CAPITULO IX

CALCULO DE LAS RAICES DE LOS POLINOMIOS

§ 38. Ecuaciones de segundo, tercero y cuarto grados

El teorema fundamental demostrado en el § 23 establece la existencia de n raíces complejas para cualquier polinomio de n-ésimo grado con coeficientes numéricos. Sus demostraciones (la expuesta anteriormente, así como otras conocidas actualmente) no proporcionan, sin embargo, métodos para la averiguación práctica de estas raíces, representando «demostraciones de existencia» puras. Naturalmente, las investigaciones hechas para descubrir tales métodos comenzaron por las pruebas de deducción de fórmulas análogas a la fórmula para la resolución de la ecuación cuadrática, bien conocida por el lector para el caso de coeficientes reales en el curso escolar de álgebra. Ahora demostraremos que esta fórmula es válida también para las ecuaciones cuadráticas con coeficientes complejos, y que se pueden deducir fórmulas análogas, aunque más complicadas, para las ecuaciones de tercero y cuarto grados.

Ecuaciones cuadráticas. Sea dada la ecuación cuadrática

$$x^2 + px + q = 0$$

con cualesquiera coeficientes complejos; sin restringir la generalidad se puede suponer que el coeficiente superior es igual a uno. Esta ecuación se puede escribir en la forma

$$\left(x + \frac{p}{2}\right)^2 + \left(q - \frac{p^2}{4}\right) = 0.$$

Como es sabido, se puede extraer la raíz cuadrada del número complejo $\frac{p^2}{4} - q$ sin salir del sistema de los números complejos. Los dos valores de la raíz, que se diferencian entre sí solamente en el signo, los escribiremos en la forma $\pm \sqrt{\frac{p^2}{4} - q}$. Por lo tanto,

$$x + \frac{p}{2} = \pm \sqrt{\frac{p^2}{4} - q},$$

o sea, las raíces de la ecuación dada se pueden hallar por la fórmula ordinaria

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Ejemplo. Resolver la ecuación

$$x^2 - 3x + (3 - i) = 0.$$

Aplicando la fórmula obtenida, resulta:

$$x = \frac{3}{2} \pm \sqrt{\frac{9}{4} - (3 - i)} = \frac{3}{2} \pm \frac{1}{2}\sqrt{-3 + 4i}.$$

Por los métodos del § 19 se halla:

$$\sqrt{-3 + 4i} = \pm (1 + 2i),$$

de donde

$$x_1 = 2 + i, \quad x_2 = 1 - i.$$

Ecuaciones cúbicas. A diferencia del caso de las ecuaciones cuadráticas, hasta ahora no tenemos un método para la resolución de las ecuaciones cúbicas, incluso en el caso de coeficientes reales. Ahora obtendremos para las ecuaciones cúbicas una fórmula análoga a la fórmula para las ecuaciones cuadráticas, suponiendo además que los coeficientes son cualesquiera números complejos.

Sea dada la ecuación cúbica

$$y^3 + ay^2 + by + c = 0 \tag{1}$$

con coeficientes complejos cualesquiera. Sustituyendo en la ecuación (1) la incógnita y por una nueva incógnita x, ligada a y por medio de la igualdad

$$y = x - \frac{a}{3}, \tag{2}$$

resulta una ecuación para la incógnita x; esta ecuación, como fácilmente se comprueba, no contiene el cuadrado de esta incógnita, o sea, es una ecuación de la forma

$$x^3 + px + q = 0. \tag{3}$$

Hallando las raíces de la ecuación (3), en virtud de (2), se obtienen también las raíces de la ecuación (1). Por consiguiente, no queda más que aprender a resolver la ecuación cúbica «reducida» (3), con cualesquiera coeficientes complejos.

Por el teorema fundamental, la ecuación (3) posee tres raíces complejas. Sea x_0 una de estas raíces. Introduzcamos una incógnita auxiliar u y examinemos el polinomio

$$f(u) = u^2 - x_0 u - \frac{p}{3}.$$

Sus coeficientes son números complejos, poseyendo por lo tanto dos raíces complejas α y β. Por las fórmulas de Vieta:

$$\alpha + \beta = x_0, \tag{4}$$

$$\alpha\beta = -\frac{p}{3}. \tag{5}$$

Poniendo en (3) la expresión (4) de la raiz x_0, resulta

$$(\alpha + \beta)^3 + p(\alpha + \beta) + q = 0,$$

o bien

$$\alpha^3 + \beta^3 + (3\alpha\beta + p)(\alpha + \beta) + q = 0.$$

Sin embargo, de (5) se deduce que $3\alpha\beta + p = 0$; de donde resulta:

$$\alpha^3 + \beta^3 = -q. \tag{6}$$

Por otra parte, de (5) se deduce que

$$\alpha^3\beta^3 = -\frac{p^3}{27}. \tag{7}$$

Las igualdades (6) y (7) muestran que los números α^3 y β^3 son raíces de la ecuación cuadrática

$$z^2 + qz - \frac{p^3}{27} = 0 \tag{8}$$

con coeficientes complejos.

Resolviendo la ecuación (8) se obtiene:

$$z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

de donde*

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{9}$$

Hemos obtenido la siguiente fórmula, conocida por el nombre de *fórmula de Cardano*, que expresa las raíces de la ecuación (3) mediante sus coeficientes valiéndose de radicales cuadrados y cúbicos:

$$x_0 = \alpha + \beta = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Como el radical cúbico tiene tres valores en el campo de los números complejos, las fórmulas (9) dan tres valores para α y tres valores para β. Sin embargo, al aplicar la fórmula de Cardano, no se puede combinar cualquier valor del radical α con cualquier valor

* No importa cuál de las raíces de la ecuación (8) se toma por α^3 y cuál por β^3, puesto que en las igualdades (6) y (7), y también en la expresión (4), α y β están situadas simétricamente.

del radical β: para un valor dado de α se debe tomar solamente aquél de los tres valores de β que satisface a la condición (5).

Sea α_1 uno de los tres valores del radical α. Entonces, como se ha demostrado en el § 19, los otros dos se pueden obtener multiplicando α_1 por las raíces cúbicas ε y ε^2 de la unidad:

$$\alpha_2 = \alpha_1\varepsilon, \quad \alpha_3 = \alpha_1\varepsilon^2.$$

Designemos con β_1 el valor del radical β que corresponde al valor α_1 del radical α según (5), de modo que $\alpha_1\beta_1 = -\frac{p}{3}$.

Los otros dos valores de β serán

$$\beta_2 = \beta_1\varepsilon, \quad \beta_3 = \beta_1\varepsilon^2.$$

Como $\varepsilon^3 = 1$,

$$\alpha_2\beta_3 = \alpha_1\varepsilon \cdot \beta_1\varepsilon^2 = \alpha_1\beta_1\varepsilon^3 = \alpha_1\beta_1 = -\frac{p}{3},$$

el valor α_2 del radical α corresponde al valor β_3 del radical β; análogamente el valor β_2 corresponde al valor α_3. Por lo tanto, todas las raíces de la ecuación (3) se pueden escribir del modo siguiente:

$$\left.\begin{aligned} x_1 &= \alpha_1 + \beta_1, \\ x_2 &= \alpha_2 + \beta_3 = \alpha_1\varepsilon + \beta_1\varepsilon^2, \\ x_3 &= \alpha_3 + \beta_2 = \alpha_1\varepsilon^2 + \beta_1\varepsilon. \end{aligned}\right\} \tag{10}$$

Ecuaciones cúbicas con coeficientes reales. Veamos lo que se puede decir de las raíces de la ecuación cúbica reducida

$$x^3 + px + q = 0, \tag{11}$$

si sus coeficientes son reales. En este caso, desempeña un papel fundamental la expresión $\frac{q^2}{4} + \frac{p^3}{27}$ que figura en la fórmula de Cardano bajo radical cuadrado. Obsérvese que el signo de esta expresión es contrario al signo de la expresión

$$D = -4p^3 - 27q^2 = -108\left(\frac{q^2}{4} + \frac{p^3}{27}\right),$$

denominada *discriminante* de la ecuación (11) (compárese más abajo, § 54); en las formulaciones posteriores se usará el signo del discriminante.

1) Sea $D < 0$. En este caso, en la fórmula de Cardano, bajo el símbolo de cada uno de los radicales cuadrados figura un número positivo. Por esto, los números que figuran bajo los símbolos de cada uno de los radicales cúbicos son **reales**. Sin embargo, la raíz cúbica de un número real tiene un valor real y dos valores imaginarios conjugados. Sea α_1 un valor real del radical α; el valor β_1 del radical β que corresponde a α_1 por la fórmula (5), también será real, pues, el

número p también es real. Por lo tanto, resulta que la raíz $x_1 = \alpha_1 + \beta_1$ de la ecuación (11) también es real. Las otras dos raíces se hallan sustituyendo en las fórmulas (10) del presente párrafo las raíces de la unidad $\varepsilon = \varepsilon_1$ y $\varepsilon^2 = \varepsilon_2$ por sus expresiones (7) del § 19:

$$x_2 = \alpha_1\varepsilon + \beta_1\varepsilon^2 = \alpha_1\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) + \beta_1\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) =$$

$$= -\frac{\alpha_1 + \beta_1}{2} + i\sqrt{3}\,\frac{\alpha_1 - \beta_1}{2},$$

$$x_3 = \alpha_1\varepsilon^2 + \beta_1\varepsilon = \alpha_1\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) + \beta_1\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) =$$

$$= -\frac{\alpha_1 + \beta_1}{2} - i\sqrt{3}\,\frac{\alpha_1 - \beta_1}{2};$$

como los números α_1 y β_1 son reales, estas dos raíces son números imaginarios conjugados, pues, el coeficiente de la parte imaginaria es diferente de cero, debido a que $\alpha_1 \neq \beta_1$; éstos son valores de distintos radicales cúbicos.

Por lo tanto, *si* $D < 0$, *la ecuación* (*11*) *tiene una raíz real y dos raíces imaginarias conjugadas.*

2) Sea $D = 0$. En este caso,

$$\alpha = \sqrt[3]{-\frac{q}{2}},\quad \beta = \sqrt[3]{-\frac{q}{2}}.$$

Sea α_1 un valor real del radical α; en virtud de (5), β_1 también será un número real, siendo $\alpha_1 = \beta_1$. Sustituyendo en las fórmulas (10), β_1 por α_1 y aplicando la igualdad $\varepsilon + \varepsilon^2 = -1$, resulta:

$$x_1 = 2\alpha_1,\quad x_2 = \alpha_1(\varepsilon + \varepsilon^2) = -\alpha_1,\quad x_3 = \alpha_1(\varepsilon^2 + \varepsilon) = -\alpha_1.$$

Por lo tanto, *si* $D = 0$, *todas las raíces de la ecuación* (*11*) *son reales, siendo dos de ellas iguales entre sí.*

3) Sea, finalmente, $D > 0$. En este caso, en la fórmula de Cardano, bajo el radical cuadrado figura un número real negativo y, por consiguiente, bajo los radicales cúbicos figuran números imaginarios conjugados. En consecuencia, todos los valores de los radicales α y β son ahora números imaginarios. No obstante, entre las raíces de la ecuación (11) tiene que haber por lo menos una real. Supongamos que ésta es la raíz

$$x_1 = \alpha_0 + \beta_0.$$

Como son reales tanto la suma de los números α_0 y β_0 como su producto, igual a $-\frac{p}{3}$, los números α_0 y β_0 son conjugados entre sí, pues son raíces de una ecuación cuadrática con coeficientes reales. Pero, entonces, son conjugados entre sí también los números $\alpha_0\varepsilon$ y $\beta_0\varepsilon^2$,

y también los números $\alpha_0\varepsilon^2$ y $\beta_0\varepsilon$, de donde se deduce que las raíces de la ecuación (11)

$$x_2 = \alpha_0\varepsilon + \beta_0\varepsilon^2, \quad x_3 = \alpha_0\varepsilon^2 + \beta_0\varepsilon$$

también son números reales.

Ha resultado que las tres raíces de la ecuación (11) son reales y, además, como fácilmente se comprueba, entre ellas no hay iguales. En caso contrario, la elección de la raíz x_1 se podría realizar de modo que se cumpliese la igualdad $x_2 = x_3$, de donde

$$\alpha_0(\varepsilon - \varepsilon^2) = \beta_0(\varepsilon - \varepsilon^2),$$

o sea, $\alpha_0 = \beta_0$, lo cual es imposible.

Por lo tanto, *si* $D > 0$, *la ecuación* (11) *tiene tres raíces reales distintas.*

El último caso que acabamos de examinar muestra que el valor práctico de la fórmula de Cardano es insignificante.

A pesar de que para $D > 0$ todas las raíces de la ecuación (11) con coeficientes reales son números reales, el cálculo de éstas por la fórmula de Cardano requiere la extracción de raíces cúbicas de números imaginarios, lo que sabemos hacer solamente pasando estos números a la forma trigonométrica. Por esta razón, la expresión de las raíces mediante los radicales pierde su valor práctico. Con métodos que están fuera de los alcances de este libro, se podría demostrar que en el caso considerado las raíces de la ecuación (11) no se pueden expresar de ningún modo mediante los coeficientes, empleando radicales con expresiones reales bajo los radicales. Este caso de solución de la ecuación (11) se llama *irreducible* (¡no confundir con la irreducibilidad de los polimonios!)

Ejemplos. 1. Resolver la ecuación

$$y^3 + 3y^2 - 3y - 14 = 0.$$

La sustitución $y = x - 1$ reduce esta ecuación a la forma

$$x^3 - 6x - 9 = 0. \tag{12}$$

Aquí $p = -6$, $q = -9$, por lo cual

$$\frac{q^2}{4} + \frac{p^3}{27} = \frac{49}{4} > 0,$$

o sea, la ecuación (12) tiene una raíz real y dos raíces imaginarias conjugadas. Según (9),

$$\alpha = \sqrt[3]{\frac{9}{2} + \frac{7}{2}} = \sqrt[3]{8}, \quad \beta = \sqrt[3]{\frac{9}{2} - \frac{7}{2}} = \sqrt[3]{1}.$$

Por consiguiente, $\alpha_1 = 2$, $\beta_1 = 1$, o sea, $x_1 = 3$. Las otras dos raíces se hallan por las fórmulas (10):

$$x_2 = -\frac{3}{2} + i\frac{\sqrt{3}}{2}, \quad x_3 = -\frac{3}{2} - i\frac{\sqrt{3}}{2}.$$

De aquí se deduce que las raíces de la ecuación dada son:

$$y_1=2,\ y_2=-\frac{5}{2}+i\,\frac{\sqrt{3}}{2},\ y_3=-\frac{5}{2}-i\,\frac{\sqrt{3}}{2}.$$

2. Resolver la ecuación

$$x^3-12x+16=0.$$

Aquí $p=-12$, $q=16$, por lo tanto,

$$\frac{q^2}{4}+\frac{p^3}{27}=0.$$

De aquí se deduce que $\alpha=\sqrt[3]{-8}$, o sea, $\alpha_1=-2$. En consecuencia,

$$x_1=-4,\ x_2=x_3=2.$$

3. Resolver la ecuación

$$x^3-19x+30=0.$$

Aquí $p=-19$, $q=30$, de donde

$$\frac{q^2}{4}+\frac{p^3}{27}=-\frac{784}{27}<0.$$

Así, manteniéndose en el campo de los números reales, la fórmula de Cardano no es aplicable a pesar de que sus raíces son los números reales 2, 3 y -5.

Ecuaciones de cuarto grado. La resolución de la ecuación de cuarto grado

$$y^4+ay^3+by^2+cy+d=0 \tag{13}$$

con coeficientes complejos arbitrarios se reduce a la resolución de una ecuación cúbica auxiliar. Esto se consigue con el método siguiente, perteneciente a Ferrari.

Se reduce previamente la ecuación (13) con la sustitución $y=x-\frac{a}{4}$, a la forma

$$x^4+px^2+qx+r=0. \tag{14}$$

Luego, el primer miembro de esta ecuación se transforma idénticamente mediante el parámetro auxiliar α, del modo siguiente:

$$x^4+px^2+qx+r=\left(x^2+\frac{p}{2}+\alpha\right)^2+qx+r-\frac{p^2}{4}-\alpha^2-2\alpha x^2-p\alpha,$$

o bien

$$\left(x^2+\frac{p}{2}+\alpha\right)^2-\left[2\alpha x^2-qx+\left(\alpha^2+p\alpha-r+\frac{p^2}{4}\right)\right]=0. \tag{15}$$

Elijamos ahora α de modo que el polinomio que figura entre corchetes sea un cuadrado completo. Para esto, es necesario que tenga una raíz múltiple, es decir, se tiene que cumplir la igualdad

$$q^2-4\cdot 2\alpha\left(\alpha^2+p\alpha-r+\frac{p^2}{4}\right)=0. \tag{16}$$

La igualdad (16) es una ecuación cúbica con respecto a la incógnita α con coeficientes complejos. Como se sabe, esta ecuación tiene tres raíces complejas. Sea α_0 una de ellas; en virtud de la fórmula de Cardano, ésta se expresa por radicales mediante los coeficientes de la ecuación (16), o sea, mediante los coeficientes de la ecuación (14).

Con tal elección del valor de α, el polinomio que figura entre corchetes en (15) tiene una raíz múltiple $\frac{q}{4\alpha_0}$, de segundo orden. Por consiguiente, la ecuación (15) toma la forma

$$\left(x^2 + \frac{p}{2} + \alpha_0\right)^2 - 2\alpha_0 \left(x - \frac{q}{4\alpha_0}\right)^2 = 0,$$

es decir, se descompone en dos ecuaciones cuadráticas:

$$\left.\begin{aligned} x^2 - \sqrt{2\alpha_0}\,x + \left(\frac{p}{2} + \alpha_0 + \frac{q}{2\sqrt{2\alpha_0}}\right) = 0, \\ x^2 + \sqrt{2\alpha_0}\,x + \left(\frac{p}{2} + \alpha_0 - \frac{q}{2\sqrt{2\alpha_0}}\right) = 0. \end{aligned}\right\} \qquad (17)$$

Como las ecuaciones (17) se han obtenido de la ecuación (14) haciendo transformaciones idénticas, las raíces de las ecuaciones (17) serán también raíces de la ecuación (14). Fácilmente se observa también que las raíces de la ecuación (14) se expresan por radicales mediante los coeficientes. Aquí no escribiremos las fórmulas correspondientes, pues son muy complicadas y prácticamente inútiles; tampoco estudiaremos separadamente el caso en que la ecuación (14) tenga coeficientes reales.

Observación sobre las ecuaciones de grado superior. A pesar de que los griegos ya conocían los métodos de resolución de las ecuaciones cuadráticas, el descubrimiento de los métodos de resolución de las ecuaciones de tercero y cuarto grado, expuesto anteriormente, pertenece al siglo XVI. Durante casi tres siglos se continuaron haciendo estériles pruebas para dar el paso siguiente, es decir, para hallar fórmulas que expresasen las raíces de cualquier ecuación de quinto grado (o sea, de una ecuación de quinto grado con coeficientes literales) mediante sus coeficientes por radicales. Estas pruebas terminaron en los años veinte del siglo pasado, después de que Abel demostró que no existen tales fórmulas para las ecuaciones de n-ésimo grado, cuando $n \geqslant 5$.

Sin embargo, el resultado de Abel no excluía la posibilidad de que las raíces de cualquier polinomio concreto con coeficientes numéricos se pudiesen expresar de algún modo mediante los coeficientes empleando alguna combinación de radicales o, como está convenido decir, que cualquier ecuación se resolviese por radicales. El problema sobre las condiciones según las cuales una ecuación dada es resoluble por radicales fue estudiado detalladamente por Galois en los años

treinta del siglo pasado. Resultó que para cualquier n, empezando desde $n = 5$, se pueden indicar ecuaciones de n-ésimo grado irresolubles por radicales, que tienen incluso coeficientes numéricos enteros. Tal es, por ejemplo, la ecuación

$$x^5 - 4x - 2 = 0.$$

Las investigaciones de Galois influyeron definitivamente en el desarrollo del álgebra. Sin embargo, nuestra tarea no incluye su exposición.

§ 39. Acotación de las raíces

Ya sabemos que no existe un método para calcular los valores exactos de las raíces de los polinomios con coeficientes numéricos. No obstante, diversos problemas de la mecánica, de la física y de la técnica se reducen al problema de las raíces de los polinomios, los cuales suelen ser a veces de grados suficientemente altos. Esta circunstancia fue la causa de numerosas investigaciones que tenían por objeto aprender a hacer tales o cuales deducciones sobre las raíces de los polinomios con coeficientes numéricos sin conocer estas raíces. Se estudiaba, por ejemplo, la cuestión sobre la posición de las raíces en el plano complejo (las condiciones según las cuales todas las raíces están dentro del círculo unidad, o sea, que en su valor absoluto son menores que la unidad, o bien, las condiciones para que todas las raíces estén situadas en el semiplano izquierdo, o sea, que sus partes reales fuesen negativas, etc). Para los polinomios de coeficientes reales, se elaboraban métodos de definición del número de raíces reales, se buscaban las cotas entre las que podían estar estas raíces, etc. Finalmente, fueron dedicadas muchas investigaciones a los métodos del cálculo aproximado de las raíces. Ordinariamente, en las aplicaciones técnicas es suficiente conocer solamente los valores aproximados de las raíces con cierta exactitud prefijada, y si, por ejemplo, las raíces del polinomio se expresasen incluso por radicales, éstos se sustituirían de todos modos por sus valores aproximados.

En su tiempo, todas estas investigaciones formaban el contenido fundamental del álgebra superior. En nuestro curso está incluida solamente una parte muy pequeña de los resultados relacionados con esto y, teniendo en cuenta las necesidades primarias de las aplicaciones, nos limitaremos al caso de polinomios de coeficientes reales y de sus raíces reales, saliéndonos pocas veces de estos límites. Además, se va a considerar sistemáticamente el polinomio $f(x)$ de coeficientes reales como una función real (continua) de la variable real x. Siempre que sea útil se emplearán los resultados y métodos del análisis matemático.

Es conveniente comenzar el estudio de las raíces reales de un polinomio $f(x)$ de coeficientes reales considerando la gráfica de este polinomio. Evidentemente, *las raíces reales del polinomio son las abscisas de los puntos de intersección de su gráfica con el eje x, y sólo éstas.*

Veamos, por ejemplo, el polinomio de quinto grado

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3.$$

Por los resultados del § 24, sobre las raíces de este polinomio, se puede afirmar lo siguiente: como es de grado impar, $h(x)$ tiene por lo menos una raíz real; si el número de raíces reales es mayor que uno, será igual a tres o a cinco, pues las raíces imaginarias son conjugadas a pares.

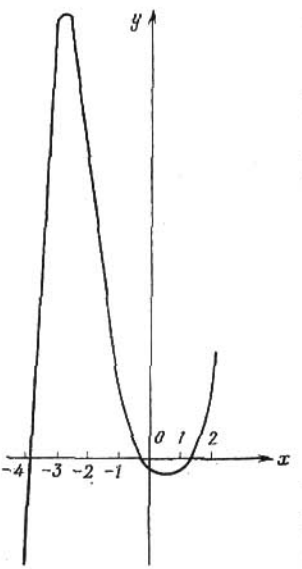

Fig. 9.

El estudio de la gráfica del polinomio $h(x)$ permite afirmar algo más sobre sus raíces. Tracemos esta gráfica (fig. 9)*, considerando sólo los valores enteros de x y calculando los valores correspondientes de $h(x)$ por el método de Horner:

x	$h(x)$
.	.
.	.
-4	-39
-3	144
-2	83
-1	18
0	-3
1	-4
2	39
.	.
.	.

Vemos, pues, que el polinomio $h(x)$ posee al menos tres raíces reales: una positiva α_1 y dos negativas α_2 y α_3, siendo

$$1 < \alpha_1 < 2, \quad -1 < \alpha_2 < 0, \quad -4 < \alpha_3 < -3.$$

La información sobre las raíces (reales) del polinomio, obtenida al examinar la gráfica, suele ser prácticamente bastante buena. Sin embargo, siempre quedan algunas dudas: no se sabe si verdaderamente se han hallado todas las raíces o no. Así, en el ejemplo consi-

* En el dibujo, en el eje y se ha tomado una escala diez veces menor que en el eje x.

derado no se ha demostrado que a la derecha del punto $x = 2$ y a la izquierda del punto $x = -4$ ya no hay raíces del polinomio. Además, como sólo se han tomado valores enteros de x, se puede suponer que la gráfica trazada refleja con poca exactitud el comportamiento de la función $h(x)$, pueda ser incluso que no tenga en cuenta algunas de sus más pequeñas oscilaciones, perdiéndose así algunas raíces.

Claro, al construir la gráfica se podrían tomar no sólo los valores enteros de x, sino también valores que se diferenciasen en 0,1 o en 0,01. Sin embargo, con esto se complicarían considerablemente los cálculos de los valores de $h(x)$, y de todos modos persistirían las dudas indicadas anteriormente. Por otra parte, con los métodos del análisis matemático se podrían hallar los máximos y mínimos de la función $h(x)$ y comparar nuestra gráfica con el comportamiento verdadero de la función; pero esto trae consigo la cuestión sobre las raíces de la derivada $h'(x)$, o sea, el mismo problema que estamos resolviendo.

De aquí surge la necesidad de métodos más perfectos para la búsqueda de cotas entre las que están comprendidas las raíces reales de un polinomio de coeficientes reales, y la determinación del número de estas raíces. Ahora nos vamos a ocupar del problema sobre las **cotas de las raíces reales**, dejando para los siguientes párrafos la cuestión sobre la cantidad de estas raíces.

La demostración del lema sobre el módulo del término superior (véase el § 23) proporciona ya una cota para los módulos de las raíces de un polinomio. En efecto, haciendo $k = 1$ en la desigualdad (3) del § 23, resulta que, para

$$|x| \geqslant 1 + \frac{A}{|a_0|}, \qquad (1)$$

donde a_0 es el coeficiente superior y A, el máximo de los módulos de los demás coeficientes, el módulo del término superior del polinomio es mayor que el módulo de la suma de todos los demás términos. Por consiguiente, ningún valor de x que satisfaga a la desigualdad (1) puede ser raíz de este polinomio.

Por lo tanto, *para un polinomio $f(x)$ con cualesquiera coeficientes numéricos, el número $1 + \frac{A}{a_0}$ es una cota superior para los módulos de todas sus raíces, reales o imaginarias.* Así, pues, para el polinomio $h(x)$ examinado más arriba, esta cota es el número 9, puesto, que $a_0 = 1$, $A = 8$.

No obstante, esta cota suele ser demasiado grande, si sólo nos interesan las cotas de las raíces reales. Ahora se expondrán otros métodos más exactos. Hay que tener presente que a pesar de que se marquen las cotas entre las que tienen que estar comprendidas las raíces reales del polinomio, **esto no significa que tales raíces existan.**

Demostremos primero que *es suficiente conocer la cota superior de las raíces positivas de cualquier polinomio.* En efecto, sea dado un polinomio $f(x)$ de grado n y sea N_0 una cota superior de sus raíces positivas. Examinemos los polinomios

$$\varphi_1(x) = x^n f\left(\frac{1}{x}\right),$$

$$\varphi_2(x) = f(-x),$$

$$\varphi_3(x) = x^n f\left(-\frac{1}{x}\right)$$

y hallemos las cotas superiores de sus raíces positivas; supongamos que éstas son los números N_1, N_2, y N_3, respectivamente. Entonces, *el número* $\frac{1}{N_1}$ *será una cota inferior de las raíces positivas del polinomio* $f(x)$, pues, si α es una raíz positiva de $f(x)$, $\frac{1}{\alpha}$ es una raíz positiva de $\varphi_1(x)$, y de $\frac{1}{\alpha} < N_1$, resulta $\alpha > \frac{1}{N_1}$. Análogamente, *los números* $-N_2$ *y* $-\frac{1}{N_3}$ *son las cotas inferior y superior, respectivamente, de las raíces negativas del polinomio* $f(x)$. Por lo tanto, todas las raíces positivas del polinomio $f(x)$ satisfacen a las desigualdades $\frac{1}{N_1} < x < N_0$ y todas las raíces negativas, satisfacen a las desigualdades

$$-N_2 < x < -\frac{1}{N_3}.$$

Para determinar una cota superior de las raíces positivas se puede aplicar el método siguiente. Sea dado un polinomio

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

con coeficientes reales, siendo $a_0 > 0$. Supongamos ahora que a_k, $k \geqslant 1$, es el primer coeficiente negativo; si no hubiese tales coeficientes, el polinomio $f(x)$ no podría tener raíces positivas. Sea, finalmente, B el máximo valor absoluto de los coeficientes negativos. Entonces *el número*

$$1 + \sqrt[k]{\frac{B}{a_0}}$$

es una cota superior de las raíces positivas del polinomio $f(x)$.

En efecto, suponiendo $x > 1$ y sustituyendo cada uno de los coeficientes $a_1, a_2, \ldots, a_{k-1}$ por cero y cada uno de los coeficientes $a_k, a_{k+1}, \ldots, a_n$ por B, se puede disminuir solamente el valor

del polinomio, resultando

$$f(x) \geqslant a_0x^n - B(x^{n-k} + x^{n-k-1} + \ldots + x + 1) = a_0x^n - B\frac{x^{n-k+1}-1}{x-1}$$

y, como $x > 1$,

$$f(x) > a_0x^n - \frac{Bx^{n-k+1}}{x-1} = \frac{x^{n-k+1}}{x-1}[a_0x^{k-1}(x-1) - B]. \qquad (2)$$

Si

$$x > 1 + \sqrt[k]{\frac{B}{a_0}}, \qquad (3)$$

entonces, como

$$a_0x^{k-1}(x-1) - B \geqslant a_0(x-1)^k - B,$$

la expresión que figura entre corchetes en la fórmula (2) resulta positiva, sea, en virtud de (2), el valor de $f(x)$ es estrictamente positivo. Por lo tanto, los valores de x que satisfacen a la desigualdad (3) no pueden ser raíces de $f(x)$, como se quería demostrar.

Para el polinomio $h(x)$ considerado anteriormente, como $k = 2$ y $B = 7$, para la cota superior de las raíces positivas este método da el número $1 + \sqrt{7}$, que se puede sustituir por el número entero próximo mayor 4.

De los numerosos métodos existentes de acotación superior de las raíces positivas expondremos solamente el *método de Newton*. Este método es más complicado que el expuesto anteriormente, pero, no obstante, da ordinariamente, muy buen resultado.

Sea dado un polinomio $f(x)$ de coeficientes reales y con el coeficiente superior positivo a_0. *Si para* $x = c$, *el polinomio* $f(x)$ *y todas sus derivadas sucesivas* $f'(x)$, $f''(x)$, . . ., $f^{(n)}(x)$ *toman valores positivos, el número* c *es una cota superior de las raíces positivas.*

En efecto, según la fórmula de Taylor (véase el § 23),

$$f(x) = f(c) + (x-c)f'(c) + (x-c)^2\frac{f''(c)}{2!} + \ldots + (x-c)^n\frac{f^{(n)}(c)}{n!}.$$

Vemos, que si $x \geqslant c$, el segundo miembro será un número estrictamente positivo, es decir, tales valores de x no pueden ser raíces de $f(x)$.

Al buscar el número correspondiente c, para un polinomio $f(x)$ dado, es conveniente obrar del modo siguiente. La derivada $f^{(n)}(x) = n!a_0$ es un número positivo, de donde, el polinomio $f^{(n-1)}(x)$ es una función creciente de x. Por consiguiente, existe un número c_1 tal, que para $x \geqslant c_1$ la derivada $f^{(n-1)}(x)$ es positiva. De esto se deduce que para $x \geqslant c_1$, la derivada $f^{(n-2)}(x)$ es una función creciente de x, por lo cual, existe un número c_2 tal ($c_2 \geqslant c_1$), que para $x \geqslant c_2$, la derivada $f^{(n-2)}(x)$ también es positiva. Continuando de este modo, llegaremos por fin al número buscado c.

Apliquemos el método de Newton al polinomio $h(x)$ examinado anteriormente.

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3,$$
$$h'(x) = 5x^4 + 8x^3 - 15x^2 + 16x - 7,$$
$$h''(x) = 20x^3 + 24x^2 - 30x + 16,$$
$$h'''(x) = 60x^2 + 48x - 30,$$
$$h^{IV}(x) = 120x + 48,$$
$$h^{V}(x) = 120.$$

Fácilmente se comprueba (aunque sea por el método de Horner), que todos estos polinomios son positivos para $x = 2$. Por lo tanto, el número 2 es una cota superior de las raíces positivas del polinomio $h(x)$, resultado que es mucho más exacto que los obtenidos por otros métodos.

Para hallar una cota inferior de las raíces negativas del polinomio $h(x)$, veamos el polinomio $\varphi_2(x) = -h(-x)$*. Como

$$\varphi_2(x) = x^5 - 2x^4 - 5x^3 - 8x^2 - 7x + 3,$$
$$\varphi_2'(x) = 5x^4 - 8x^3 - 15x^2 - 16x - 7,$$
$$\varphi_2''(x) = 20x^3 - 24x^2 - 30x - 16,$$
$$\varphi_2'''(x) = 60x^2 - 48x - 30,$$
$$\varphi_2^{IV}(x) = 120x - 48,$$
$$\varphi^{V}(x) = 120,$$

y todos estos polinomios son positivos para $x = 4$, lo que fácilmente se comprueba, el número 4 es una cota superior de las raíces positivas de $\varphi_2(x)$, de donde, el número -4 es una cota inferior de las raíces negativas de $h(x)$.

Examinando, finalmente, los polinomios

$$\varphi_1(x) = -x^5 h\left(\frac{1}{x}\right) = 3x^5 + 7x^4 - 8x^3 + 5x^2 - 2x - 1,$$

$$\varphi_3(x) = -x^5 h\left(-\frac{1}{x}\right) = 3x^5 - 7x^4 - 8x^3 - 5x^2 - 2x + 1,$$

y aplicando de nuevo el método de Newton, para las cotas superiores de las raíces positivas de estos polinomios hallamos los números 1 y 4, respectivamente; de aquí el número $\frac{1}{1} = 1$ es una cota inferior de las raíces positivas del polinomio $h(x)$; el número $-\frac{1}{4}$ es una cota superior de las raíces negativas de éste.

Por lo tanto, las raíces positivas del polinomio $h(x)$ están comprendidas entre los números 1 y 2, y las raíces negativas, entre los números -4 y $-\frac{1}{4}$. Este resultado concuerda perfectamente con lo hallado antes al examinar la *gráfica*.

---

* Aquí tomamos $-h(-x)$ en lugar de $h(-x)$, porque para la aplicación del método de Newton, el coeficiente superior tiene que ser positivo. Naturalmente, este cambio de signo no influye en las raíces del polinomio $\varphi_2(x)$.

§ 40. Teorema de Sturm

Ahora estudiaremos el problema sobre **el número de raíces reales que tiene un polinomio $f(x)$ de coeficientes reales.** Mas, nos interesará tanto el número total de las raíces reales como los números de las raíces positivas y negativas por separado y, en general, el número de raíces comprendidas entre dos números dados a y b. Existen unos cuantos métodos para la averiguación del número exacto de raíces, siendo éstos demasiado complicados; entre ellos, el más sensillo es el *método de Sturm* que se expondrá a continuación.

Introduzcamos primero una definición que se utilizará también en el párrafo siguiente.

Sea dado un sistema finito ordenado de números reales diferentes de cero, por ejemplo,

$$1,\ 3,\ -2,\ 1,\ -4,\ -8,\ -3,\ 4,\ 1. \tag{1}$$

Escribamos sucesivamente los signos de estos números:

$$+,\ +,\ -,\ +,\ -,\ -,\ -,\ +,\ +. \tag{2}$$

Observamos que en el sistema (2) figuran cuatro veces signos contrarios consecutivos. En virtud de esto, se dice que el sistema ordenado (1) presenta cuatro *variaciones de signo*. Naturalmente, **el número de variaciones de signo** puede ser calculado para cualquier sistema finito ordenado de números reales diferentes de cero.

Consideremos ahora un polinomio $f(x)$ de coeficientes reales y supongamos que éste **carece de raíces múltiples**, pues, en caso contrario, se le podría dividir por el máximo común divisor del mismo y su derivada. Un sistema finito ordenado de polinomios, no nulos, de coeficientes reales

$$f(x) = f_0(x),\ f_1(x),\ f_2(x),\ \ldots,\ f_s(x) \tag{3}$$

se llama *sistema de Sturm* del polinomio $f(x)$ si se cumplen las condiciones siguientes:

1) Los polinomios consecutivos del sistema (3) no tienen raíces comunes.

2) El último polinomio $f_s(x)$ no tiene raíces reales.

3) Si α es una raíz real de uno de los polinomios intermedios $f_k(x)$ del sistema (3), $1 < k < s-1$, entonces, $f_{k-1}(\alpha)$ y $f_{k+1}(\alpha)$ tienen diferente signo.

4) Si α es una raíz real del polinomio $f(x)$, el producto $f(x)\,f_1(x)$ cambia su signo de menos a más, cuando al crecer x pasa por el punto α.

El problema de la existencia de un sistema de Sturm para cualquier polinomio se estudiará más adelante; ahora, suponiendo que $f(x)$

posea tal sistema, señalaremos el modo de utilizarlo para averiguar el número de raíces reales.

Si el número real c no es raíz del polinomio dado $f(x)$ y (3) es el sistema de Sturm de este polinomio, tomamos el sistema de números reales

$$f(c),\ f_1(c),\ f_2(c)\ \ldots,\ f_s(c),$$

eliminamos en éste todos los números iguales a cero, y designamos con $W(c)$ el número de variaciones de signo que presenta el sistema obtenido; diremos que $W(c)$ *es el número de variaciones de signo que presenta el sistema de Sturm* (3) *del polinomio* $f(x)$ *para* $x=c$ *.

Subsiste el siguiente

Teorema de Sturm. *Si los números reales* a *y* b, $a<b$, *no son raíces del polinomio* $f(x)$, *el cual carece de raíces múltiples, entonces* $W(a)\geqslant W(b)$, *y la diferencia* $W(a)-W(b)$ *es igual al número de raíces reales del polinomio* $f(x)$ *comprendidas entre* a *y* b.

Por lo tanto, para la determinación del número de raíces reales del polinomio $f(x)$ comprendidas entre a y b (recordamos que, por hipótesis, $f(x)$ no tiene raíces múltiples), sólo hay que averiguar en cuánto disminuye el número de variaciones de signo que presenta el sistema de Sturm de este polinomio al pasar del valor a al valor b.

Para la demostración del teorema, veamos cómo cambia el número $W(x)$ al crecer x. Mientras x no pase por alguna raíz de alguno de los polinomios del sistema de Sturm (3), los signos de los polinomios de este sistema no cambiarán y no variará el número $W(x)$. En virtud de esto, y también debido a la condición 2) de la definición del sistema de Sturm, no queda más que examinar dos casos: el paso de x por una raíz de uno de los polinomios intermedios $f_k(x)$, $1\leqslant k\leqslant s-1$, y el paso de x por una raíz del mismo polinomio $f(x)$.

Sea α una raíz del polinomio $f_k(x)$, $1\leqslant k\leqslant s-1$. Entonces, por la condición 1), $f_{k-1}(\alpha)$ y $f_{k+1}(\alpha)$ son diferentes de cero. Por consiguiente, se podrá hallar un número positivo ε, posiblemente muy pequeño, de tal modo que en el intervalo $(\alpha-\varepsilon,\ \alpha+\varepsilon)$ los polinomios $f_{k-1}(x)$ y $f_{k+1}(x)$ no tengan raíces, conservando por ello constantes los signos, que serán además **distintos**, por la condición (3). De esto se deduce que cada uno de los sistemas de números

$$f_{k-1}(\alpha-\varepsilon),\ f_k(\alpha-\varepsilon),\ f_{k+1}(\alpha-\varepsilon), \tag{4}$$

$$f_{k-1}(\alpha+\varepsilon),\ f_k(\alpha+\varepsilon),\ f_{k+1}(\alpha+\varepsilon) \tag{5}$$

prensentan exactamente una variación de signo, independientemente de los signos que tengan los números $f_k(\alpha-\varepsilon)$ y $f_k(\alpha+\varepsilon)$. Por

* Naturalmente, las variaciones de signo que presenta el sistema de Sturm de un polinomio $f(x)$ no tiene nada de común con la variación de signo del mismo polinomio $f(x)$, debida al paso de x por una raíz de este polinomio.

ejemplo, si en el intervalo considerado $f_{k-1}(x)$ es negativo y $f_{k+1}(x)$ es positivo, y si $f_k(\alpha - \varepsilon) > 0$, $f_k(\alpha + \varepsilon) < 0$, a los sistemas (4) y (5) les corresponderán los sistemas de signos:

$$-, +, +; \quad -, -, +.$$

Por lo tanto, al pasar x por una raíz de uno de los polinomios intermedios del sistema de Sturm, la variación de signos en este sistema sólo puede trasladarse, mas no podrá aparecer de nuevo ni desaparecer, por lo que **durante tal paso el número $W(x)$ no variará.**

Supongamos, por otra parte, que α es una raíz del mismo polinomio $f(x)$. Según la condición 1), en este caso α no será raíz de $f_1(x)$. Por consiguiente, existe un número positivo ε tal, que el intervalo $(\alpha - \varepsilon, \alpha + \varepsilon)$ no contiene raíces del polinomio $f_1(x)$, por lo cual este último mantiene constante el signo en este intervalo. Si este signo es positivo, en virtud de la condición 4), al pasar x por α, el mismo polinomio $f(x)$ cambia el signo de menos a más, es decir, $f(\alpha - \varepsilon) < 0$, $f(\alpha + \varepsilon) > 0$. Luego, a los sistemas de números

$$f(\alpha - \varepsilon),\ f_1(\alpha - \varepsilon) \text{ y } f(\alpha + \varepsilon),\ f_1(\alpha + \varepsilon) \tag{6}$$

les corresponden los sistemas de signos

$$-, + \text{ y } +, +,$$

o sea, en el sistema de Sturm **se pierde una variación.** Si el signo de $f_1(x)$ es negativo en el intervalo $(\alpha - \varepsilon, \alpha + \varepsilon)$, de nuevo en virtud de la condición 4), el polinomio $f(x)$ cambia el signo de más a menos al pasar x por α, o sea, $f(\alpha - \varepsilon) > 0$, $f(\alpha + \varepsilon) < 0$; a los sistemas de números (6) les corresponden ahora los sistemas de signos

$$+, - \text{ y } -, -,$$

es decir, en el sistema de Sturm **se pierde de nuevo una variación.**

Por lo tanto, *el número $W(x)$ varía (al crecer x) solamente cuando x pasa por una raíz del polinomio $f(x)$, disminuyendo exactamente, en este caso, en una unidad.*

Naturalmente, con esto queda demostrado el teorema de Sturm. Para aplicar este teorema a la averiguación del número total de raíces reales de un polinomio $f(x)$, es suficiente tomar por a el límite inferior de las raíces negativas y por b, el límite superior de las raíces positivas. Sin embargo, es más fácil obrar del modo siguiente. En virtud del lema demostrado en el § 23, existe un número positivo N, posiblemente muy grande, tal que para $|x| > N$ los signos **de todos** los polinomios del sistema de Sturm coinciden con los signos de sus términos superiores. En otras palabras, existe un valor positivo tan grande de la indeterminada x, que los signos de los valores correspondientes de todos los polinomios del sistema de Sturm coinciden con los signos de sus **coeficientes** superiores; este valor

de x, cuyo cálculo no es necesario, se designa convencionalmente con el símbolo ∞. Por otra parte, existe un número negativo x, cuyo valor absoluto es tan grande que los signos de los valores correspondientes de los polinomios del sistema de Sturm coinciden con los signos de sus coeficientes superiores para los polinomios de grado par, y son contrarios a los signos de los coeficientes superiores para los polinomios de grado impar; convengamos en designar este valor de x mediante $-\infty$. Está claro que en el intervalo $(-\infty, \infty)$ están contenidas todas las raíces reales de todos los polinomios del sistema de Sturm y, en particular, todas las raíces reales del polinomio $f(x)$. Aplicando el teorema de Sturm a este intervalo, se halla el número de estas raíces; la aplicación del teorema de Sturm a los intervalos $(-\infty, 0)$ y $(0, \infty)$ proporciona el número de raíces negativas y el número de raíces positivas del polinomio $f(x)$, respectivamente.

No queda más que demostrar que *cualquier polinomio $f(x)$ de coeficientes reales que no tenga raíces múltiples posee un sistema de Sturm*. Entre los diversos métodos que se emplean para la construcción de tal sistema expondremos el más usual. Hagamos $f_1(x) = f'(x)$, con lo que se garantiza el cumplimiento de la condición 4) de la definición del sistema de Sturm. En efecto, si α es una raíz real del polinomio $f(x)$, se tiene $f'(\alpha) \neq 0$. Si $f'(\alpha) > 0$, entonces $f'(x) > 0$ en un entorno del punto α. Por lo tanto, al pasar x por α, $f(x)$ cambia el signo de menos a más; esto mismo se cumple también para el producto $f(x) f_1(x)$. Razonamientos análogos son válidos también para el caso en que $f'(\alpha) < 0$. Se divide luego $f(x)$ por $f_1(x)$ y el residuo de esta división, **tomado con signo contrario,** se toma por $f_2(x)$:

$$f(x) = f_1(x) q_1(x) - f_2(x).$$

En general, si ya se han hallado los polinomios $f_{k-1}(x)$ y $f_k(x)$, el polinomio $f_{k+1}(x)$ será el residuo de la división de $f_{k-1}(x)$ por $f_k(x)$, tomado con signo contrario:

$$f_{k-1}(x) = f_k(x) q_k(x) - f_{k+1}(x). \tag{7}$$

El método expuesto se diferencia del algoritmo de Euclides, aplicado a los polinomios $f(x)$ y $f'(x)$, solamente en que cada vez se cambia el signo al residuo, y la división consiguiente se efectúa ya por este residuo, tomado con el signo contrario. Como al buscar el máximo común divisor este cambio de signos no importa, nuestro proceso terminará en cierto $f_s(x)$, que será el máximo común divisor de los polinomios $f(x)$ y $f'(x)$; además, como $f(x)$ no tiene raíces múltiples, o sea, es primo con $f'(x)$, resulta que en realidad $f_s(x)$ será un número real diferente de cero.

De aquí que el sistema construido de polinomios

$$f(x) = f_0(x),\ f'(x) = f_1(x),\ f_2(x),\ \ldots,\ f_s(x)$$

también satisface a la condición 2) de la definición del sistema de Sturm. Para demostrar que se cumple la condición 1), supongamos que los polinomios consecutivos $f_k(x)$ y $f_{k+1}(x)$ tienen una raíz común α. Entonces, por la igualdad (7), α también es raíz del polinomio $f_{k-1}(x)$. Pasando a la igualdad

$$f_{k-2}(x) = f_{k-1}(x)\, q_{k-1}(x) - f_k(x),$$

resulta que α es también raíz de $f_{k-2}(x)$. Continuando de este modo, hallamos que α es una raíz común de $f(x)$ y $f'(x)$, lo que contradice a las hipótesis hechas. Finalmente, el cumplimiento de la condición 3) es consecuencia inmediata de la igualdad (7), pues, si $f_k(\alpha) = 0$, resulta $f_{k-1}(\alpha) = -f_{k+1}(\alpha)$.

Apliquemos el método de Sturm al polinomio

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3,$$

examinado en el párrafo anterior. Aquí no comprobaremos previamente que $h(x)$ carece de raíces múltiples, puesto que el método de construcción del sistema de Sturm, sirve a la vez para comprobar si el polinomio y su derivada son primos entre sí.

Hallemos el sistema de Sturm para $h(x)$ aplicando el método indicado. Mas, a diferencia del algoritmo de Euclides, en el proceso de división multiplicaremos y simplificaremos solamente por números **positivos** arbitrarios, puesto que los signos de los residuos desempeñan un papel fundamental en el método de Sturm. Obtendremos el sistema siguiente:

$$\begin{aligned}
h(x) &= x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3,\\
h_1(x) &= 5x^4 + 8x^3 - 15x^2 + 16x - 7,\\
h_2(x) &= 66x^3 - 150x^2 + 172x + 61,\\
h_3(x) &= -464x^2 + 1135x + 723,\\
h_4(x) &= -32\,599\,457x - 8\,486\,093,\\
h_5(x) &= -1.
\end{aligned}$$

Determinemos los signos de los polinomios de este sistema para $x = -\infty$ y $x = \infty$, para lo cual, según lo indicado, se deben observar solamente los signos de los coeficientes superiores y los grados de estos polinomios. Resulta la tabla:

	$h(x)$	$h_1(x)$	$h_2(x)$	$h_3(x)$	$h_4(x)$	$h_5(x)$	Número de variaciones de signo
$-\infty$	−	+	−	−	+	−	4
∞	+	+	+	−	−	−	1

Por lo tanto, al pasar x de $-\infty$ a ∞, el sistema de Sturm pierde tres variaciones de signo y, por esto, el polinomio $h(x)$ tiene exactamente tres raíces

reales. De aquí vemos que, al construir la gráfica de este polinomio en el párrafo anterior, no habíamos perdido ninguna raíz.

Apliquemos el método de Sturm a otro polinomio más simple. Sea dado el polinomio

$$f(x) = x^3 + 3x^2 - 1.$$

Hallemos el número de sus raíces reales y también las cotas enteras entre las que está comprendida cada una de estas raíces, sin construir previamente la gráfica del mismo.

El sistema de Sturm de este polinomio es

$$f(x) = x^3 + 3x^2 - 1,$$
$$f_1(x) = 3x^2 + 6x,$$
$$f_2(x) = 2x + 1,$$
$$f_3(x) = 1.$$

Hallemos el número de variaciones de signo que presenta este sistema para $x = -\infty$ y $x = \infty$.

	$f(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	Número de variaciones de signo
$-\infty$	$-$	$+$	$-$	$+$	3
∞	$+$	$+$	$+$	$+$	0

Por consiguiente, el polinomio $f(x)$ tiene tres raíces reales. Para determinar más exactamente la posición de estas raíces, continuemos la tabla anterior:

	$f(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	Número de variacones de signo
$x=-3$	$-$	$+$	$-$	$+$	3
$x=-2$	$+$	0	$-$	$+$	2
$x=-1$	$+$	$-$	$-$	$+$	2
$x=0$	$-$	0	$+$	$+$	1
$x=1$	$+$	$+$	$+$	$+$	0

Por lo tanto, el sistema de Sturm del polinomio $f(x)$ pierde una variación de signo cada vez que x pasa de -3 a -2, de -1 a 0 y de 0 a 1. Luego, las raíces α_1, α_2 y α_3 del polinomio satisfacen a las desigualdades:

$$-3 < \alpha_1 < -2, \quad -1 < \alpha_2 < 0, \quad 0 < \alpha_3 < 1.$$

§ 41. Otros teoremas sobre el número de raíces reales

El teorema de Sturm resuelve por completo el problema del número de raíces reales de un polinomio. No obstante, su defecto fundamental consiste en que los cálculos necesarios para la construcción del sistema de Sturm son muy engorrosos, de lo cual se puede convencer el lector realizando todos los cálculos respectivos en el primero de los ejemplos considerados anteriormente. En virtud de esto, se demostrarán ahora dos teoremas que no proporcionarán el número exacto de raíces reales, sino solamente una cota **superior** de este número. Después de haber hallado mediante la gráfica una cota **inferior** para el número de raíces reales, la aplicación de estos teoremas dará la posibilidad de hallar a veces el número exacto de raíces reales sin recurrir al método de Sturm.

Sea dado un polinomio $f(x)$ de n-ésimo grado, de coeficientes reales, que puede tener raíces múltiples. Consideremos el sistema formado por sus derivadas sucesivas

$$f(x) = f^{(0)}(x),\ f'(x),\ f''(x),\ \ldots,\ f^{(n-1)}(x),\ f^{(n)}(x), \qquad (1)$$

en el cual la última es igual al coeficiente superior a_0 del polinomio $f(x)$, multiplicado por $n!$, conservando por consiguiente constante el signo. Si el número real c no es raíz de ninguno de los polinomios del sistema (1), el número de variaciones de signo que presenta el sistema ordenado de números

$$f(c),\ f'(c),\ f''(c),\ \ldots,\ f^{(n-1)}(c),\ f^{(n)}(c).$$

se designará con $S(c)$.

Por lo tanto, se puede considerar la función $S(x)$, definida para los valores de x que no anulan a ninguno de los polinomios del sistema (1).

Veamos cómo varía el número $S(x)$ al crecer x. Mientras x no pase por una raíz de alguno de los polinomios (1), el número $S(x)$ no puede variar. En virtud de esto, tenemos que examinar dos casos: el paso de x por una raíz del polinomio $f(x)$ y el paso de x por una raíz de una de las derivadas $f^{(k)}(x)$, $1 \leqslant k \leqslant n-1$.

Sea α una raíz múltiple de orden l del polinomio $f(x)$, $l \geqslant 1$, o sea,

$$f(\alpha) = f'(\alpha) = \ldots = f^{(l-1)}(\alpha) = 0,\ f^{(l)}(\alpha) \neq 0.$$

Sea ε un número positivo tan pequeño que el intervalo $(\alpha - \varepsilon, \alpha + \varepsilon)$ no contenga raíces de los polinomios $f(x)$, $f'(x)$, $\ldots$ $\ldots$, $f^{(l-1)}(x)$ diferentes de α y no contenga tampoco ninguna raíz del polinomio $f^{(l)}(x)$. Demostremos que en el sistema de números

$$f(\alpha-\varepsilon),\ f'(\alpha-\varepsilon),\ \ldots,\ f^{(l-1)}(\alpha-\varepsilon),\ f^{(l)}(\alpha-\varepsilon),$$

dos números consecutivos cualesquiera tienen signos contrarios, mientras que todos los números

$$f(\alpha+\varepsilon),\ f'(\alpha+\varepsilon),\ \ldots,\ f^{(l-1)}(\alpha+\varepsilon),\ f^{(l)}(\alpha+\varepsilon)$$

tienen un mismo signo. Como cada uno de los polinomios del sistema (1) es la derivada del polinomio anterior, no nos queda más que demostrar que si x pasa por una raíz α del polinomio $f(x)$, entonces, independientemente del orden de multiplicidad de esta raíz, $f(x)$ y $f'(x)$ tenían signos contrarios antes del paso, y después del paso sus signos coinciden. Si $f(\alpha-\varepsilon)>0$, entonces $f(x)$ decrece en el intervalo $(\alpha-\varepsilon,\ \alpha)$, de donde, $f'(\alpha-\varepsilon)<0$; si $f(\alpha-\varepsilon)<0$, entonces $f(x)$ crece y, por lo tanto, $f'(\alpha-\varepsilon)>0$. Por consiguiente, en ambos casos los signos son distintos. Por otra parte, si $f(\alpha+\varepsilon)>0$, entonces $f(x)$ crece en el intervalo $(\alpha,\ \alpha+\varepsilon)$ y $f'(\alpha+\varepsilon)>0$; análogamente, de $f(\alpha+\varepsilon)<0$ se deduce que $f'(\alpha+\varepsilon)<0$. Por lo tanto, después de pasar por la raíz α, los signos de $f(x)$ y $f'(x)$ tienen que coincidir.

De lo demostrado se deduce que al pasar x por una raíz de orden l del polinomio $f(x)$, el sistema

$$f(x),\ f'(x),\ \ldots,\ f^{(l-1)}(x),\ f^{(l)}(x)$$

pierde l variaciones de signo.

Sea ahora α una raíz de las derivadas

$$f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ 1\leqslant k\leqslant n-1,\ l\geqslant 1,$$

no siendo raíz de $f^{(k-1)}(x)$ y tampoco de $f^{(k+1)}(x)$. Por lo demostrado anteriormente, el paso de x por α da lugar a una pérdida de l variaciones de signo en el sistema:

$$f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ f^{(k+l)}(x).$$

Por cierto, este paso puede crear una nueva variación de signo entre $f^{(k-1)}(x)$ y $f^{(k)}(x)$; sin embargo, como $l\geqslant 1$, al pasar x por α, el número de variaciones de signo en el sistema

$$f^{(k-1)}(x),\ f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ f^{(k+l)}(x),$$

o no varía, o disminuye. Pero, puede disminuir solamente en un número par, pues los polinomios $f^{(k-1)}(x)$ y $f^{(k+l)}(x)$ no cambian sus signos al pasar x por el valor α.

De los resultados obtenidos se deduce que, *si los números a y b, $a<b$, no son raíces de ninguno de los polinomios del sistema* (1), *el número de raíces reales del polinomio $f(x)$, comprendidas entre a y b y contadas cada una de ellas tantas veces como lo indique su orden de multiplicidad, es igual a la diferencia $S(a)-S(b)$ o es menor que esta diferencia en un número par.*

Para debilitar las restricciones impuestas a los números a y b, introduzcamos las siguientes notaciones. Supongamos que el número real c no es raíz del polinomio $f(x)$, pudiendo ser, posiblemente, raíz de otros polinomios del sistema (1). Designemos con $S_+(c)$ el número de variaciones de signo que presenta el sistema de números

$$f(c),\ f'(c),\ f''(c),\ \ldots,\ f^{(n-1)}(c),\ f^{(n)}(c) \tag{2}$$

calculado del modo siguiente: si

$$f^{(k)}(c) = f^{(k+1)}(c) = \ldots = f^{(k+l-1)}(c) = 0, \tag{3}$$

pero

$$f^{(k-1)}(c) \neq 0,\ f^{(k+l)}(c) \neq 0, \tag{4}$$

entonces se supone que $f^{(k)}(c)$, $f^{(k+1)}(c)$, $\ldots$, $f^{(k+l+1)}(c)$ tienen el mismo signo que $f^{(k+1)}(c)$; por supuesto, esto equivale a suponer que al calcular el número de variaciones de signo que presenta el sistema (2), los ceros se han eliminado. Por otra parte, designemos con $S_-(c)$ el número de variaciones de signo que presenta el sistema (2), calculado del modo siguiente: cumpliéndose las condiciones (3) y (4), se supone que $f^{(k+i)}(c)$, $0 \leqslant i \leqslant l-1$, tiene el mismo signo que $f^{(k+l)}(c)$, si la diferencia $l - i$ es par, y el signo contrario, si esta diferencia es impar.

Si se quiere determinar ahora el número de raíces reales del polinomio $f(x)$, comprendidas entre a y b, $a < b$, donde a y b no son raíces de $f(x)$, pudiendo ser, posiblemente, raíces de otros polinomios del sistema (1), se obra del modo siguiente. Sea ε tan pequeño que el intervalo $(a,\ a + 2\varepsilon)$ no contenga raíces del polinomio $f(x)$ y tampoco raíces diferentes de a de los demás polinomios del sistema (1); sea, por otra parte, η tan pequeño que el intervalo $(b - 2\eta,\ b)$ no contenga raíces de $f(x)$ y tampoco raíces, diferentes de b, de los demás polinomios del sistema (1). Entonces, el número buscado de raíces reales del polinomio $f(x)$ será igual al número de raíces reales de este polinomio, comprendidas entre $a + \varepsilon$ y $b - \eta$, o sea, por lo demostrado anteriormente, será igual a la diferencia $S(a + \varepsilon) - S(b - \eta)$ o será menor que esta diferencia en un número par. Mas, fácilmente se observa que

$$S(a+\varepsilon) = S_+(a),\ S(b-\eta) = S_-(b).$$

Con esto queda demostrado el siguiente

Teorema de Budan — Fourier. *Si los números reales a y b, $a < b$, no son raíces del polinomio $f(x)$ de coeficientes reales, el número de raíces reales de este polinomio, comprendidas entre a y b, y contadas cada una de ellas tantas veces como indique su orden de multiplicidad, es igual a la diferencia $S_+(a) - S_-(b)$ o es menor que esta diferencia en un número par.*

Designemos con el símbolo ∞ un valor positivo tan grande de la indeterminada x que los signos de los valores correspondientes de todos los polinomios del sistema (1) coincidan con los signos de sus coeficientes superiores. Como estos coeficientes son sucesivamente los números $a_0, na_0, n(n-1)a_0, \ldots, n!a_0$, cuyos signos coinciden, resulta $S(\infty) = S_-(\infty) = 0$. Por otra parte, como

$$f(0) = a_n,\ f'(0) = a_{n-1},\ f''(0) = a_{n-2}2!,$$
$$f'''(0) = a_{n-3}3!,\ \ldots,\ f^{(n)}(0) = a_0 \cdot n!,$$

donde $a_0, a_1, \ldots, a_n$ son los coeficientes del polinomio $f(x)$, resulta que $S_+(0)$ coincide con el número de variaciones de signo que presenta el sistema de coeficientes del polinomio $f(x)$, en el cual no se cuentan los coeficientes iguales a cero. Así, aplicando el teorema de Budan—Fourier al intervalo $(0, \infty)$, resulta el teorema siguiente:

Teorema de Descartes. *El número de raíces positivas de un polinomio $f(x)$, contadas cada una tantas veces como indique su orden de multiplicidad, es igual al número de variaciones de signo que presenta el sistema de coeficientes de este polinomio (los coeficientes iguales a cero no se cuentan) o es menor que este número en un número par.*

Está claro que para la determinación del número de raíces negativas del polinomio $f(x)$ es suficiente aplicar el teorema de Descartes al polinomio $f(-x)$. Naturalmente, si en este caso ninguno de los coeficientes del polinomio $f(x)$ es igual a cero, a las variaciones de signo que presenta el sistema de coeficientes del polinomio $f(-x)$ corresponden **permanencias** de signo que presenta el sistema de coeficientes del polinomio $f(x)$, y viceversa. Por lo tanto, *si un polinomio $f(x)$ no tiene coeficientes iguales a cero, el número de sus raíces negativas (contadas con su orden de multiplicidad) es igual al número de permanencias de signo que presenta el sistema de coeficientes o es menor que éste en un número par.*

He aquí *otra demostración más del teorema de Descartes* que no se basa en el teorema de Budan — Fourier. Demostremos primero el lema siguiente:

Si $c > 0$, entonces el número de variaciones de signo que presenta el sistema de coeficientes del polinomio $f(x)$, es menor en un número impar que el número de variaciones de signo que presenta el sistema de los coeficientes del producto $(x - c) f(x)$.

En efecto, encerrando entre paréntesis los términos consecutivos de un mismo signo, expresemos el polinomio $f(x)$, cuyo coeficiente superior a_0 se supone positivo, del modo siguiente:

$$f(x) = (a_0x^n + \ldots + b_1x^{k_1+1}) - (a_1x_1^{k_1} + \ldots + b_2x^{k_2+1}) + \ldots$$
$$\ldots + (-1)^s (a_sx^{k_s} + \ldots + b_{s+1}x^t). \qquad (5)$$

Aquí $a_0 > 0$, $a_1 > 0$, . . ., $a_s > 0$, mientras que b_1, b_2, . . ., b_s son positivos o iguales a cero; pero b_{s+1} se supone estrictamente positivo, de modo que x^t, donde $t \geqslant 0$, es la potencia mínima de la indeterminada x que figura en el polinomio $f(x)$, con un coeficiente diferente de cero. La expresión

$$a_0x^n + \ldots + b_1x^{k_1+1})$$

puede constar eventualmente de un solo sumando; esto sucede cuando $k_1 + 1 = n$. Observaciones análogas se refieren también a otras expresiones entre paréntesis que figuran en la fórmula (5).

Escribamos ahora el polinomio igual al producto $(x - c) f(x)$, en el que separaremos solamente los términos que contengan las potencias $n + 1$, $k_1 + 1$, . . ., $k_s + 1$ y t de la indeterminada x. Resulta

$$(x-c) f(x) = (a_0x^{n+1} + \ldots) - (a_1'x^{k_1+1} + \ldots) + \ldots$$
$$\ldots + (-1)^s (a_s'x^{k_s+1} + \ldots - cb_{s+1}x^t), \quad (6)$$

donde $a_i' = a_i + cb_i$, $i = 1, 2, \ldots, s$, por lo cual, como $c > 0$, todas las a_i' son estrictamente positivas. Por lo tanto, el sistema de coeficientes del polinomio $f(x)$ presenta entre los términos a_0x^n y $-a_1x^{k_1}$ (y también entre los términos $-a_1x^{k_1}$ y $a_2x^{k_2}$, etc). una variación de signo, y el polinomio $(x - c) f(x)$ presenta entre los términos correspondientes a a_0x^{n+1} y $-a_1'x^{k_1+1}$ (respectivamente, entre los términos $-a_1'x^{k_1+1}$ y $a_2x^{k_2+1}$, etc.) una variación de signo o más, pero en este último caso, inevitablemente, en **un número par** más. Aquí no nos interesan los lugares exactos de estas variaciones de signo; por ejemplo, puede ocurrir que el coeficiente de x^{k_1+2} en (6) sea negativo, igual que el coeficiente $-a_1'$ y que, por esto, estos dos coeficientes consecutivos no presenten variación de signo, es decir, que entre los paréntesis primeros las variaciones de signo estén situadas antes. Obsérvese ahora que los últimos paréntesis en (5) no presentaban ninguna variación de signo, mientras que los últimos paréntesis en (6) sí presentan, y, además, un número **impar** de ellas. Téngase en cuenta que los últimos coeficientes de los polinomios $f(x)$ y $(x - c) f(x)$, diferentes de cero, o sea, $(-1)^s b_{s+1}$ y $(-1)^{s+1}b_{s+1}c$, tienen signos contrarios. Por lo tanto, al pasar de $f(x)$ a $(x - c) f(x)$ el número total de variaciones de signo que presenta el sistema de coeficientes aumenta inevitablemente en un número impar (naturalmente, la suma de unos cuantos términos, de los cuales uno es impar y los demás son pares, es impar). El lema está demostrado.

Para demostrar el teorema de Descartes, designemos con $\alpha_1, \alpha_2, \ldots, \alpha_k$ todas las raíces positivas del polinomio $f(x)$.

Por lo tanto,

$$f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_h)\varphi(x),$$

donde $\varphi(x)$ es un polinomio de coeficientes reales sin raíces reales positivas. De aquí se deduce que el primero y el último coeficiente del polinomio $\varphi(x)$, diferentes de cero, son de un mismo signo, o sea, el sistema de coeficientes de este polinomio presenta un número par de variaciones de signo. Aplicando ahora sucesivamente el lema demostrado anteriormente a los polinomios

$$\varphi(x),\ (x-\alpha_1)\varphi(x),\ (x-\alpha_1)(x-\alpha_2)\varphi(x),\ \ldots,\ f(x),$$

se obtiene que el número de variaciones de signo que presenta el sistema de coeficientes aumenta cada vez en un número impar, o sea, en una unidad más un número par; por esto, el número de variaciones de signo que presenta el sistema de coeficientes del polinomio $f(x)$ es mayor que el número k en un número par.

Apliquemos los teoremas de Descartes y de Budan-Fourier al polinomio *examinado anteriormente*:

$$h(x) = x^6 + 2x^4 - 5x^3 + 8x^2 - 7x - 3.$$

El *número de variaciones de signo* que presenta el sistema de coeficientes es igual a tres y, por consiguiente, según el teorema de Descartes, $h(x)$ puede tener una o tres raíces positivas. Por otra parte, $h(x)$ no tiene coeficientes iguales a cero, y como el sistema de coeficientes presenta dos permanencias de signo, resulta que $h(x)$ o bien tiene dos raíces negativas, o bien, no tiene ninguna. Comparando con los resultados obtenidos antes mediante la gráfica, vemos que dos es el número exacto de raíces negativas de nuestro polinomio.

Para la determinación exacta del número de raíces positivas, aplicaremos el teorema de Budan-Fourier al intervalo $(1, \infty)$, pues, en el § 39 ya se había demostrado que 1 es una cota inferior de las raíces positivas del polinomio $h(x)$. Las derivadas sucesivas de $h(x)$ también fueron halladas en el § 39. Hallemos sus signos para $x = 1$ y $x = \infty$:

	$h(x)$	$h'(x)$	$h''(x)$	$h'''(x)$	$h^{IV}(x)$	$h^{V}(x)$	Número de variaciones de signo
$x=1$	−	+	+	+	+	+	1
$x=\infty$	+	+	+	+	+	+	0

De aquí se deduce, que el sistema de derivadas, al pasar x de 1 a ∞, pierde una variación de signo, por lo que, $h(x)$ tiene exactamente una raíz positiva.

Obsérvese que, en general, **al buscar el número de raíces reales de un polinomio, se debe comenzar con la construcción de la gráfica y aplicar los teoremas de Descartes y Budan-Fourier; solamente en casos muy extremos se debe pasar a construir el sistema de Sturm.**

El teorema de Descartes se puede precisar cuando se sabe previamente que todas las raíces del polinomio son reales, como esto tiene lugar, por ejemplo, en el caso del polinomio característico de una matriz simétrica. Resulta que:

Si todas las raíces del polinomio $f(x)$ son reales y el término independiente es diferente de cero, el número k_1 de raíces positivas de este polinomio es igual al número s_1 de variaciones de signo que presenta el sistema de sus coeficientes, y el número k_2 de raíces negativas es igual al número s_2 de variaciones de signo que presenta el sistema de coeficientes del polinomio $f(-x)$.

En efecto, en estas condiciones,

$$k_1 + k_2 = n, \tag{7}$$

donde n es el grado del polinomio $f(x)$, y, según el teorema de Descartes

$$k_1 \leqslant s_1, \quad k_2 \leqslant s_2. \tag{8}$$

Demostremos que

$$s_1 + s_2 \leqslant n. \tag{9}$$

La demostración se hará por el método de inducción sobre n, puesto que, como $a_0 \neq 0$, $a_1 \neq 0$, para $n = 1$ presenta variación de signo solamente uno de los polinomios

$$f(x) = a_0 x + a_1, \quad f(-x) = -a_0 x + a_1,$$

o sea, en este caso $s_1 + s_2 = 1$. Supongamos que la fórmula (9) ya está demostrada para los polinomios de grado menor que n. Si

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

donde $l \leqslant n-1$, $a_{n-l} \neq 0$, hacemos

$$g(x) = a_{n-l} x^l + \ldots + a_n.$$

Entonces

$$f(x) = a_0 x^n + g(x), \quad f(-x) = (-1)^n a_0 x^n + g(-x).$$

Si s_1' y s_2' son los números de variaciones de signo que presentan los sistemas de coeficientes de los polinomios $g(x)$ y $g(-x)$, respectivamente, entonces, según la hipótesis de inducción (claro que $l \geqslant 1$),

$$s_1' + s_2' \leqslant l.$$

Si $l = n-1$, entonces, solamente uno de los polinomios $f(x)$ o $f(-x)$ presentará una variación de signo en el primer sitio, o sea, para $f(x)$, entre a_0 y $a_1 \quad a_{n-l}$; por consiguiente

$$s_1 + s_2 = s_1' + s_2' + 1 \leqslant l + 1 = n.$$

Si $l \leqslant n-2$, entonces, cada uno de los polinomios $f(x)$, $f(-x)$ puede presentar variaciones de signo en los primeros lugares, pero, en este caso,

$$s_1 + s_2 \leqslant s_1' + s_2' + 2 \leqslant l + 2 \leqslant (n-2) + 2 = n.$$

Confrontando (7), (8) y (9), se obtiene que

$$k_1 = s_1, \quad k_2 = s_2,$$

como se quería demostrar.

§ 42. Cálculo aproximado de las raíces

Los métodos expuestos en los párrafos anteriores permiten efectuar la *separación* de las raíces reales de un polinomio $f(x)$ de coeficientes reales, es decir, indicar para cada raíz las cotas entre las que la raíz está comprendida. Si estas cotas son bastante estrechas, cualquier número comprendido entre ellas se puede tomar por valor aproximado de la raíz buscada. Por lo tanto, después de establecer, por el método de Sturm (o por otro método más sencillo), que entre los números **racionales** a y b está comprendida una sola raíz del polinomio $f(x)$, se plantea el problema de aproximar estas cotas entre sí, de modo que las nuevas cotas a' y b' tengan un número prefijado de sus primeras cifras decimales iguales; con esto, la raíz buscada quedará calculada con la exactitud dada.

Existen muchos métodos que permiten hallar con suficiente rapidez el valor aproximado de la raíz con la exactitud deseada. Aquí se indicarán dos de ellos, los que teóricamente son más simples y generales; al aplicarlos simultáneamente se obtiene el resultado con una rapidez satisfactoria. Es menester observar que los métodos que se van a exponer, no sólo pueden aplicarse a los polinomios, sino también a clases más amplias de funciones continuas.

A continuación se supondrá que α es una raíz **simple** del polinomio $f(x)$ (ya que podemos librarnos siempre de las raíces múltiples) y que la raíz α ya está separada de las demás raíces por las cotas a y b, $a < \alpha < b$; en particular, de aquí se deduce que $f(a)$ y $f(b)$ tienen signo contrario.

Método de interpolación lineal (llamado también *regula falsi*). Por valor aproximado de la raíz α se podría tomar, por ejemplo, la semisuma de las cotas a y b, $\frac{a+b}{2}$, o sea, el punto medio del intervalo limitado por los puntos a y b. Sin embargo, es más natural suponer que la raíz está más cerca de la cota que corresponde a un valor absoluto menor del polinomio. El método de interpolación lineal consiste en que se toma por valor aproximado de la raíz α el número c que divide el intervalo (a, b) en partes proporcionales

a los valores absolutos de los números $f(a)$ y $f(b)$, o sea,

$$\frac{c-a}{b-c} = -\frac{f(a)}{f(b)};$$

el signo menos del segundo miembro es debido a que $f(a)$ y $f(b)$ tienen signos contrarios. De aquí que

$$c = \frac{bf(a) - af(b)}{f(a) - f(b)}. \tag{1}$$

Como muestra la fig. 10, el método de interpolación lineal consiste en que en el intervalo (a, b) la curva $y = f(x)$ se sustituye por la cuerda que une los puntos $A\,(a, f(a))$ y $B\,(b, f(b))$, tomando por valor aproximado de la raíz α la abscisa del punto de intersección de esta cuerda con el eje x.

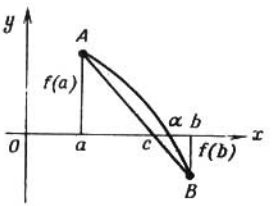

Fig. 10.

Método de Newton. Como α es una raíz simple del polinomio $f(x)$, se tiene $f'(\alpha) \neq 0$. Supongamos que también $f''(\alpha) \neq 0$, pues, en caso contrario, el problema se reduciría al cálculo de la raíz del polinomio $f''(x)$, que es de menor grado que $f(x)$. Supongamos que el intervalo (a, b) no contiene raíces de $f(x)$ diferentes de α, ni contiene tampoco ninguna raíz del polinomio $f'(x)$ y del

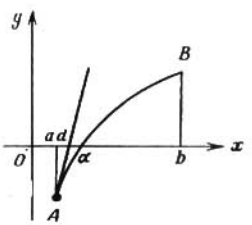

Fig. 11.

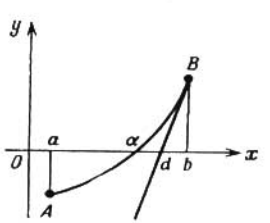

Fig. 12.

polinomio $f''(x)$ *. Por lo tanto, como se deduce del curso de análisis matemático, en el intervalo (a, b) la curva $y = f(x)$ es monótona creciente, o es monótona decreciente; además, en todos los puntos

* El estrechamiento de las cotas que da lugar a que se satisfaga esta condición se consigue ordinariamente sin dificultad alguna, pues los métodos expuestos anteriormente permiten determinar el número de raíces de los polinomios $f'(x)$ y $f''(x)$ en cualquier intervalo.

de este intervalo la convexidad está dirigida hacia arriba, o en todos los puntos la convexidad está dirigida hacia abajo. Por consiguiente, en la representación de la curva en el intervalo (a, b) pueden presentarse cuatro casos, expuestos en las figs. 11—14.

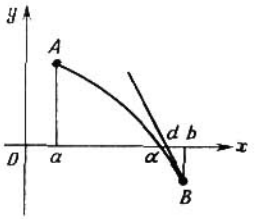

Fig. 13.

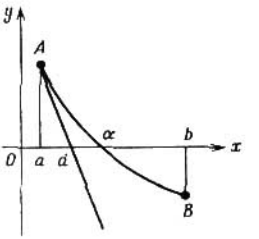

Fig. 14.

Designemos con a_0 uno de los extremos a o b, en el que **el signo de** $f(x)$ **coincide con el signo de** $f''(x)$. Como $f(a)$ y $f(b)$ tienen signos distintos y $f''(x)$ conserva el signo en todo el intervalo (a, b), tal a_0 puede ser indicado. En los casos representados en las figs. 11 y 14,

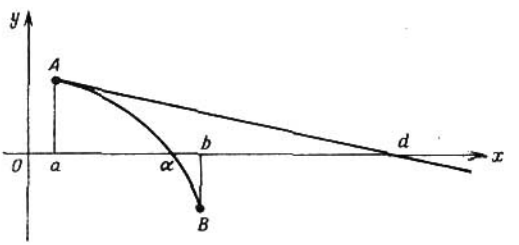

Fig. 15.

$a_0 = a$; en los otros dos casos, $a_0 = b$. Tracemos por el punto de abscisa a_0, es decir, por el punto de coordenadas $(a_0, f(a_0))$, la tangente a la curva $y = f(x)$ y designemos con d la abscisa del punto de intersección de esta tangente con el eje x. Las figs. 11—14 muestran que el número d se puede tomar por valor aproximado de la raíz α. Por consiguiente, el método de Newton consiste en sustituir la curva $y = f(x)$ en el intervalo (a, b) por su tangente, trazada en uno de los extremos de este intervalo. La condición impuesta a la elección del punto a_0 es esencial: la fig. 15 muestra que omitiendo

esta condición el punto de intersección de la tangente con el eje x puede estar muy lejos de ser una aproximación de la raíz buscada.

Hallemos la fórmula según la cual se busca el número d. Como se sabe, la ecuación de la tangente a la curva $y = f(x)$ en el punto $(a_0, f(a_0))$ se puede escribir en la forma

$$y - f(a_0) = f'(a_0)(x - a_0).$$

Poniendo aquí las coordenadas $(d, 0)$ del punto de intersección de la tangente con el eje x, resulta

$$-f(a_0) = f'(a_0)(d - a_0),$$

de donde

$$d = a_0 - \frac{f(a_0)}{f'(a_0)}. \qquad (2)$$

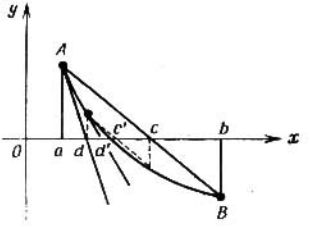

Fig. 16.

Si el lector une en las figs. 11—14 los puntos A y B con cuerdas, observará que *en todos los casos los métodos de interpolación lineal y de Newton dan una aproximación al valor verdadero de la raíz α por lados diversos*. Por esto, si el intervalo (a, b) satisface a las condiciones que se piden en el método de Newton, es conveniente **combinar** estos dos métodos. De este modo se obtienen para la raíz unas cotas más estrechas: c y d. Si éstas no dan todavía la exactitud de aproximación pedida, se les pueden aplicar otra vez más a estos límites ambos métodos (véase la fig. 16), etc; además, se puede demostrar que este proceso permite calcular verdaderamente la raíz α con la exactitud que se desee.

Apliquemos estos métodos al polinomio

$$h(x) \quad x^5 - 2x^4 - 5x^3 + 8x^2 - 7x - 3,$$

considerado en los párrafos anteriores.

Ya sabemos que este polinomio tiene una raíz simple α_1 comprendida entre los límites $1 < \alpha_1 < 2$. Se puede afirmar previamente, que estas cotas son demasiado amplias para que los métodos de interpolación lineal y de Newton, aplicados una sola vez, puedan dar un buen resultado. Sin embargo, los aplicaremos para tener un ejemplo de cálculos poco complicados.

Como ya vimos en el párrafo anterior, para $x = 1$ las derivadas $h'(x)$, $h''(x)$, ..., $h^{V}(x)$ toman valores positivos. Basándose en los resultados del § 39, se deduce que el valor $x = 1$ es, para $h'(x)$, y también para $h''(x)$, una cota superior de las raíces positivas. Por consiguiente, el intervalo $(1, 2)$ no contiene raíces de estas derivadas, pudiéndose aplicarle el método de Newton. Además, $h''(x)$ es positiva en todo este intervalo, y como

$$h(1) = -4, \quad h(2) = 39,$$

hay que poner $a_0 = 2$. Teniendo en cuenta que $h'(2) = 109$, aplicando la fórmula (2), hallamos:

$$d = 2 - \frac{39}{109} = \frac{179}{109} = 1{,}64\ldots$$

Por otra parte, la fórmula (1) da

$$c = \frac{2\cdot(-4)-1\cdot 39}{-4-39} = \frac{47}{43} = 1{,}09\ldots$$

y, por consiguiente, la raíz α_1 está comprendida entre las cotas

$$1{,}09 < \alpha_1 < 1{,}65.$$

Hemos obtenido un estrechamiento de las cotas demasiado insignificante para que este resultado sea satisfactorio. Claro, a las nuevas cotas obtenidas se les podrían aplicar de nuevo nuestros métodos. Sin embargo, sería conveniente hallar desde el principio para α_1 unas cotas bastante estrechas, por ejemplo, con una exactitud de 0,1 e incluso hasta de 0,01, y solamente después aplicar estos métodos. Naturalmente, esto daría lugar a que los cálculos se complicasen muchísimo, pero al resolver problemas concretos, en los que se necesitan conocer las raíces de un polinomio con bastante exactitud, no hay más remedio que actuar de este modo.

Volvamos a examinar nuestro polinomio $h(x)$ y su raíz α_1. Obsérvese que todos los valores de los polinomios que aparecen a continuación se calculan por la regla de Horner. Como

$$h(1{,}3) = -0{,}13987,\quad h(1{,}31) = 0{,}0662923851,$$

se tiene

$$1{,}3 < \alpha_1 < 1{,}31,$$

es decir, hemos hallado el valor de la raíz α_1 con una exactitud de 0,01. Apliquemos ahora los métodos de interpolación lineal a estas nuevas cotas:

$$c = \frac{1{,}31\cdot(-0{,}13987)-1{,}3\cdot 0{,}0662923851}{-0{,}13987-0{,}0662923851} = \frac{0{,}26940980063}{0{,}2061623851} = 1{,}30678\ldots$$

Apliquemos el método de Newton a estas mismas cotas, en donde se debe poner $a_0 = 1{,}31$. Como

$$h'(1{,}31) = 20{,}92822405,$$

se tiene

$$d = 1{,}31 - \frac{0{,}0662923851}{20{,}92822405} = \frac{27{,}3496811204}{20{,}92822405} = 1{,}30683\ldots$$

Por lo tanto

$$1{,}30678 < \alpha_1 < 1{,}30683,$$

por consiguiente, poniendo $\alpha_1 = 1{,}30681$, se comete un error menor que 0,00003.

Hasta ahora no hemos demostrado que los métodos expuestos anteriormente permiten calcular la raíz con la exactitud deseada, o sea, no hemos demostrado la convergencia de estos métodos. Demostremos esto únicamente para el método de Newton.

Supongamos de nuevo que la raíz simple α del polinomio $f(x)$ está contenida en el intervalo (a, b), siendo éste elegido de la forma necesaria para la aplicación del método de Newton. De aquí se deduce, en particular, la existencia de unos números positivos A y B tales, que en todo el intervalo (a, b)

$$|f'(x)| > A,\quad |f''(x)| < B. \tag{3}$$

Hagamos la notación

$$C = \frac{B}{2A}$$

y supongamos que

$$C(b-a) < 1. \tag{4}$$

Para que se cumpla esta desigualdad, habrá posiblemente que sustituir las cotas (a, b) de la raíz α por otras más estrechas, lo cual no influye para que se cumplan las desigualdades (3). Sea a_0 la cota a o b, a la que se debe aplicar el método de Newton. Aplicando la fórmula (2), por valores aproximados de la raíz α obtenemos, sucesivamente, los números $a_1, a_2, \ldots, a_k, \ldots$, situados en el intervalo (a, b) y relacionados entre sí por las igualdades

$$a_k = a_{k-1} - \frac{f(a_{k-1})}{f'(a_{k-1})}, \quad k = 1, 2, \ldots \tag{5}$$

Sea

$$\alpha = a_k + h_k, \quad k = 0, 1, 2, \ldots \tag{6}$$

Entonces

$$0 = f(\alpha) = f(a_k) + h_k f'(a_k) + \frac{h_k^2}{2} f''(a_k + \theta h_k),$$

donde $0 < \theta < 1$. Debido a las condiciones impuestas al intervalo (a, b), $f'(a_k) \neq 0$, y teniendo en cuenta (5) y (6), resulta:

$$-\frac{h_k^2}{2}\frac{f''(a_k+\theta h_k)}{f'(a_k)} = h_k + \frac{f(a_k)}{f'(a_k)} = \alpha - \left(a_k - \frac{f(a_k)}{f'(a_k)}\right) = \alpha - a_{k+1} = h_{k+1}.$$

De aquí

$$|h_{k+1}| = h_k^2 \left|\frac{f''(a_k+\theta h_k)}{2f'(a_k)}\right| < h_k^2 \frac{B}{2A} = Ch_k^2, \qquad k = 0, 1, 2, \ldots$$

Por lo tanto,

$$|h_{k+1}| < Ch_k^2 < C^3 h_{k-1}^4 < C^7 h_{k-2}^8 < \ldots < C^{2^{k+1}-1} h_0^{2^{k+1}},$$

o bien, como $|h_0| = |\alpha - a_0| < b - a$,

$$|h_{k+1}| < C^{-1}|C(b-a)|^{2^{k+1}}, \qquad k = 0, 1, 2, \ldots \tag{7}$$

En virtud de la condición (4), de aquí se deduce que *la diferencia h_k entre la raíz α y su valor aproximado a_k, obtenido por aplicación reiterada del método de Newton, tiende a cero al crecer k*, como se quería demostrar.

Señalemos que la fórmula (7) da una *cota del error* para la $(k+1)$-ésima aproximación, lo cual es importante si el método de Newton se aplica solo, y no en combinación con el método de interpolación lineal.

En los cursos de la teoría del cálculo aproximado, el lector podrá hallar procedimientos más racionales para realizar los cálculos con los métodos expuestos. En estos mismos cursos se puede hallar la exposición de muchos métodos de cálculo aproximado de raíces. *Entre éstos, el más perfecto es el método de Lobachevski* (a veces, llamado equivocadamente método de Gräffe). Este método permite hallar simultáneamente los valores aproximados de todas las raíces, incluyendo las imaginarias, sin exigir la separación previa de ellas; no obstante, requiere cálculos muy complicados. Este método se basa *en la teoría de los polinomios simétricos expuesta en el cap. 11.*

CAPITULO X

CAMPOS Y POLINOMIOS

§ 43. Anillos y campos numéricos

En muchos de los apartados anteriores del curso nos encontrábamos en la situación siguiente: exponiendo un tema, se permitía operar, o bien con números complejos arbitrarios, o bien solamente con números reales. Pero, después advertimos que los resultados obtenidos tienen también valor cuando se consideran solamente números reales (o que se generalizan respectivamente, palabra por palabra, para el caso de números complejos arbitrarios). Por regla general, en todos estos casos se podía observar que la teoría expuesta se conservaría enteramente también en el caso en que se permitiese tratar solamente con números racionales. Ha llegado ya el momento de explicar al lector las causas verdaderas de este paralelismo, para exponer el material ulterior en su generalidad natural, es decir, en el idioma algebraico usual. Con este fin, introduciremos el concepto de **campo** y también el de **anillo**. A pesar de ser este último un concepto más amplio, en nuestro curso va a desempeñar un papel auxiliar.

Está claro que los sistemas de todos los números complejos, de todos los números reales y de todos los números racionales, al igual que el sistema de todos los números enteros, *poseen la propiedad común de que en cada uno de ellos, manteniéndose dentro de los límites del mismo sistema, no sólo se puede efectuar la suma y el producto, sino también la resta.* Esta propiedad de los sistemas numéricos indicados los distingue, por ejemplo, del sistema de los números enteros positivos o de los números reales positivos.

Todo sistema de números complejos, o, en particular, reales, que contiene la suma, la diferencia y el producto de dos cualesquiera de sus números, se llama *anillo numérico.* Por lo tanto, los sistemas de todos los números enteros, racionales, reales o complejos, son anillos numéricos. Por otra parte, ningún sistema de números positivos será un anillo, pues, si a y b son dos números positivos diferentes, entonces, $a - b$ o $b - a$ será negativo. Un sistema cualquiera de números negativos tampoco será anillo, aunque sólo sea por el hecho de que el producto de dos números negativos es positivo.

Con los cuatro ejemplos considerados anteriormente no se agotan ni mucho menos los anillos numéricos. Ahora se van a señalar otros ejemplos, cuya comprobación de que el sistema considerado de números es verdaderamente anillo, se dejará al lector.

Los números pares forman un anillo; en general, para cualquier número natural n, el conjunto de números enteros divisibles por n *es un anillo. Los números impares no forman anillo*, pues la suma de dos números impares es par.

Es anillo el conjunto de los números racionales cuyos denominadores, en las expresiones en forma de fracciones irreducibles, son potencias del número 2; en particular, a este conjunto pertenecen todos los números enteros, pues, sus expresiones irreducibles tienen en el denominador el número 1, o sea, dos elevado a la potencia cero. *En este ejemplo, en lugar del número 2 se podría tomar, naturalmente*, cualquier número primo p. En general, tomando cualquier conjunto de números primos, finito e incluso infinito, y considerando el sistema de los números racionales cuyos denominadores, en las expresiones en forma de fracciones irreducibles, pueden dividirse solamente por los números primos que *pertenecen al conjunto considerado*, se obtiene también un anillo. Por otra parte, el conjunto de los números racionales cuyos denominadores, en las expresiones en fracciones irreducibles no se dividen por el cuadrado de ningún número primo, no es un anillo, puesto que la propiedad indicada no se conserva al multiplicar.

Veamos ejemplos de anillos numéricos que no pertenecen enteramente *al anillo de los números racionales. El conjunto de los números* de la forma

$$a + b\sqrt{2}, \tag{1}$$

donde a y b son números racionales arbitrarios, es un anillo; a éste pertenecen, en particular, todos los números racionales (cuando $b = 0$), y también el mismo número $\sqrt{2}$ (cuando $a = 0$, $b = 1$). También obtendríamos un anillo, si nos limitásemos a considerar solamente los números de la forma (1) con coeficientes enteros a, b. Claro, en estos ejemplos, en lugar del número $\sqrt{2}$ se podría tomar $\sqrt{3}$ o $\sqrt{5}$, etc.

El sistema de números de la forma

$$a + b\sqrt[3]{2} \tag{2}$$

con cualesquiera coeficientes racionales (o solamente con enteros cualesquiera) a, b, no forma anillo, pues, como fácilmente se com-

prueba, el producto del número $\sqrt[3]{2}$ por sí mismo no puede ser expresado en la forma (2) *.

Sin embargo, el sistema de números de la forma

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \tag{3}$$

con cualesquiera coeficientes racionales a, b, c, es ya un anillo, y esto mismo tiene lugar si se considera el caso de coeficientes enteros.

Examinemos ahora todos los números reales que se pueden obtener aplicando varias veces las operaciones de adición, multiplicación y sustracción al número π, bien conocido por el lector, y a números racionales cualesquiera. Estos son los números que se pueden escribir en la forma

$$a_0 + a_1\pi + a_2\pi^2 + \ldots + a_n\pi^n, \tag{4}$$

donde a_0, a_1, a_2, . . ., a_n son números racionales, $n \geqslant 0$. Obsérvese que ningún número puede poseer dos expresiones distintas de la forma (4), puesto que, en caso contrario, tomando la diferencia de dos expresiones de éstas obtendríamos que el número π tendría que satisfacer a una ecuación de coeficientes racionales; sin embargo, con los métodos del análisis matemático se demuestra que π no puede satisfacer a ninguna ecuación de coeficientes racionales, o sea, es un número trascendente. Por cierto, sin aplicar este resultado, o sea, sin suponer que la expresión de un número en la forma (4) sea única, se puede demostrar que los números de la forma (4) forman un anillo.

El conjunto de los números que se obtienen del número π y de los números racionales aplicando varias veces las operaciones de sumar, multiplicar, restar y dividir, es también anillo. Para la demostración no hay necesidad de buscar alguna expresión especial buena para los números considerados (a pesar de que podría hallarse): si los números

* En efecto, supongamos que

$$\sqrt[3]{4} = a + b\sqrt[3]{2}, \tag{2'}$$

donde los números a y b son racionales. Multiplicando ambos miembros de esta igualdad por $\sqrt[3]{2}$, obtenemos:

$$2 = a\sqrt[3]{2} + b\sqrt[3]{4}.$$

Poniendo aquí la expresión (2') para $\sqrt[3]{4}$, después de ciertas transformaciones simples llegamos a la igualdad

$$(a + b^2)\sqrt[3]{2} = 2 - ab. \tag{2''}$$

Si $a + b^2 \neq 0$, resulta,

$$\sqrt[3]{2} = \frac{2 - ab}{a + b^2},$$

lo cual es imposible, pues, el segundo miembro es un número racional. Si $a + b^2 = 0$, en virtud de (2''), también $2 - ab = 0$. De estas dos igualdades resulta que $b^3 = -2$, lo cual de nuevo es imposible, pues el número b es racional.

α y β se han obtenido del número π y de ciertos números racionales, empleando las operaciones indicadas, esto mismo es cierto para los números $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, y también (siendo $\beta \neq 0$) para el número $\frac{\alpha}{\beta}$.

Por fin, tomando el conjunto de números complejos $a + bi$ con cualesquiera coeficientes **racionales** a, b, se obtiene un anillo; esto mismo resulta cuando nos limitamos a coeficientes **enteros** a, b.

Los ejemplos examinados no pueden dar una idea completa de la diversidad de anillos numéricos existentes. Sin embargo, aquí *no vamos a continuar la lista de ejemplos y pasaremos a estudiar un* caso especial y muy importante de anillos numéricos. Por supuesto, ya sabemos que en los sistemas de todos los números racionales, de todos los números reales y de todos los números complejos, se puede efectuar la división ilimitadamente (excepto la división por cero), *mientras que la división de los números enteros sale fuera de los límites* del sistema de estos números. Hasta ahora no habíamos prestado atención a esta distinción pero, en realidad, es muy importante y conduce a la definición siguiente.

Un anillo numérico se llama *campo numérico*, si éste contiene el *cociente de dos cualesquiera de sus números (se supone que el divisor* es diferente de cero). Por consiguiente, se puede hablar del campo de números racionales, del campo de números reales, del campo de números complejos, por otra parte, el anillo de los números enteros no forma un campo.

En realidad, algunos de los ejemplos considerados anteriormente de anillos numéricos son campos. Ante todo, obsérvese que no existen campos numéricos distintos del campo de números racionales y contenidos totalmente en éste (no se considera campo el sistema formado por el cero único). Se cumple incluso la siguiente afirmación más general:

El campo de números racionales está contenido totalmente en cualquier campo numérico.

En efecto, sea dado un campo numérico, que designaremos con la letra P. Si a es un número arbitrario del campo P y diferente de cero, *P contiene también el cociente de la división del número a* por sí mismo, o sea, el número uno. Sumando unas cuantas veces la unidad consigo misma, obtenemos que todos los números naturales están contenidos en el campo P. Por otra parte, en el campo P tiene que estar contenida la diferencia $a - a$, o sea, el número cero, y, *por esto, también pertenece a P el resultado que se obtiene al restar* de cero cualquier número natural, es decir, cualquier número entero negativo. Finalmente, en el campo P están contenidos también los cocientes de los números enteros, o sea, en general, todos los números racionales.

En el campo de los números complejos están contenidos muchos campos distintos, siendo el campo de números racionales el menor de ellos. Así, pues, el anillo de los números de la forma

$$a + b\sqrt{2} \tag{5}$$

con coeficientes **racionales** (y no sólo con enteros) **arbitrarios** a, b, es un campo. En efecto, consideremos el cociente de dos números de la forma (5), $a + b\sqrt{2}$ y $c + d\sqrt{2}$, donde se supone que este último es diferente de cero; por consiguiente, también es diferente de cero el número $c - d\sqrt{2}$ de donde,

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2}.$$

Hemos obtenido de nuevo un número de la forma (5), manteniéndose racionales los coeficientes. Naturalmente, en este ejemplo se puede sustituir el número $\sqrt{2}$ por la raíz cuadrada de cualquier número racional, cuya raíz cuadrada no pudiese ser extraída en el mismo campo de números racionales. Así, pues, los números de la forma $a + bi$ con coeficientes racionales a, b forman un campo.

§ 44. Anillo

En distintas ramas de las matemáticas y en sus aplicaciones, suele ocurrir frecuentemente que las operaciones algebraicas no se efectúan con números, sino con objetos de naturaleza distinta. En los capítulos anteriores se pueden hallar muchos de estos ejemplos recordemos el producto y la suma de matrices, la suma de vectores, las operaciones con los polinomios, las operaciones con las transformaciones lineales. La definición general de *operación algebraica* a que satisfacen las operaciones de sumar y de multiplicar en los anillos numéricos, y también las operaciones en los ejemplos indicados, consiste en lo siguiente.

Sea dado un conjunto M que conste de números o de objetos de naturaleza geométrica, o en general, de algunos entes, que llamaremos *elementos* de este conjunto. Se dice que *en el conjunto M está definida una operación algebraica*, si está indicada una regla según la cual, **a cada par** de elementos a, b de este conjunto se pone en correspondencia **de un modo unívoco** un tercer elemento c, perteneciente también a M. Esta operación puede llamarse adición (o suma), y entonces, c se llamará *suma* de los elementos a y b, representándose con la notación $c = a + b$; esta operación puede llamarse *multiplicación*, o sea, c será el *producto* de los elementos a y b ($c = ab$); finalmente, es posible que para la operación definida en el conjunto M se introduzca una nueva terminología y simbolismo.

En cada uno de los anillos numéricos están definidas dos operaciones independientes, la adición y la multiplicación. En lo que se refiere a la resta y a la división, éstas no pueden considerarse operaciones nuevas, pues son las *inversas* de la adición y multiplicación, respectivamente, si convenimos en tomar la siguiente definición general de *operación inversa*.

Supongamos que en el conjunto M está definida una operación algebraica, por ejemplo, la suma. Se dice que *para esta operación existe una operación inversa*, la resta, si **para cada** par de elementos a, b de M, existe en M un elemento d, **unívocamente determinado**, que satisface a la igualdad: $b + d = a$. En este caso, el elemento d *se llama diferencia de los elementos* a *y* b *y se designa con la notación* $d = a - b$.

Está claro que tanto la suma como la multiplicación poseen operación inversa en los campos numéricos (por cierto, la multiplicación *con cierta restricción*: el divisor *tiene que ser* diferente de cero). En los anillos numéricos que no son campos (como, por ejemplo, en el anillo de los números enteros), solamente la suma posee operación inversa.

Por otra parte, en el sistema de todos los polinomios en la indeterminada x, cuyos coeficientes pertenecen a un campo numérico fijado P, también están definidas dos operaciones: la suma y el producto; además, *la suma posee operación inversa: la resta.*

Como se sabe, tanto en los anillos numéricos como en el sistema de los polinomios, las operaciones de sumar y multiplicar poseen las propiedades siguientes (a, b, c, son números arbitrarios del anillo *numérico considerado o polinomios arbitrarios del sistema considerado*):

I. La adición es conmutativa: $a + b = b + a$.

II. La adición es asociativa: $a + (b + c) = (a + b) + c$.

III. La multiplicación es conmutativa: $ab = ba$.

IV. La multiplicación es asociativa: $a(bc) = (ab)c$.

V. La adición y la multiplicación están ligadas por la ley distributiva:

$$(a + b)c = ac + bc.$$

Ahora ya estamos preparados para hacer la definición general del concepto de anillo, que es uno de los conceptos fundamentales del álgebra.

Un conjunto R se denomina *anillo*, si se han definido en él dos operaciones, llamadas adición o suma y multiplicación, siendo ambas conmutativas y asociativas, y ligadas por la ley distributiva, poseyendo además la suma la operación inversa, llamada resta.

Por lo tanto, son ejemplos de anillos, los anillos numéricos y los anillos de polinomios en la indeterminada x con coeficientes de un

campo numérico dado e incluso de un anillo numérico dado. Señalemos otro ejemplo más que aclara con amplitud el concepto de anillo.

El curso de análisis matemático comienza con la definición de **función** de la variable real x. Consideremos el conjunto de las funciones, determinadas para **todos** los valores reales de x y que toman valores reales. En él definiremos las operaciones algebraicas del modo siguiente: la *suma* de dos funciones $f(x)$ y $g(x)$ será una función cuyo valor para cualquier $x = x_0$ será igual a la suma de los valores de las funciones dadas, o sea, igual a $f(x_0) + g(x_0)$; el *producto* de estas funciones será una función cuyo valor para cualquier $x = x_0$ será igual al producto $f(x_0) \cdot g(x_0)$. Es evidente que la suma y el producto existen para cualesquiera dos funciones del conjunto considerado. La validez de las propiedades I-V se comprueba sin dificultad alguna: la suma y multiplicación de funciones se reducen a la suma y multiplicación de sus valores para cualquier x, es decir, a operaciones con números reales para los que se cumplen las propiedades I-V. Finalmente, tomando por *diferencia* de las funciones $f(x)$ y $g(x)$ la función cuyo valor para cualquier $x = x_0$ sea igual a la diferencia $f(x_0) - g(x_0)$, obtenemos la sustracción, operación inversa a la adición. Con esto queda demostrado que *el conjunto de las funciones determinadas para todas las x reales, después de haber introducido del modo descrito anteriormente las operaciones de sumar y multiplicar, se convierte en un anillo.*

Se pueden obtener otros ejemplos de anillos de funciones, conservando las definiciones de las operaciones con las funciones dadas anteriomente, pero, considerando, por ejemplo, las funciones determinadas sólo para los valores positivos de la variable x o las funciones determinadas para los valores x del segmento $[0, 1]$. En general, el sistema de todas las funciones que tienen un campo dado de definición, es un anillo. También se podrían obtener ejemplos de anillos sin considerar todas las funciones determinadas en un campo dado, sino solamente las funciones continuas que se estudian en el curso de análisis matemático. Por otro lado, se podrían considerar las funciones complejas de variable compleja. Existen muchísimos anillos distintos de funciones, así como distintos anillos numéricos.

Establezcamos algunas **propiedades elementales** de los anillos que se deducen inmediatamente de su definición.

Estas propiedades son ordinarias para el caso de los números, sin embargo, pueda ser que al lector le sorprenda que éstas sean consecuencia solamente de las condiciones I-V y de la existencia unívoca de la resta.

Hagamos primero unas cuantas observaciones sobre la importancia de las condiciones I—V. El papel de las *leyes conmutativas* no necesita explicaciones. El valor de las *leyes asociativas* consiste

en lo siguiente: *en la definición de la operación algebraica se trata* de la suma o del producto de dos elementos solamente. Si, por ejemplo, probamos definir el producto de tres elementos a, b, c, nos *encontramos con la dificultad* de que, por lo general, los productos au y vc, donde $bc = u$, $ab = v$, pueden no coincidir, o sea, $a\,(bc) \neq (ab)\,c$. La ley asociativa exige que estos productos sean iguales a un mismo elemento del anillo: resulta natural tomar este elemento por producto abc, escribiéndolo ya sin paréntesis. *La ley asociativa permite también definir unívocamente el producto (respectivamente, la suma) de cualquier número finito de elementos del anillo*, es decir, permite demostrar la independencia del producto de cualesquiera n elementos de la distribución primaria de los paréntesis.

Demostremos esta afirmación por el método de inducción sobre n. Esta se ha demostrado ya para $n = 3$, por lo cual suponemos que $n > 3$ y que nuestra afirmación ya está demostrada para todos los números menores que n. Sean dados los elementos $a_1, a_2, \ldots, a_n$ y supongamos que en este sistema se han distribuido *los paréntesis de algún modo, indicando el orden en que se debe efectuar* la multiplicación. La última operación consistirá en multiplicar el producto de los primeros k elementos $a_1a_2 \ldots a_k$ (donde $1 \leqslant k \leqslant n-1$) por el producto $a_{k+1}\,a_{k+2} \ldots a_n$. Como estos productos constan de un número de factores menor *que* n, y *que por la hipótesis están definidos unívocamente, no queda más que* demostrar la igualdad

$$(a_1a_2 \ldots a_k)\,(a_{k+1}a_{k+2} \ldots a_n) = (a_1a_2 \ldots a_l)\,(a_{l+1}a_{l+2} \ldots a_n),$$

para cualesquiera k y l.

Con este fin, es suficiente considerar el caso $l = k+1$. En este caso, poniendo

$$a_1a_2 \ldots a_k = b, \quad a_{k+2}\,a_{k+3} \ldots a_n = c,$$

y, basándonos en la ley asociativa, obtenemos

$$b\,(a_{k+1}c) = (ba_{k+1})\,c.$$

Con esto queda demostrada nuestra afirmación.

En particular, se puede hablar del producto de n elementos *iguales entre sí, o sea, se puede introducir el concepto de potencia* a^n del elemento a con exponente entero y positivo n. Se comprueba fácilmente que son válidos en cualquier anillo las reglas de operación con los exponentes. De modo análogo, la ley asociativa de la adición nos lleva al concepto de *múltiplo na* del elemento a con un coeficiente entero y positivo n.

La *ley distributiva*, es decir, la regla ordinaria para abrir paréntesis, es la única exigencia en la definición de anillo que liga la suma y la multiplicación; el hecho de que el estudio simultáneo de las dos operaciones indicadas proporcione algo más que lo que se podría obtener al estudiarlas por separado, se debe solamente a esta ley. En la formulación de la ley distributiva participa únicamente la suma de dos términos. Pero sin dificultad se demuestra

que se verifica la igualdad

$$(a_1 + a_2 + \ldots + a_k)\, b = a_1 b + a_2 b + \ldots + a_k b$$

para cualquier k, y la regla general para multiplicar una suma por otra.

En cualquier anillo también se cumple la ley distributiva para la resta. En efecto, según la definición de la resta, el elemento $a - b$ satisface a la igualdad

$$b + (a - b) = a.$$

Multiplicando por c ambos miembros de esta igualdad y aplicando al primer miembro de ésta la ley distributiva, obtenemos:

$$bc + (a - b)\, c = ac.$$

Por consiguiente, el elemento $(a - b)\, c$ es la diferencia de los elementos ac y bc:

$$(a - b)\, c = ac - bc.$$

De la existencia de la resta se deducen unas propiedades muy importantes de los anillos. Si a es un elemento arbitrario del anillo R, la diferencia $a - a$ es un elemento del anillo completamente determinado. Su papel es análogo al del cero en los anillos numéricos, mas, según la definición, éste puede depender de la elección del elemento a y, por esto, lo designaremos por ahora mediante 0_a.

Demostremos que para todos los a, los elementos 0_a son iguales entre sí. En efecto, si b es otro elemento arbitrario del anillo R, agregando el elemento 0_a a ambos miembros de la igualdad

$$a + (b - a) = b$$

y aplicando la igualdad $0_a + a = a$, resulta:

$$0_a + b = 0_a + a + (b - a) = a + (b - a) = b.$$

Por lo tanto,

$$0_a = b - b = 0_b.$$

Hemos demostrado que *todo anillo R posee un elemento unívocamente determinado, cuya suma con cualquier elemento a de este anillo es igual a a.* Este elemento se llamará cero del anillo R y se designará con el símbolo 0, no representando un peligro serio el que sea confundido con el número cero. Por lo tanto,

$$a + 0 = a \text{ para todos los elementos } a \text{ de } R$$

En cualquier anillo, para cada elemento a existe un elemento opuesto $-a$ unívocamente determinado que satisface a la igualdad:

$$a + (-a) = 0;$$

precisamente, este elemento es la diferencia $0-a$; la unicidad es consecuencia de la unicidad de la resta. Evidentemente $-(-a)=a$. La diferencia $b-a$ de dos elementos cualesquiera del anillo se puede escribir ahora de la forma

$$b-a=b+(-a).$$

En efecto,

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

Para cualquier elemento a de un anillo y cualquier número entero positivo n, se cumple la igualdad:

$$n(-a)=-(na).$$

En efecto, agrupando los términos resulta:

$$na+n(-a)=n[a+(-a)]=n\cdot 0=0.$$

Hemos obtenido ahora la posibilidad de definir los *múltiplos negativos* de un elemento del anillo: siendo $n>0$, los elementos iguales $n(-a)$ y $-(na)$ se designarán mediante $(-n)a$. Finalmente, convengamos tomar por cero del anillo considerado el *múltiplo nulo* $0\cdot a$ de cualquier elemento.

Hemos dado la definición del cero empleando solamente la suma y su operación inversa, o sea, sin utilizar la multiplicación. Sin embargo, en el caso de los números, el cero posee respecto a la multiplicación una propiedad característica, que es además muy importante. El cero de cualquier anillo posee la propiedad: *en cualquier anillo, el producto de cualquier elemento por el cero es igual a cero.* La demostración se basa directamente en la ley distributiva: siendo a un elemento arbitrario del anillo R, cualquiera que sea el elemento auxiliar x de este anillo, se tiene:

$$a\cdot 0=a(x-x)=ax-ax=0.$$

Aplicando esta propiedad del cero se puede demostrar que *en cada anillo, para cualesquiera elementos a, b, se cumple la igualdad*:

$$(-a)b=-ab.$$

En efecto,

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

De aquí se deduce que la conocida regla de la multiplicación de los números negativos, «menos por menos da más», también se deduce de la definición de anillo, es decir, que *en cualquier anillo se verifica la igualdad*

$$(-a)(-b)=ab.$$

En efecto,

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

El lector demostrará ahora sin dificultad que en cualquier anillo, para los múltiplos (incluyendo los negativos) de cualquier elemento son válidas todas las reglas de operaciones con los múltiplos de un número.

Por lo tanto, las operaciones algebraicas en cualquier anillo poseen muchas propiedades ordinarias de las operaciones con los números. Sin embargo, no hay que creer que en cualquier anillo se conservan todas las propiedades de la suma y multiplicación de los números. Así, pues, la multiplicación de los números posee una propiedad que es recíproca a la considerada anteriormente: **si el producto de dos números es igual a cero, al menos uno de los factores es igual a cero.** Esta propiedad ya no se puede generalizar para cualquier anillo, pues, en algunos anillos se pueden señalar pares de elementos diferentes de cero, cuyo producto es igual a cero, es decir, $a \neq 0$, $b \neq 0$, pero $ab = 0$; los elementos a, b, que poseen esta propiedad se llaman *divisores de cero*.

Claro, entre los anillos numéricos no se pueden hallar ejemplos de anillos con divisores de cero. Tampoco contienen divisores de cero los anillos de polinomios de coeficientes numéricos. Pero hay muchos anillos de funciones que poseen divisores de cero. Obsérvese primeramente que en cualquier anillo de funciones el cero es la función que se convierte en cero para todos los valores de la variable x. Consideremos ahora las funciones $f(x)$ y $g(x)$ que siguen, definidas para todos los valores reales de x:

$$f(x) = 0 \text{ para } x \leqslant 0, \qquad f(x) = x \text{ para } x > 0;$$
$$g(x) = x \text{ para } x \leqslant 0, \qquad g(x) = 0 \text{ para } x > 0.$$

Estas funciones son diferentes de cero, pues, sus valores no son iguales a cero para todos los valores de x; sin embargo, el producto de estas funciones es igual a cero.

No todas las condiciones I-V que figuran en la definición de anillo son necesarias en igual medida. El desarrollo de la ciencia muestra que mientras las propiedades I y II de la suma y la ley distributiva V se cumplen en todas las aplicaciones, la introducción de las propiedades III y IV de la multiplicación en la definición de anillo resulta demasiado incómoda, reduciendo el posible campo de aplicación de este concepto. Así, pues, el conjunto de las matrices cuadradas de orden n de elementos reales, considerado con las operaciones de adición y multiplicación de matrices, satisface a todas las condiciones que figuran en la definición de anillo, excluyendo la ley conmutativa de la multiplicación. Las multiplicaciones no conmutativas aparecen con tanta frecuencia y en casos tan importantes que actualmente el término de «anillo» se entiende ordinariamente como anillo *no conmutativo* (mejor dicho, como un anillo que no es necesariamente conmutativo, en el sentido de que la multiplicación puede ser no conmutativa), llamando *anillo conmutativo* al tipo particular de anillos en los que se cumple la condición III.

Ultimamente ha aumentado el interés hacia los anillos con multiplicación no asociativa, elaborándose ya la teoría general de los anillos como la teoría

de los anillos no asociativos (es decir, que no son necesariamente asociativos). El conjunto de vectores del espacio euclídeo de tres dimensiones respecto a las operaciones de la suma y de la multiplicación vectorial (conocida por el curso de geometría analítica) es un ejemplo simple de tales anillos.

§ 45. Campo

Del mismo modo que entre los anillos numéricos fueron elegidos y denominados campos numéricos aquellos anillos en los que se podía efectuar la división (excepto la división por cero), resulta natural hacer lo mismo en el caso general. Obsérvese primeramente que *en ningún anillo es posible la división por cero*, debido a la propiedad del cero respecto a la multiplicación, demostrada anteriormente: dividir un elemento a por cero significa hallar en el anillo un elemento x tal, que $0 \cdot x = a$, lo cual es imposible si $a \neq 0$, pues, el primer miembro es igual a cero.

Hagamos la definición siguiente:

Un anillo P se llama *campo*, si consta no sólo del cero y en él es posible la división en todos los casos (a excepción de la división por cero), determinándose ésta unívocamente, o sea, si para cualesquiera elementos a, b de P, **de los cuales b es diferente de cero**, existe en P un elemento q, y sólo uno, que satisface a la igualdad: $bq = a$. El elemento q se llama *cociente* de los elementos a y b y se designa con la notación $q = \frac{a}{b}$ *.

Naturalmente, todos los campos numéricos son ejemplos de campos. El anillo de los polinomios en la indeterminada x con coeficientes reales o, en general, con coeficientes de algún campo numérico, no es campo: la división con resto que existe para los polinomios se diferencia, naturalmente, de la división «exacta», supuesta en la definición de campo. Por otra parte, se ve fácilmente que *el conjunto*

---

* En realidad, la unicidad de la división en un campo, así como la unicidad de la resta, supuesta en la definición de anillo, se puede demostrar sin dificultad aplicando otras condiciones que figuran en la definición de campo o, respectivamente, de anillo (*Nota del A.*).

Un caso más general resulta cuando no se insiste en que la operación de multiplicar satisfaga a la ley conmutativa (o sea, cuando el anillo puede ser no conmutativo; véase la última parte del § 44). En este caso, además del elemento q, tiene que existir en P un elemento q' (que puede ser distinto de q), y sólo uno, que satisfaga a la igualdad: $q'b = a$. El anillo P se llama entonces cuerpo. Por lo tanto, se puede decir que campo es un cuerpo conmutativo.

Según parece, el vocablo «campo», para la denominación abreviada de un cuerpo conmutativo, ha sido empleado por primera vez en castellano por R. Rodríguez Vidal, en su traducción de la obra de Birkhoff y MacLane «Algebra Moderna». Teniendo también en cuenta que en los libros soviéticos, el vocablo «поле» («campo») está ya admitido hace muchos años, creemos conveniente emplear a continuación este último como traducción del primero. (*Nota del T.*).

de las funciones racionales con coeficientes reales (véase el § 25) *forma un campo* que contiene al anillo de los polinomios, del mismo modo que el campo de los números racionales contiene al anillo de los números enteros.

Entre los anillos de funciones se pueden indicar otros ejemplos de campos; sin embargo, aquí no vamos a detenernos en ellos y pasaremos a examinar otros ejemplos de distinto género.

Todos los anillos numéricos y, en general, los anillos que hasta ahora hemos examinado, contienen una infinidad de elementos. Sin embargo, existen anillos e incluso campos que constan de un número finito de elementos. Los ejemplos más simples de *anillos finitos* y *campos finitos*, empleados esencialmente en la teoría de los números, se forman del modo siguiente.

Se toma un número natural cualquiera n, diferente de 1. Los números enteros a y b se llaman *congruentes respecto del módulo* n,

$$a \equiv b \,(\text{mód}\, n),$$

si al dividirlos por n dan un mismo residuo, o sea, si su diferencia es divisible por n. Todo el anillo de los números enteros se descompone en n clases disjuntas,

$$C_0,\ C_1,\ \ldots,\ C_{n-1}, \tag{1}$$

de números congruentes entre sí respecto del módulo n, donde la clase C_k, $k = 0, 1, \ldots, n-1$, consta de los números que al dividirlos por n dan el residuo k. Resulta que se puede definir la suma y el producto de estas clases de un modo muy natural.

Con este fin, tomemos unas clases cualesquiera C_k y C_l (no necesariamente distintas) del sistema (1). Sumando cualquier número de la clase C_k con cualquier número de la clase C_l, obtenemos cada vez números que pertenecen a una clase determinada: a la clase C_{k+l}, si $k + l < n$, o a la clase C_{k+l-n}, si $k + l \geqslant n$. Esto nos lleva a la siguiente definición de *suma de las clases*:

$$\begin{aligned} C_k + C_l &= C_{k+l} \quad \text{si} \quad k + l < n, \\ C_k + C_l &= C_{k+l-n} \quad \text{si} \quad k + l \geqslant n. \end{aligned} \tag{2}$$

Por otra parte, multiplicando cualquier número de la clase C_k por cualquier número de la clase C_l, obtenemos números que están de nuevo en una clase determinada: precisamente en la clase C_r, donde r es el residuo de la división del producto kl por n. Por lo tanto, tomamos la definición siguiente de *producto de clases*:

$$C_k \cdot C_l = C_r, \text{ donde } kl = nq + r,\ 0 \leqslant r < n. \tag{3}$$

El sistema (1) *de clases de números enteros, congruentes entre sí respecto del módulo* n, *es un anillo respecto de las operaciones definidas*

por las condiciones (2) *y* (3). En efecto, la validez de las condiciones I-V de la definición de anillo se establece comprobándolas directamente. Además, es también consecuencia de la validez de estas condiciones *en el anillo de los números enteros* y de la relación indicada anteriormente entre las operaciones con los números enteros y las operaciones con las clases. Está claro que la clase C_0, compuesta de los números divisibles por n, desempeña el papel del cero. El elemento opuesto para la clase C_k, $k = 1, 2, \ldots, n-1$, es la clase C_{n-k}. Por consiguiente, en el sistema de las clases (1) se puede definir la resta, es decir, este sistema satisface a todas las condiciones que figuran en la definición de anillo. Convengamos en designar el anillo obtenido mediante Z_n.

Si el número n es compuesto, el anillo Z_n *posee divisores de cero* y, por esto, como se demostrará más abajo, no puede ser campo. En efecto, si $n = kl$, donde $1 < k < n$, $1 < l < n$, las clases C_k y C_l son distintas de la clase cero C_0, pero, según la definición del producto de las clases (véase (3)), $C_k \cdot C_l = C_0$.

Si el número n es primo, el anillo Z_n *es un campo.*

En efecto, sean dadas las clases C_k y C_m, donde $C_k \neq C_0$, o sea, $1 \leqslant k \leqslant n-1$. Hay que demostrar que se puede dividir C_m por C_k, o sea, que se puede hallar una clase C_l tal, que $C_k \cdot C_l = C_m$. Si $C_m = C_0$, se tiene $C_l = C_0$. Si $C_m \neq C_0$ consideramos el sistema de números

$$k,\ 2k,\ 3k,\ \ldots,\ (n-1)\,k. \tag{4}$$

Todos estos números están fuera de la clase cero C_0, pues, el producto de dos números naturales menores que el número primo n no puede ser divisible por éste. Por otra parte, *ninguno* de los dos *números* sk y tk del sistema (4), $s < t$, puede estar situado en una clase, puesto que, en caso contrario, su diferencia

$$tk - sk = (t-s)\,k$$

sería divisible por n, lo cual es absurdo, debido a que el número n es primo. Por lo tanto, en cada clase no nula está situado exactamente *un número del sistema* (4). *En particular, en la clase* C_m *está situado* el número lk, donde $1 \leqslant l \leqslant n-1$, o sea, $C_l \cdot C_k = C_m$, y entonces la clase C_l es el cociente buscado de la división de C_m por C_k.

Por consiguiente, hemos obtenido una infinidad de campos finitos distintos: el campo Z_2, compuesto de dos elementos solamente, y también los campos Z_3, Z_5, Z_7, Z_{11}, etc.

Ahora veremos **algunas propiedades de los campos** que se deducen *de la existencia de la división. Estas propiedades son análogas* a las propiedades de los anillos basados en la existencia de la resta y se demuestran con los mismos razonamientos, por lo cual, la demostración la dejamos al lector.

Todo campo P posee un elemento, unívocamente determinado, cuyo producto por cualquier elemento a de este campo es igual a a. Este elemento, que coincide con los cocientes iguales entre sí $\frac{a}{a}$ para todos los a, diferentes de cero, se llama *unidad* del campo P y se designa con el símbolo 1. Por lo tanto,

$$a \cdot 1 = a \text{ para todos los elementos } a \text{ de } P.$$

En todo campo, para cualquier elemento a diferente de cero, existe un elemento recíproco a^{-1}, unívocamente determinado, que satisface a la igualdad

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

este elemento es precisamente $a^{-1} = \frac{1}{a}$. Está claro que $(a^{-1})^{-1} = a$. El cociente $\frac{b}{a}$ se puede escribir ahora en la forma

$$\frac{b}{a} = b \cdot a^{-1}.$$

Para cualquier elemento a diferente de cero, y cualquier entero positivo n, se verifica la igualdad

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

Designando estos elementos iguales entre sí mediante a^{-n}, obtenemos las *potencias negativas* de un elemento del campo, para las que rigen las reglas de operación ordinarias. Hagamos, finalmente, $a^0 = 1$ para todos los a.

La existencia de unidad no es una propiedad característica de los campos, pues, por ejemplo, el anillo de los números enteros posee unidad. Sin embargo, el ejemplo del anillo de los números pares muestra que no todos los anillos poseen unidad. Por otra parte, *todo anillo que posea unidad y que contenga al elemento recíproco de cualquier elemento diferente de cero, es un campo.* En efecto, en este caso el producto ba^{-1}, $a \neq 0$, servirá de cociente $\frac{b}{a}$. La unicidad de este cociente se demuestra sin dificultad alguna.

Obsérvese que *ningún campo contiene divisores de cero.* En efecto, sea $ab = 0$, pero $a \neq 0$. Multiplicando ambos miembros de la igualdad por el elemento a^{-1}, en el primer miembro resulta $(a^{-1} a) b = 1 \cdot b = b$, y en el segundo, $a^{-1} \cdot 0 = 0$, o sea, $b = 0$. De aquí se deduce que *en todo campo cualquier igualdad se puede simplificar por un factor común diferente de cero.* En efecto, si $ac = bc$ y $c \neq 0$, se tiene $(a - b) c = 0$, de donde $a - b = 0$, o sea, $a = b$.

De la definición del cociente $\frac{a}{b}$ (donde $b \neq 0$) y de la posibilidad, anteriormente demostrada, de escribirlo en forma de producto ab^{-1}, se puede demostrar sin dificultad que *en todo campo se conservan las reglas ordinarias de operación con los quebrados.* A saber,

$$\frac{a}{b} = \frac{c}{d} \text{ cuando, y sólo cuando, } ad = bc;$$

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd};$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};$$

$$\frac{-a}{b} = -\frac{a}{b}.$$

Característica de un campo. No todas propiedades de los campos numéricos se conservan en el caso de un campo arbitrario. Así, pues, sumando así mismo el número 1 unas cuantas veces, o sea, tomando cualquier entero positivo que sea múltiplo de la unidad, nunca se obtendrá el cero. En general, todos estos múltiplos, es decir, todos los números naturales, son distintos entre sí. Si se toman enteros múltiplos de 1 de algún campo finito, entre ellos habrá indispensablemente algunos que sean iguales, pues este campo tiene sólo un número finito de elementos distintos. Si todos los múltiplos enteros de la unidad del campo P son elementos distintos de este campo, o sea, si $k \cdot 1 \neq l \cdot 1$ cuando $k \neq l$, se dice que P es un campo de *característica cero*; tales son, por ejemplo, todos los campos numéricos. Si existen unos números enteros k y l, $k > l$ tales, que en P se cumple la igualdad $k \cdot 1 = l \cdot 1$, entonces $(k - l) \cdot 1 = 0$, es decir, existe en P un múltiplo positivo de la unidad igual a cero, llamándose entonces P *campo de característica finita.* Precisamente ésta es igual a p, si p es el primer coeficiente positivo con el que se anula la unidad del campo P. Todos los campos finitos son ejemplos de campos de característica finita; existen también campos infinitos de característica finita.

Si p es la característica del campo P, el número p es primo.

En efecto, de la igualdad $p = st$, donde $s < p$, $t < p$, resultaría la igualdad $(s \cdot 1)(t \cdot 1) = p \cdot 1 = 0$, y como el campo no puede tener divisores de cero, se tendría $s \cdot 1 = 0$, o bien, $t \cdot 1 = 0$, lo cual contradice a la definición de la característica como el coeficiente positivo **menor** que convierte en cero a la unidad del campo.

Si la característica del campo P es igual a p, para cualquier elemento a de este campo se verifica la igualdad $pa = 0$. Si la característica del campo P es igual a cero, a es un elemento de este campo y n es un número entero, entonces las condiciones $a \neq 0$ y $n \neq 0$ implican la desigualdad $na \neq 0$.

En efecto, en el primer caso, el elemento pa, o sea, la suma de p términos iguales a a, sacando a fuera de paréntesis, se puede representar en la forma

$$pa = a\,(p \cdot 1) = a \cdot 0 = 0.$$

En el segundo caso, para $a \neq 0$, de la igualdad $na = 0$, o sea, $a\,(n \cdot 1) = 0$, resultaría la igualdad $n \cdot 1 = 0$, y, como la característica del campo es igual a cero, se tendría $n = 0$.

Subcampos, ampliaciones (extensiones). Supongamos que una parte de los elementos de un campo P, formando un conjunto P', también forma un campo con respecto a las operaciones definidas en el campo P, es decir, que para dos elementos cualesquiera a, b de P', los elementos $a + b$, ab, $a - b$, y para $b \neq 0$, $\frac{a}{b}$, contenidos en el campo P, también pertenecen a P' (claro, cumpliéndose las leyes I-V en P también se cumplen en P'). En este caso, P' se llama *subcampo* del campo P, y P, *ampliación* (o extensión) del campo P'. Es evidente que el cero y la unidad del campo P también están contenidos en P' y en éste sirven también de cero y unidad. Así, pues, el campo de los números racionales es un subcampo del campo de los números reales; todos los campos numéricos son subcampos del campo de los números complejos.

Supongamos que en el campo P se han dado un subcampo P' y un elemento c situado fuera de P', y que hemos hallado el subcampo mínimo P'' del campo P que contiene a P' y a c. Este subcampo mínimo tiene que ser único, pues si P''' fuese otro subcampo más con estas propiedades, la intersección de los subcampos P'' y P''' (o sea, el conjunto de los elementos comunes a ambos subcampos) contendría a P' y al elemento c y, junto con dos elementos cualesquiera suyos, contendría también a su suma (esta suma tiene que estar contenida en P'' y en P''' y, por lo tanto, en su intersección), y también a su producto, resta y cociente; en otras palabras, esta intersección misma sería un subcampo, lo cual es absurdo, pues el subcampo P'' es mínimo. Se dice que el campo P'' *se ha obtenido por adjunción del elemento* c *al campo* P', empleándose la notación $P'' = P'(c)$.

Evidentemente, el campo $P'(c)$, además del elemento c y de todos los elementos del campo P', contiene también todos los elementos que se obtienen de ellos mediante la suma, multiplicación, resta y división. Como ejemplo, señalemos la ampliación del campo de los números racionales, considerado en el § 43, que consta de los números de la forma $a + b\sqrt{2}$ con racionales a, b; esta ampliación se obtiene por adjunción del número $\sqrt{2}$ al campo de los números racionales.

§ 46. Isomorfismo de los anillos (de los campos). Unicidad del campo de los números complejos

En la teoría de los anillos desempeña un gran papel el concepto de isomorfismo. Los anillos L y L' se llaman *isomorfos* si entre sus elementos se puede establecer una correspondencia biunívoca tal que, para cualesquiera elementos a, b de L y sus correspondientes elementos a', b' de L', a la suma $a + b$ le corresponda la suma $a' + b'$ y al producto ab, el producto $a'b'$.

Supongamos que entre los anillos L y L' se ha establecido una correspondencia de isomorfismo. *Entonces al cero* 0 *del anillo* L *le corresponde el cero* 0' *del anillo* L'. En efecto, supongamos que al elemento 0 le corresponde el elemento c' de L'. Tomemos un elemento arbitrario a de L y el elemento a' de L' que le corresponde. *Entonces, al elemento* $a + 0$ *le tiene que corresponder el elemento* $a' + c'$; pero como $a + 0 = a$, se tiene, $a' + c' = a'$, de donde $c' = 0'$. *Al elemento* $-a$ *le corresponde el elemento* $-a'$. En efecto, supongamos que al elemento $-a$ le corresponde el elemento d'. Entonces al elemento $a + (-a) = 0$ le tiene que corresponder el elemento $a' + d'$, o sea, $a' + d' = 0'$, de donde $d' = -a'$. De aquí resulta que *a la diferencia de elementos de* L *le corresponde la diferencia de los elementos correspondientes de* L'. Con razonamientos análogos se puede demostrar que, si el anillo L posee unidad, la imagen de este elemento (o sea, el elemento que le corresponde en L', en el isomorfismo considerado) es la unidad del anillo L', y si el elemento a de L tiene elemento recíproco a^{-1}, la imagen del elemento a^{-1} en L' es el elemento recíproco de a'.

De aquí se deduce que *un anillo que es isomorfo a un campo, es también un campo.* Fácilmente se ve también que la propiedad de un anillo de no tener divisores de cero se conserva también en la correspondencia de isomorfismo. En general, los anillos isomorfos pueden diferenciarse entre sí por la naturaleza de sus elementos, pero, por sus propiedades algebraicas, son idénticos. Cualquier teorema demostrado para un anillo subsiste también para los anillos que son isomorfos a él, si en la demostración del teorema se emplean solamente las propiedades de las operaciones y no las propiedades individuales de los elementos de este anillo. Por esta razón, *no vamos a considerar como diferentes los anillos o los campos que son isomorfos*; éstos serán para nosotros distintos ejemplares de un mismo anillo o campo.

Apliquemos este concepto al problema de la construcción del campo de los números complejos. La construcción del campo de los números complejos expuesta en el § 17, y basada en la aplicación de los puntos del plano, no es la única posible. En lugar de puntos se podrían haber tomado segmentos (vectores) en el plano que parten

del origen de coordenadas y, dando estos vectores por sus componentes a, b sobre los ejes coordenados, se determinaría la suma y el producto de vectores mediante las mismas fórmulas (2) y (3) del § 17, así como en el caso de los puntos del plano. En general, se podría no insistir en aplicar objetos geométricos. Observando que los puntos en el plano, así como los vectores en el plano, se determinan por pares ordenados de números reales (a, b), se puede tomar simplemente el conjunto de tales pares e introducir en él la suma y el producto según las fórmulas (2) y (3) del párrafo indicado.

En realidad, estos campos no se distinguirían por sus propiedades algebraicas, como muestra el teorema siguiente:

Todas las ampliaciones del campo de números reales D, obtenidas por adjunción al campo D de la raíz de la ecuación

$$x^2 + 1 = 0, \tag{1}$$

son isomorfas entre sí.

En efecto, sea dado algún campo P que represente una ampliación del campo D y que contenga al elemento que satisface a la ecuación (1). La elección de la notación de este elemento corre a nuestro cargo y, para este fin, emplearemos la letra i. Por lo tanto, se cumple la igualdad $i^2 + 1 = 0$ (de donde $i^2 = -1$), aquí la elevación a potencia y la suma se deben entender en el sentido de las operaciones definidas en el campo P. Queremos hallar ahora el campo $D(i)$ que se obtiene por adjunción del elemento i al campo D, es decir, hallar el subcampo mínimo del campo P que contiene al campo D y al elemento i.

Examinemos con este fin todos los elementos α del campo P que se pueden escribir de la forma

$$\alpha = a + bi, \tag{2}$$

donde a y b son números reales arbitrarios, y el producto del número b por el elemento i, así como la suma del número a y este producto, se deben entender en el sentido de las operaciones definidas en el campo P. Ningún elemento α del campo P puede poseer dos distintas expresiones de esta forma, puesto que de

$$\alpha = a + bi = \overline{a} + \overline{b}i,$$

siendo $b \neq \overline{b}$, resultaría

$$i = \frac{\overline{a} - a}{b - \overline{b}},$$

o sea, i sería un número real; si $b = \overline{b}$, resulta $a = \overline{a}$. En particular, entre los elementos del campo P que se expresan en la forma (2), figuran todos los números reales (cuando $b = 0$), y también el mismo elemento i (cuando $a = 0$, $b = 1$).

Demostremos que *el conjunto de todos los elementos de la forma* (2) *forman un subcampo del campo P*; éste será precisamente el campo buscado $D(i)$. Sean dados los elementos $\alpha = a + bi$ y $\beta = c + di$. Aplicando las leyes conmutativa y asociativa de la adición, así como la ley distributiva, que rigen en el campo P, obtenemos:

$$\alpha + \beta = (a + bi) + (c + di) = (a + c) + (bi + di),$$

de donde,

$$\alpha + \beta = (a + c) + (b + d)\, i, \tag{3}$$

o sea, esta suma pertenece de nuevo al conjunto de elementos considerado. Por otra parte,

$$-\beta = (-c) + (-d)\, i,$$

pues, en virtud de (3), se cumple la igualdad $\beta + (-\beta) = 0 + 0i = 0$; por lo tanto,

$$\alpha - \beta = \alpha + (-\beta) = (a - c) + (b - d)\, i, \tag{3'}$$

es decir, la resta no sale fuera de los límites del conjunto considerado. Aplicando de nuevo las propiedades I-V a que satisfacen las operaciones en el campo P (véase § 44) y basándose en la igualdad $i^2 = -1$, obtenemos:

$$\alpha\beta = (a + bi)(c + di) = ac + adi + bci + bdi^2,$$

o sea,

$$\alpha\beta = (ac - bd) + (ad + bc)\, i; \tag{4}$$

por lo tanto, el producto de dos elementos cualesquiera de la forma (2) es de nuevo un elemento de esta misma forma. Finalmente, supongamos que $\beta \neq 0$, es decir, que al menos uno de los números c, d, sea diferente de cero. Entonces también $c - di \neq 0$ y

$$(c + di)(c - di) = c^2 - (di)^2 = c^2 - d^2 i^2 = c^2 + d^2,$$

siendo $c^2 + d^2 \neq 0$. Por consiguiente, aplicando la afirmación hecha en el párrafo anterior, de que en cualquier campo se conservan todas las reglas de las operaciones con los quebrados y, por ende, un quebrado no varía al multiplicar su numerador y denominador por un elemento diferente de cero, obtenemos:

$$\frac{\alpha}{\beta} = \frac{a + bi}{c - di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)\, i}{c^2 + d^2},$$

es decir, el elemento

$$\frac{\alpha}{\beta} = \frac{ac + bd}{c^2 + d^2} + \frac{bc + ad}{c^2 + d^2}\, i \tag{4'}$$

tiene de nuevo la forma (2).

Demostremos ahora que *el subcampo obtenido* $D(i)$ *del campo P es isomorfo al campo de puntos del plano construido en el* § 17. Asocian-

do al elemento $a + bi$ del campo $D(i)$ el punto (a, b), en virtud de la unicidad de la expresión de la forma (2) para los elementos del campo $D(i)$, se obtiene una correspondencia biunívoca entre los elementos de este campo y todos los puntos del plano. En esta correspondencia, al número real a le corresponde el punto $(a, 0)$, debido a la igualdad $a = a + 0i$, y al elemento $i = 0 + 1 \cdot i$, el punto $(0, 1)$. Por otra parte, comparando las fórmulas (3) y (4) del presente párrafo con las fórmulas (2) y (3) del § 17, obtenemos que a la suma y al producto de los elementos α y β del campo $D(i)$ les corresponden los puntos que son la suma y, respectivamente, el producto de los puntos correspondientes de α y β.

Como todos los campos que son isomorfos a un campo dado son isomorfos entre sí el teorema queda demostrado. Vemos, en particular, que la elección de las fórmulas (2) y (3) en el § 17 para la definición de las operaciones con los puntos no fue casual y no puede ser modificada.

Además de los métodos de construcción del campo de los números complejos, examinados anteriormente, existen muchos otros métodos. Señalemos uno de estos, aplicando la suma y multiplicación de matrices.

Examinemos el anillo no conmutativo de las matrices de segundo orden sobre el campo de los números reales. Es evidente que las matrices escalares

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

forman en este anillo un subcampo que es isomorfo al campo de los números reales. Pero, resulta que *en el anillo de las matrices de segundo orden sobre el campo de los números reales, se puede hallar también un subcampo que es isomorfo al campo de los números complejos.* En efecto, pongamos en correspondencia a cada número complejo $a + bi$ la *matriz*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

De este modo, resulta una aplicación biunívoca de todo el campo de números complejos en una parte del anillo de las matrices de segundo orden; además, de las igualdades

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

se desprende que esta aplicación es isomorfa, puesto que las matrices que figuran en los segundos miembros de estas igualdades corresponden a los números complejos $(a + c) + (b + d)i = (a + bi) + (c + di)$ y $(ac - bd) + (ad + bc)i = (a + bi)(c + di)$. En particular la matriz

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

desempeña el papel de unidad imaginaria.

El resultado obtenido señala otro posible método de construcción del campo de números complejos, que es tan satisfactorio como los considerados anteriormente.

§ 47. Algebra lineal y álgebra de los polinomios sobre un campo arbitrario

En los capítulos precedentes dedicados al **álgebra lineal**, el campo de números reales desempeñaba ordinariamente el papel de campo fundamental. No obstante, se comprueba sin dificultad alguna que *muchos teoremas de estos capítulos se generalizan palabra por* palabra al caso de un campo fundamental arbitrario.

Así, pues, *para un campo fundamental arbitrario P son válidos el método de Gauss de resolución de los sistemas de ecuaciones lineales, la teoría de los determinantes y la regla de Cramer*, expuestas en el cap. 1. Solamente la observación sobre los determinantes antisimétricos, expuesta al final del § 4, exige la suposición de que la característica del campo P **sea diferente de dos.** Por cierto, la demostración de la propiedad 4 de este mismo párrafo carece de valor si la característica del campo P es igual a dos, a pesar de que sea válida la propiedad misma.

Es conveniente señalar también que la afirmación, enunciada a menudo en el cap. 1, sobre la existencia de un conjunto infinito de soluciones distintas de un sistema indeterminado de ecuaciones lineales, es válida también en el caso de cualquier campo fundamental P ***infinito***, pero carece de valor si el campo P *es* ***finito***.

La teoría de la dependencia lineal de los vectores, la teoría del rango de una matriz y la teoría general de los sistemas de ecuaciones lineales, expuestas en el cap. 2, así como el álgebra de las matrices del cap. 3 se generalizan también totalmente al caso de un campo fundamental arbitrario.

La teoría general de las formas cuadráticas, expuesta en el § 26, *se generaliza al caso de cualquier campo fundamental P, cuya característica sea diferente de dos.* Sin esta restricción, pierde su valor el teorema fundamental de este párrafo.

Supongamos, por ejemplo, que $P = Z_2$, es decir, que es un campo constituido por dos elementos, 0 y 1, siendo $1 + 1 = 0$, de donde $-1 = 1$, y supongamos que sobre este campo se ha dado una forma cuadrática $f = x_1x_2$. Si existe una transformación lineal

$$x_1 = b_{11}y_1 b_{12}y_2.$$

$$x_2 = b_{21}y_1 b_{22}y_2,$$

que lleve f a la forma canónica, en la igualdad

$$f = (b_{11}y_1 + b_{12}y_2)(b_{21}y_1 + b_{22}y_2) = b_{11}b_{21}y_1^2 + (b_{11}b_{22} + b_{12}b_{21})\, y_1y_2 + b_{12}b_{22}y_2^2$$

tiene que ser igual a cero el coeficiente $b_{11}b_{22} + b_{12}b_{21}$ del producto y_1y_2. Sin embargo, este coeficiente es igual al determinante de la transformación lineal considerada, pues, ya sea $b_{12}b_{21} = 1$, o $b_{12}b_{21} = 0$, en ambos casos, $b_{12}b_{21} = -b_{12}b_{21}$. Resulta que nuestra transformación lineal es degenerada.

El contenido ulterior del cap. 6 se refiere esencialmente a las formas cuadráticas de coeficientes complejos o reales.

Finalmente, *para el caso de un campo fundamental arbitrario P es válida toda la teoría de los espacios lineales y sus transformaciones lineales, expuesta en el cap. 7.* Por cierto, el concepto de raíz característica está ligado con la teoría de los polinomios sobre un campo arbitrario, de la que se hablará más adelante. Obsérvese que el teorema del § 33, sobre la relación entre las raíces características y los valores propios, se enuncia ahora del modo siguiente: las raíces características de una transformación lineal φ, pertenecientes al campo fundamental P, y sólo éstas, son valores propios de esta transformación.

La teoría de los espacios euclídeos (cap. 8) está ligada esencialmente con el campo de los números reales.

También se pueden generalizar para el caso de un campo fundamental arbitrario P algunos de los apartados del **álgebra de los polinomios** expuestos anteriormente. Sin embargo, es necesario fijar previamente el sentido exacto del concepto de polinomio sobre un campo arbitrario.

Esto se debe a que en el § 20 se señalaron dos puntos de vista sobre el concepto de polinomio: el concepto formal algebraico y el teórico funcional. Ambos se pueden generalizar al caso de un campo fundamental arbitrario. No obstante, siendo equivalentes para el caso de campos numéricos (véase el § 24) y, como fácilmente se comprueba para campos infinitos en general, *dejan de ser equivalentes ya para campos finitos.*

Veamos, por ejemplo, el campo Z_2 introducido en el § 45, compuesto de dos elementos 0 y 1, siendo $1 + 1 = 0$. Los polinomios $x + 1$ y $x^2 + 1$ con coeficientes de este campo, son distintos, o sea, no satisfacen a la definición algebraica de igualdad de polinomios. Sin embargo, ambos polinomios toman el valor 1 para $x = 0$ y el valor 0 para $x = 1$, es decir, como «funciones» de la «variable» x, que toma valores en el campo Z_2, tienen que suponerse iguales.

En el campo Z_3 compuesto de tres elementos: 0, 1, 2, donde $1 + 2 = 0$, se encuentran en la misma situación los polinomios: $x^3 + x + 1$ y $2x + 1$. En general, se pueden indicar ejemplos de este tipo para todos los campos finitos.

Por lo tanto, en la teoría relacionada al caso de un campo arbitrario P, es imposible admitir el punto de vista teórico funcional sobre los polinomios. Por consiguiente, es necesario aclarar definitivamente la definición formal algebraica de polinomio. Con este fin, realizaremos una **construcción del anillo de los polinomios sobre un campo arbitrario** P, que no utiliza desde el mismo comienzo la expresión ordinaria de los polinomios mediante «la indeterminada» x.

Examinemos todos los sistemas finitos ordenados posibles de elementos del campo P que tienen la forma

$$(a_0, a_1, \ldots, a_{n-1}, a_n), \tag{1}$$

donde n *es arbitrario,* $n \geqslant 0$; *para* $n > 0$ *tiene que ser* $a_n \neq 0$. Determinando para los sistemas de la forma (1), la suma y el producto de acuerdo a las fórmulas (3) y (4) del § 20, convertimos el conjunto de estos sistemas en un anillo conmutativo; para demostrar que se cumplen las propiedades necesarias no hay más que repetir palabra por palabra lo que se hizo en el § 20 para los polinomios numéricos.

En el anillo que hemos construido, los sistemas de la forma (a) (caso de $n = 0$) forman un subcampo que es isomorfo al campo P. Esto permite identificar tales sistemas con los elementos correspondientes a del campo P, o sea, suponer

$$(a) = a \text{ para todos los } a \text{ de } P. \tag{2}$$

Por otra parte, designemos el sistema $(0, 1)$ *con la letra* x,

$$x = (0, 1).$$

Entonces, aplicando la definición de producto indicada anteriormente, obtenemos que $x^2 = (0, 0, 1)$ y, en general,

$$x^k = (\underbrace{0, 0, \ldots, 0}_{k \text{ veces}}, 1) \tag{3}$$

Aplicando ahora la definición de suma y producto de sistemas *ordenados, y también las igualdades* (2) y (3), resulta:

$$\begin{aligned}(a_0, a_1, a_2, \ldots, a_{n-1}, a_n) &= \\ &= (a_0) + (0, a_1) + (0, 0, a_2) + \ldots \\ \ldots &+ (\underbrace{0, 0, \ldots, 0}_{n-1 \text{ veces}}, a_{n-1}) + (\underbrace{0, 0, \ldots, 0}_{n \text{ veces}}, a_n) = \\ = (a_0) &+ (a_1)(0, 1) + (a_2)(0, 0, 1) + \ldots \\ \ldots &+ (a_{n-1})(\underbrace{0, 0, \ldots, 0}_{n-1 \text{ veces}}, 1) + (a_n)(\underbrace{0, 0, \ldots, 0}_{n \text{ veces}}, 1) = \\ &= a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n.\end{aligned}$$

Por lo tanto, todo sistema ordenado de la forma (1) se puede expresar en forma de un polinomio con respecto a x, con coeficientes del campo P, siendo evidentemente esta expresión única. Basándose finalmente en la conmutatividad ya demostrada de la suma, se puede pasar a la expresión según las potencias decrecientes de x.

Por consiguiente, construimos aquí un anillo conmutativo que, naturalmente, se debe denominar *anillo de los polinomios en la indeterminada x sobre el campo P*. Este anillo se designa con la notación $P[x]$.

En el anillo $P[x]$ está contenido el mismo P, lo cual ya se había demostrado antes. Así como en el caso de anillos de polinomios sobre campos numéricos (véase § 20), *el anillo $P[x]$ posee unidad, no contiene divisores de cero y no es campo.*

Si el campo P está contenido en un campo más amplio $\bar{P}$, el anillo $P[x]$ es un subanillo del anillo $\bar{P}[x]$: puesto que todo polinomio con coeficientes de P se puede considerar como polinomio sobre el campo P, y la suma y el producto de polinomios dependen sólo de sus coeficientes, no variando al pasar a un campo más amplio.

Para tener una idea mejor acerca del concepto verdadero del «anillo de los polinomios sobre el campo P», examinémoslo también desde otro ángulo.

Supongamos que el campo P está contenido como subanillo en algún anillo conmutativo L. Un elemento α del anillo L se llama *algebraico sobre el campo P*, si existe una ecuación de grado n, $n \geqslant 1$, con coeficientes del campo P, a la cual satisface el elemento α; si tal ecuación no existe, el elemento α se llama *trascendente sobre el campo P*. Está claro que el elemento x del anillo $P[x]$ es trascendente sobre el campo P.

Subsiste el **teorema** siguiente:

Si el elemento α del anillo L es trascendente sobre el campo P, el subanillo L', obtenido por adjunción del elemento α al campo P (o sea, el subanillo mínimo del anillo L que contiene al campo P y al elemento α), *es isomorfo al anillo de los polinomios $P[x]$*.

En efecto, cualquier elemento β del anillo L que se puede expresar en la forma

$$\beta = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n, \quad n \geqslant 0, \tag{4}$$

con coeficientes $a_0, a_1, \ldots, a_{n-1}, a_n$ del campo P, estará contenido en el subanillo L'. El elemento β no puede poseer dos expresiones distintas de la forma (4), pues, restando una expresión de la otra resultaría una ecuación sobre el campo P a la que satisfaría el elemento α, lo cual contradice a la hipótesis de que el elemento α es trascendente. Sumando los elementos de la forma (4), según las reglas de la adición en el anillo L, se pueden sumar los coeficientes de potencias iguales de α; sin embargo, ésto coincide con la regla de adición de los polinomios. Por otra parte, multiplicando los elementos de la forma (4) según las leyes de la multiplicación en el anillo L y aplicando la ley de distribución, podemos efectuar la multiplicación término a término y reunir después los términos semejan-

tes; evidentemente, esto nos lleva a la conocida regla de la multiplicación de los polinomios. Con esto queda demostrado que los elementos de la forma (4) forman en el anillo L un subanillo que contiene al campo P y al elemento α, es decir, que coincide con L', y que este subanillo es isomorfo al anillo de los polinomios $P[x]$.

Vemos, pues, que la elección que hicimos de las definiciones para las operaciones con los polinomios no fue casual: ésta queda completamente determinada debido a que el elemento x del anillo $P[x]$ tiene que ser trascendente sobre el campo P.

Obsérvese que al construir el anillo de los polinomios $P[x]$ nunca se aplicó la división de los elementos del campo P y solamente una vez, cuando se demostraba la proposición sobre el grado del producto de los polinomios, hubo que referirse a la ausencia de divisores de cero en el campo P. Por consiguiente, se puede tomar un anillo conmutativo arbitrario L, y repitiendo la construcción realizada anteriormente, resulta *el anillo de los polinomios* $L[x]$ *sobre el anillo* L; **si en este caso el anillo L no contiene divisores de cero,** el grado del producto de los polinomios será igual a la suma de los grados de los factores y, por consiguiente, **el anillo de los polinomios** $L[x]$ ***tampoco contendrá divisores de cero.***

Volviendo a considerar los polinomios con coeficientes de un ***campo*** *arbitrario* P, observemos que, substancialmente, toda la **teoría de la divisibilidad de los polinomios** (véanse §§ 20-22) se generaliza a este caso. Precisamente, *en el anillo* $P[x]$ *tiene valor el algoritmo de la división con resto*, en la que el cociente, así como el residuo, pertenecen también al anillo $P[x]$. También tiene *sentido en el anillo* $P[x]$ *el concepto de divisor y se conservan todas sus propiedades principales.* Además, como el algoritmo de la división no nos saca fuera de los límites del campo fundamental P, se puede afirmar que *la propiedad del polinomio* $\varphi(x)$ *de ser divisor de* $f(x)$ *no depende de que se considere el campo* P *o cualquier ampliación de él.*

En el anillo $P[x]$ *se conservan también la definición y todas las propiedades del máximo común divisor, incluyendo el algoritmo de Euclides y el teorema demostrado en el § 21 mediante este algoritmo.* Obsérvese que, como el algoritmo de la división con resto no depende, como ya sabemos, del campo fundamental elegido, se puede afirmar que *el máximo común divisor de dos polinomios dados tampoco depende de que se considere el campo* P *o una ampliación arbitraria* $\bar{P}$ *del mismo.* Finalmente, *para los polinomios sobre el campo* P *tiene sentido el concepto de raíz y conservan su valor las propiedades fundamentales de las raíces.*

También se conserva la teoría de las raíces múltiples; por cierto, al final del párrafo siguiente volveremos a examinar esta cuestión.

Estas observaciones nos permitirán referirnos en adelante a los §§ 20-22 al estudiar los polinomios sobre cualquier campo P.

§ 48. Descomposición de los polinomios en factores irreducibles

En virtud del teorema de existencia de raíz (§ 24), para los campos de números complejos y reales quedó demostrada la existencia y unicidad de la descomposición de un polinomio en factores irreducibles. Estos resultados son casos particulares de los teoremas generales referentes a polinomios sobre un campo arbitrario P. El presente párrafo está dedicado a la exposición de esta teoría general, que es análoga a la teoría de la descomposición de los números enteros en factores primos.

Determinemos primero los polinomios que desempeñan en el anillo de los polinomios el mismo papel que los números primos en el anillo de los números enteros. Subrayemos previamente que en esta definición se va a tratar solamente de **polinomios de grado mayor o igual a la unidad**; esto corresponde al hecho de que en la definición de los números primos, al estudiar las descomposiciones de los números enteros en factores primos, los números 1 y -1 se excluyan.

Sea dado un polinomio $f(x)$ de grado n, $n \geqslant 1$, con coeficientes pertenecientes al campo P. En virtud de la propiedad V del § 21, todos los polinomios de grado cero son divisores de $f(x)$. Por otra parte, en virtud de VII, también son divisores de $f(x)$ todos los polinomios $cf(x)$, donde c es un elemento de P diferente de cero, agotándose con éstos todos los divisores de $f(x)$ de grado n. En cuanto a los divisores de $f(x)$, de grado mayor que 0, pero menor que n, éstos pueden existir en el anillo $P[x]$, o pueden no existir. En el primer caso, el polinomio $f(x)$ se llama *reducible* en el campo P (o sobre el campo P); en el segundo caso, *irreducible* en este campo (o sobre este campo).

Recordando la definición de divisor se puede decir que *un polinomio $f(x)$ de grado n es reducible en el campo P, si se puede descomponer sobre este campo (o sea, en el anillo $P[x]$) en el producto de dos factores de grados menores que n:*

$$f(x) = \varphi(x)\,\psi(x); \tag{1}$$

$f(x)$ es irreducible en el campo P, si en cualquiera de sus descomposiciones de la forma (1), uno de los factores es de grado 0 y otro, de grado n.

Es menester tener en cuenta que se puede hablar de reducibilidad o irreducibilidad de un polinomio solamente con respecto a un campo dado P, pues, un polinomio que es irreducible en este campo puede ser reducible en cierta ampliación $\bar{P}$ de él. Por ejemplo, el polinomio $x^2 - 2$ de coeficientes enteros es irreducible en el campo de números racionales, puesto que no se puede descomponer en un producto de dos factores de primer grado con coeficientes racionales.

Sin embargo, este polinomio es reducible en el campo de números reales, como muestra la igualdad

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

El polinomio $x^2 + 1$ no sólo es irreducible en el campo de números racionales, sino también en el campo de números reales; sin embargo, se hace reducible en el campo de números complejos, puesto que

$$x^2 + 1 = (x - i)(x + i).$$

Indiquemos unas cuantas propiedades fundamentales de los polinomios irreducibles, recordando que se trata de polinomios irreducibles en el **campo** P.

α) *Todo polinomio de primer grado es irreducible.*

En efecto, si este polinomio se descompusiese en un producto de factores de menor grado, éstos tendrían que ser de grado cero. No obstante, el producto de cualesquiera polinomios de grado cero es de nuevo un polinomio de grado cero, y no de grado uno.

β) *Si el polinomio $p(x)$ es irreducible, lo es también cualquier polinomio $cp(x)$, donde c es un elemento de P diferente de cero.*

Esta propiedad es consecuencia de las propiedades I y VII § 21 y nos permitirá limitarnos, allí donde hiciese falta, al estudio de los polinomios irreducibles cuyos coeficientes superiores sean iguales a la unidad.

γ) *Si $f(x)$ es un polinomio arbitrario y $p(x)$ es un polinomio irreducible, entonces $f(x)$ es divisible por $p(x)$, o estos polinomios son primos entre sí.*

Si $(f(x), p(x)) = d(x)$, el polinomio $d(x)$, siendo divisor del polinomio irreducible $p(x)$, es de grado 0 o bien es un polinomio de la forma $cp(x)$, $c \neq 0$. En el primer caso, $f(x)$ y $p(x)$ son primos entre sí, en el segundo, $f(x)$ es divisible por $p(x)$.

δ) *Si el producto de los polinomios $f(x)$ y $g(x)$ es divisible por un polinomio irreducible $p(x)$, al menos uno de estos factores es divisible por $p(x)$.*

En efecto, *si $f(x)$ no es divisible por $p(x)$*, según γ), $f(x)$ y $p(x)$ son primos entre sí, y, entonces, según la propiedad b) del § 21, *el polinomio $g(x)$ tiene que ser divisible por $p(x)$.*

La propiedad δ) se generaliza sin dificultad al caso del producto *de cualquier número finito de factores.*

Los dos teoremas que siguen son el objeto principal del presente párrafo.

Todo polinomio $f(x)$ de grado n, $n \geqslant 1$, del anillo $P[x]$, se descompone en un producto de factores irreducibles.

En efecto, si el mismo polinomio $f(x)$ es irreducible, el producto indicado consta de un solo factor. Si es reducible, se puede descomponer en un producto de factores de menor grado. Si entre estos factores

hay de nuevo reducibles, efectuamos la descomposición siguiente en factores, etc. Este proceso tiene que terminarse después de un número finito de ensayos, pues, sea cual fuese la descomposición de $f(x)$ en factores, la suma de sus grados tiene que ser igual a n, por lo que el número de factores que dependen de x no puede ser mayor que n.

La descomposición de los números enteros en factores primos es única, si nos limitamos a considerar los números enteros positivos. Sin embargo, en el anillo de todos los números enteros la unicidad subsiste, salvo el signo: así pues, $-6 = 2\cdot(-3) = (-2)\cdot 3$, $10 = 2\cdot 5 = (-2)(-5)$, etc. En el anillo de los polinomios nos encontramos con una situación análoga. Si

$$f(x) = p_1(x)\, p_2(x) \ldots p_s(x)$$

es una descomposición del polinomio $f(x)$ en un producto de factores irreducibles y si los elementos $c_1, c_2, \ldots, c_s$ del campo P son tales que su producto es igual a 1, entonces en virtud de β),

$$f(x) = [c_1 p_1(x)]\cdot[c_2 p_2(x)] \ldots [c_s p_s(x)]$$

también será una descomposición de $f(x)$ en un producto de factores irreducibles. Con éstas se agotan todas las descomposiciones de $f(x)$:

Si un polinomio $f(x)$ del anillo $P[x]$ se descompone de dos modos en un producto de factores irreducibles:

$$f(x) = p_1(x)\, p_2(x) \ldots p_s(x) = q_1(x)\, q_2(x) \ldots q_t(x), \tag{2}$$

entonces, $s = t$ y, con una numeración adecuada, se verifican las igualdades:

$$q_i(x) = c_i p_i(x), \quad i = 1, 2, \ldots, s, \tag{3}$$

donde c_i son elementos del campo P diferentes de cero.

Este teorema subsiste para los polinomios de primer grado, pues, éstos son irreducibles. Por lo tanto, la demostración se hará empleando el método de inducción sobre el grado del polinomio, es decir, se demostrará el teorema para $f(x)$, suponiendo que ya está demostrado para los polinomios de menor grado.

Como $q_1(x)$ es divisor de $f(x)$, en virtud de la propiedad δ) y de la igualdad (2), $q_1(x)$ será divisor por lo menos de uno de los polinomios $p_i(x)$, por ejemplo, de $p_1(x)$. Mas, como el polinomio $p_1(x)$ es irreducible y el grado de $p_1(x)$ es mayor que cero, existe un elemento c_1 tal que

$$q_1(x) = c_1 p_1(x). \tag{4}$$

Poniendo en (2) esta expresión de $q_1(x)$ y simplificando por $p_1(x)$ (lo cual se permite, puesto que en el anillo $P[x]$ no hay divisores

de cero), se obtiene la igualdad

$$p_2(x)\, p_3(x) \ldots p_s(x) = [c_1 q_2(x)]\, q_3(x) \ldots q_t(x).$$

Como el grado del polinomio que es igual a estos productos, es menor que el grado de $f(x)$, queda ya demostrado que $s - 1 = t - 1$, de donde $s = t$, y que existen unos elementos $c_2', c_3, \ldots, c_s$, tales que $c_2' p_2(x) = c_1 q_2(x)$, de donde $q_2(x) = (c_1^{-1} c_2')\, p_2(x)$, y $c_i p_i(x) = q_i(x)$, $i = 3, \ldots, s$. Haciendo $c_1^{-1} c_2' = c_2$ y teniendo en cuenta (4), obtenemos la igualdad (3).

El teorema que acabamos de demostrar se puede enunciar más brevemente: *todo polinomio se descompone en factores irreducibles de un modo único, salvo factores de grado cero.*

Por cierto, siempre se puede considerar la descomposición de la siguiente forma especial, que *para cada polinomio ya es completamente única*: se toma cualquier descomposición del polinomio $f(x)$ en factores irreducibles y de cada uno de estos factores se saca fuera de paréntesis su coeficiente superior. Se obtiene la descomposición

$$f(x) = a_0 p_1(x)\, p_2(x) \ldots p_s(x), \tag{5}$$

donde todos los $p_i(x)$, $i = 1, 2, \ldots, s$, son polinomios irreducibles cuyos coeficientes superiores son iguales a la unidad. El factor a_0 será igual al coeficiente superior del polinomio $f(x)$, lo que se *comprueba fácilmente efectuando las multiplicaciones en el segundo* miembro de la igualdad (5).

Los factores irreducibles que forman parte de la descomposición (5), no son todos necesariamente distintos. Si el polinomio irreducible $p(x)$ figura unas cuantas veces en la descomposición (5), se llama *factor múltiple* de $f(x)$: precisamente, k es el orden de multiplicidad, si en la descomposición (5) hay exactamente k factores iguales a $p(x)$. Si el factor $p(x)$ figura en (5) una sola vez, se llama *factor simple* (el orden de multiplicidad es igual a uno) de $f(x)$.

Si en la descomposición (5) los factores $p_1(x)$, $p_2(x)$, $\ldots$, $p_l(x)$ son distintos entre sí y cualquier otro factor es igual a uno de éstos, siendo k_i, $i = 1, 2, \ldots, l$, el orden de multiplicidad del factor $p_i(x)$, la descomposición (5) se puede escribir en la forma siguiente:

$$f(x) = a_0 p_1^{k_1}(x)\, p_2^{k_2}(x) \ldots p_l^{k_l}(x). \tag{6}$$

A continuación se utilizará, por lo general, esta expresión, sin advertir ya que los exponentes son los órdenes de multiplicidad de los factores respectivos, es decir, que $p_i(x) \neq p_j(x)$ para $i \neq j$.

Dadas las descomposiciones de los polinomios $f(x)$ y $g(x)$ en factores irreducibles, el máximo común divisor $d(x)$ de estos polinomios es igual al producto de los factores que figuran simultáneamente en ambas descomposiciones, elevado cada factor a una potencia igual al mínimo de los órdenes de su multiplicidad en ambos polinomios.

En efecto, el producto indicado es divisor de cada uno de los polinomios $f(x)$ y $g(x)$, y, por esto, lo es también de $d(x)$. Si este producto fuese distinto de $d(x)$, en la descomposición de $d(x)$ en factores irreducibles estaría contenido un factor que no figura en la descomposición de alguno de los polinomios $f(x)$ y $g(x)$, lo cual es imposible, o bien, uno de los factores estaría elevado a una mayor potencia que la que tiene en la descomposición de alguno de los polinomios $f(x)$ y $g(x)$, lo cual, de nuevo, es imposible.

Este teorema es análogo a la regla según la cual se busca ordinariamente el máximo común divisor de los números enteros. Sin embargo, este teorema no puede sustituir al algoritmo de Euclides en el caso de los polinomios. En efecto, como sólo hay un número finito de números primos menores que un número entero positivo dado, la descomposición de un número entero en factores primos se consigue mediante un número finito de ensayos. Esto ya no se verifica en el anillo de los polinomios sobre un campo fundamental infinito y, en el caso general, no se puede señalar un método para la descomposición práctica de los polinomios en factores irreducibles. Incluso la resolución del problema para averiguar si el polinomio $f(x)$ es irreducible en un campo dado P, en el caso general, es muy difícil. Así pues, la descripción de todos los polinomios irreducibles para el caso de los campos de números complejos y reales fue obtenida en el § 24 como consecuencia de un teorema muy importante de existencia de la raíz. En lo que se refiere al campo de números racionales, se harán solamente algunas proposiciones de carácter particular en el § 56 con respecto a los polinomios irreducibles sobre este campo

Hemos demostrado que en el anillo de los polinomios, al igual que en el anillo de los números enteros, subsiste la descomposición en factores «primos» (irreducibles)* y que esta descomposición en cierto sentido es única. Surge la pregunta, ¿se pueden generalizar estos resultados a clases de anillos más amplios? En este caso nos limitaremos a considerar anillos conmutativos que posean unidad y no contengan divisores de cero.

Llamaremos *divisor de la unidad* a un elemento a del anillo para el que existe en este anillo el elemento recíproco a^{-1},

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

En el anillo de los números enteros, éstos son los números 1 y —1; en el anillo de los polinomios $P[x]$, todos los polinomios de grado cero, o sea, los números del campo P, distintos de cero. Un elemento c diferente de cero, que no es divisor de la unidad, se llama elemento *primo* del anillo, si en cualquiera de sus descomposiciones en un producto de dos factores, $c = ab$, uno de estos factores es inevitablemente divisor de la unidad. En el anillo de los números enteros son elementos primos los números primos, en el anillo de los polinomios, los polinomios irreducibles.

¿Se descompone en un producto de factores primos cualquier elemento del anillo considerado, que no sea divisor de la unidad y sea diferente de cero? En

* Llamada descomposición factorial. (*Nota del T.*).

caso de afirmacion, ¿será única tal descomposición? Esto último hay que entenderlo en el sentido siguiente: si

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

son dos descomposiciones del elemento a en factores primos, entonces, $k = l$ y (posiblemente, después de cambiar la numeración)

$$q_i = p_i c_i, \quad i = 1, 2, \ldots, k,$$

donde c_i es divisor de la unidad.

En el caso general, ambas preguntas tienen una respuesta negativa. Aquí nos limitaremos con un ejemplo: **indicaremos un anillo en el que la descomposición en factores primos, aunque es posible, no es única.**

Examinemos los números complejos de la forma

$$\alpha = a + b\sqrt{-3}, \tag{7}$$

donde a y b son números enteros. Todos estos números forman un anillo sin divisores de cero que contiene la unidad; en efecto,

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (bc + ad)\sqrt{-3}. \tag{8}$$

Llamemos *norma* del número $\alpha = a + b\sqrt{-3}$ al número entero positivo

$$N(\alpha) = a^2 + 3b^2.$$

En virtud de (8), *la norma del producto es igual al producto de las normas de los factores*:

$$N(\alpha\beta) = N(\alpha)\, N(\beta). \tag{9}$$

En efecto,

$$(ac - 3bd)^2 + 3(bc + ad)^2 = a^2c^2 + 9b^2c^2 + 3b^2c^2 + 3a^2d^2 =$$
$$= (a^2 + 3b^2)(c^2 + 3d^2).$$

Si en nuestro anillo el número α es divisor de la unidad, o sea, que el número α^{-1} también tiene la forma (7), entonces, por (9),

$$N(\alpha) \cdot N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1,$$

de aquí que, $N(\alpha) = 1$, pues los números $N(\alpha)$ y $N(\alpha^{-1})$ son enteros y positivos. Si $\alpha = a + b\sqrt{-3}$, de $N(\alpha) = 1$ se deduce que

$$N(\alpha) = a^2 + 3b^2 = 1;$$

sin embargo, esto es posible sólo cuando $b = 0$, $a = \pm 1$. Por lo tanto, *en nuestro anillo, así como en el anillo de los números enteros, son divisores de la unidad solamente los números* 1 *y* -1 *y solamente estos números tienen la norma igual a la unidad.*

Naturalmente, la igualdad (9) para la norma del producto se generaliza para el caso de un número finito de factores. De aquí fácilmente se deduce que *todo número* α *de nuestro anillo se puede descomponer en un producto de un número finito de factores primos*; la demostración se la dejamos al lector.

No obstante, *ya no se puede afirmar que la descomposición en factores primos es única*. Por ejemplo, se cumplen las igualdades.

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

En nuestro anillo no hay otros divisores de la unidad más que los números 1 y -1, por lo que el número $1 + \sqrt{-3}$ (así como el número $1 - \sqrt{-3}$) no puede diferenciarse del número 2 solamente en un factor que sea divisor de la unidad. No queda más que demostrar que en el anillo considerado, *cada uno de los números*

2, $1+\sqrt{-3}$, $1-\sqrt{-3}$ *es primo*. En efecto, la norma de cada uno de estos tres números es igual al número 4. Sea α uno de estos números y supongamos que

$$\alpha = \beta\gamma.$$

Entonces, según (9), es posible uno de los tres casos:
1) $N(\beta)=4$, $N(\gamma)=1$; 2) $N(\beta)=1$, $N(\gamma)=4$;
3) $N(\beta)=N(\gamma)=2$.
En el primer caso, como ya sabemos, el número γ es divisor de la unidad, en el segundo caso, el divisor de la unidad es β. En lo que se refiere al tercer caso, éste es imposible, en general, puesto que, para enteros a y b, la igualdad

$$a^2+3b^2=2$$

es imposible.

Factores múltiples. A pesar de que más arriba se indicó que no sabemos descomponer los polinomios en factores irreducibles, existen métodos para saber si un polinomio dado posee factores múltiples o no, y, en caso de una respuesta positiva, éstos permiten reducir el estudio de este polinomio al estudio de otros que ya no poseen factores múltiples. Sin embargo, estos métodos exigen la imposición de ciertas restricciones al campo fundamental. Precisamente, todo el contenido ulterior del presente párrafo se va a exponer suponiendo que **la característica del campo P es cero.** Sin esta restricción, los teoremas sobre los factores múltiples que se demostrarán a continuación, pierden su valor; además, desde el punto de vista de las aplicaciones, el caso de campos de característica cero es el más importante, pues, incluye a todos los campos numéricos.

Obsérvese primero que el concepto de **derivada** de un polinomio, introducido en el § 22 para los polinomios de coeficientes complejos, y las propiedades principales de este concepto, también se generalizan para el caso considerado*. Demostremos ahora el siguiente teorema:

Si $p(x)$ es un factor irreducible múltiple de orden k, $k \geqslant 1$, del polinomio $f(x)$, entonces, es también un factor múltiple de orden $(k-1)$ de la derivada de este polinomio. En particular, un factor simple del polinomio no figura en la descomposición de la derivada.

En efecto, supongamos que

$$f(x) = p^k(x)\, g(x), \tag{10}$$

donde $g(x)$ ya no es divisible por $p(x)$. Derivando la igualdad (10), resulta:

$$f'(x) = p^k(x)\, g'(x) + kp^{k-1}(x)\, p'(x)\, g(x) =$$
$$= p^{k-1}(x)\,[p(x)\, g'(x) + kp'(x)\, g(x)].$$

El segundo término que figura entre paréntesis no es divisible por $p(x)$; en efecto, $g(x)$ no es divisible por $p(x)$ según la hipótesis y

* Para los campos de característica finita carece de valor la afirmación de que la derivada de un polinomio de grado n es de grado $n-1$.

$p'(x)$ es de grado menor, o sea, tampoco es divisible por $p(x)$. De aquí, en virtud de la irreducibilidad del polinomio $p(x)$ y de las *propiedades δ) del presente párrafo y IX del § 21, resulta nuestra* afirmación. Por otra parte, el primer término que figura entre corchetes es divisible por $p(x)$, por lo cual, toda esta suma no puede ser divisible por $p(x)$, o sea, el factor $p(x)$ figura, efectivamente, en $f'(x)$ con la multiplicidad $k-1$.

De nuestro teorema y del método indicado anteriormente para la averiguación del máximo común divisor de dos polinomios, se deduce que, dada la descomposición del polinomio $f(x)$ en factores irreducibles:

$$f(x) = a_0 p_1^{k_1}(x)\, p_2^{k_2}(x) \ldots p_l^{k_l}(x), \tag{11}$$

el máximo común divisor del polinomio $f(x)$ y su derivada posee la siguiente descomposición en factores irreducibles:

$$(f(x),\ f'(x)) = p_1^{k_1-1}(x)\, p_2^{k_2-1}(x) \ldots p_l^{k_l-1}(x), \tag{12}$$

en la que, naturalmente, si $k_i = 1$, el factor $p_i^{k_i-1}(x)$ se debe sustituir por la unidad. En particular, *el polinomio $f(x)$ no contiene factores múltiples cuando, y sólo cuando, éste es primo con su derivada.*

Por consiguiente, hemos aprendido a responder a la pregunta sobre la existencia de factores múltiples de un polinomio dado. Además, como la derivada de un polinomio, así como el máximo común divisor de dos polinomios, no dependen de que se considere *el campo P o cualquiera de sus ampliaciones $\overline{P}$, como consecuencia* del resultado que acabamos de demostrar obtenemos que:

Si un polinomio $f(x)$ con coeficientes de un campo P de característica cero, no tiene sobre este campo factores múltiples, no los tendrá tampoco sobre ninguna ampliación $\overline{P}$ del campo P.

En particular, si $f(x)$ es irreducible sobre P, y $\overline{P}$ es alguna ampliación del campo P, entonces, aunque $f(x)$ pueda ser ya reducible *sobre $\overline{P}$, no puede ser divisible por el cuadrado de un polinomio* irreducible (sobre $\overline{P}$).

Separación de los factores múltiples. Dado un polinomio $f(x)$ con la descomposición (11) y designando con $d_1(x)$ el máximo común divisor de $f(x)$ y su derivada $f'(x)$, la expresión (12) representa la descomposición de $d_1(x)$. Dividiendo (11) por (12), resulta:

$$v_1(x) = \frac{f(x)}{d_1(x)} = a_0 p_1(x)\, p_2(x) \ldots p_l(x),$$

o sea, obtenemos un polinomio que carece de factores múltiples. Además, cualquier factor irreducible de $v_1(x)$ *es también* factor de $f(x)$. Con esto, la averiguación de los factores irreducibles de $f(x)$ se reduce a la averiguación de los mismos para el polinomio

$v_1(x)$, que, por lo general, es de menor grado y contiene solamente factores primos. Resolviendo este problema para $v_1(x)$, no queda más que determinar la multiplicidad en $f(x)$ de los factores irreducibles hallados, lo cual se consigue aplicando el algoritmo de la división.

Generalizando el método que acabamos de exponer, se puede pasar a examinar inmediatamente unos cuantos polinomios sin factores múltiples. Hallando sus factores irreducibles, no sólo obtenemos todos los factores irreducibles de $f(x)$, sino también sus órdenes de multiplicidad.

Sea (11) la descomposición de $f(x)$ en factores irreducibles y s, $s \geqslant 1$, el orden superior de multiplicidad de los factores. Designemos con $F_1(x)$ el producto de todos los factores de primer orden del polinomio $f(x)$; designemos con $F_2(x)$ el producto de todos los factores de segundo orden, pero tomados una sola vez cada uno, etc; finalmente, con $F_s(x)$ el producto de todos los factores de orden s, pero tomados también una sola vez cada uno. Si para cierto número j no existen en $f(x)$ factores de orden j, se supone que $F_j(x) = 1$. Entonces, $f(x)$ es divisible por la k-ésima potencia del polinomio $F_k(x)$, $k = 1, 2, \ldots, s$, y la descomposición (11) toma la forma

$$f(x) = a_0 F_1(x) F_2^2(x) F_3^3(x) \ldots F_s^s(x),$$

y la descomposición (12) para $d_1(x) = (f(x), f'(x))$ se escribe así:

$$d_1(x) = F_2(x) F_3^2(x) \ldots F_s^{s-1}(x).$$

Designando con $d_2(x)$ el máximo común divisor del polinomio $d_1(x)$ y su derivada y, en general, con $d_k(x)$, el máximo común divisor de los polinomios $d_{k-1}(x)$ y $d'_{k-1}(x)$, obtenemos:

$$\begin{aligned} d_2(x) &= F_3(x) F_4^2(x) \ldots F_s^{s-2}(x), \\ d_3(x) &= F_4(x) F_5^2(x) \ldots F_s^{s-3}(x), \\ &\cdots\cdots\cdots\cdots\cdots \\ d_{s-1}(x) &= F_s(x), \\ d_s(x) &= 1. \end{aligned}$$

De aquí que

$$\begin{aligned} v_1(x) &= \frac{f(x)}{d_1(x)} = a_0 F_1(x) F_2(x) F_3(x) \ldots F_s(x), \\ v_2(x) &= \frac{d_1(x)}{d_2(x)} = F_2(x) F_3(x) \ldots F_s(x), \\ v_3(x) &= \frac{d_2(x)}{d_3(x)} = F_3(x) \ldots F_s(x), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ v_s(x) &= \frac{d_{s-1}(x)}{d_s(x)} = F_s(x), \end{aligned}$$

y, finalmente,

$$F_1(x) = \frac{v_1(x)}{a_0 v_2(x)}, \quad F_2(x) = \frac{v_2(x)}{v_3(x)}, \ \ldots, \ F_s(x) = v_s(x).$$

Por lo tanto, aplicando sólo métodos que no exigen el conocimiento de los factores irreducibles de $f(x)$, como la derivación, la aplicación del algoritmo de Euclides y del algoritmo de la división, se pueden hallar los polinomios

$F_1(x)$, $F_2(x)$, ..., $F_s(x)$ que carecen de factores múltiples, siendo cada factor irreducible del polinomio $F_k(x)$, $k = 1, 2, \ldots, s$, un factor de $f(x)$ de orden k.

El método expuesto no se puede considerar como método de descomposición de un polinomio en factores irreducibles, pues, para $s = 1$, es decir, para un polinomio sin factores múltiples se obtendría solamente $f(x) = F_1(x)$.

§ 49. Teorema de existencia de la raíz

El teorema fundamental demostrado en el § 23, sobre la existencia de una raíz en el campo de números complejos para cualquier polinomio numérico, no se puede generalizar para el caso de un campo arbitrario. En el presente párrafo se va a demostrar un teorema que, en cierta medida, sustituye en la teoría general de los campos al teorema fundamental indicado del álgebra de los números complejos.

Sea dado un polinomio $f(x)$ sobre el campo P. Surge la pregunta: ¿existe alguna ampliación $\overline{P}$ del campo P en la que $f(x)$ tenga ya por lo menos una raíz, si el polinomio $f(x)$ carece totalmente de raíces en el campo P? Aquí se puede suponer que el grado de $f(x)$ es mayor que la unidad, pues, para los polinomios de grado cero la pregunta no tiene sentido y cualquier polinomio de primer grado $ax + b$ tiene la raíz $-\frac{b}{a}$ en el mismo campo P. Por otra parte, está claro que podemos limitarnos al caso en que el polinomio $f(x)$ sea irreducible en el campo P, puesto que, en caso contrario, la raíz de cualquiera de sus factores irreducibles serviría de raíz para sí mismo.

La respuesta nos la da el siguiente **teorema de existencia de la raíz:**

Para cualquier polinomio $f(x)$, irreducible sobre el campo P, existe una ampliación de este campo en la que está contenida una raíz de $f(x)$. Todos los campos mínimos que contienen al campo P y a alguna raíz de este polinomio, son isomorfos entre sí.

Demostremos primero la segunda mitad del teorema.

Sea dado un polinomio

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

$n \geqslant 2$, *irreducible sobre P, de modo que $f(x)$ no tiene raíces en el* mismo campo P. Supongamos que existe una ampliación $\overline{P}$ del *campo P, que contiene una raíz α de $f(x)$*, y *demostremos el siguiente* **lema** que, además de ser necesario para nuestra demostración, es también de interés particular:

Si la raíz α, perteneciente a $\overline{P}$, de un polinomio $f(x)$ irreducible en P, es también raíz de un polinomio $g(x)$ del anillo $P[x]$, entonces $f(x)$ es un divisor de $g(x)$.

En efecto, en el campo $\overline{P}$ los polinomios $f(x)$ y $g(x)$ tienen un común divisor, $x - \alpha$, por lo que no son primos entre sí. No obstante

la propiedad de los polinomios de no ser primos entre sí no depende del campo que se haya elegido, por lo cual, se puede pasar al campo P y aplicar la propiedad γ) del párrafo anterior.

Hallemos ahora el subcampo mínimo $P(\alpha)$ del campo $\overline{P}$ que contiene al campo P y al elemento α. Ante todo, al campo buscado pertenecen todos los elementos de la forma

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1}, \qquad (2)$$

donde b_0, b_1, b_2, . . ., b_{n-1} son elementos del campo P. Ningún elemento del campo $\overline{P}$ puede poseer dos expresiones distintas de la forma (2), pues si se cumpliese también la igualdad

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1},$$

donde por lo menos para un k fuese $c_k \neq b_k$, α sería raíz del polinomio

$$g(x) = (b_0 - c_0) + (b_1 - c_1)x + (b_2 - c_2)x^2 + \ldots + (b_{n-1} - c_{n-1})x^{n-1},$$

lo cual contradice al lema demostrado anteriormente, puesto que el grado de $g(x)$ es menor que el de $f(x)$.

Entre los elementos del campo $\overline{P}$ que tienen la forma (2), figuran todos los elementos del campo P (cuando $b_1 = b_2 = \ldots = b_{n-1} = 0$), y también el mismo elemento α (cuando $b_1 = 1$, $b_0 = b_2 = \ldots = b_{n-1} = 0$). Demostremos que *los elementos de la forma* (2) *forman todo el subcampo* $P(\alpha)$ *buscado*. En efecto, dados el elemento β (con la expresión (2)) y

$$\gamma = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1},$$

en virtud de las propiedades de las operaciones en el campo $\overline{P}$, se tiene

$$\beta \pm \gamma = (b_0 \pm c_0) + (b_1 \pm c_1)\alpha + (b_2 \pm c_2)\alpha^2 + \ldots + (b_{n-1} \pm c_{n-1})\alpha^{n-1}$$

o sea, la suma y la diferencia de dos elementos cualesquiera de la forma (2) son de nuevo elementos de la misma forma.

Multiplicando β por γ resulta una expresión que contiene a α^n y a potencias más superiores de α. Sin embargo, de (1) y de la igualdad $f(\alpha) = 0$, se deduce que α^n y, por lo tanto, α^{n+1}, α^{n+2}, etc, se pueden expresar mediante potencias menores del elemento α. El método más simple para hallar la expresión de $\beta\gamma$ consiste en lo siguiente: sean

$$\varphi(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}, \quad \psi(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1},$$

de donde, $\varphi(\alpha) = \beta$, $\psi(\alpha) = \gamma$. Multiplicando los polinomios $\varphi(x)$ y $\psi(x)$ y dividiendo este producto por $f(x)$, resulta

$$\varphi(x)\psi(x) = f(x)q(x) + r(x), \qquad (3)$$

donde

$$r(x) = d_0 + d_1 x + \ldots + d_{n-1} x^{n-1}.$$

Hallando los valores de ambos miembros de la igualdad (3) para $x = \alpha$, resulta:

$$\varphi(\alpha)\,\psi(\alpha) = f(\alpha)\,q(\alpha) + r(\alpha),$$

o sea, como $f(\alpha) = 0$,

$$\beta\gamma = d_0 + d_1\alpha + \ldots + d_{n-1}\alpha^{n-1}.$$

Por lo tanto, el producto de dos elementos de la forma (2) es de nuevo un elemento de la misma forma.

Demostremos, finalmente, que si el elemento β *es de la forma* (2) y $\beta \neq 0$, el elemento β^{-1}, que existe en el campo $\overline{P}$, también se puede expresar en la forma (2). Para esto, tomemos el polinomio

$$\varphi(x) = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}$$

del anillo $P[x]$. Como el grado de $\varphi(x)$ *es inferior al de* $f(x)$ y el polinomio $f(x)$ es irreducible sobre P, los polinomios $\varphi(x)$ y $f(x)$ son primos entre sí y, *en virtud de los* §§ 21 y 47, en el *anillo* $P[x]$ existen unos polinomios $u(x)$ y $v(x)$ tales que

$$\varphi(x)\,u(x) + f(x)\,v(x) = 1;$$

además, se puede suponer que el grado de $u(x)$ es menor que n:

$$u(x) = s_0 + s_1 x + \ldots + s_{n-1} x^{n-1}.$$

De aquí, en virtud de la igualdad $f(\alpha) = 0$, resulta:

$$\varphi(\alpha)\,u(\alpha) = 1;$$

y, por esto, debido a la igualdad $\varphi(\alpha) = \beta$, se tiene:

$$\beta^{-1} = u(\alpha) = s_0 + s_1\alpha + \ldots + s_{n-1}\alpha^{n-1}.$$

Por lo tanto, el *conjunto de los elementos* del campo $\overline{P}$ que tienen la forma (2) forman un subcampo del campo $\overline{P}$; éste será el campo buscado $P(\alpha)$. Como hemos visto, para hallar la suma y el producto de los elementos β y γ de la forma (2) solamente hay que conocer los coeficientes de las expresiones de estos elementos mediante las potencias de α, *por lo cual, se puede afirmar que subsiste el resultado* siguiente: si además de $\overline{P}$ existe otra ampliación $\overline{P}'$ del campo P que contiene también una raíz α' del polinomio $f(x)$, y si $P(\alpha')$ es el subcampo mínimo del campo $\overline{P}'$ que contiene a P y a α', *los campos* $P(\alpha)$ *y* $P(\alpha')$ *son isomorfos*, donde, para obtener la correspondencia de *isomorfismo* entre ellos hay que *asociar al elemento* β de la forma (2) de $P(\alpha)$ el elemento

$$\beta' = b_0 + b_1\alpha' + b_2\alpha'^2 + \ldots + b_{n-1}\alpha'^{n-1}$$

de $P(\alpha')$ que tiene los mismos coeficientes. Con esto, queda demostrada la segunda mitad del teorema.

Pasemos ahora a demostrar la primera mitad de este teorema, que es la fundamental; lo expuesto anteriormente nos indicará el camino a seguir. Dado un polinomio $f(x)$ de grado $n \geqslant 2$, irreducible sobre el campo P, se necesita construir una ampliación del campo P que contenga una raíz de $f(x)$. Consideremos para esto todo el anillo de los polinomios $P[x]$ y dividámosle en clases disjuntas, incluyendo en una clase a los polinomios que al ser divididos por el polinomio dado $f(x)$ proporcionen residuos iguales. En otras palabras, los polinomios $\varphi(x)$ y $\psi(x)$ pertenecerán a una misma clase, si su diferencia es divisible por $f(x)$.

Convengamos en designar las clases obtenidas con las letras A, B, C, etc, y definamos la suma y el producto de las clases del siguiente modo. Tomemos dos clases cualesquiera A y B; elijamos en la clase A algún polinomio $\varphi_1(x)$, en la clase B, algún polinomio $\psi_1(x)$, y designemos con $\chi_1(x)$ la suma de estos polinomios,

$$\chi_1(x) = \varphi_1(x) + \psi_1(x),$$

y con $\theta_1(x)$, su producto

$$\theta_1(x) = \varphi_1(x) \cdot \psi_1(x).$$

Elijamos ahora en la clase A cualquier otro polinomio $\varphi_2(x)$, en la clase B, cualquier polinomio $\psi_2(x)$, y designemos respectivamente con $\chi_2(x)$ y $\theta_2(x)$ su suma y producto:

$$\chi_2(x) = \varphi_2(x) + \psi_2(x),$$
$$\theta_2(x) = \varphi_2(x) \cdot \psi_2(x).$$

Según la condición, los polinomios $\varphi_1(x)$ y $\varphi_2(x)$ pertenecen a una misma clase A, por lo cual su diferencia $\varphi_1(x) - \varphi_2(x)$ es divisible por $f(x)$; la diferencia $\psi_1(x) - \psi_2(x)$ posee esta misma propiedad. De aquí que la diferencia

$$\chi_1(x) - \chi_2(x) = [\varphi_1(x) + \psi_1(x)] - [\varphi_2(x) + \psi_2(x)] = [\varphi_1(x) - \varphi_2(x)] + [\psi_1(x) - \psi_2(x)] \quad (4)$$

también es divisible por el polinomio $f(x)$. Esto mismo se cumple también para la diferencia $\theta_1(x) - \theta_2(x)$, puesto que

$$\theta_1(x) - \theta_2(x) = \varphi_1(x)\,\psi_1(x) - \varphi_2(x)\,\psi_2(x) = \varphi_1(x)\,\psi_1(x) - \varphi_1(x)\,\psi_2(x) + \varphi_1(x)\,\psi_2(x) - \varphi_2(x)\,\psi_2(x) = \varphi_1(x)\,[\psi_1(x) - \psi_2(x)] + [\varphi_1(x) - \varphi_2(x)]\,\psi_2(x). \quad (5)$$

La igualdad (4) muestra que los polinomios $\chi_1(x)$ y $\chi_2(x)$ están situados en una misma clase. En otras palabras, la suma de cualquier

polinomio de la clase A y cualquier polinomio de la clase B pertenece a una clase C completamente determinada, que no depende de los polinomios que se hayan elegido como «representantes» de las clases A y B; llamemos a esta clase C, *suma* de las clases A y B:

$$C = A + B.$$

Análogamente, en virtud de (5), no depende tampoco de la elección de los representantes en las clases A y B la clase D, a la que pertenece el producto de cualquier polinomio de A por cualquier polinomio de B; llamemos a esta clase, *producto* de las clases A y B:

$$D = AB.$$

Demostremos que el conjunto de clases en que se ha dividido nuestro anillo de polinomios $P[x]$, después de haber introducido las operaciones anteriores de suma y producto, se convierte en un campo. En efecto, el cumplimiento de las **leyes asociativa y conmutativa** para ambas operaciones y de la **ley distributiva** es consecuencia de la subsistencia de estas leyes en el anillo $P[x]$, puesto que las operaciones con las clases se reducen a las operaciones con los polinomios situados en estas clases. Evidentemente, la clase formada por los polinomios que son divisibles por el polinomio $f(x)$ desempeña el papel del **cero**. Esta se denominará *clase cero* y se designará con el símbolo 0. La **opuesta** a la clase A, formada por los polinomios que al ser divididos por $f(x)$ dan un residuo $\varphi(x)$, será la clase formada por los polinomios que al ser divididos por $f(x)$ dan el residuo $-\varphi(x)$. De aquí se deduce que en el conjunto de los polinomios es posible la **resta**, siendo ésta unívoca.

Para demostrar que es posible la **división** en el conjunto de las clases, hay que mostrar que existe una clase que desempeña el papel de la unidad y que existe una clase recíproca para cualquier clase distinta de la clase cero. La **unidad** es evidentemente la clase de los polinomios que al ser divididos por $f(x)$ dan un residuo igual a 1; a ésta la llamaremos *clase unidad* y la designaremos con la notación E.

Sea dada ahora una clase A, distinta de la clase cero. Por consiguiente, un polinomio $\varphi(x)$, elegido en la clase A como representante, no será divisible por $f(x)$ y, como el polinomio $f(x)$ es irreducible, estos dos polinomios serán primos entre sí. Por lo tanto, en el anillo $P[x]$ existen unos polinomios $u(x)$ y $v(x)$ que satisfacen a la igualdad

$$\varphi(x)\,u(x) + f(x)\,v(x) = 1,$$

de donde

$$\varphi(x)\,u(x) = 1 - f(x)\,v(x). \tag{6}$$

El segundo miembro de la igualdad (6), al ser dividido por $f(x)$, da un residuo igual a 1 y, por lo tanto, pertenece a la clase unidad E.

Designando con B la clase a que pertenece el polinomio $u(x)$, la igualdad (6) muestra que

$$AB = E,$$

de donde $B = A^{-1}$. Con esto queda demostrada la existencia de una clase inversa para cualquier clase distinta de la clase cero, es decir, queda terminada la demostración de que las clases forman un campo.

Designemos este campo mediante $\overline{P}$ y demostremos que *éste es una ampliación del campo* P. A cada elemento a del campo P le corresponde la clase formada por los polinomios que al dividirlos por $f(x)$ dan un residuo igual a a; el mismo elemento a, considerado como un polinomio de grado cero, pertenece a esta clase. Todas las clases de esta forma especial forman en el campo $\overline{P}$ un subcampo isomorfo al campo P. En efecto, es evidente que la correspondencia es biunívoca; por otra parte, en estas clases se pueden elegir como representantes los elementos del campo P y, por consiguiente, a la suma (producto) de los elementos de P le va a corresponder la suma (producto) de las clases correspondientes. En consecuencia, tenemos derecho de no hacer diferencia entre los elementos del campo P y las clases que les corresponden.

Por último, designemos con X la clase formada por los polinomios que al ser divididos por $f(x)$ dan un residuo igual a x. Esta clase es un elemento del campo $\overline{P}$ completamente determinado, y queremos demostrar que *este elemento es raíz del polinomio* $f(x)$. Sea

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

Designemos mediante A_i la clase que corresponde, en el sentido indicado anteriormente, al elemento a_i del campo P, $i = 0, 1, \ldots \ldots, n$ y veamos a qué es igual el elemento

$$A_0X^n + A_1X^{n-1} + \ldots + A_{n-1}X + A_n \tag{7}$$

del campo $\overline{P}$. Tomando los elementos a_i, $i = 0, 1, \ldots, n$, por representantes de las clases A_i y el polinomio x por representante de la clase X, y aplicando la definición de suma y producto de las clases, obtenemos que el mismo polinomio $f(x)$ está contenido en la clase (7). Pero, $f(x)$ es divisible por sí mismo, de donde resulta que (7) es la clase cero. Sustituyendo en (7) las clases A_i por sus elementos correspondientes a_i del campo P, obtenemos que en el campo $\overline{P}$ se verifica la igualdad

$$a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n = 0,$$

o sea, la clase X es verdaderamente raíz del polinomio $f(x)$.

Con esto queda terminada la demostración del teorema de existencia de la raíz. Obsérvese que, **tomando por P el campo de los números**

reales y poniendo $f(x) = x^2 + 1$, resulta otro método más de construcción del campo de los números complejos.

Del teorema de existencia de la raíz se pueden deducir consecuencias análogas a las que se dedujeron del teorema fundamental del álgebra de los números complejos (véase § 24). Hagamos primero una observación. Como cada factor lineal $x - c$ del polinomio $f(x)$ es irreducible, éste tiene que figurar en la descomposición **única** en factores irreducibles que posee $f(x)$.

Sin embargo, el número de factores lineales que hay en la descomposición de $f(x)$ en factores irreducibles no puede superar al grado de este polinomio. Así, llegamos al siguiente resultado:

Un polinomio $f(x)$ de grado n no puede tener en el campo P más de n raíces, incluso si cada raíz se cuenta tantas veces como indique su orden de multiplicidad.

Llamemos *campo de descomposición* del polinomio $f(x)$ de grado n sobre el campo P a una ampliación Q del campo P en la que estén contenidas n raíces de $f(x)$ (contando las raíces múltiples tantas veces cuantas indiquen sus órdenes de multiplicidad). Por consiguiente, el polinomio $f(x)$ se descompone sobre el campo Q en factores lineales. Además, ninguna otra ampliación del campo Q puede dar lugar a la aparición de nuevas raíces de $f(x)$.

Para cualquier polinomio $f(x)$ del anillo $P[x]$, existe sobre el campo P un campo de descomposición.

En efecto, si el polinomio $f(x)$ de grado n, $n \geqslant 1$, tiene n raíces en el mismo campo P, éste será el campo buscado de descomposición. Si $f(x)$ no se descompone sobre P en factores lineales, tomamos uno de sus factores irreducibles no lineales $\varphi(x)$ y, basándose en el teorema de la existencia de la raíz, ampliamos P hasta obtener un campo P' que contenga una raíz de $\varphi(x)$. Si el polinomio $f(x)$ no se descompone todavía sobre P' en factores lineales, ampliamos de nuevo el campo, creando una raíz para otro de los factores irreducibles no lineales que queden. Evidentemente, después de un número finito de operaciones, llegaremos a obtener para $f(x)$ un campo de descomposición.

Está claro que $f(x)$ puede poseer muchos campos distintos de descomposición. Se podría demostrar que todos los campos mínimos que contienen al campo P y a las n raíces del polinomio $f(x)$ (donde n es el grado del polinomio), son isomorfos entre sí. Como esta proposición no va a ser utilizada a continuación, no expondremos su demostración.

Raíces múltiples. En el párrafo anterior se había demostrado que un polinomio $f(x)$, dado sobre un campo P de característica 0, no tiene factores múltiples cuando, y sólo cuando, es primo con su derivada; también se había señalado que la carencia de factores múltiples de $f(x)$ sobre el campo P implica la carencia de factores

de este tipo sobre cualquier ampliación $\overline{P}$ del campo P. Aplicando esto al caso en que $\overline{P}$ sea un campo de descomposición para $f(x)$ y recordando la definición de raíz múltiple, llegamos al resultado siguiente:

Si un polinomio $f(x)$, dado sobre un campo P de característica 0, no tiene raíces múltiples en un campo dado de descomposición, éste es primo con su derivada $f'(x)$. Recíprocamente, si $f(x)$ es primo con su derivada, entonces no tiene raíces múltiples en ninguno de sus campos de descomposición.

En particular, de aquí se deduce que *un polinomio $f(x)$ irreducible sobre un campo P de característica 0, no puede tener raíces múltiples en ninguna ampliación de este campo.* Esta proposición deja de ser cierta para los campos de característica finita, circunstancia que desempeña un papel notable en la teoría general de los campos.

En conclusión, obsérvese que *para el caso de un campo arbitrario se conservan también las fórmulas de Vieta* (véase el § 24); en este caso, las raíces del polinomio se toman en un campo de descomposición del mismo.

§ 50. Campo de fracciones racionales

La teoría de las fracciones racionales, expuesta en el § 25, *se conserva también totalmente en el caso de un campo fundamental arbitrario.* Mas al pasar del campo de los números reales a un campo arbitrario P, el punto de vista según el cual la expresión $\frac{f(x)}{g(x)}$ se considera como una **función** de la variable x, tiene que ser desechado, puesto que, como ya se sabe, éste ya no es aplicable a los polinomios. Ante nosotros se plantea el problema de determinar el sentido que hay que atribuir a estas expresiones cuando los coeficientes pertenecen a un campo arbitrario P. Más exactamente, queremos construir un campo en el que esté contenido el anillo de los polinomios $P[x]$, pero de modo que las operaciones de suma y producto definidas en este nuevo campo, al ser aplicadas a los polinomios, coincidan con las operaciones en el anillo $P[x]$; abreviando, el anillo $P[x]$ tiene que ser un **subanillo** de este campo nuevo. Por otra parte, todo elemento de este nuevo campo tiene que representarse (en el sentido de la división en este campo) en forma de un cociente de dos polinomios. Como ahora se enseñará, tal campo puede ser construido para cualquier P; se designará con la notación $P(x)$ (obsérvese que la indeterminada está encerrada entre paréntesis) y se llamará *campo de fracciones racionales* sobre el campo P.

Supongamos primero que el anillo $P[x]$ ya es un subanillo de cierto campo Q. Si $f(x)$ y $g(x)$ son polinomios arbitrarios de $P[x]$, siendo $g(x) \neq 0$, existe en el campo Q un elemento unívocamente determinado, igual al cociente de la división de $f(x)$ por $g(x)$.

Designando este elemento, como ordinariamente se hace en el caso de un campo, mediante $\frac{f(x)}{g(x)}$, en virtud de la definición del cociente, se puede escribir la igualdad

$$f(x) = g(x) \cdot \frac{f(x)}{g(x)}, \tag{1}$$

donde el producto se debe entender en el sentido de la multiplicación en el campo Q. Puede ocurrir que algunos cocientes $\frac{f(x)}{g(x)}$ y $\frac{\varphi(x)}{\psi(x)}$ sean unos mismos elementos del campo Q; la condición para esto es la condición ordinaria de igualdad de las fracciones:

$$\frac{f(x)}{g(x)} = \frac{\varphi(x)}{\psi(x)} \text{ cuando, y sólo cuando, } f(x)\psi(x) = \psi(x)g(x).$$

En efecto, si $\frac{f(x)}{g(x)} = \frac{\varphi(x)}{\psi(x)} = \alpha$, en virtud de (1),

$$f(x) = g(x)\alpha, \quad \varphi(x) = \psi(x)\alpha,$$

de donde

$$f(x)\psi(x) = g(x)\psi(x)\alpha = g(x)\varphi(x).$$

Recíprocamente, si $f(x)\psi(x) = g(x)\varphi(x) = u(x)$ en el sentido de la multiplicación en el anillo $P[x]$, pasando al campo Q obtenemos las igualdades

$$\frac{f(x)}{g(x)} = \frac{u(x)}{g(x)\psi(x)} = \frac{\varphi(x)}{\psi(x)}.$$

Fácilmente se ve luego que la suma y el producto de cualesquiera elementos de Q, que son cocientes de polinomios de $P[x]$, se pueden representar de nuevo en forma de tales cocientes, cumpliéndose además las reglas comunes de adición y multiplicación de fracciones:

$$\frac{f(x)}{g(x)} + \frac{\varphi(x)}{\psi(x)} = \frac{f(x)\psi(x) + g(x)\varphi(x)}{g(x)\psi(x)}, \tag{2}$$

$$\frac{f(x)}{g(x)} \cdot \frac{\varphi(x)}{\psi(x)} = \frac{f(x)\cdot\varphi(x)}{g(x)\cdot\psi(x)}. \tag{3}$$

En efecto, multiplicando ambos miembros de cada una de estas igualdades por el producto $g(x)\psi(x)$ y aplicando (1), obtenemos igualdades válidas en el anillo $P[x]$. La subsistencia de las igualdades (2) y (3) se deduce ahora de que, debido a la ausencia de divisores de cero en el campo Q, ambos miembros de cada una de las igualdades obtenidas se pueden simplificar por el elemento $g(x)\psi(x)$, diferente de cero, sin infringir las igualdades.

Estas observaciones previas señalan el camino que hay que seguir para construir el campo $P(x)$. Sea dado un campo arbitrario P y sobre él, el anillo de los polinomios $P[x]$. A cada par ordenado

de polinomios $f(x)$, $g(x)$, donde $g(x) \neq 0$, ponemos en correspondencia el símbolo $\frac{f(x)}{g(x)}$, denominado *fracción racional con numerador* $f(x)$ *y denominador* $g(x)$. Subrayemos que esto es, simplemente, un símbolo que corresponde al par dado de polinomios, pues, por lo general, la división de los polinomios en el anillo mismo $P[x]$ no es posible y, por ahora, el anillo $P[x]$ no está contenido en ningún campo; incluso si $g(x)$ fuese divisor de $f(x)$, el nuevo símbolo $\frac{f(x)}{g(x)}$ se debe distinguir por ahora del polinomio que se obtiene como cociente al dividir $f(x)$ por $g(x)$.

Llamemos ahora *iguales* a las fracciones racionales $\frac{f(x)}{g(x)}$ y $\frac{\varphi(x)}{\psi(x)}$:

$$\frac{f(x)}{g(x)} = \frac{\varphi(x)}{\psi(x)}, \tag{4}$$

si en el anillo $P[x]$ se cumple la igualdad $f(x)\,\psi(x) = g(x)\,\varphi(x)$. Es evidente que cualquier fracción es igual a sí misma, y también que si una fracción es igual a otra, la segunda es igual a la primera. Demostremos que para este concepto de igualdad se cumple la **ley transitiva**. Sean dadas las igualdades (4) y

$$\frac{\varphi(x)}{\psi(x)} = \frac{u(x)}{v(x)}. \tag{5}$$

De las igualdades equivalentes a éstas en el anillo $P[x]$

$$f(x)\,\psi(x) = g(x)\,\varphi(x), \quad \varphi(x)\,v(x) = \psi(x)\,u(x)$$

se deduce que

$$f(x)\,v(x)\,\psi(x) = g(x)\,\varphi(x)\,v(x) = g(x)\,u(x)\,\psi(x);$$

por consiguiente, después de simplificar por el polinomio $\psi(x)$, distinto de cero (como denominador de una de las fracciones), resulta:

$$f(x)\,v(x) = g(x)\,u(x),$$

de donde, por la definición de igualdad de las fracciones,

$$\frac{f(x)}{g(x)} = \frac{u(x)}{v(x)},$$

que es lo que se quería demostrar.

Reunamos ahora en una clase todas las fracciones que sean iguales a una dada, las cuales, en virtud de la ley transitiva de la igualdad, serán iguales entre sí. Si en una clase hay por lo menos una fracción que no está contenida en otra clase, entonces, como se deduce de la ley transitiva de la igualdad, estas dos clases no tienen ningún elemento común.

Por lo tanto, el conjunto de todas las fracciones racionales, *escritas mediante los polinomios del anillo* $P[x]$, *se descompone en* clases disjuntas de fracciones iguales entre sí. Ahora queremos definir las operaciones algebraicas en este **conjunto de clases** de fracciones iguales, de modo que éste sea un campo. Para esto, vamos a definir las operaciones con las fracciones racionales y vamos a comprobar cada vez que la sustitución de los términos (o de los factores) por fracciones iguales a los mismos sustituye también la suma (o el producto) por una fracción igual. Esto permitirá hablar de la suma y producto de clases de fracciones iguales.

Hagamos previamente la siguiente observación que se aplicará a continuación: *una fracción racional se convierte en una fracción igual, si su numerador y denominador se multiplican por un mismo polinomio, diferente de cero, o si se simplifican por cualquier factor común.* En efecto,

$$\frac{f(x)}{g(x)} = \frac{f(x)\,h(x)}{g(x)\,h(x)},$$

pues en el anillo $P[x]$,

$$f(x)\,[g(x)\,h(x)] = g(x)\,[f(x)\,h(x)].$$

Definamos la *suma* de fracciones racionales por la fórmula (2); como $g(x) \neq 0$ y $\psi(x) \neq 0$, resulta que $g(x)\,\psi(x) \neq 0$, y el segundo miembro de esta fórmula es, evidentemente, una fracción racional. Si se ha dado que

$$\frac{f(x)}{g(x)} = \frac{f_0(x)}{g_0(x)}, \quad \frac{\varphi(x)}{\psi(x)} = \frac{\varphi_0(x)}{\psi_0(x)},$$

o sea, que

$$f(x)\,g_0(x) = g(x)\,f_0(x), \quad \varphi(x)\,\psi_0(x) = \psi(x)\,\varphi_0(x), \tag{6}$$

entonces, multiplicando ambos miembros de la primera de las *igualdades (6) por* $\psi(x)\,\psi_0(x)$, *ambos miembros de la segunda por* $g(x)\,g_0(x)$ y sumando después término a término estas igualdades, obtenemos:

$$[f(x)\,\psi(x) + g(x)\,\varphi(x)]\,g_0(x)\,\psi_0(x) = [f_0(x)\,\psi_0(x) + g_0(x)\,\varphi_0(x)]\,g(x)\,\psi(x),$$

lo cual es equivalente a la igualdad

$$\frac{f(x)\,\psi(x) + g(x)\,\varphi(x)}{g(x)\,\psi(x)} = \frac{f_0(x)\,\psi_0(x) + g_0(x)\,\varphi_0(x)}{g_0(x)\,\psi_0(x)}.$$

Por lo tanto, dadas dos clases de fracciones iguales entre sí, las sumas de cualquier fracción de una clase y cualquier fracción de otra clase son todas iguales entre sí, es decir, están situadas en una tercera clase completamente determinada. Esta clase se llama *suma* de las dos clases dadas.

La **conmutatividad** de esta suma es consecuencia inmediata de (2); la **asociatividad** se demuestra del modo siguiente:

$$\left[\frac{f(x)}{g(x)}+\frac{\varphi(x)}{\psi(x)}\right]+\frac{u(x)}{v(x)}=\frac{f(x)\psi(x)+g(x)\varphi(x)}{g(x)\psi(x)}+\frac{u(x)}{v(x)}=$$

$$=\frac{f(x)\psi(x)v(x)+g(x)\varphi(x)v(x)+g(x)\psi(x)u(x)}{g(x)\psi(x)v(x)}=$$

$$=\frac{f(x)}{g(x)}+\frac{\varphi(x)v(x)+\psi(x)u(x)}{\psi(x)v(x)}=\frac{f(x)}{g(x)}+\left[\frac{\varphi(x)}{\psi(x)}+\frac{u(x)}{v(x)}\right].$$

De la definición de igualdad de fracciones se deduce fácilmente que todas las fracciones de la forma $\frac{0}{g(x)}$, o sea, las fracciones con el numerador igual a cero, son iguales entre sí y forman una clase completa de fracciones iguales. A ésta la llamaremos *clase cero*; demostremos que esta clase desempeña en nuestra suma el papel del cero. En efecto, dada una fracción arbitraria $\frac{\varphi(x)}{\psi(x)}$, se tiene

$$\frac{0}{g(x)}+\frac{\varphi(x)}{\psi(x)}=\frac{0\cdot\psi(x)+g(x)\varphi(x)}{g(x)\psi(x)}=\frac{g(x)\varphi(x)}{g(x)\psi(x)}=\frac{\varphi(x)}{\psi(x)}.$$

De la igualdad

$$\frac{f(x)}{g(x)}+\frac{-f(x)}{g(x)}=\frac{0}{g^2(x)},$$

cuyo segundo miembro pertenece a la clase cero, se deduce ahora que la clase de las fracciones, iguales a la fracción $\frac{-f(x)}{g(x)}$, es la *opuesta* a la clase de las fracciones que son iguales a la fracción $\frac{f(x)}{g(x)}$. Como ya sabemos, de aquí se deduce la posibilidad de la *resta* unívoca.

Determinemos el *producto* de fracciones racionales por la fórmula (3). Como $g(x)\psi(x)\not\equiv 0$, el segundo miembro de esta fórmula es, evidentemente, una fracción racional. Si, luego,

$$\frac{f(x)}{g(x)}=\frac{f_0(x)}{g_0(x)},\quad \frac{\varphi(x)}{\psi(x)}=\frac{\varphi_0(x)}{\psi_0(x)},$$

o sea,

$$f(x)g_0(x)=g(x)f_0(x),\quad \varphi(x)\psi_0(x)=\psi(x)\varphi_0(x),$$

entonces, multiplicando término a término estas últimas igualdades, obtenemos:

$$f(x)g_0(x)\varphi(x)\psi_0(x)=g(x)f_0(x)\psi(x)\varphi_0(x),$$

lo cual es equivalente a la igualdad

$$\frac{f(x)\varphi(x)}{g(x)\psi(x)}=\frac{f_0(x)\varphi_0(x)}{g_0(x)\psi_0(x)}.$$

Por lo tanto, por analogía con la definición de la suma de las clases, dada anteriormente, se puede hablar del *producto* de clases de fracciones iguales entre sí.

La **conmutatividad** y **asociatividad** de este producto es consecuencia directa de (3). El cumplimiento de la **ley distributiva** se demuestra del modo siguiente:

$$\left[\frac{f(x)}{g(x)}+\frac{\varphi(x)}{\psi(x)}\right]\frac{u(x)}{v(x)}=\frac{f(x)\psi(x)+g(x)\varphi(x)}{g(x)\psi(x)}\cdot\frac{u(x)}{v(x)}=$$

$$=\frac{[f(x)\psi(x)+g(x)\varphi(x)]u(x)}{g(x)\psi(x)v(x)}=\frac{f(x)\psi(x)u(x)+g(x)\varphi(x)u(x)}{g(x)\psi(x)v(x)}=$$

$$=\frac{f(x)\psi(x)u(x)v(x)+g(x)\varphi(x)u(x)v(x)}{g(x)\psi(x)v^2(x)}=\frac{f(x)u(x)}{g(x)v(x)}+\frac{\varphi(x)u(x)}{\psi(x)v(x)}=$$

$$=\frac{f(x)}{g(x)}\cdot\frac{u(x)}{v(x)}+\frac{\varphi(x)}{\psi(x)}\cdot\frac{u(x)}{v(x)}.$$

Fácilmente se observa que las fracciones de la forma $\frac{f(x)}{f(x)}$, o sea, las fracciones cuyos numeradores son iguales a sus denominadores, son iguales entre sí y forman una clase individual. Esta se llama *clase unidad* y en nuestra multiplicación desempeña el papel de la unidad:

$$\frac{f(x)}{f(x)}\cdot\frac{\varphi(x)}{\psi(x)}=\frac{f(x)\varphi(x)}{f(x)\psi(x)}=\frac{\varphi(x)}{\psi(x)}.$$

Si, finalmente, la fracción $\frac{f(x)}{g(x)}$ no pertenece a la clase cero, o sea, $f(x)\neq 0$, existe la fracción $\frac{g(x)}{f(x)}$. Como

$$\frac{f(x)}{g(x)}\cdot\frac{g(x)}{f(x)}=\frac{f(x)g(x)}{g(x)f(x)},$$

y el segundo miembro de esta igualdad pertenece a la clase unidad, la clase de las fracciones, iguales a la fracción $\frac{g(x)}{f(x)}$, será *repíproca* a la clase de las fracciones, iguales a la fracción $\frac{f(x)}{g(x)}$. De aquí se deduce que es posible la *división* unívoca.

Por lo tanto, *en virtud de las definiciones anteriores de las operaciones, las clases de fracciones racionales, iguales entre sí, con coeficientes del campo P, forman un campo conmutativo.* Este es el campo buscado $P(x)$. Por cierto, todavía tenemos que demostrar que en el campo construido está contenido un subanillo, isomorfo al anillo $P[x]$, y que cada elemento del campo se representa en forma de un cociente de dos elementos de este subanillo.

Si a un polinomio arbitrario $f(x)$ del anillo $P[x]$ ponemos en correspondencia la clase de fracciones racionales, iguales a la frac-

ción $\frac{f(x)}{1}$ (naturalmente, entre éstas también están contenidas las fracciones cuyos denominadores son iguales a la unidad), obtenemos una *aplicación biyectiva* del anillo $P[x]$ en el interior del campo que hemos construido. En efecto, de la igualdad

$$\frac{f(x)}{1} = \frac{\varphi(x)}{1}$$

resultaría $f(x) \cdot 1 = 1 \cdot \varphi(x)$, o sea, $f(x) = \varphi(x)$. Como muestran las igualdades

$$\frac{f(x)}{1} + \frac{g(x)}{1} = \frac{f(x) \cdot 1 + g(x) \cdot 1}{1^2} = \frac{f(x) + g(x)}{1},$$

$$\frac{f(x)}{1} \cdot \frac{g(x)}{1} = \frac{f(x) \cdot g(x)}{1},$$

esta aplicación es incluso un isomorfismo.

Por lo tanto, *las clases de fracciones, iguales a las fracciones de la forma* $\frac{f(x)}{1}$, *forman en nuestro campo un subanillo que es isomorfo al anillo* $P[x]$. Por esto, la fracción $\frac{f(x)}{1}$ se puede designar simplemente mediante $f(x)$. Finalmente, como la clase de las fracciones, iguales a la fracción $\frac{1}{g(x)}$, siendo $g(x) \neq 0$, es recíproca a la clase de las fracciones, iguales a la fracción $\frac{g(x)}{1}$, de la igualdad

$$\frac{f(x)}{1} \cdot \frac{1}{g(x)} = \frac{f(x)}{g(x)}$$

se deduce que *todos los elementos de nuestro campo se pueden considerar* (en el sentido de las operaciones definidas en este campo) *como cocientes de polinomios del anillo* $P[x]$.

De este modo, hemos construido el campo de fracciones racionales $P(x)$ sobre un campo arbitrario P. Tomando el anillo de los números enteros, en lugar del anillo de los polinomios, se puede construir de este mismo modo el campo de los números racionales. Agrupando estos dos casos y aplicando un método igual, se podría demostrar el teorema de que, en general, cualquier anillo conmutativo sin divisores de cero es un subanillo de algún campo.

CAPITULO XI

POLINOMIOS EN VARIAS INDETERMINADAS

§ 51. Anillo de los polinomios en varias indeterminadas

A veces se suelen considerar polinomios que no dependen de una, sino de dos, tres, y en general, de varias indeterminadas. Así, en los primeros capítulos del libro se estudiaron las formas lineales y cuadráticas, que representan ejemplos de estos polinomios. En general, se llama *polinomio* $f(x_1, x_2, \ldots, x_n)$ *en n indeterminadas* $x_1, x_2, \ldots, x_n$ *sobre un campo* P, a la suma de un número finito de términos de la forma $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$, donde $k_i \geqslant 0$, con coeficientes del campo P; se supone que el polinomio $f(x_1, x_2, \ldots, x_n)$ no contiene términos semejantes y que se consideran solamente términos con coeficientes diferentes de cero. Dos polinomios en n indeterminadas, $f(x_1, x_2, \ldots, x_n)$ y $g(x_1, x_2, \ldots, x_n)$, se consideran *iguales* (o *idénticamente iguales*), si son iguales sus coeficientes de potencias iguales.

Dado un polinomio $f(x_1, x_2, \ldots, x_n)$ sobre un campo P, se llama *grado con respecto a la indeterminada* x_i, $i = 1, 2, \ldots, n$, al exponente máximo con que figura x_i en los términos de este polinomio. Puede ocurrir eventualmente que este grado sea igual 0, lo cual significa que a pesar de que f se considere como polinomio en n indeterminadas $x_1, x_2, \ldots, x_i, \ldots, x_n$, en realidad, la indeterminada x_i no figura en su expresión.

Por otra parte, si llamamos *grado del término*

$$x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

al número $k_1 + k_2 + \ldots + k_n$, o sea, a la suma de los exponentes de las indeterminadas, el *grado del polinomio* $f(x_1, x_2, \ldots, x_n)$ (o sea, el grado respecto del **conjunto de las indeterminadas**) será el grado superior de sus términos. En particular, al igual que en el caso de una indeterminada, son polinomios de grado cero solamente los elementos del campo P, diferentes de cero. Por otra parte, del mismo modo que en el caso de los polinomios en una indeterminada, el cero es el único polinomio en n indeterminadas cuyo grado está indefinido. Claro, en el caso general, un polinomio puede contener

unos cuantos términos de grado superior, por lo cual, no se puede hablar de un término superior (según el grado) del polinomio.

Para los polinomios en n indeterminadas sobre un campo P, las operaciones de sumar y multiplicar se definen del modo siguiente:

Se llama *suma* de los polinomios $f(x_1, x_2, \ldots, x_n)$ y $g(x_1, x_2, \ldots, x_n)$ al polinomio cuyos coeficientes se obtienen sumando los coeficientes correspondientes de los polinomios f y g; naturalmente, si en este caso algún término figura solamente en uno de los polinomios f, g, el coeficiente de éste en el otro polinomio se supone igual a cero. El producto de dos «monomios» se define por la igualdad:

$$ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}\cdot bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}=(ab)\,x_1^{k_1+l_1}x_2^{k_2+l_2}\ldots x_n^{k_n+l_n},$$

después de lo cual, el *producto* de los polinomios $f(x_1, x_2, \ldots, x_n)$ y $g(x_1, x_2, \ldots, x_n)$ se define como el resultado de la multiplicación término a término y la consiguiente reducción de términos semejantes.

Definidas las operaciones de este modo, el conjunto de los polinomios en n indeterminadas sobre el campo P se convierte en un anillo conmutativo que, además, carece de divisores de cero. En efecto, para $n = 1$ nuestras definiciones coinciden con las que se dieron en el § 20 para el caso de polinomios en una indeterminada. Supongamos que se ha demostrado que los polinomios en $n-1$ indeterminadas $x_1, x_2, \ldots, x_{n-1}$ con coeficientes del campo P forman un anillo sin divisores de cero. Todo polinomio en n indeterminadas $x_1, x_2, \ldots, x_{n-1}, x_n$ se puede representar de un modo único como un polinomio en la indeterminada x_n con coeficientes que son polinomios en $x_1, x_2, \ldots, x_{n-1}$; recíprocamente, todo polinomio en x_n con coeficientes del anillo de los polinomios en $x_1, x_2, \ldots, x_{n-1}$ sobre el campo P se puede considerar, naturalmente, como un polinomio sobre el mismo campo P en todo el conjunto de las indeterminadas $x_1, x_2, \ldots, x_{n-1}, x_n$. Se comprueba sin dificultad que la correspondencia biunívoca, obtenida entre los polinomios en n indeterminadas y los polinomios en una indeterminada sobre el anillo de los polinomios en $n-1$ indeterminadas, es un isomorfismo con respecto a las operaciones de sumar y multiplicar. La proposición que se demuestra se deduce de que los polinomios en una indeterminada sobre el anillo de los polinomios en $n-1$ indeterminadas forman ellos mismos un anillo que, además, por ser un anillo de polinomios en una indeterminada sobre un anillo sin divisores de cero, tampoco contiene divisores de cero (véase § 47).

Por consiguiente, queda demostrada la existencia del *anillo de los polinomios en n indeterminadas sobre el campo P*; este anillo se designa con la notación $P[x_1, x_2, \ldots, x_n]$.

El estudio siguiente permite examinar el anillo de los polinomios en n indeterminadas desde otro punto de vista. Supongamos que el

campo P está contenido como subanillo en un anillo conmutativo L. Tomemos en L n elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ y hallemos el subanillo mínimo L' del anillo L que contiene a estos elementos y a todo el campo P, o sea, el subanillo que se obtiene *por adjunción* de los elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ al campo P. El subanillo L' consta de todos los elementos del anillo L que se expresan mediante los elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ y los elementos del campo P aplicando la suma, resta y multiplicación. Fácilmente se observa que éstos son exactamente los elementos del anillo L que se pueden expresar (aplicando las operaciones que subsisten en el anillo L) en forma de polinomios en $\alpha_1, \alpha_2, \ldots, \alpha_n$ con coeficientes de P; además, estos elementos, como elementos del anillo L, se pueden sumar y multiplicar precisamente según las leyes de adición y multiplicación de los polinomios en n indeterminadas.

Claro, por lo general, un elemento dado β del subanillo L' puede poseer muchas expresiones distintas en forma de polinomio en $\alpha_1, \alpha_2, \ldots, \alpha_n$ con coeficientes del campo P. Si esta expresión es **única** para cualquier β de L', es decir, que diferentes polinomios en $\alpha_1, \alpha_2, \ldots, \alpha_n$ son elementos distintos del anillo L' (y, por consiguiente, del anillo L), el sistema de elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ se llama *algebraicamente independiente* sobre el campo P. En caso contrario, se llama *algebraicamente dependiente**. De aquí, se puede hacer la siguiente conclusión:

Si un campo P es un subanillo de un anillo conmutativo L y si el sistema de elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ de L es algebraicamente independiente sobre P, el subanillo L' del anillo L, engendrado por adjunción de los elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ al campo P, es isomorfo al anillo de los polinomios $P[x_1, x_2, \ldots, x_n]$.

Entre otras propiedades del anillo de los polinomios en n indeterminadas $P[x_1, x_2, \ldots, x_n]$, señalemos la siguiente: este anillo se puede incluir en el *campo de fracciones racionales* $P(x_1, x_2, \ldots, x_n)$ *en n indeterminadas sobre el campo P*. Todo elemento de este campo se puede expresar en la forma $\frac{f}{g}$, donde f y g son polinomios del anillo $P[x_1, x_2, \ldots x_n]$, siendo, además, $\frac{f}{g} = \frac{\varphi}{\psi}$ cuando, y sólo cuando, $f\psi = g\varphi$. La suma y el producto de estas fracciones racionales se efectúan según las leyes que, como se indicó en el § 45, se cumplen para los cocientes en cualquier campo. La demostración de la existencia del campo $P(x_1, x_2, \ldots, x_n)$ se hace igual que en el § 50 para el caso $n = 1$.

* Los conceptos correspondientes para el caso $n = 1$ fueron introducidos en el § 47: un elemento α, algebraicamente independiente sobre el campo P, en el sentido de la definición que se acaba de dar, se llamaba entonces ***trascendente*** sobre P; en el caso contrario, ***algebraico*** sobre P.

Para los polinomios en varias indeterminadas se puede construir la teoría de la divisibilidad que generaliza a la teoría de la divisibilidad de los polinomios en una indeterminada, estudiada en los cap. 5 y 10. Mas, como no entra en nuestro plan el estudio detallado del anillo de los polinomios en varias indeterminadas, nos limitaremos solamente a la cuestión de la descomposición de un polinomio en factores irreducibles.

Introduzcamos primero el siguiente concepto: si todos los términos de un polinomio $f(x_1, x_2, \ldots, x_n)$ son de un mismo grado s, éste se llama *polinomio homogéneo* o, abreviadamente, *forma* de grado s (ya conocemos las *formas lineales* y *cuadráticas*, se pueden considerar luego las formas cúbicas, todos los términos de las cuales son de grado 3 con respecto del conjunto de las indeterminadas, etc). **Todo polinomio en n indeterminadas se representa unívocamente en forma de una suma de unas cuantas formas en estas indeterminadas que son, además, de distinto grado:** para obtener la representación buscada es suficiente agrupar todos los términos de un mismo grado. Así, pues, el polinomio de cuarto grado $f(x_1, x_2, x_3) = 3x_1x_3^2 - 7x_1^2x_3^2 + x_2 - 5x_1x_2x_3 + x_1^4 - 2x_3 - 6 + x_3^3$ es la suma de la forma de cuarto grado $x_1^4 - 7x_1^2x_3^2$, de la forma cúbica $3x_1x_3^2 - 5x_1x_2x_3 + x_3^3$, de la forma lineal $x_2 - 2x_3$ y del término independiente -6 (forma de grado cero).

Demostremos ahora el siguiente **teorema:**

El grado del producto de dos polinomios en n indeterminadas, diferentes de cero, es igual a la suma de los grados de estos polinomios.

Supongamos primero que se dan dos **formas:** $\varphi(x_1, x_2, \ldots, x_n)$ de grado s y $\psi(x_1, x_2, \ldots, x_n)$ de grado t. El producto de cualquier término de la forma φ por cualquier término de la forma ψ es, evidentemente, de grado $s + t$ y, por esto, el producto $\varphi\psi$ será una forma de grado $s + t$, pues, el producto de términos semejantes no puede anular a todos los coeficientes de este producto, ya que en el anillo $P[x_1, x_2, \ldots, x_n]$ no hay divisores de cero.

Si se dan ahora unos polinomios arbitrarios $f(x_1, x_2, \ldots, x_n)$ y $g(x_1, x_2, \ldots, x_n)$ de grado s y t, respectivamente, representando cada uno de ellos en forma de una suma de formas de grados distintos, obtenemos:

$$f(x_1, x_2, \ldots, x_n) = \varphi(x_1, x_2, \ldots, x_n) + \ldots,$$
$$g(x_1, x_2, \ldots, x_n) = \psi(x_1, x_2, \ldots, x_n) + \ldots,$$

donde φ y ψ son formas de grado s y t, respectivamente, y los puntos suspensivos sustituyen a las sumas de las formas de grado menor. Entonces,

$$fg = \varphi\psi + \ldots;$$

por lo demostrado, la forma $\varphi\psi$ es de grado $s + t$, y como todos los términos sustituidos por puntos suspensivos tienen menor grado, el grado del producto fg será igual a $s + t$. El teorema queda demostrado.

El polinomio φ se llama *divisor* del polinomio f y f es *divisible* por φ, si en el anillo $P[x_1, x_2, \ldots, x_n]$ existe un polinomio ψ tal, que $f = \varphi\psi$. Fácilmente se observa que las propiedades de divisibilidad I-IX del § 21 se conservan también en el caso general que ahora estudiamos. Se dice que un polinomio f de grado k, $k \geqslant 1$, es *reducible* sobre un campo P, si se descompone en un producto de polinomios del anillo $P[x_1, x_2, \ldots, x_n]$, de grados menores que k, e *irreducible*, en caso contrario.

Todo polinomio del anillo $P[x_1, x_2, \ldots, x_n]$, de grado distinto de cero, se descompone en un producto de factores irreducibles. Esta descomposición es única, salvo factores de grado cero.

Este teorema generaliza los resultados correlativos del § 48, referentes a los polinomios en una indeterminada. Su primera tesis se demuestra repitiendo palabra por palabra los razonamientos del párrafo indicado. La demostración de la segunda tesis presenta ya dificultades considerables. Antes

de exponerla, observemos que de la segunda tesis se deduce este corolario: *si el producto de dos polinomios, f y g, del anillo P* $[x_1, x_2, \ldots, x_n]$, *es divisible por un polinomio irreducible p, al menos uno de estos polinomios es divisible por p.* En efecto, en caso contrario obtendríamos para el producto fg dos descomposiciones en factores irreducibles, una de las cuales no contendría a p, mientras que la otra le contendría.

Supongamos que el teorema ya está demostrado para los polinomios en n indeterminadas y queremos demostrarlo para los polinomios en $n + 1$ indeterminadas, $x, x_1, x_2, \ldots, x_n$. Escribamos este polinomio en la forma $\varphi(x)$; por consiguiente, sus coeficientes serán polinomios en $x_1, x_2, \ldots, x_n$. Para estos coeficientes el teorema ya está demostrado, es decir, cada uno de ellos se descompone unívocamente en un producto de factores irreducibles. Llamemos *primitivo* (más exacto, *primitivo sobre el anillo* $P[x_1, x_2, \ldots, x_n]$) al polinomio $\varphi(x)$, si sus coeficientes no contienen ningún factor común irreducible, o sea, si éstos son primos entre sí, y demostremos el siguiente **lema de Gauss:**

El producto de dos polinomios primitivos también es un polinomio primitivo.

En efecto, sean dados los polinomios primitivos

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

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

con coeficientes del anillo $P[x_1, x_2, \ldots, x_n]$ 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, los coeficientes $c_0, c_1, \ldots, c_{k+l}$ tienen que poseer un factor común irreducible $p = p(x_1, x_2, \ldots, x_n)$. Como no todos los coeficientes del polinomio primitivo $f(x)$ son divisibles por p, supongamos que a_i es el primer coeficiente que no es divisible por p; análogamente, designamos con b_j el primer coeficiente del polinomio $g(x)$ que no es divisible por p. Multiplicando término a término los polinomios $f(x)$ y $g(x)$ y agrupando los términos que contienen a $x^{k+l-(i+j)}$, obtenemos:

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

El primer miembro de esta igualdad es divisible por el polinomio irreducible p. Sin duda, son divisibles por éste 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 $a_{i-1}, a_{i-2}, \ldots$, y también $b_{j-1}, b_{j-2}, \ldots$, *son divisibles por p. De esto se deduce que el producto* a_ib_j *también* es divisible por p y, por esto, como se indicó anteriormente, tiene que ser divisible por p al menos uno de los polinomios a_i, b_j, lo cual, sin embargo, no tiene lugar. Con esto se termina la demostración del lema, suponiendo que el teorema fundamental se verifica para los polinomios en n indeterminadas.

Como ya sabemos, el anillo $P[x_1, x_2, \ldots, x_n]$ está contenido en el campo de fracciones racionales $P(x_1, x_2, \ldots, x_n)$ que designaremos con Q:

$$Q = P(x_1, x_2, \ldots, x_n).$$

Consideremos el anillo de los polinomios $Q[x]$. Si un polinomio $\varphi(x)$ pertenece a este anillo, cada uno de sus coeficientes se representa en forma de un *cociente de polinomios del anillo* $P[x_1, x_2, \ldots, x_n]$. Sacando fuera de paréntesis el común denominador de estos cocientes, y después, los factores comunes de los numeradores, se puede representar $\varphi(x)$ en la forma

$$\varphi(x) = \frac{a}{b} f(x).$$

Aquí, a y b son polinomios del anillo $P[x_1, x_2, \ldots, x_n]$ y $f(x)$ es un polinomio en x con coeficientes de $P[x_1, x_2, \ldots, x_n]$, que es además primitivo, pues sus coeficientes ya no tienen factores comunes.

De este modo, a cada polinomio $\varphi(x)$ del anillo $Q[x]$ se pone en correspondencia un polinomio primitivo $f(x)$. *Dado $\varphi(x)$, el polinomio $f(x)$ queda determinado univocamente, salvo un factor de P distinto de cero.* En efecto, supongamos que

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

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 sobre el anillo $P[x_1, x_2, \ldots, x_n]$. Como en este anillo subsiste (por la hipótesis de inducción) el teorema de unicidad de la descomposición, de esto se deduce que ad y bc pueden diferenciarse entre sí solamente en un factor de grado cero. Por consiguiente, los polinomios primitivos $f(x)$ y $g(x)$ se diferencian entre sí en este mismo factor.

Al producto de dos polinomios del anillo $Q[x]$ le corresponde el producto de los polinomios primitivos correspondientes. En efecto, si

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

donde $f(x)$ y $g(x)$ son polinomios primitivos, resulta

$$\varphi(x)\,\psi(x) = \frac{ac}{bd} f(x)\, g(x).$$

Pero, como se ha demostrado más arriba, el producto $f(x)\,g(x)$ es un polinomio primitivo.

Señalemos también que, *si el polinomio $\varphi(x)$ del anillo $Q[x]$ es irreducible sobre el campo Q, su polinomio primitivo correspondiente $f(x)$, considerado como un polinomio en $x, x_1, x_2, \ldots, x_n$, también será irreducible, y viceversa.* En efecto, si el polinomio f es reducible, $f = f_1 f_2$, ambos factores tienen que contener la indeterminada x, pues, en caso contrario, el polinomio f no sería primitivo. De aquí resulta la descomposición del polinomio $\varphi(x)$ sobre el campo Q:

$$\varphi(x) = \frac{a}{b} f(x) = \left(\frac{a}{b} f_1\right) f_2.$$

Recíprocamente, si el polinomio $\varphi(x)$ es reducible sobre Q, $\varphi(x) = \varphi_1(x)\,\varphi_2(x)$, los polinomios primitivos $f_1(x)$ y $f_2(x)$ correspondientes a $\varphi_1(x)$ y $\varphi_2(x)$ contendrán x, pero como se demostró antes, su producto es igual a $f(x)$ (salvo un factor del campo P).

Tomemos ahora un polinomio primitivo f y descompongámoslo en factores irreducibles, $f = f_1 \cdot f_2 \ldots f_k$. Todos estos factores no sólo tienen que contener a la indeterminada x, sino que tienen que ser incluso polinomios primitivos, pues, en caso contrario, el polinomio f no sería primitivo. *Esta descomposición del polinomio primitivo f es única salvo factores del campo P.* En efecto, en virtud del lema precedente, se puede considerar esta descomposición como la descomposición de $f(x)$ en factores irreducibles sobre el campo Q; mas, para los polinomios en una indeterminada sobre un campo dado, ya es conocida la unicidad de la descomposición que se verifica, salvo factores de Q; pero, en nuestro caso, como todos los factores f_i son primitivos, ésta se verifica, salvo factores de P.

Después de haber demostrado estos lemas, partiendo de la hipótesis de inducción, se hace sin dificultad alguna la demostración de nuestro teorema fundamental. En efecto, todo polinomio irreducible del anillo $P\,[x,\ x_1,\ x_2,\ \ldots,\ x_n]$, o es un polinomio irreducible del anillo $P\,[x_1,\ x_2,\ \ldots,\ x_n]$, o es un polinomio primitivo irreducible. De aquí se deduce que, dada una descomposición del polinomio $\varphi\,(x,\ x_1,\ x_2,\ \ldots,\ x_n)$ en factores irreducibles, agrupando los factores se puede representar φ en la forma

$$\varphi\,(x,\ x_1,\ x_2,\ \ldots,\ x_n) = a\,(x_1,\ x_2,\ \ldots,\ x_n)\,f\,(x,\ x_1,\ x_2,\ \ldots,\ x_n),$$

donde a no depende de x y f es un polinomio primitivo. Sin embargo, ya sabemos que esta descomposición de φ es única, salvo factores de P. Pero, por otra *parte, como, por la hipótesis de inducción, subsiste la unicidad de la descomposición* en factores irreducibles para el polinomio a en n indeterminadas, y como esta unicidad está demostrada en el lema anterior para el polinomio primitivo f, *queda también completamente demostrado nuestro teorema* para el caso de $n + 1$ indeterminadas.

De los lemas demostrados anteriormente se deduce un corolario interesante: *si un polinomio $\varphi\,(x)$ con coeficientes de $P\,[x_1,\ x_2,\ \ldots,\ x_n]$ es reducible sobre el campo $Q = P\,(x_1,\ x_2,\ \ldots,\ x_n)$, entonces se puede descomponer en factores que dependen de x y cuyos coeficientes son polinomios del anillo $P\,[x_1,\ x_2,\ \ldots,\ x_n]$.* En efecto, si al polinomio $\varphi\,(x)$ le corresponde el polinomio primitivo $f\,(x)$, de modo que $\varphi\,(x) = af\,(x)$, entonces la descomposición de $\varphi\,(x)$ implica la descomposición de $f\,(x)$; pero esto último implica a su vez la descomposición de $\varphi\,(x)$ sobre el anillo $P\,[x_1,\ x_2,\ \ldots,\ x_n]$.

A diferencia del caso de los polinomios en una indeterminada que, como ya sabemos por el § 49, se pueden descomponer en factores lineales sobre una ampliación adecuadamente elegida del campo fundamental considerado, *existen sobre cualquier campo P polinomios de cualquier grado en varias* (dos o más) *indeterminadas que son* **absolutamente irreducibles**, o sea, polinomios que se mantienen irreducibles sobre cualquier ampliación de este campo.

De este tipo es el polinomio

$$f\,(x,\ y) = \varphi\,(x) + y,$$

donde $\varphi\,(x)$ es un polinomio arbitrario en una indeterminada sobre un campo P. En efecto, si en cierta ampliación $\overline{P}$ del campo P existiese la descomposición

$$f\,(x,\ y) = g\,(x,\ y)\,h\,(x,\ y),$$

entonces, expresando g y h según las potencias de y, obtendríamos, por ejemplo,

$$g\,(x,\ y) = a_0\,(x)\,y + a_1\,(x),\ h\,(x,\ y) = b_0\,(x),$$

o sea, h no dependería de y; y como $a_0(x)b_0(x) = 1$, resultaría que $b_0\,(x)$ sería de grado cero y, por lo tanto, h no dependería tampoco de x.

Ordenación lexicográfica de los términos de un polinomio. Para los polinomios en una indeterminada se tienen dos métodos naturales de ordenación de los términos: según las potencias decrecientes de la indeterminada y según las potencias crecientes de la misma. En el caso de polinomios en varias indeterminadas, tales métodos no existen; *por ejemplo*, el polinomio de quinto grado en tres indeterminadas

$$f\,(x_1,\ x_2,\ x_3) = x_1x_2^2x_3^2 + x_1^4x_3 + x_2^3x_3^2 + x_1^2x_2x_3^2,$$

puede escribirse también en la forma

$$f(x_1, x_2, x_3) = x_1^4 x_3 + x_1^2 x_2 x_3^2 + x_1 x_2^2 x_3^2 + x_2^3 x_3^2,$$

sin que haya ningún motivo para dar preferencia a una de estas expresiones ante la otra. Pero existe, sin embargo, un método completamente determinado de ordenación de los términos de un polinomio en varias indeterminadas que depende, por cierto, de la numeración elegida de las indeterminadas; para los polinomios en una indeterminada, este método se reduce a la ordenación de los términos según las potencias decrecientes de la indeterminada. Este método, denominado *lexicográfico*, está dictado por el procedimiento común de ordenación de las palabras en los diccionarios («vocabularios»): suponiendo que las letras están ordenadas como está convenido en el alfabeto, la posición relativa en el diccionario de dos palabras dadas se determina por sus primeras letras; si éstas coinciden, por sus segundas letras, etc.

Sea dado un polinomio $f(x_1, x_2, \ldots, x_n)$ del anillo $P[x_1, x_2, \ldots, x_n]$ y dos términos distintos de él:

$$x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}, \tag{1}$$

$$x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}, \tag{2}$$

cuyos coeficientes son elementos de P, diferentes de cero. Como los términos (1) y (2) son distintos, al menos una de las diferencias de los exponentes de las indeterminadas

$$k_i - l_i, \quad i = 1, 2, \ldots, n,$$

es diferente de cero. El término (1) se considerará *superior* al término (2) (y el término (2), *inferior* al término (1)), si la primera de estas diferencias, distinta de cero, es positiva, o sea, si existe una i, $1 \leqslant i \leqslant n$, tal que

$$k_1 = l_1, \quad k_2 = l_2, \ \ldots, \ k_{i-1} = l_{i-1}, \text{ pero } k_i > l_i.$$

En otras palabras, el término (1) será superior al término (2), si el exponente de x_1 en (1) es mayor que en (2) o, siendo estos exponentes iguales, si el exponente de x_2 en (1) es mayor que en (2), etc. Por supuesto, el hecho de que el término (1) sea superior al término (2) no implica que el grado del primero con respecto al conjunto de las indeterminadas sea mayor que el del segundo. Por ejemplo, el primero de los términos

$$x_1^3 x_2 x_3, \quad x_1 x_2^5 x_3^2$$

es superior al segundo, a pesar de que es de menor grado.

Es evidente que, de dos términos distintos de un polinomio $f(x_1, x_2, \ldots, x_n)$, uno de ellos es superior al otro. Fácilmente se

comprueba también que, si el término (1) es superior al término (2), y éste, a su vez, es superior al término

$$x_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}, \tag{3}$$

o sea, que existe una j, $1 \leqslant j \leqslant n$, tal, que

$$l_1 = m_1,\ l_2 = m_2,\ \ldots,\ l_{j-1} = m_{j-1},\ \text{pero}\ l_j > m_j,$$

el término (1) es superior al término (3), independiente de que sea i mayor, igual o menor que j. Por lo tanto, de cada dos términos, poniendo delante el que sea superior, obtenemos una ordenación determinada de los términos del polinomio $f(x_1, x_2, \ldots, x_n)$, llamada lexicográfica.

Así, pues, la ordenación de los términos en el polinomio

$$f(x_1, x_2, x_3, x_4) = x_1^4 + 3x_1^2x_2^3x_3 - x_1^2x_2^3x_4^2 + 5x_1x_3x_4^2 + 2x_2 + x_3^3x_4 - 4$$

es lexicográfica.

En la expresión lexicográfica de un polinomio $f(x_1, x_2, \ldots, x_n)$, uno de sus términos ocupará el primer lugar, o sea, será superior a todos los demás. Este se llama *término superior del polinomio*; en el ejemplo precedente, el término superior es x_1^4. Respecto a los términos superiores, demostraremos un **lema** que se aplicará en la demostración del teorema fundamental del siguiente párrafo:

El término superior del producto de dos polinomios en n indeterminadas es igual al producto de los términos superiores de los factores.

En efecto, supongamos que se multiplican los polinomios $f(x_1, x_2, \ldots, x_n)$ y $g(x_1, x_2, \ldots, x_n)$. Si

$$ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} \tag{4}$$

es el término superior del polinomio $f(x_1, x_2, \ldots, x_n)$, y

$$a'x_1^{s_1}x_2^{s_2}\ldots x_n^{s_n} \tag{5}$$

es otro término cualquiera del mismo, existe un valor i, $1 \leqslant i \leqslant n$, tal que

$$k_1 = s_1,\ \ldots,\ k_{i-1} = s_{i-1},\quad k_i > s_i.$$

Si, por otra parte,

$$bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}, \tag{6}$$

$$b'x_2^{t_1}x_2^{t_2}\ldots x_n^{t_n} \tag{7}$$

son el término superior y otro término cualquiera del polinomio $g(x_1, x_2, \ldots, x_n)$, existe un valor j, $1 \leqslant j \leqslant n$, tal que

$$l_1 = t_1,\ \ldots,\ l_{j-1} = t_{j-1},\ l_j > t_j.$$

Multiplicando los términos (4) y (6), y también los términos (5) y (7), obtenemos:

$$abx_1^{k_1+l_1}x_2^{k_2+l_2}\ldots x_n^{k_n+l_n}, \tag{8}$$

$$a'b'x_1^{s_1+l_1}x_2^{s_2+l_2}\ldots x_n^{s_n+l_n}. \tag{9}$$

Sin embargo, fácilmente se comprueba que el término (8) es superior al término (9); si, por ejemplo, $i \leqslant j$, resulta,

$$k_1+l_1=s_1+t_1,\ \ldots,\ k_{i-1}+l_{i-1}=s_{i-1}+t_{i-1},\ \text{pero}\ k_i+l_i>s_i+t_i,$$

pues $k_i > s_i$, $l_i \geqslant t_i$. Del mismo modo se comprueba que el término (8) es superior al producto de los términos (4) y (7), y superior al producto de los términos (5) y (6). Por consiguiente, el término (8), que es el producto de los términos superiores de los polinomios f y g, es superior a todos los demás términos que se obtienen multiplicando término a término los polinomios f y g, y, por lo tanto, este término no puede eliminarse al reducir los términos semejantes, o sea, se mantiene en el producto fg como término superior.

§ 52. Polinomios simétricos

Entre los polinomios en varias indeterminadas se distinguen los que no varían con cualquier permutación de las indeterminadas. Por consiguiente, en tales polinomios figuran todas las indeterminadas de un modo simétrico, por lo cual se llaman *polinomios simétricos* (o *funciones simétricas*). Los ejemplos más elementales son: la suma de todas las indeterminadas $x_1 + x_2 + \ldots + x_n$, la suma de los cuadrados de las indeterminadas $x_1^2 + x_2^2 + \ldots + x_n^2$, el producto de las indeterminadas $x_1x_2 \ldots x_n$, etc. En virtud de la posibilidad de expresar cualquier sustitución de n símbolos en forma de un producto de trasposiciones (véase el § 3), para demostrar que un polinomio es simétrico, es suficiente comprobar que éste no varía al efectuar una trasposición cualquiera de dos indeterminadas.

A continuación se estudiarán los polinomios simétricos en n indeterminadas con coeficientes de un campo P. Está claro que *la suma, diferencia y producto de dos polinomios simétricos son también simétricos*, es decir, los polinomios simétricos forman un subanillo en el anillo $P[x_1, x_2, \ldots, x_n]$ de todos los polinomios en n indeterminadas sobre el campo P, denominado *anillo de los polinomios simétricos en n indeterminadas sobre el campo P*. Todos los elementos del campo P pertenecen a este anillo (o sea, todos los polinomios de grado cero, y también el cero), ya que éstos no varían al efectuar cualquier permutación de las indeterminadas. Cualquier otro polinomio simétrico contiene indispensablemente todas las n indeterminadas, e incluso con respecto a ellas tiene un mismo grado. En efecto, si el polinomio simétrico $f(x_1, x_2, \ldots, x_n)$ tiene un término en el

que la indeterminada x_i figura con el exponente k, entonces tiene también el término que se obtiene de este último mediante la trasposición de las indeterminadas x_i y x_j, o sea, el que contiene a la indeterminada x_j con el mismo exponente k.

Los n polinomios simétricos en n indeterminadas que se exponen a continuación se llaman *polinomios simétricos elementales*:

$$\left.\begin{aligned}
\sigma_1 &= x_1 + x_2 + \ldots + x_n,\\
\sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,\\
\sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\sigma_{n-1} &= x_1x_2 \ldots x_{n-1} + x_1x_2 \ldots x_{n-2}x_n + \ldots + x_2x_3 \ldots x_n\\
\sigma_n &= x_1x_2 \ldots x_n.
\end{aligned}\right\} \quad (1)$$

Estos polinomios que, evidentemente, son simétricos, desempeñan un papel muy importante en la teoría de los polinomios simétricos. Su origen se debe a las fórmulas de Vieta (véase el § 24). Por esto, se puede decir que *los coeficientes de un polinomio en una indeterminada, cuyo coeficiente superior es igual a la unidad, son, salvo el signo, los polinomios simétricos elementales en sus raíces.* Esta relación de los *polinomios simétricos elementales con las fórmulas de Vieta* es muy importante para las aplicaciones de los polinomios simétricos a la teoría de los polinomios en una indeterminada, y es la causa por la que ahora los estudiamos.

Como los polinomios simétricos en n indeterminadas $x_1, x_2, \ldots, x_n$ sobre el campo P forman un anillo, resultan evidentes las proposiciones siguientes: es un polinomio simétrico cualquier potencia entera y positiva de cualquiera de los polinomios elementales simétricos, y también el producto de tales potencias, tomado además con cualquier coeficiente de P y, finalmente, cualquier suma de los productos indicados. En otras palabras, *cualquier polinomio en los polinomios simétricos elementales* $\sigma_1, \sigma_2, \ldots, \sigma_n$, *con coeficientes de* P, *considerado como un polinomio en las indeterminadas* $x_1, x_2, \ldots, x_n$, *es simétrico.* Así, pues, pongamos $n = 3$ y tomemos el polinomio $\sigma_1\sigma_2 + 2\sigma_3$. Sustituyendo σ_1, σ_2 y σ_3 por sus expresiones, obtenemos:

$$\sigma_1\sigma_2 + 2\sigma_3 = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2 + 5x_1x_2x_3;$$

evidentemente, en el segundo miembro figura un polinomio simétrico en x_1, x_2, x_3.

Recíproco a este resultado es el siguiente **teorema fundamental de los polinomios simétricos:**

Todo polinomio simétrico en las indeterminadas $x_1, x_2, \ldots, x_n$ *sobre el campo* P *es un polinomio en los polinomios simétricos elementales* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *con coeficientes pertenecientes al campo* P.

En efecto, sea dado un polinomio simétrico

$$f(x_1, x_2, \ldots, x_n)$$

y supongamos que en su expresión lexicográfica el término superior es

$$a_0 x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}. \tag{2}$$

Los exponentes de las indeterminadas en este término tienen que satisfacer a las desigualdades

$$k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n. \tag{3}$$

En efecto, supongamos que para cierta i, $k_i < k_{i+1}$. El polinomio $f(x_1, x_2, \ldots, x_n)$, siendo simétrico, tiene que contener el término

$$a_0 x_1^{k_1} x_2^{k_2} \ldots x_i^{k_{i+1}} x_{i+1}^{k_i} \ldots x_n^{k_n}, \tag{4}$$

que se obtiene del término (2) mediante una trasposición de las indeterminadas x_i y x_{i+1}. Sin embargo, esto es absurdo, puesto que el término (4), en el sentido de la ordenación lexicográfica, es superior al término (2); en efecto, los exponentes de $x_1, x_2, \ldots, x_{i-1}$ en ambos términos coinciden, pero el exponente de x_i en el término (4) es mayor que en el término (2).

Consideremos ahora el siguiente producto de polinomios elementales simétricos (en virtud de las desigualdades (3), todos los exponentes son no negativos):

$$\varphi_1 = a_0 \sigma_1^{k_1 - k_2} \sigma_2^{k_2 - k_3} \ldots \sigma_{n-1}^{k_{n-1} - k_n} \sigma_n^{k_n}. \tag{5}$$

Este polinomio en las indeterminadas $x_1, x_2, \ldots, x_n$ es simétrico y su término superior es igual al término (2). En efecto, los términos superiores de los polinomios $\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n$ son iguales a $x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2 \ldots x_n$, respectivamente, y como al final del párrafo anterior se demostró que el término superior del producto es igual al producto de los términos superiores de los factores, el término superior del polinomio φ_1 es

$$a_0 x_1^{k_1 - k_2} (x_1x_2)^{k_2 - k_3} (x_1x_2x_3)^{k_3 - k_4} \ldots$$
$$\ldots (x_1x_2 \ldots x_{n-1})^{k_{n-1} - k_n} (x_1x_2 \ldots x_n)^{k_n} = a_0 x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}.$$

De aquí se deduce que, al restar φ_1 de f, los términos superiores de estos polinomios se eliminan entre sí, o sea, el término superior del polinomio simétrico $f - \varphi_1 = f_1$ resulta menor que el término (2), que es el superior en el polinomio f. Repitiendo este mismo procedimiento para el polinomio f_1, cuyos coeficientes pertenecen evidentemente al campo P, llegamos a la igualdad

$$f_1 = \varphi_2 + f_2,$$

donde φ_2 es un producto de potencias de polinomios simétricos elementales con cierto coeficiente del campo P, y f_2, un polinomio *simétrico cuyo término superior es inferior al término superior de* f_1. De aquí, resulta la igualdad

$$f = \varphi_1 + \varphi_2 + f_2.$$

Continuando este proceso, para cierto s obtenemos $f_s = 0$. De este modo, llegaremos a obtener para f una expresión en forma de un polinomio en $\sigma_1, \sigma_2, \ldots, \sigma_n$ con coeficientes de P:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{s} \varphi_i = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

En efecto, si este proceso fuese indefinido*, obtendríamos una *sucesión indefinida* de polinomios simétricos

$$f_1, f_2, \ldots, f_s, \ldots, \tag{6}$$

donde el término superior de cada uno de ellos sería inferior a los términos superiores de los precedentes polinomios y, por lo tanto, inferior a (2). Pero, si

$$bx_1^{l_1}x_2^{l_2} \ldots x_n^{l_n} \tag{7}$$

es el término superior del polinomio f_s, como este último es simétrico, resultan las desigualdades

$$l_1 \geqslant l_2 \geqslant \ldots \geqslant l_n, \tag{8}$$

semejantes a las desigualdades (3). Por otra parte, como el término (2) es superior al término (7), se tiene

$$k_1 \geqslant l_1. \tag{9}$$

Además, se observa fácilmente que los sistemas de números enteros *no negativos* $l_1, l_2, \ldots, l_n$, *que satisfacen a las desigualdades* (8) y (9), se pueden elegir solamente de un número finito de modos. En efecto, incluso cuando no se insiste en el cumplimiento de la condición (8), si se supone solamente que todas las l_i, $i = 1, 2, \ldots, n$, no son mayores que k_i, resulta ya que los números l_i se pueden elegir solamente de $(k_1 + 1)^n$ modos. De aquí se deduce que la sucesión de polinomios (6) con los términos superiores estrictamente decrecientes, no puede ser indefinida.

El teorema queda demostrado.

De la relación entre los polinomios elementales simétricos y las fórmulas de Vieta, indicadas anteriormente, se desprende el siguiente

* Hay que tener presente que, por lo general, el polinomio φ_s contiene también términos que no existen en el polinomio f_{s-1} y, por esto, el paso de f_{s-1} a $f_s = f_{s-1} - \varphi_s$ no sólo está ligado con la eliminación de ciertos términos de f_{s-1}, *sino también con la aparición de nuevos términos*. Aquí $s = 1, 2, \ldots$

corolario importante del teorema fundamental de los polinomios simétricos:

Sea $f(x)$ un polinomio en una indeterminada sobre el campo P, con el coeficiente superior igual a la unidad. Entonces, cualquier polinomio simétrico (con coeficientes de P) en las **raíces** *del polinomio $f(x)$, pertenecientes a un campo de descomposición del polinomio $f(x)$ sobre P, es un polinomio (con coeficientes de P) en los* **coeficientes** *del polinomio $f(x)$ y, por lo tanto, es un elemento del campo P.*

La demostración expuesta del teorema fundamental proporciona a la vez un método para la averiguación práctica de las expresiones de los polinomios simétricos mediante los polinomios elementales. Hagamos primero la siguiente notación: siendo

$$ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n} \tag{10}$$

un producto de potencias de las indeterminadas $x_1, x_2, \dots, x_n$ (algunos de los exponentes pueden ser iguales a cero), mediante

$$S(ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}) \tag{11}$$

designaremos la suma de todos los términos que se obtienen de (10) al permutar las indeterminadas de todos los modos posibles. Evidentemente, éste es un polinomio simétrico y homogéneo. También es evidente que cualquier polinomio simétrico en n indeterminadas que contenga al término (10), contiene también todos los demás términos del polinomio (11). Por ejemplo, $S(x_1) = \sigma_1$, $S(x_1x_2) = \sigma_2$, $S(x_1^2)$ es la suma de los cuadrados de todas las indeterminadas, etc.

Ejemplo. Expresar el polinomio simétrico $f = S(x_1^2x_2)$ en n indeterminadas mediante los polinomios simétricos elementales.

Aquí, el término superior es $x_1^2x_2$, y por esto, $\varphi_1 = \sigma_1^{2-1}\sigma_2 = \sigma_1\sigma_2$, o sea,

$$\varphi_1 = (x_1 + x_2 + \dots + x_n)(x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n) = \\ = S(x_1^2x_2) + 3S(x_1x_2x_3),$$

de donde

$$f_1 = f - \varphi_1 = -3S(x_1x_2x_3) = -3\sigma_3.$$

Por esto $f = \varphi_1 + f_1 = \sigma_1\sigma_2 - 3\sigma_3$.

En ejemplos más complicados es conveniente determinar primero qué términos pueden figurar en la expresión del polinomio dado mediante los polinomios elementales y hallar después los coeficientes de estos términos por el método de los coeficientes indeterminados.

Ejemplos. 1. Hallar la expresión para el polinomio simétrico $f = S(x_1^2x_2^2)$. Ya sabemos (véase la demostración del teorema fundamental) que los términos del polinomio buscado $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ se determinan mediante los términos superiores de los polinomios simétricos $f_1, f_2, \dots$, siendo inferiores estos términos al término superior del polinomio dado f, o sea, inferiores a $x_1^2x_2^2$. Hallemos todos los productos $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ que satisfacen a las condiciones siguientes: 1) son inferiores al término $x_1^2x_2^2$; 2) pueden servir de términos superiores para los polinomios simétricos, o sea, satisfacen a las desigualdades $l_1 \geqslant l_2 \geqslant \dots \geqslant l_n$; 3) son de cuarto grado con respecto al conjunto de las indeterminadas (pues, como ya sabemos, todos los polinomios $f_1, f_2, \dots$ tienen el mismo grado que el polinomio homogéneo f). Escribiendo solamente las combinaciones correspondientes de los exponentes e indicando al lado los productos de las

potencias de σ determinados por ellos, obtenemos la tabla siguiente:

$$22\,000 \ldots \sigma_1^{2-2}\sigma_2^{2-0} = \sigma_2^2,$$
$$21\,100 \ldots \sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^{1-0} = \sigma_1\sigma_3,$$
$$11\,110 \ldots \sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^{1-1}\sigma_4^{1-0} = \sigma_4.$$

Por lo tanto, el polinomio f tiene la forma

$$f = \sigma_2^2 + A\sigma_1\sigma_3 + B\sigma_4.$$

Hemos hecho el coeficiente de σ_2 igual a la unidad, pues, este término se determina por el término superior del polinomio f que, como ya sabemos por la demostración del teorema fundamental, tiene este mismo coeficiente. Los coeficientes A y B los hallaremos del modo siguiente.

Pongamos $x_1 = x_2 = x_3 = 1$, $x_4 = \ldots = x_n = 0$. Fácilmente se observa que, para estos valores de las indeterminadas, el polinomio f toma el valor 3 y los polinomios σ_1, σ_2, σ_3 y σ_4, los valores 3, 3, 1 y 0, respectivamente. Por esto

$$3 = 9 + A \cdot 3 \cdot 1 + B \cdot 0,$$

de donde $A = -2$. Pongamos ahora $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = \ldots = x_n = 0$. Los valores de los polinomios f, σ_1, σ_2, σ_3 y σ_4 son 6, 4, 6, 4, 1, respectivamente. Por esto,

$$6 = 36 - 2 \cdot 4 \cdot 4 + B \cdot 1,$$

de donde $B = 2$. Por lo tanto, la expresión buscada para f es

$$f = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4.$$

2. Hallar la suma de los cubos de las raíces del polinomio

$$f(x) = x^4 + x^3 + 2x^2 + x + 1.$$

Para la resolución de este problema, hallemos la expresión mediante los polinomios simétricos elementales para el polinomio simétrico $S(x_1^3)$. Aplicando el mismo método que en el ejemplo anterior, obtenemos la tabla

$$3\,000 \ldots \sigma_1^3,$$
$$2\,100 \ldots \sigma_1\sigma_2,$$
$$1\,110 \ldots \sigma_3.$$

y, por esto,

$$S(x_1^3) = \sigma_1^3 + A\sigma_1\sigma_2 + B\sigma_3.$$

Poniendo primero $x_1 = x_2 = 1$, $x_3 = \ldots = x_n = 0$, y después, $x_1 = x_2 = x_3 = 1$, $x_4 = \ldots = x_n = 0$, obtenemos, $A = -3$, $B = 3$, o sea,

$$S(x_1^3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \qquad (12)$$

Para hallar la suma de los cubos de las raíces del polinomio $f(x)$ dado, en virtud de las fórmulas de Viéta, en la expresión que hemos hallado hay que sustituir σ_1 por el coeficiente de x^3 con signo contrario, o sea, por -1; σ_2, por el coeficiente de x^2, o sea, por 2; y, por fin, σ_3, por el coeficiente de x con signo contrario, o sea, por -1. Por consiguiente, la suma de los cubos de las raíces que nos interesa es igual a

$$(-1)^3 - 3 \cdot (-1) \cdot 2 + 3 \cdot (-1) = 2.$$

El lector puede comprobar este resultado teniendo en cuenta que las raíces de $f(x)$ son: i, $-i$, $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ y $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$. Está claro también que la fórmula (12) no depende del polinomio $f(x)$ dado y permite hallar la suma de los cubos de las raíces de cualquier polinomio.

El método obtenido en la demostración del teorema fundamental para expresar un polinomio simétrico f mediante los polinomios elementales, conduce a un polinomio en $\sigma_1, \sigma_2, \ldots, \sigma_n$ completamente determinado. Resulta que de ningún modo se puede obtener para f otra expresión distinta mediante $\sigma_1, \sigma_2, \ldots, \sigma_n$. Esto muestra el siguiente **teorema de unicidad:**

Todo polinomio simétrico posee una expresión única en forma de un polinomio en los polinomios simétricos elementales.

Demostremos este teorema. Si un polinomio simétrico $f(x_1, x_2, \ldots, x_n)$ sobre el campo P poseyese dos expresiones distintas mediante $\sigma_1, \sigma_2, \ldots, \sigma_n$:

$$f(x_1, x_2, \ldots, x_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) = \psi(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

la diferencia

$$\chi(\sigma_1, \sigma_2, \ldots, \sigma_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) - \psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

sería un polinomio en $\sigma_1, \sigma_2, \ldots, \sigma_n$, diferente de cero, es decir, que no todos sus coeficientes serían iguales a cero, mientras que la sustitución en este polinomio de $\sigma_1, \sigma_2, \ldots, \sigma_n$ por sus expresiones mediante $x_1, x_2, \ldots, x_n$ nos daría el cero del anillo $P[x_1, x_2, \ldots, x_n]$. Por esto, no queda más que demostrar que, si un polinomio $\chi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ es diferente de cero, o sea, que tiene por lo menos un coeficiente diferente de cero, el polinomio $g(x_1, x_2, \ldots, x_n)$, obtenido de χ sustituyendo $\sigma_1, \sigma_2, \ldots, \sigma_n$ por sus expresiones mediante $x_1, x_2, \ldots, x_n$:

$$\chi(\sigma_1, \sigma_2, \ldots, \sigma_n) = g(x_1, x_2, \ldots, x_n), \tag{13}$$

es también diferente de cero.

Si $a\sigma_1^{k_1}\sigma_2^{k_2} \ldots \sigma_n^{k_n}$ es uno de los términos del polinomio χ, siendo $a \neq 0$, entonces, como ya sabemos por la demostración del teorema fundamental, después de sustituir todas las σ por sus expresiones (1), obtenemos un polinomio en $x_1, x_2, \ldots, x_n$, cuyo término superior (en el sentido de la ordenación lexicográfica) es

$$ax_1^{l_1}(x_1x_2)^{k_2} \ldots (x_1x_2 \ldots x_n)^{k_n} = ax_1^{l_1}x_2^{l_2} \ldots x_n^{l_n},$$

donde

$$\begin{aligned} l_1 &= k_1 + k_2 + \ldots + k_n, \\ l_2 &= \quad k_2 + \ldots + k_n, \\ &\ldots\ldots\ldots\ldots \\ l_n &= \qquad\qquad k_n. \end{aligned}$$

De aquí resulta,

$$k_i = l_i - l_{i+1}, \quad k_n = l_n, \quad i = 1, 2, \ldots, n-1,$$

o sea, conociendo los exponentes $l_1, l_2, \ldots, l_n$ se pueden restituir los exponentes $k_1, k_2, \ldots, k_n$ del término inicial del polinomio χ. Por lo tanto, distintos términos del polinomio χ, considerados como polinomios en $x_1, x_2, \ldots, x_n$, tienen términos superiores **diferentes.**

Consideremos ahora todos los términos del polinomio χ; para cada uno de ellos, hallemos el término superior de su expresión en forma de un polinomio en $x_1, x_2, \ldots, x_n$ y entre estos términos superiores elijamos el que sea **superior** en el sentido de la ordenación lexicográfica. Como ya se advirtió antes, este término no tiene semejantes entre los términos superiores que se obtienen de los demás términos del polinomio χ y, como por la condición, este término es superior a cada uno de estos términos **superiores**, es superior, por consiguiente, a todos los demás términos que se obtienen sustituyendo los elementos $\sigma_1, \sigma_2, \ldots, \sigma_n$ en los términos del polinomio χ por sus expresiones (1). Por lo tanto, hemos hallado un término que, al pasar de $\chi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ a $g(x_1, x_2, \ldots, x_n)$, aparece (con un coeficiente diferente de cero) una sola vez, por lo cual, no puede simplificarse con ninguno. De aquí se deduce que no todos los coeficientes del polinomio $g(x_1, x_2, \ldots, x_n)$ son iguales a cero, o sea, que este polinomio no es el cero del anillo $P[x_1, x_2, \ldots, x_n]$, como se quería demostrar.

Es evidente que el teorema demostrado se puede enunciar también del modo siguiente:

El sistema de los polinomios simétricos elementales $\sigma_1, \sigma_2, \ldots, \sigma_n$, *considerados como elementos del anillo de los polinomios* $P[x_1, x_2, \ldots, x_n]$, *es algebraicamente independiente sobre el campo* P.

§ 53. Observaciones complementarias sobre los polinomios simétricos

Observaciones sobre el teorema fundamental. La demostración del teorema fundamental de los polinomios simétricos expuesta en el párrafo anterior, permite hacer algunos complementos esenciales al enunciado del teorema, los cuales se aplicarán más adelante. Ante todo, los coeficientes del polinomio $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$, hallado como expresión del polinomio simétrico $f(x_1, x_2, \ldots, x_n)$ mediante los polinomios simétricos elementales, no sólo pertenecen al campo P, sino que *se obtienen incluso de los coeficientes del polinomio f aplicando las operaciones de adición y sustracción, o sea, pertenecen al anillo L engendrado por los coeficientes del polinomio f dentro del campo P.*

En efecto, como fácilmente se observa, todos los coeficientes del polinomio φ_1 (véase la fórmula (5) del párrafo precedente) son, con respecto a las indeterminadas $x_1, x_2, \ldots, x_n$, múltiplos enteros

del coeficiente a_0 del término superior del polinomio f y, por lo tanto, pertenecen al anillo L. Supongamos que ya está demostrado que pertenecen a L todos los coeficientes (con respecto a $x_1, x_2, \ldots, x_n$) de los polinomios $\varphi_1, \varphi_2, \ldots, \varphi_l$, entonces, los coeficientes del polinomio $f_l = f - \varphi_1 - \varphi_2 - \ldots - \varphi_l$ también pertenecen a L y, por ende, pertenecen también a L todos los coeficientes del polinomio φ_{l+1} con respecto a $x_1, x_2, \ldots, x_n$.

Por otra parte, *el grado del polinomio* $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ *con respecto al conjunto* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *es igual al grado que tiene el polinomio* $f(x_1, x_2, \ldots, x_n)$ *con respecto a cada una de las indeterminadas* x_i. En efecto, como, por el párrafo anterior, (2) es el término superior del polinomio f, k_1 es el grado de f con respecto a x_1 y por esto, en virtud de la simetría, es también el grado de f con respecto a cualquiera otra de las indeterminadas x_i. Mas, por la igualdad (5) del párrafo anterior, el grado de φ_1 con respecto al conjunto σ es igual al número

$$(k_1 - k_2) + (k_2 - k_3) + \ldots + (k_{n-1} - k_n) + k_n = k_1.$$

Por otra parte, como el término superior del polinomio f_1 es inferior al término superior del polinomio f, el grado de f_1 con respecto a cada x_i no será superior al grado de f con respecto a cada una de estas indeterminadas. Pero el polinomio φ_2 desempeña para f_1 el mismo papel que φ_1 para f, por consiguiente, el grado de φ_2 con respecto al conjunto σ es igual al grado de f_1 con respecto a cada x_i, o sea, no es mayor que k_1, etc. Por lo tanto, el grado de $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ tampoco es mayor que k_1. Pero, como ninguna φ_i con $i > 1$, puede contener todas las $\sigma_1, \sigma_2, \ldots, \sigma_n$ elevadas a las mismas potencias que φ_1, el grado de $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ es exactamente igual a k_1. Con esto, nuestra proposición queda demostrada.

Sea, finalmente, $a\sigma_1^{l_1}\sigma_2^{l_2} \ldots \sigma_n^{l_n}$ uno de los términos del polinomio $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Llamemos *peso* de este término al número

$$l_1 + 2l_2 + \ldots + nl_n,$$

o sea, a la suma de los exponentes multiplicados por los índices que corresponden a σ_i. En otras palabras, como se deduce del teorema del grado de un producto de polinomios, demostrado en el § 51, el peso es el grado del término que consideramos con respecto al conjunto de las indeterminadas $x_1, x_2, \ldots, x_n$. Entonces, se verifica la siguiente proposición:

Si un polinomio simétrico homogéneo $f(x_1, x_2, \ldots, x_n)$ *es de grado* s *con respecto al conjunto de las indeterminadas, todos los términos de su expresión* $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ *mediante* σ *tienen un mismo peso, igual a* s.

En efecto, si (2) del párrafo anterior es el término superior del polinomio homogéneo f, se tiene

$$s = k_1 + k_2 + \ldots + k_n.$$

Mas, el peso del término φ_1, según (5) del párrafo precedente, es igual a

$$(k_1 - k_2) + 2(k_2 - k_3) + \ldots + (n-1)(k_{n-1} - k_n) + nk_n = \\ = k_1 + k_2 + k_3 + \ldots + k_n,$$

o sea, también es igual a s. Luego, el polinomio $f_1 = f - \varphi_1$, como diferencia de dos polinomios homogéneos de grado s, también es un polinomio homogéneo de grado s y, por esto, el peso del término φ_2 del polinomio φ también es igual a s, etc.

Fracciones racionales simétricas. *El teorema fundamental* de los polinomios simétricos se puede generalizar para el caso de fracciones racionales. Llamemos *simétrica* a la fracción racional $\frac{f}{g}$ en n indeterminadas $x_1, x_2, \ldots, x_n$, si se mantiene igual a sí misma al hacer cualquier permutación de las indeterminadas. Fácilmente se demuestra que *esta definición no depende de que se tome la fracción* $\frac{f}{g}$ *o una fracción* $\frac{f_0}{g_0}$ *equivalente a ella*. En efecto, si ω es una permutación de las indeterminadas y φ es un polinomio arbitrario en estas indeterminadas, convengamos en designar con φ^ω el polinomio en que se transforma φ al efectuar la permutación ω. Según la hipótesis, para cualquier ω, se tiene,

$$\frac{f}{g} = \frac{f^\omega}{g^\omega},$$

o sea, $fg^\omega = gf^\omega$. Por otra parte, de la igualdad

$$\frac{f}{g} = \frac{f_0}{g_0}$$

resulta, $fg_0 = gf_0$, de donde $f^\omega g_0^\omega = g^\omega f_0^\omega$. Multiplicando por f ambos miembros de la última igualdad, obtenemos:

$$ff^\omega g_0^\omega = fg^\omega f_0^\omega = gf^\omega f_0^\omega,$$

de donde, después de simplificar por f^ω, resulta: $fg_0^\omega = gf_0^\omega$, o sea,

$$\frac{f_0^\omega}{g_0^\omega} = \frac{f}{g} = \frac{f_0}{g_0}.$$

Se verifica el siguiente **teorema**:

Toda fracción racional simétrica en las indeterminadas $x_1, x_2, \ldots, x_n$ *con coeficientes del campo* P, *se expresa en forma de una*

fracción racional en los polinomios simétricos elementales $\sigma_1, \sigma_2, \ldots, \sigma_n$, *con coeficientes pertenecientes de nuevo a* P.

En efecto, sea dada una fracción racional simétrica

$$\frac{f(x_1, x_2, \ldots, x_n)}{g(x_1, x_2, \ldots, x_n)}.$$

Suponiendo que ésta es irreducible, se podría demostrar que, tanto f como g, son polinomios simétricos. Sin embargo, el camino que se sigue a continuación es el más sencillo. Si el polinomio g no es simétrico, multiplicamos el numerador y el denominador por el producto de todos los $n! - 1$ polinomios que se obtienen de g efectuando todas las sustituciones posibles no idénticas de las indeterminadas. Fácilmente se comprueba que ahora el denominador es un polinomio simétrico. En virtud de la simetría de toda la fracción, de aquí se deduce ahora que el numerador es también simétrico y, por esto, para la demostración del teorema no queda más que expresar el numerador y denominador mediante los polinomios simétricos elementales.

Sumas de potencias. En las aplicaciones aparecen frecuentemente los polinomios simétricos $s_k = x_1^k + x_2^k + \ldots + x_n^k$, $k = 1, 2, \ldots$, o sea, las sumas de las potencias k-ésimas de las indeterminadas $x_1, x_2, \ldots, x_n$. Estos polinomios, llamados *sumas de potencias*, tienen que expresarse mediante los polinomios simétricos elementales, según el teorema fundamental. Sin embargo, es bastante difícil encontrar estas expresiones para valores grandes de k y, por lo tanto, ofrece interés la relación existente entre los polinomios $s_1, s_2, \ldots$ y $\sigma_1, \sigma_2, \ldots, \sigma_n$, que se va a establecer ahora.

En primer lugar, $s_1 = \sigma_1$. Por otra parte, siendo $k \leqslant n$, fácilmente se comprueba que se verifican las igualdades:

$$\left.\begin{aligned}
&s_{k-1}\sigma_1 = s_k + S(x_1^{k-1}x_2)\ *,\\
&s_{k-2}\sigma_2 = S(x_1^{k-1}x_2) + S(x_1^{k-2}x_2x_3),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&s_{k-i}\sigma_i = S(x_1^{k-i+1}x_2\ldots x_i) + S(x_1^{k-i}x_2\ldots x_ix_{i+1}),\ 2 \leqslant i \leqslant k-2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&s_1\sigma_{k-1} = S(x_1^2x_2\ldots x_{k-1}) + k\sigma_k.
\end{aligned}\right\} \quad (1)$$

Tomando la suma alternada de estas igualdades (o sea, la suma con los signos alternados), y pasando después todos los términos a una parte de la igualdad, obtenemos la fórmula siguiente:

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \ldots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0 \quad (k \leqslant n). \quad (2)$$

* Véase (11) del párrafo precedente.

Si $k > n$, el sistema de igualdades (1) toma la forma:

$$s_{k-1}\sigma_1 = s_k + S(x_1^{k-1}x_2),$$

$$s_{k-2}\sigma_2 = S(x_1^{k-1}x_3) + S(x_1^{k-2}x_2x_3),$$

. . . . . .

$$s_{k-i}\sigma_i = S(x_1^{k-i+1}x_2 \ldots x_i) + S(x_1^{k-i}x_2 \ldots x_ix_{i+1}), \qquad 2 \leqslant i \leqslant n-1,$$

. . . . . .

$$s_{k-n}\sigma_n = S(x_1^{k-n+1}x_2 \ldots x_n),$$

de donde se deduce la fórmula

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \ldots + (-1)^n s_{k-n}\sigma_n = 0 \quad (k > n). \qquad (3)$$

Las fórmulas (2) y (3) *se llaman fórmulas de Newton.* Estas ligan a las sumas de potencias con los polinomios simétricos elementales y, *por consiguiente, permiten hallar sucesivamente las expresiones* de s_1, s_2, s_3, . . . mediante σ_1, σ_2, . . ., σ_n. Así, pues, ya sabemos que $s_1 = \sigma_1$, *lo cual se deduce también de la fórmula* (2). Si $k = 2 \leqslant n$ entonces, en virtud de (2), se tiene $s_2 - s_1\sigma_1 + 2\sigma_2 = 0$, de donde

$$s_2 = \sigma_1^2 - 2\sigma_2.$$

Si $k = 3 \leqslant n$, *se tiene* $s_3 - s_2\sigma_1 + s_1\sigma_2 - 3\sigma_3 = 0$, *de donde, aplicando* las expresiones ya obtenidas para s_1 y s_2, obtenemos:

$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3,$$

lo cual ya conocemos (*véase* (12) *del párrafo precedente*). Si $k = 3$, pero $n = 2$, por (3) se tiene $s_3 - s_2\sigma_1 + s_1\sigma_2 = 0$, de donde $s_3 = \sigma_1^3 - 3\sigma_1\sigma_2$. *Aplicando las fórmulas de Newton, se puede obtener* una fórmula general que exprese s_k mediante σ_1, σ_2, . . ., σ_n. Pero, *debido a la complejidad de esta fórmula, omitimos su exposición.*

Si el campo fundamental P es de característica 0 y, por lo tanto, *tiene sentido la división por cualquier número natural* n*, la fórmula (2) permite expresar sucesivamente los polinomios simétricos *elementales* σ_1, σ_2, . . ., σ_n, *mediante las primeras* n sumas de potencias s_1, s_2, . . ., s_n. Así, pues, $\sigma_1 = s_1$, y, por esto,

$$\sigma_2 = \frac{1}{2}(s_1\sigma_1 - s_2) = \frac{1}{2}(s_1^2 - s_2),$$

$$\sigma_3 = \frac{1}{3}(s_3 - s_2\sigma_1 + s_1\sigma_2) = \frac{1}{6}(s_1^3 - 3s_1s_2 + 2s_3)$$

etc. De aquí, y del teorema fundamental, se desprende el siguiente resultado:

---

* En un campo de característica p, la expresión $\frac{a}{p}$ carece de sentido si $a \neq 0$, pues, en este campo, para cualquier x, se tiene $px = 0$.

Todo polinomio simétrico en n indeterminadas $x_1, x_2, \ldots, x_n$, *sobre un campo P de característica cero, se puede expresar en forma de un polinomio en las sumas de potencias* $s_1, s_2, \ldots, s_n$ *con coeficientes pertenecientes al campo P.*

Polinomios simétricos con respecto a dos sistemas de indeterminadas. En el siguiente párrafo, así como en el § 58, se va a utilizar una generalización del concepto de polinomio simétrico. Sean dados dos sistemas de indeterminadas, $x_1, x_2, \ldots, x_n$ e $y_1, y_2, \ldots, y_r$, donde su unión

$$x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r \qquad (4)$$

es algebraicamente independiente sobre el campo P. Un polinomio $f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r)$ sobre el campo P se llama *simétrico con respecto a los dos sistemas de indeterminadas*, si no varía al hacer cualesquiera permutaciones de las indeterminadas $x_1, x_2, \ldots, x_n$ entre sí y de las indeterminadas $y_1, y_2, \ldots, y_r$ entre sí. Si para los polinomios simétricos elementales en $x_1, x_2, \ldots, x_n$ conservamos las notaciones $\sigma_1, \sigma_2, \ldots, \sigma_n$, y designamos con $\tau_1, \tau_2, \ldots, \tau_r$, los polinomios simétricos elementales en $y_1, y_2, \ldots, y_r$, el teorema fundamental se generaliza del modo siguiente:

Todo polinomio $f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r)$ *sobre el campo P, que es simétrico con respecto a los sistemas de indeterminadas* $x_1, x_2, \ldots, x_n$ *e* $y_1, y_2, \ldots, y_r$, *se expresa en forma de un polinomio (con coeficientes de P) en los polinomios simétricos elementales respecto de estos dos sistemas de indeterminadas:*

$$f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_r).$$

En efecto, el polinomio f se puede considerar como un polinomio $\overline{f}(y_1, y_2, \ldots, y_r)$ de coeficientes que son polinomios en $x_1, x_2, \ldots, x_n$. Como f no varía al permutar las indeterminadas $x_1, x_2, \ldots, x_n$, los coeficientes del polinomio $\overline{f}$ serán polinomios simétricos en $x_1, x_2, \ldots, x_n$, por lo cual, en virtud del teorema fundamental, se expresan en forma de polinomios (con coeficientes de P) en $\sigma_1, \sigma_2, \ldots, \sigma_n$. Por otra parte, el polinomio $\overline{f}(y_1, y_2, \ldots, y_r)$, considerado sobre el campo $P(x_1, x_2, \ldots, x_n)$, es simétrico con respecto a $y_1, y_2, \ldots, y_r$, por lo cual, se expresa en forma de un polinomio $\overline{\varphi}(\tau_1, \tau_2, \ldots, \tau_r)$. Como se ha mostrado al principio del presente párrafo, los coeficientes del polinomio $\overline{\varphi}$ se expresan mediante los coeficientes del polinomio $\overline{f}$ mediante la suma y la resta y, por consiguiente, también son polinomios en $\sigma_1, \sigma_2, \ldots, \sigma_n$. Evidentemente, esto nos conduce a la expresión buscada de f mediante $\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_r$.

Ejemplo. El polinomio

$$f(x_1, x_2, x_3, y_1, y_2) = x_1x_2x_3 - x_1x_2y_1 - x_1x_2y_2 - x_1x_3y_1 - x_1x_3y_2 - x_2x_3y_1 - x_2x_3y_2 + x_1y_1y_2 + x_2y_1y_2 + x_3y_1y_2$$

es simétrico con respecto a las indeterminadas x_1, x_2, x_3, así como con respecto a las indeterminadas y_1, y_2, pero no es simétrico con respecto al conjunto de todas las cinco indeterminadas, lo cual se observa trasponiendo las indeterminadas x_i e y_i. Hallemos la expresión de f mediante σ_1, σ_2, σ_3, τ_1, τ_2:

$$f = x_1x_2x_3 - (x_1x_2 + x_1x_3 + x_2x_3)\,y_1 - (x_1x_2 + x_1x_3 + x_2x_3)\,y_2 + (x_1 + x_2 + x_3)\,y_1y_2 = \sigma_3 - \sigma_2y_1 - \sigma_2y_2 + \sigma_1y_1y_2 = \sigma_3 - \sigma_2\tau_1 + \sigma_1\tau_2.$$

Naturalmente, el teorema que se acaba de demostrar se generaliza también al caso de tres y de un número mayor de sistemas de indeterminadas.

Para los polinomios que son simétricos con respecto a dos sistemas de indeterminadas se verifica también el **teorema de unicidad** de la representación mediante los polinomios simétricos elementales. En otras palabras, se verifica el siguiente **teorema:**

El sistema unido

$$\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_r$$

de polinomios simétricos elementales en los sistemas dados de indeterminadas $x_1, x_2, \ldots, x_n$ *e* $y_1, y_2, \ldots, y_r$, *es algebraicamente independiente sobre el campo* P.

En efecto, supongamos que existe un polinomio

$$\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_r)$$

sobre el campo P, que es igual a cero, a pesar de que no todos sus coeficientes son iguales a cero. Este polinomio se puede considerar como un polinomio $\psi(\tau_1, \tau_2, \ldots, \tau_r)$ de coeficientes que son polinomios en $\sigma_1, \sigma_2, \ldots, \sigma_n$. Por consiguiente, se puede suponer que ψ es un polinomio en $\tau_1, \tau_2, \ldots, \tau_r$ sobre el campo de fracciones racionales:

$$Q = P(x_1, x_2, \ldots, x_n).$$

El sistema $y_1, y_2, \ldots, y_r$ se mantiene algebraicamente independiente sobre el campo Q, pues, si para este sistema existiese una dependencia algebraica con coeficientes de Q, eliminando los denominadores obtendríamos una dependencia algebraica en el sistema (4), en contra de la hipótesis. Basándose en el teorema de unicidad del párrafo anterior, resulta ahora que el sistema $\tau_1, \tau_2, \ldots, \tau_r$ también tiene que ser algebraicamente independiente sobre el campo Q y, por esto, todos los coeficientes del polinomio ψ son iguales a cero. Pero, estos coeficientes son polinomios en $\sigma_1, \sigma_2, \ldots, \sigma_n$, por lo cual, de nuevo, en virtud del teorema de unicidad para el caso de un sistema de indeterminadas (esta vez, para el sistema

$x_1, x_2, \ldots, x_n$), los mismos coeficientes de estos últimos polinomios son iguales a cero. Con esto queda demostrado que, en contra de la hipótesis, todos los coeficientes del polinomio φ tienen que ser iguales a cero.

§ 54. Resultante. Eliminación de una indeterminada. Discriminante

Dado un polinomio $f(x_1, x_2, \ldots, x_n)$ del anillo $P[x_1, x_2, \ldots, x_n]$, se llama *solución* del mismo a un sistema de valores de las indeterminadas

$$x_1 = \alpha_1, \; x_2 = \alpha_2, \; \ldots, \; x_n = \alpha_n,$$

tomados en el campo P o en alguna ampliación $\overline{P}$ de este campo, que convierte en cero al polinomio f:

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0.$$

Todo polinomio f, cuyo grado sea mayor que cero, posee soluciones. En efecto, si la indeterminada x_1 figura en la expresión de este polinomio, entonces, se pueden tomar por $\alpha_2, \ldots, \alpha_n$ los elementos arbitrarios del campo P, con la condición solamente de que el grado del polinomio $f(x_1, \alpha_2, \ldots, \alpha_n)$ se mantenga estrictamente positivo, y después, aplicando el teorema de existencia de la raíz (§ 49), se puede tomar una ampliación $\overline{P}$ del campo P, en la que el polinomio $f(x_1, \alpha_2, \ldots, \alpha_n)$ en una indeterminada x_1 tenga una raíz α_1. A la vez, observamos que la propiedad (de los polinomios de grado n en una indeterminada) de poseer en cualquier campo no más de n raíces, no se cumple para los polinomios en varias indeterminadas.

Dados unos cuantos polinomios en n indeterminadas, se puede plantear el problema del cálculo de las soluciones que son comunes a todos ellos, o sea, de las soluciones del sistema de ecuaciones que resulta al igualar a cero los polinomios dados. En el segundo capítulo se estudió detalladamente un caso particular de este problema, precisamente, el caso de sistemas de ecuaciones lineales. Sin embargo, en el caso particular inverso de una ecuación en una indeterminada, pero de grado arbitrario, no sabemos nada sobre las raíces, a excepción de que éstas existen en cierta ampliación del campo fundamental. Naturalmente, la búsqueda y el estudio de las soluciones de un sistema no lineal de ecuaciones en varias indeterminadas es un problema más complicado que, por cierto, está fuera de los márgenes de nuestro curso y es el objeto de una rama de las matemáticas, denominada geometría algebraica. Aquí nos limitaremos solamente al caso de un sistema de **dos** ecuaciones de grado arbitrario en **dos** indeterminadas y demostraremos que éste se puede reducir al caso de **una** ecuación en **una** indeterminada.

Ocupémonos primero del problema de la existencia de raíces comunes de dos polinomios en una indeterminada. Sean dados los polinomios

$$\left.\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \\ g(x) &= b_0x^s + b_1x^{s-1} + \ldots + b_{s-1}x + b_s \end{aligned}\right\} \tag{1}$$

sobre el campo P, siendo $a_0 \neq 0$, $b_0 \neq 0$.

De los resultados del párrafo precedente, sin dificultad alguna se deduce que *los polinomios $f(x)$ y $g(x)$ poseen raíz común en cierta ampliación del campo P cuando, y sólo cuando, éstos no son primos entre sí*. Por lo tanto, el problema de la existencia de raíces comunes para los polinomios dados se puede resolver aplicándoles el algoritmo de Euclides.

Ahora señalaremos otro método para dar una respuesta a este problema. Sea $\overline{P}$ una ampliación tal del campo P, en la que $f(x)$ tenga n raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$, y $g(x)$ tenga s raíces, $\beta_1, \beta_2, \ldots, \beta_s$; por $\overline{P}$ se puede tomar el campo de descomposición del producto $f(x)\,g(x)$. El elemento

$$R(f, g) = a_0^s b_0^n \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j) \tag{2}$$

del campo $\overline{P}$ se llama *resultante* de los polinomios $f(x)$ y $g(x)$. Es evidente que *$f(x)$ y $g(x)$ poseen en $\overline{P}$ raíz común cuando, y sólo cuando*, $R(f, g) = 0$. Como

$$g(x) = b_0 \prod_{j=1}^{s} (x - \beta_j)$$

se tiene,

$$g(\alpha_i) = b_0 \prod_{j=1}^{s} (\alpha_i - \beta_j);$$

la resultante $R(f, g)$ se puede expresar también en la forma

$$R(f, g) = a_0^s \prod_{i=1}^{n} g(\alpha_i). \tag{3}$$

En la definición de la resultante, los polinomios $f(x)$ y $g(x)$ no se emplean de un modo simétrico. En efecto,

$$R(g, f) = b_0^n a_0^s \prod_{j=1}^{s} \prod_{i=1}^{n} (\beta_j - \alpha_i) = (-1)^{ns} R(f, g). \tag{4}$$

En correspondencia con (3), $R(g, f)$ se puede expresar en la forma

$$R(g, f) = b_0^n \prod_{j=1}^{s} f(\beta_j). \tag{5}$$

La expresión (2) para la resultante exige conocer las raíces de los polinomios $f(x)$ y $g(x)$ y, por esto, prácticamente es inútil para la resolución del problema de la existencia de una raíz común de estos polinomios. Sin embargo, resulta que *la resultante $R(f, g)$ se puede expresar en forma de un polinomio en los coeficientes $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s$ de los polinomios $f(x)$ y $g(x)$.*

La posibilidad de tal representación se deduce fácilmente de los resultados del párrafo anterior. En efecto, la fórmula (2) muestra que la resultante $R(f, g)$ es un polinomio simétrico en dos sistemas de indeterminadas: en el sistema $\alpha_1, \alpha_2, \ldots, \alpha_n$ y en el sistema $\beta_1, \beta_2, \ldots, \beta_s$. Por esto, como se demostró al fin del párrafo anterior, ésta se representa en forma de un polinomio en los polinomios simétricos elementales en estos dos sistemas de indeterminadas, o sea, en virtud de las fórmulas de Vieta, en forma de un polinomio en los cocientes $\frac{a_i}{a_0}$, $i = 1, 2, \ldots, n$, y $\frac{b_j}{b_0}$, $j = 1, 2, \ldots, s$; el factor $a_0^s b_0^n$, incluido en (2), libra de a_0 y b_0 al denominador de la expresión obtenida. Por cierto, sería muy difícil hallar la expresión de la resultante mediante los coeficientes con los métodos expuestos en los párrafos anteriores, por lo que emplearemos otro método.

La expresión que hallaremos para la resultante de los polinomios (1) será válida para cualquier par de estos polinomios. Precisando, se supondrá que el **sistema de raíces**

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s \tag{6}$$

de los polinomios (1) es un sistema de $n + s$ indeterminadas independientes, o sea, es un sistema de $n + s$ elementos, algebraicamente independiente sobre el campo P en el sentido del § 51.

Obtendremos una expresión para la resultante que, considerada como un polinomio en las indeterminadas (6) (después de sustituir los coeficientes mediante las raíces por las fórmulas de Vieta), será también igual al segundo miembro de la igualdad (2), considerado también como un polinomio en las indeterminadas (6).

Entendiendo la igualdad precisamente en el sentido de identidad con respecto al sistema de las indeterminadas (6), demostraremos que *la resultante $R(f, g)$ de los polinomios* (1) *es igual al siguiente determinante de orden $n + s$:*

$$D = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & & \\ & a_0 & a_1 & \ldots & a_n & \\ & \ldots & \ldots & \ldots & \ldots & \\ & & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_s & & \\ & b_0 & b_1 & \ldots & b_s & \\ & \ldots & \ldots & \ldots & \ldots & \\ & & b_0 & b_1 & \ldots & b_s \end{vmatrix} \begin{matrix} \\ \\ \\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} s \text{ filas} \\ \\ \\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} n \text{ filas} \end{matrix} \tag{7}$$

(en los lugares libres figuran ceros). La estructura de este determinante está suficientemente clara; señalemos solamente que en su diagonal principal figura s veces el coeficiente a_0 y, después, n veces el coeficiente b_s.

Para la demostración de nuestra afirmación, calcularemos de dos modos el producto $a_0^s b_0^n DM$, donde M es el siguiente determinante auxiliar de orden $n + s$:

$$M = \begin{vmatrix} \beta_1^{n+s-1} & \beta_2^{n+s-1} & \dots & \beta_s^{n+s-1} & \alpha_1^{n+s-1} & \alpha_2^{n+s-1} & \dots & \alpha_n^{n+s-1} \\ \beta_1^{n+s-2} & \beta_2^{n+s-2} & \dots & \beta_s^{n+s-2} & \alpha_1^{n+s-2} & \alpha_2^{n+s-2} & \dots & \alpha_n^{n+s-2} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \beta_1^2 & \beta_2^2 & \dots & \beta_s^2 & \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \beta_1 & \beta_2 & \dots & \beta_s & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \end{vmatrix}.$$

M es el determinante de Vandermonde y, por esto, como se indicó en el § 6, es igual al producto de las diferencias de los elementos de su penúltima fila, donde, de cada elemento precedente se resta cualquier elemento posterior. Por lo tanto,

$$M = \prod_{1 \le i < j \le s} (\beta_i - \beta_j) \cdot \prod_{j=1}^{s} \prod_{i=1}^{n} (\beta_j - \alpha_i) \cdot \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j).$$

de donde, en virtud de (4),

$$a_0^s b_0^n DM = D \cdot R(g, f) \cdot \prod_{1 \le i < j \le s} (\beta_i - \beta_j) \cdot \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j). \qquad (8)$$

Por otra parte, calculemos el producto DM basándonos en el teorema del determinante del producto de las matrices. Multiplicando las matrices correspondientes y teniendo en cuenta que todas las α son raíces de $f(x)$ y todas las β son raíces de $g(x)$, obtenemos:

$$a_0^s b_0^n DM = \begin{vmatrix} \beta_1^{s-1} f(\beta_1) & \beta_2^{s-1} f(\beta_2) & \dots & \beta_s^{s-1} f(\beta_s) & 0 & 0 & \dots & 0 \\ \beta_1^{s-2} f(\beta_1) & \beta_2^{s-2} f(\beta_2) & \dots & \beta_s^{s-2} f(\beta_s) & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \beta_1 f(\beta_1) & \beta_2 f(\beta_2) & \dots & \beta_s f(\beta_s) & 0 & 0 & \dots & 0 \\ f(\beta_1) & f(\beta_2) & \dots & f(\beta_s) & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \alpha_1^{n-1} g(\alpha_1) & \alpha_2^{n-1} g(\alpha_2) & \dots & \alpha_n^{n-1} g(\alpha_n) \\ 0 & 0 & \dots & 0 & \alpha_1^{n-2} g(\alpha_1) & \alpha_2^{n-2} g(\alpha_2) & \dots & \alpha_n^{n-2} g(\alpha_n) \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \alpha_1 g(\alpha_1) & \alpha_2 g(\alpha_2) & \dots & \alpha_n g(\alpha_n) \\ 0 & 0 & \dots & 0 & g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \end{vmatrix}$$

Aplicando el teorema de Laplace, sacando después los factores comunes de las columnas de los determinantes y calculando los determinantes que quedan como determinantes de Vandermonde, resulta:

$$a_0^s b_0^n DM = a_0^s b_0^n \prod_{j=1}^{s} f(\beta_s) \cdot \prod_{1 \le i < j \le s} (\beta_i - \beta_j) \cdot \prod_{i=1}^{n} g(\alpha_i) \cdot \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j),$$

o bien, aplicando (3) y (5),

$$a_0^s b_0^n DM = R(f, g) R(g, f) \cdot \prod_{1 \le i < j \le s} (\beta_i - \beta_j) \cdot \prod_{1 \le i < j \le s} (\alpha_i - \alpha_j). \quad (9)$$

Ha resultado que los segundos miembros de las igualdades (8) y (9), considerados como polinomios en las indeterminadas (6), son iguales entre sí. Ambos miembros de la igualdad obtenida se pueden simplificar por sus factores comunes, que no son idénticamente iguales a cero. El factor común $R(g, f)$ no es igual a cero. En efecto, como por la hipótesis, $a_0 \neq 0$ y $b_0 \neq 0$, es suficiente elegir para las indeterminadas (6) valores que no sean iguales entre sí (en el campo fundamental o en alguna ampliación del mismo), para obtener en (4) un valor diferente de cero del polinomio $R(g, f)$. Del mismo modo se demuestra que los otros dos factores comunes son diferentes de cero. Simplificando por todos estos factores comunes, llegamos a la igualdad:

$$R(f, g) = D \quad (10)$$

como se quería demostrar.

Desistamos ahora de la condición de que los coeficientes superiores de los polinomios (1) sean diferentes de cero *. Por consiguiente, acerca de los grados verdaderos de estos polinomios solamente se puede afirmar que éstos no son superiores a sus grados «formales» n y s, respectivamente. Ahora, la expresión (2) para la resultante carece de sentido, pues, posiblemente, los polinomios considerados tienen una cantidad de raíces menor que n o s. Por otra parte, ahora también se puede escribir el determinante (7) y como ya está demostrado que, siendo $a_0 \neq 0$, $b_0 \neq 0$, este determinante es igual a la resultante, le llamaremos también, en el caso general, *resultante* de los polinomios $f(x)$ y $g(x)$, designándole con la notación $R(f, g)$.

Pero ya no se puede asegurar que la igualdad a cero de la resultante es equivalente a la existencia de una raíz común de nuestros

* El hecho de que por ahora nos neguemos de la condición que habíamos impuesto al coeficiente superior del polinomio, se debe a las aplicaciones ulteriores, puesto que queremos estudiar los sistemas de polinomios en dos indeterminadas, refiriendo una de éstas a los coeficientes. Por consiguiente, el coeficiente superior puede anularse para valores particulares de esta indeterminada.

polinomios. En efecto, si $a_0 = 0$ y $b_0 = 0$, resulta que $R(f, g) = 0$, independientemente de que tengan los polinomios f y g raíces comunes o no. Sin embargo, éste es el único caso en que de la igualdad a cero de la resultante no se puede hacer la conclusión de que existen *raíces comunes de estos polinomios**. *Precisando, se verifica* el siguiente teorema:

Dados los polinomios (1) *con cualesquiera coeficientes superiores, su resultante es igual a cero cuando, y sólo cuando, estos polinomios tienen una raíz común, o bien, cuando ambos coeficientes superiores son iguales a cero.*

Demostración. El caso en que $a_0 \neq 0$, $b_0 \neq 0$, ya se estudió anteriormente y el caso en que $a_0 = b_0 = 0$ se tiene en cuenta en el enunciado del teorema. No queda más que considerar el caso en que uno de los coeficientes superiores de los polinomios (1), por ejemplo a_0, *es diferente de cero, mientras que* b_0 *es igual a cero.*

Si $b_i = 0$ para todos los i, $i = 0, 1, \ldots, s$, entonces $R(f, g) = 0$, pues el determinante (7) contiene filas que constan de ceros. Pero, entonces el polinomio $g(x)$ será idénticamente igual a cero, por lo cual, tendrá raíces comunes con $f(x)$. Si

$$b_0 = b_1 = \ldots = b_{k-1} = 0, \text{ pero } b_k \neq 0, \ k \leqslant s,$$

y

$$\overline{g}(x) = b_k x^{s-k} + b_{k+1} x^{s-k-1} + \ldots + b_{s-1} x + b_s,$$

entonces, sustituyendo por ceros los elementos $b_0, b_1, \ldots, b_{k-1}$ en el determinante (7), y aplicando el teorema de Laplace, obtenemos, evidentemente, la igualdad:

$$R(f, g) = a_0^k R(f, \overline{g}). \tag{11}$$

Sin embargo, como los coeficientes superiores de ambos polinomios f y $\overline{g}$ son diferentes de cero, por lo demostrado anteriormente, la igualdad $R(f, \overline{g}) = 0$ es condición necesaria y suficiente para la existencia de una raíz común de los polinomios f y $\overline{g}$. Por otra parte, en virtud de (11), las igualdades $R(f, g) = 0$ y $R(f, \overline{g}) = 0$ son equivalentes, y como los polinomios g y $\overline{g}$ tienen raíces iguales, obtenemos que, en el caso considerado, la igualdad a cero de la resultante $R(f, g)$ es equivalente a la existencia de una raíz común de los polinomios $f(x)$ y $g(x)$. Con esto, el teorema queda demostrado.

---

* Naturalmente, el determinante (7) también es igual a cero cuando $a_n = b_s = 0$. Mas, *en este caso, los polinomios* (1) *tienen la raíz común* 0.

Hallemos la resultante de los dos polinomios cuadrados

$$f(x) = a_0x^2 + a_1x + a_2, \quad g(x) = b_0x^2 + b_1x + b_2.$$

Según (7)

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix},$$

o, calculando el determinante, desarrollándolo para esto por la primera y tercera filas,

$$R(f, g) = (a_0b_2 - a_2b_0)^2 - (a_0b_1 - a_1b_0)(a_1b_2 - a_2b_1). \tag{12}$$

Así, pues, dados los polinomios

$$f(x) = x^2 - 6x + 2, \quad g(x) = x^2 + x + 5,$$

en virtud de (12), se tiene, $R(f, g) = 233$, y por esto, estos polinomios no tienen raíces comunes. Dados los polinomios

$$f(x) = x^2 - 4x - 5, \quad g(x) = x^2 - 7x + 10,$$

se tiene, $R(f, g) = 0$, o sea, estos polinomios tienen una raíz común e igual a 5.

Eliminación de una indeterminada en un sistema de dos ecuaciones con dos indeterminadas. Sean dados dos polinomios f y g en dos indeterminadas x e y, con coeficientes pertenecientes a un campo P. Escribiremos estos polinomios según las potencias decrecientes de la indeterminada x:

$$\left.\begin{aligned} f(x, y) &= a_0(y)\,x^k + a_1(y)\,x^{k-1} + \ldots + a_{k-1}(y)\,x + a_k(y), \\ g(x, y) &= b_0(y)\,x^l + b_1(y)\,x^{l-1} + \ldots + b_{l-1}(y)\,x + b_l(y); \end{aligned}\right\} \tag{13}$$

los coeficientes son polinomios del anillo $P[y]$. Hallemos la resultante de los polinomios f y g, considerados como polinomios en x, y designémosla mediante $R_x(f, g)$; en virtud de (7), ésta es un polinomio en una indeterminada y, con coeficientes del campo P:

$$R_x(f, g) = F(y). \tag{14}$$

Supongamos que el sistema de polinomios (13) posee una solución común $x = \alpha$, $y = \beta$ en una ampliación del campo P. Poniendo en (13), en lugar de y el valor β, obtenemos dos polinomios, $f(x, \beta)$ y $g(x, \beta)$, en una indeterminada x. Estos polinomios tienen una raíz común α y, por consiguiente, su resultante, que en virtud de (14), es igual a $F(\beta)$, tiene que ser igual a cero, o sea, β *tiene que ser raíz de la resultante* $R_x(f, g)$. Recíprocamente, si la resultante $R_x(f, g)$ de los polinomios (13) tiene una raíz β, la resultante de los polinomios $f(x, \beta)$ y $g(x, \beta)$ es igual a cero, o sea, *o bien estos polinomios tienen una raíz común, o bien sus coeficientes superiores son iguales a cero*,

$$a_0(\beta) = b_0(\beta) = 0.$$

De este modo, el cálculo de las soluciones comunes del sistema de polinomios (13) se ha reducido al cálculo de las raíces de un polinomio (14) en una indeterminada y, o sea, como está convenido decir, *se ha eliminado la indeterminada x en el sistema de polinomios (13).*

El teorema que sigue responde a la pregunta sobre el grado del polinomio que se obtiene al eliminar una indeterminada en un sistema de dos polinomios en dos indeterminadas:

Si los polinomios $f(x, y)$ y $g(x, y)$ tienen con respecto al conjunto de las indeterminadas los grados n y s, respectivamente, el grado del polinomio $R_x(f, g)$ con respecto a la indeterminada y no es mayor que el producto ns, naturalmente, si este polinomio no es igual a cero idénticamente.

Ante todo, si se consideran dos polinomios en una indeterminada con los coeficientes superiores iguales a la unidad, según (2) su resultante $R(f, g)$ es un polinomio homogéneo en $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s$, de grado ns. De aquí se deduce que, si en la expresión de la resultante mediante los coeficientes $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_s$ figura el término

$$a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} b_1^{l_1} b_2^{l_2} \ldots b_s^{l_s}$$

y si el número

$$k_1 + 2k_2 + \ldots + nk_n + l_1 + 2l_2 + \ldots + sl_s$$

lo denominamos *peso* del término, *todos los términos de la expresión de $R(f, g)$ mediante los coeficientes tienen un mismo peso, igual a ns.* Esta proposición es verídica también en el caso general para los términos de la resultante (7), si se llama *peso* del término $a_0^{h_0} a_1^{k_1} \ldots a_n^{k_n} b_0^{l_0} b_1^{l_1} \ldots b_s^{l_s}$ al número

$$0 \cdot k_0 + 1 \cdot k_1 + \ldots + nk_n + 0 \cdot l_0 + 1 \cdot l_1 + \ldots + sl_s. \tag{15}$$

En efecto, sustituyendo en los términos del determinante (7) los factores a_0 y b_0 por la unidad, llegamos al caso ya considerado, pero los exponentes de estos factores figuran en (15) con los coeficientes 0.

Escribamos ahora los polinomios f y g en la forma siguiente:

$$f(x, y) = a_0(y)\, x^n + a_1(y)\, x^{n-1} + \ldots + a_n(y),$$
$$g(x, y) = b_0(y)\, x^s + b_1(y)\, x^{s-1} + \ldots + b_s(y).$$

Como n es el grado de $f(x, y)$ con respecto al conjunto de las indeterminadas, el grado del coeficiente $a_r(y)$, $r = 0, 1, 2, \ldots, n$, no puede ser mayor que su índice r; esto mismo es cierto también para $b_r(y)$. De aquí se deduce, que el grado de cada término de la resultante $R_x(f, g)$ no es mayor que el peso de este término, o sea, no es mayor que el número ns, como se quería demostrar.

Ejemplos.

1. Hallar las soluciones del sistema de polinomios

$$f(x, y) = x^2y + 3xy + 2y + 3,$$
$$g(x, y) = 2xy - 2x + 2y + 3.$$

Eliminemos la indeterminada x en este sistema, para lo cual, lo escribimos en la forma:

$$\left.\begin{aligned} f(x, y) &= y \cdot x^2 + (3y) \cdot x + (2y + 3), \\ g(x, y) &= (2y - 2)\, x + (2y + 3); \end{aligned}\right\} \tag{16}$$

entonces,

$$R_x(f, g) = \begin{vmatrix} y & 3y & 2y+3 \\ 2y-2 & 2y+3 & 0 \\ 0 & 2y-2 & 2y-3 \end{vmatrix} = 2y^2 + 11y + 12.$$

Las raíces de la resultante son: $\beta_1 = -4$, $\beta_2 = -\frac{3}{2}$. Para estos valores de la indeterminada y, los coeficientes superiores de los polinomios (16) no se anulan y, por esto, cada uno de ellos, junto con cierto valor de x, forma una solución del sistema dado de polinomios. Los polinomios

$$f(x, -4) = -4x^2 - 12x - 5,$$
$$g(x, -4) = -10x - 5$$

tienen una raíz común, $\alpha_1 = -\frac{1}{2}$. Los polinomios

$$f\left(x, -\frac{3}{2}\right) = -\frac{3}{2}x^2 - \frac{9}{2}x,$$
$$g\left(x, -\frac{3}{2}\right) = -5x$$

tienen una raíz común $\alpha_2 = 0$. Por lo tanto, el sistema dado de polinomios tiene dos soluciones:

$$\alpha_1 = -\frac{1}{2}, \quad \beta_1 = -4 \quad \text{y} \quad \alpha_2 = 0, \quad \beta_2 = -\frac{3}{2}.$$

2. Eliminar una indeterminada en el sistema de polinomios:

$$f(x, y) = 2x^3y - xy^2 + x + 5,$$
$$g(x, y) = x^2y^2 + 2xy^2 - 5y + 1.$$

Como estos dos polinomios son de grado 2 con respecto a la indeterminada y, mientras que uno de ellos es de grado 3 con respecto a la indeterminada x, conviene eliminar la y. Escribamos el sistema en la forma

$$\left.\begin{aligned} f(x, y) &= (-x)\cdot y^2 + (2x^3)\cdot y + (x+5), \\ g(x, y) &= (x^2+2x)\, y^2 - 5y + 1 \end{aligned}\right\} \tag{17}$$

y hallemos su resultante, aplicando la fórmula (12):

$$R_y(f, g) = [(-x)\cdot 1 - (x+5)(x^2+2x)]^2 -$$
$$- [(-x)(-5) - 2x^3(x^2+2x)][2x^3\cdot 1 - (x+5)(-5)] =$$
$$= 4x^8 + 8x^7 + 11x^6 + 84x^5 + 161x^4 + 154x^3 + 96x^2 - 125x.$$

Una de las raíces de la resultante es igual a 0. Sin embargo, para este valor de la indeterminada x, ambos coeficientes superiores de los polinomios (17) se convierten en cero, y, además, como fácilmente se observa, los polinomios $f(0, y)$ y $g(0, y)$ no tienen raíces comunes. No conocemos un método para hallar las otras raíces de la resultante. Solamente se puede afirmar que si las hallásemos (por ejemplo, en el campo de descomposición de $R_y(f, g)$), ninguna de ellas anularía a ambos coeficientes superiores de los polinomios (17) y, por esto, cada una de estas raíces, junto con cierto valor de y (con uno, e incluso con varios) formaría una solución del sistema dado de polinomios.

Existen métodos que permiten eliminar sucesivamente las indeterminadas en un sistema con un número arbitrario de polinomios e indeterminadas. Pero estos métodos son demasiado complicados, por lo cual, no pueden ser incluidos en nuestro curso.

Discriminante. *Por analogía con el problema que nos ha llevado* al concepto de resultante, se puede plantear la cuestión sobre las condiciones según las cuales un polinomio $f(x)$ de grado n del anillo $P[x]$ posee raíces múltiples. Sea

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \quad a_0 \neq 0,$$

y supongamos que en cierta ampliación del campo P este polinomio tiene las raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$. Evidentemente, *entre estas raíces hay iguales cuando, y sólo cuando, es igual a cero el producto*

$$\begin{aligned}\Delta = {} & (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1) \ldots (\alpha_n - \alpha_1) \times \\ & \times (\alpha_3 - \alpha_2)(\alpha_4 - \alpha_2) \ldots (\alpha_n - \alpha_2) \times \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & \times (\alpha_n - \alpha_{n-1}) = \prod_{n \geqslant i > j \geqslant 1} (\alpha_i - \alpha_j)\end{aligned}$$

o, lo que es lo mismo, si es igual a cero el producto

$$D = a_0^{2n-2} \prod_{n \geqslant i > j \geqslant 1} (\alpha_i - \alpha_j)^2,$$

denominado *discriminante* del polinomio $f(x)$.

A diferencia del producto Δ, que puede cambiar de signo al permutar las raíces, *el discriminante D es simétrico con respecto a* $\alpha_1, \alpha_2, \ldots, \alpha_n$ y, por esto, se puede expresar mediante los coeficientes del polinomio $f(x)$. Para hallar esta expresión, **suponiendo que la característica del campo P es igual a cero**, se puede utilizar la relación existente entre el discriminante del polinomio $f(x)$ y la resultante de este polinomio y su derivada. Es natural esperar la existencia de tal relación, pues, como ya sabemos por el § 49, un polinomio tiene raíces múltiples cuando, y sólo cuando, tiene raíces comunes con su derivada $f'(x)$, por lo cual, $D = 0$ cuando, y sólo cuando, $R(f, f') = 0$.

Por la fórmula (3) del presente párrafo, se tiene:

$$R(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

Derivando la igualdad

$$f(x) = a_0 \prod_{k=1}^{n} (x - \alpha_k),$$

resulta:

$$f'(x) = a_0 \sum_{k=1}^{n} \prod_{j \neq k} (x - \alpha_j).$$

Después de poner aquí α_i en lugar de x, todos los sumandos, a excepción del i-ésimo, se anulan, por lo cual,

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j),$$

de donde

$$R(f, f') = a_0^{n-1} \cdot a_0^n \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j).$$

En este producto, para cualesquiera i y j, $i > j$, figuran dos factores: $\alpha_i - \alpha_j$ y $\alpha_j - \alpha_i$. El producto de éstos es igual a $(-1) \cdot (\alpha_i - \alpha_j)^2$, y como existen $\frac{n(n-1)}{2}$ pares de índices i, j, que satisfacen a las desigualdades $n \geqslant i > j \geqslant 1$, resulta:

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} \prod_{n \geqslant i > j \geqslant 1} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_0 D.$$

Ejemplo. Hallemos el discriminante del trinomio cuadrático

$$f(x) = ax^2 + bx + c.$$

Como $f'(x) = 2ax + b$, se tiene.

$$R(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(-b^2 + 4ac).$$

En el caso considerado, $\frac{n(n-1)}{2} = 1$, por lo cual,

$$D = -a^{-1} R(f, f') = b^2 - 4ac.$$

Esto coincide con lo que en el álgebra escolar llaman ordinariamente discriminante de la ecuación cuadrática.

Otro método para hallar el discriminante consiste en lo siguiente. Formemos el determinante de Vandermonde de las potencias de las raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$. Como se demostró en el § 6,

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{n \geqslant i > j \geqslant 1} (\alpha_i - \alpha_j) = \Delta,$$

y por esto, el discriminante es igual al cuadrado de este determinante multiplicado por a_0^{2n-2}. Multiplicando este determinante por su traspuesto según la regla de multiplicación de las matrices y recordando las sumas de potencias, definidas en el párrafo precedente, resulta:

$$D = a_0^{2n-2} \begin{vmatrix} n & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix}, \tag{18}$$

donde s_k es la suma de las k-ésimas potencias de las raíces $\alpha_1, \alpha_2, \dots, \alpha_n$.

Ejemplo. Hallemos el discriminante del polinomio cúbico $f(x) = x^3 + ax^2 + bx + c$. Por (18), se tiene,

$$D = \begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}.$$

Como ya sabemos por el párrafo anterior,

$$s_1 = \sigma_1 = -a,$$
$$s_2 = \sigma_1^2 - 2\sigma_2 = a^2 - 2b,$$
$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = -a^3 + 3ab - 3c.$$

Aplicando la fórmula de Newton, y teniendo en cuenta que $\sigma_4 = 0$, hallamos también que

$$s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 = a^4 - 4a^2b + 4ac + 2b^2.$$

De aquí,

$$D = 3s_2s_4 + 2s_1s_2s_3 - s_2^3 - s_1^2s_4 - 3s_3^2 = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2. \tag{19}$$

En particular, siendo $a = 0$, o sea, para el polinomio cúbico incompleto, resulta:

$$D = -4b^3 - 27c^2,$$

lo cual está en correspondencia con lo que se dijo en el § 38.

§ 55. Segunda demostración del teorema fundamental del álgebra de los números complejos

La demostración del teorema fundamental, expuesta en el § 23, se efectuó de un modo no algebraico. Aquí queremos exponer otra demostración, en la que se emplea esencialmente el método algebraico. Así, pues, se aplicará el teorema fundamental de los polinomios simétricos (§ 52), y también el teorema de la existen-

cia de un campo de descomposición para cualquier polinomio (§ 48). Por otra parte, la parte no algebraica de la demostración será mínima y se reducirá a una afirmación muy sencilla.

Obsérvese primero que en el § 23 se demostró el lema del módulo del término superior de un polinomio. Suponiendo que los coeficientes del polinomio $f(x)$ son reales y poniendo $k = 1$, de este lema obtenemos el siguiente **corolario**:

Para valores reales de x suficientemente grandes en valor absoluto, el signo de un polinomio $f(x)$ de coeficientes reales coincide con el signo de su término superior.

De aquí se desprende el resultado siguiente:

Un polinomio de grado impar, de coeficientes reales, tiene por lo menos una raíz real.

En efecto, sea

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

donde todos los coeficientes son reales. Como n es impar, el término superior a_0x^n, para valores positivos y negativos de x, tiene diferentes signos, por lo cual, como se ha demostrado más arriba, para valores positivos y negativos de x, suficientemente grandes en valor absoluto, el polinomio $f(x)$ también tiene signos distintos. Por consiguiente, existen unos valores reales de x, por ejemplo, a y b, tales que

$$f(a) < 0, \quad f(b) > 0.$$

Sin embargo, por el curso de análisis se sabe, que el polinomio $f(x)$ (o sea, la función racional entera) es una función continua y, por esto, en virtud de una de las principales propiedades de las funciones continuas, para ciertos valores reales de x comprendidos entre a y b, $f(x)$ toma cualquier valor previamente asignado, intermedio entre $f(a)$ y $f(b)$. En particular, existe un α, comprendido entre a y b, tal que $f(\alpha) = 0$.

Basándonos en este resultado, demostraremos ahora la proposición siguiente:

Todo polinomio de coeficientes reales, de un grado arbitrario, tiene por lo menos una raíz compleja.

En efecto, sea dado un polinomio $f(x)$ de coeficientes reales y de grado $n = 2^kq$, donde q es un número impar. Como el caso $k = 0$ ya se ha estudiado antes, supondremos que $k > 0$, o sea, que n es un número par, y haremos la demostración por inducción sobre k, suponiendo que nuestra afirmación ya está demostrada para **todos** los polinomios de coeficientes reales, cuyos grados son divisibles por 2^{k-1}, pero no son divisibles por 2^k*.

* Por consiguiente, estos grados pueden ser incluso mayores que n.

Sea P un campo de descomposición del polinomio $f(x)$ sobre el campo de los números complejos (véase el § 49) y sean $\alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de $f(x)$ contenidas en el campo P. Tomemos un número real arbitrario c y consideremos los elementos del campo P que son de la forma

$$\beta_{ij} = \alpha_i \alpha_j + c(\alpha_i + \alpha_j), \quad i < j. \tag{1}$$

Evidentemente, el número de elementos β_{ij} es igual a

$$\frac{n(n-1)}{2} = \frac{2^k q(2^k q - 1)}{2} = 2^{k-1} q(2^k q - 1) = 2^{k-1} q', \tag{2}$$

donde q' es un número impar.

Formemos ahora un polinomio $g(x)$ del anillo $P[x]$ que tenga por raíces todos estos elementos β_{ij} y sólo éstos:

$$g(x) = \prod_{i,j,\, i<j} (x - \beta_{ij}).$$

Los coeficientes de este polinomio son polinomios simétricos elementales en β_{ij}. Por consiguiente, en virtud de (1), son polinomios en $\alpha_1, \alpha_2, \ldots, \alpha_n$ de coeficientes reales (puesto que el número c es real) y, además, son simétricos. En efecto, la trasposición de cualesquiera dos α, por ejemplo, de α_k y α_l, implica solamente una permutación en el sistema de todas las β_{ij}; cualquiera β_{kj}, donde j es distinto de k y de l, se convierte en β_{lj} y viceversa, mientras que β_{kl} y todas las β_{ij}, para i y j diferentes de k y l, se quedan *en el sitio*. Mas, *los coeficientes del polinomio* $g(x)$ *no varían al* permutar sus raíces.

En virtud del teorema fundamental de los polinomios simétricos, de aquí se deduce que los coeficientes del polinomio $g(x)$ son polinomios (de coeficientes reales) en los coeficientes del polinomio dado $f(x)$ y, por esto, ellos mismos son números reales. El grado de este polinomio, igual al número de las raíces β_{ij}, en virtud de (2), es divisible por 2^{k-1}, pero no lo es por 2^k. Por esto, por la hipótesis de la inducción, al menos una de las raíces β_{ij} del *polinomio* $g(x)$ *tiene que ser un número complejo.*

Por lo tanto, cualquiera que sea el número real elegido c, se puede indicar un par de índices i, j, donde $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, de modo que el elemento $\alpha_i \alpha_j + c(\alpha_i + \alpha_j)$ sea un número complejo; recordemos, que el campo P contiene al campo de los números complejos como subcampo. Se entiende que, por lo general, para otra elección del número c, a éste le va a corresponder en el sentido indicado otro par de índices. Sin embargo, existe una infinidad de números reales c distintos, mientras que nosotros dis*ponemos solamente de un número finito de pares* i, j *distintos.* De aquí se deduce, que se pueden elegir dos números reales distin-

tos c_1 y c_2, $c_1 \neq c_2$, tales, que a éstos les corresponde **un mismo par** de índices, para los cuales, los números

$$\left.\begin{aligned} \alpha_i\alpha_j + c_1(\alpha_i + \alpha_j) &= a, \\ \alpha_i\alpha_j + c_2(\alpha_i + \alpha_j) &= b \end{aligned}\right\} \tag{3}$$

son complejos.

De la igualdad (3), resulta:

$$(c_1 - c_2)(\alpha_i + \alpha_j) = a - b,$$

de donde se deduce que

$$\alpha_i + \alpha_j = \frac{a-b}{c_1 - c_2},$$

o sea, esta suma es un número complejo. De aquí, y si se quiere de la primera de las igualdades (3), se deduce que el producto $\alpha_i\alpha_j$ también es un número complejo. Por lo tanto, resulta que los elementos α_i y α_j son raíces de la ecuación cuadrática

$$x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j = 0,$$

de coeficientes complejos, por lo cual, como esto se deduce de la fórmula para la resolución de la ecuación cuadrática con coeficientes complejos, obtenida en el § 38, ellos mismos tienen que ser números complejos. Por consiguiente, entre las raíces del polinomio $f(x)$ hemos hallado incluso dos complejas, con lo cual queda demostrada nuestra afirmación.

Para demostrar por completo el teorema fundamental, queda por considerar el caso de un polinomio de coeficientes complejos arbitrarios. Sea

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

un polinomio de este tipo. Consideremos el polinomio

$$\bar{f}(x) = \bar{a}_0x^n + \bar{a}_1x^{n-1} + \ldots + \bar{a}_n,$$

obtenido de $f(x)$ por sustitución de todos los coeficientes por sus conjugados, y examinemos el producto

$$F(x) = f(x)\bar{f}(x) = b_0x^{2n} + b_1x^{2n-1} + \ldots + b_kx^{2n-k} + \ldots + b_{2n},$$

donde, evidentemente,

$$b_k = \sum_{i+j=k} a_i\bar{a}_j, \quad k = 0, 1, 2, \ldots, 2n.$$

Basándose en las propiedades de los números complejos conjugados, conocidas por el § 18, obtenemos que

$$\bar{b}_k = \sum_{i+j=k} \bar{a}_i a_j = b_k,$$

o sea, todos los coeficientes del polinomio $F(x)$ son números reales.

Como se ha demostrado más arriba, de aquí se deduce que el polinomio $F(x)$ tiene por lo menos una raíz compleja β,

$$F(\beta) = f(\beta)\,\bar{f}(\beta) = 0,$$

o sea, o $f(\beta) = 0$, o bien, $\bar{f}(\beta) = 0$. En el primer caso, el teorema queda demostrado. Si es que se cumple el segundo caso, o sea, si

$$\bar{a}_0\beta^n + \bar{a}_1\beta^{n-1} + \ldots + \bar{a}_n = 0,$$

entonces, sustituyendo todos los números que figuran aquí por sus conjugados (que, como ya sabemos, no infringe la igualdad), obtenemos:

$$f(\bar{\beta}) = a_0\bar{\beta}^n + a_1\bar{\beta}^{n-1} + \ldots + a_n = 0,$$

o sea, el número complejo $\bar{\beta}$ es raíz de $f(x)$. La demostración del teorema fundamental se ha terminado.