Supongamos que ya se han elegido los elementos $a_1, a_2, \ldots, a_{i-1}$. El subgrupo del grupo P, engendrado por sus subgrupos cíclicos, lo indicaremos mediante $\{a_1, a_2, \ldots, a_{i-1}\}$,

$$\{\{a_1\}, \{a_2\}, \ldots, \{a_{i-1}\}\} = \{a_1, a_2, \ldots, a_{i-1}\}. \tag{4}$$

Es evidente, que éste se compone de todos los elementos del grupo P que se pueden expresar en forma de una suma de elementos, múltiplos de los elementos $a_1, a_2, \ldots, a_{i-1}$; diremos que este subgrupo *está engendrado* por los elementos $a_1, a_2, \ldots, a_{i-1}$. Designemos ahora con a_i uno de los elementos de orden máximo entre los elementos del grupo P, las intersecciones de cuyos subgrupos cíclicos con el subgrupo $\{a_1, a_2, \ldots, a_{i-1}\}$ son iguales a cero; por lo tanto,

$$\{a_1, a_2, \ldots, a_{i-1}\} \cap \{a_i\} = 0. \tag{5}$$

Como el grupo P es finito, este proceso tendrá fin; supongamos que esto ocurre después de que se han elegido los elementos $a_1, a_2, \ldots, a_s$. Designando con P' el subgrupo engendrado por estos elementos,

$$P' = \{a_1, a_2, \ldots, a_s\},$$

o sea,

$$P' = \{\{a_1\}, \{a_2\}, \ldots, \{a_s\}\}, \tag{6}$$

se tiene que **el subgrupo cíclico engendrado por cualquier elemento del grupo P, diferente de cero, tiene con el subgrupo P' una intersección no nula.**

En virtud de (4), la igualdad (6) y la igualdad (5), que se verifican para $i = 2, 3, \ldots, s$, muestran que **el subgrupo P' es una suma directa de los subgrupos cíclicos** $\{a_1\}, \{a_2\}, \ldots, \{a_s\}$,

$$P' = \{a_1\} + \{a_2\} + \ldots + \{a_s\}. \tag{7}$$

Queda por demostrar que **el subgrupo P' coincide en la realidad con todo el grupo P.**

Sea x un elemento cualquiera del grupo P que tenga el orden p. Como

$$P' \cap \{x\} \neq 0,$$

y el subgrupo $\{x\}$ no tiene subgrupos no nulos, diferentes de sí mismo (recordemos, que el orden de un subgrupo es divisor del orden del grupo, y que el número p es primo), el subgrupo $\{x\}$ verdaderamente está contenido en el subgrupo P' y, por consiguiente, x pertenece a P'. Por lo tanto, todos los elementos de orden p del grupo P pertenecen al subgrupo P'.

Supongamos que ya está demostrado que al subgrupo P' pertenecen todos los elementos del grupo P, cuyos órdenes no son mayores que el número p^{k-1}, y sea x un elemento cualquiera de P de orden p^k.

Como muestra la elección de los elementos $a_1, a_2, \ldots, a_s$, el orden de éstos no va creciendo y, por esto, se puede señalar tal i, $1 \leqslant i - 1 \leqslant s$, que los órdenes de los elementos $a_1, a_2, \ldots, a_{i-1}$ son mayores o iguales a p^k, y para $i - 1 < s$, el orden del elemento a_i es estrictamente menor que este número, es decir, es menor que el orden del elemento x. En virtud de las condiciones a que está ajustada la elección del elemento a_i, de aquí se deduce que, si

$$Q = \{a_1, a_2, \ldots, a_{i-1}\},$$

entonces,

$$Q \cap \{x\} \neq 0.$$

Sin embargo, en el párrafo anterior se había demostrado que todo subgrupo no nulo de un grupo cíclico primario $\{x\}$ de orden p^k contiene el elemento

$$y = p^{k-1}x. \tag{8}$$

Por consiguiente, este elemento y pertenece a la intersección $Q \cap \cap \{x\}$, y, por lo tanto, al subgrupo Q. Esto da la posibilidad de expresar y en forma de una suma de elementos, múltiplos de los elementos $a_1, a_2, \ldots, a_{i-1}$:

$$y = l_1a_1 + l_2a_2 + \ldots + l_{i-1}a_{i-1}. \tag{9}$$

De (8) se deduce, que el elemento y tiene el orden p. Por eso,

$$(pl_1)\,a_1 + (pl_2)\,a_2 + \ldots + (pl_{i-1})\,a_{i-1} = 0,$$

o sea, que en virtud de la existencia de la descomposición directa (7),

$$(pl_j)\,a_j = 0, \qquad j = 1, 2, \ldots, i-1.$$

Por lo tanto, el número pl_j tiene que dividirse por el orden del elemento a_j, y por esto, también por el número p^k, de donde se deduce que l_j se divide por p^{k-1},

$$l_j = p^{k-1}m_j, \qquad j = 1, 2, \ldots, i-1. \tag{10}$$

Sea

$$z = m_1a_1 + m_2a_2 + \ldots + m_{i-1}a_{i-1}.$$

Este elemento pertenece al subgrupo Q y, por consiguiente, al subgrupo P'; además, en virtud de (9) y (10),

$$y = p^{k-1}z. \tag{11}$$

De (8) y (11) se deduce la igualdad

$$p^{k-1}(x - z) = 0,$$

es decir, que el orden del elemento

$$t = x - z$$

no es mayor que p^{k-1} y, por consiguiente, en virtud de la hipotesis de la inducción, t pertenece al subgrupo P'. Por esto, el elemento x, como suma de dos elementos de P', $x = z + t$, también pertenece al subgrupo P'. De este modo, queda demostrado que todos los elementos de orden p^k del grupo P pertenecen a P'. Por consiguiente, nuestra demostración por inducción da la posibilidad de afirmar que todos los elementos del grupo P pertenecen al subgrupo P', o sea, que $P' = P$. La demostración del teorema fundamental está terminada.

Como resultado complementario, obtenemos que *un grupo abeliano finito es primario respecto al número primo p, cuando, y sólo cuando, su orden es una potencia de este número p.* En efecto, se había demostrado que todo grupo abeliano finito P que es primario (respecto a p), se descompone en una suma directa de grupos cíclicos primarios (respecto a p), y por eso, el orden del grupo P es igual al producto de los órdenes de estos grupos cíclicos, o sea, es una potencia del número p. Recíprocamente, si el orden de un grupo abeliano finito es igual a p^k, donde p es un número primo, entonces, el orden de cualquiera de sus elementos es divisor de este número, es decir, también es una potencia del número p, y, por lo tanto, el grupo resulta ser primario respecto a p.

Con el teorema fundamental no se agota todavía el problema de la descripción total de los grupos abelianos finitos, puesto que todavía no se ha excluido la posibilidad de que las sumas directas de dos conjuntos distintos de grupos cíclicos, primarios respecto a ciertos números primos, sean grupos isomorfos. En la realidad esto no se verifica, como muestra el **teorema** que sigue:

Si, de dos modos distintos, se ha descompuesto un grupo abeliano finito G en una suma directa de subgrupos cíclicos primarios,

$$G = \{a_1\} + \{a_2\} + \ldots + \{a_s\} = \{b_1\} + \{b_2\} + \ldots + \{b_t\}, \qquad (12)$$

entonces, ambas descomposiciones directas poseen el mismo número de sumandos directos, $s = t$, y entre los sumandos directos de estas descomposiciones se puede establecer una correspondencia biunívoca tal, que los sumandos correspondientes sean grupos cíclicos de un mismo orden, es decir, isomorfos.

Observemos primero, que si tomamos en la primera de las descomposiciones directas (12), por ejemplo, los sumandos directos que se relacionan al número primo dado p, su suma directa será un subgrupo primario (respecto a p) del grupo G, e incluso componente primaria de este grupo, puesto que su orden es igual a la potencia máxima del número p por la que se divide el orden del grupo G. Reuniendo de este modo todos los sumandos directos en cada una de las descomposiciones (12), obtenemos en ambos casos la descomposición del grupo G en componentes primarias, cuya unicidad ya fue señalada anteriormente.

Esto nos permite demostrar el teorema, suponiendo que **el mismo grupo G es primario respecto al número primo p.** Sea elegida la numeración de los sumandos directos en cada una de las descomposiciones (12) de tal modo, que los órdenes de estos sumandos no vayan creciendo, es decir, que teniendo los elementos $a_1, a_2, \ldots, a_s$ los órdenes

$$p^{k_1},\ p^{k_2},\ \ldots,\ p^{k_s},$$

respectivamente, sea,

$$k_1 \geqslant k_2 \geqslant \ldots \geqslant k_s,$$

y teniendo los elementos $b_1, b_2, \ldots, b_t$ los órdenes

$$p^{l_1},\ p^{l_2},\ \ldots,\ p^{l_t},$$

respectivamente, sea,

$$l_1 \geqslant l_2 \geqslant \ldots \geqslant l_t.$$

Si no se cumpliese la tesis de nuestro teorema, se hallaría un $i \geqslant 1$, tal, que

$$k_1 = l_1, \ldots, k_{i-1} = l_{i-1}, \tag{13}$$

pero,

$$k_i \neq l_i.$$

Está claro, que $i \leqslant \min(s, t)$, puesto que para cada una de las descomposiciones (12), el producto de los órdenes de todos los *sumandos directos es igual al orden del grupo* G. Mostremos que nuestra suposición nos lleva a una contradicción.

Sea, por ejemplo,

$$k_i < l_i. \tag{14}$$

Designemos con H el conjunto de los elementos del grupo G cuyos órdenes no sobrepasan a p^{k_i}. *Este representa un subgrupo del grupo* G, puesto que si x e y son elementos de H, entonces, $x + y$ y $-x$ son de orden no superior al número p^{k_i}.

Obsérvese, que al subgrupo H pertenecen, en particular, los elementos siguientes:

$$p^{k_1-k_i}a_1,\ p^{k_2-k_i}a_2,\ \ldots,\ p^{k_{i-1}-k_i}a_{i-1},\ a_i,\ a_{i+1},\ \ldots,\ a_s.$$

Por otra parte, si $1 \leqslant j \leqslant i-1$, entonces, el orden del elemento $p^{k_j-k_i-1}a_j$ es igual a p^{k_i+1}, y por eso, no pertenece a H. De aquí se deduce, que la clase adjunta $a_j + H$ (irecordemos, que estamos empleando la expresión aditiva!) tiene, como elemento del grupo cociente G/H, el orden $p^{k_j-k_i}$; este mismo orden tiene *su subgrupo* cíclico $\{a_j + H\}$. Demostremos que **el grupo G/H es una suma directa de los subgrupos cíclicos** $\{a_j + H\}$, $j = 1, 2, \ldots, i-1$,

$$G/H = \{a_1 + H\} + \{a_2 + H\} + \ldots + \{a_{i-1} + H\}, \tag{15}$$

y que, por esto, su orden es igual al número

$$p^{(k_1-k_i)+(k_2-k_i)+\ldots+(k_{i-1}-k_i)}. \tag{16}$$

Si x es un elemento arbitrario del grupo G, existe la expresión

$$x = m_1a_1 + m_2a_2 + \ldots + m_sa_s.$$

Supongamos que, para $j = 1, 2, \ldots, i-1$,

$$m_j = p^{k_j-k_i}q_j + n_j,$$

donde

$$0 \leqslant n_j < p^{k_j-k_i}. \tag{17}$$

Entonces,

$$m_ja_j = q_j(p^{k_j-k_i}a_j) + n_ja_j,$$

y como el primer sumando del segundo miembro está contenido en H, se tiene

$$m_ja_j + H = n_ja_j + H.$$

Por otra parte,

$$m_ia_i + H = H, \ldots, m_sa_s + H = H,$$

por eso,

$$x + H = (m_1a_1 + H) + (m_2a_2 + H) + \ldots + (m_sa_s + H) =$$
$$= (n_1a_1 + H) + (n_2a_2 + H) + \ldots + (n_{i-1}a_{i-1} + H). \tag{18}$$

Supongamos que existe una expresión más de éstas,

$$x + H = (n'_1a_1 + H) + (n'_2a_2 + H) + \ldots + (n'_{i-1}a_{i-1} + H), \tag{19}$$

donde

$$0 \leqslant n'_j < p^{k_j-k_i}, \quad j = 1, 2, \ldots, i-1. \tag{20}$$

Entonces, los elementos

$$n_1a_1 + n_2a_2 + \ldots + n_{i-1}a_{i-1}$$

y

$$n'_1a_1 + n'_2a_2 + \ldots + n'_{i-1}a_{i-1}$$

están en una misma clase adjunta relativa a H, o sea, su diferencia pertenece a H y, por esto,

$$p^{k_i}[(n_1-n'_1)a_1 + (n_2-n'_2)a_2 + \ldots + (n_{i-1}-n'_{i-1})a_{i-1}] = 0.$$

De aquí se deduce (ya que la primera de las descomposiciones (12) es directa) que

$$p^{k_i}(n_j-n'_j)a_j = 0, \quad j = 1, 2, \ldots, i-1,$$

y, por lo tanto, el número $p^{k_i}(n_j - n'_j)$ tiene que dividirse por el orden p^{k_j} del elemento a_j y, por consiguiente, la diferencia $n_j - n'_j$ se divide por el número $p^{k_j - k_i}$. En virtud de (17) y (20), de aquí se deduce que

$$n_j = n'_j, \quad j = 1, 2, \ldots, i-1,$$

es decir, las expresiones (18) y (19) son idénticas. De este modo, queda demostrada la existencia de la descomposición directa (15).

Consideraciones análogas, realizadas para la segunda de las descomposiciones (12), muestran que este mismo grupo cociente G/H posee una descomposición directa

$$G/H = \{b_1 + H\} + \{b_2 + H\} + \ldots + \{b_{i-1} + H\} + \{b_i + H\} + \ldots,$$

es decir, que en virtud de (13) y (14), su orden tiene que ser **estrictamente mayor** que el número (16). Esta contradicción demuestra el teorema.

Ya hemos obtenido una exposición completa de los grupos abelianos finitos. Así, pues, *tomamos todos los conjuntos finitos posibles de números naturales*

$$(n_1, n_2, \ldots, n_h),$$

diferentes de la unidad, pero no indispensablemente distintos, de modo que cada uno de ellos sea una potencia de cierto número primo. A cada conjunto de éstos ponemos en correspondencia una suma directa de grupos cíclicos, cuyos órdenes sean iguales a los números de este conjunto. Todos los grupos abelianos finitos obtenidos de este modo, resultan ser no isomorfos dos a dos, y cualquier otro grupo abeliano finito es isomorfo a uno de estos grupos.

INDICE ALFABETICO

KISELEV A., KRASNOV M., MAKARENKO G.

PROBLEMAS DE ECUACIONES DIFERENCIALES ORDINARIAS

Los autores de este libro son Mijail Krasnov, *Grigori Makarenko, candidatos a doctores en ciencias* físico-matemáticas y docentes del Instituto Energético de Moscú, y Alejandro Kiselev, colaborador científico superior del Instituto Unificado de investigaciones nucleares de la ciudad de Dubno.

En este libro se han recopilado cerca de 1 000 problemas y ejercicios del curso de ecuaciones diferenciales ordinarias.

Se ha incluido también el método de isoclinas para las ecuaciones de I y II orden, problemas para hallar las trayectorias ortogonales, dependencia e independencia lineales de los sistemas de funciones. Además, contiene problemas para hallar la estabilidad de las soluciones, el método del parámetro pequeño, el método para resolver ecuaciones y los sistemas.

Cada *parágrafo empieza con una breve introducción* teórica. Después se exponen las determinaciones y métodos principales de solución de los problemas. Todos los problemas van acompañados de su resultado; para algunos de ellos hay indicaciones de cómo resolverlos.

En esta obra se ha incluido también cierta cantidad de problemas muy complejos.

Es un libro de texto para los estudiantes de los centros de enseñanza superior. Ha aparecido dos veces editado en ruso.

Formato 13,5 × 20,5 cm. Encuadernado en tela. 208 págs.