EL ORIGEN DE LA TEORIA DE GRUPOS. EL TEOREMA DE LAGRANGE (1771)

por

Richard ROTH

En la actualidad, la teoría de grupos se estudia de una manera abstracta y sistemática; es decir, primero se da la definición abstracta de grupo, luego se ilustra esta definición, con unos ejemplos y se sigue con la demostración de varios Teoremas. Quizás el primer teorema importante que se demuestra es el llamado por la mayoría de los autores Teorema de Lagrange:

TEOREMA (Lagrange). Si H es un subgrupo de un grupo finito G, entonces el orden de H es divisor del orden de G.

La demostración consiste en construir una partición del conjunto G en subconjuntos de la forma $H_g = \{ hg \mid h \in H \}$ es decir, cogrupos. Si hay r cogrupos entonces $o(G) = r\, o(H)$ (donde $o(T)$ indica el número de elementos del conjunto T). r se llama el índice de H en G.

Generalmente se dice que la teoría de grupos se originó con los trabajos de Galois y Cauchy en el período 1825 - 1850. Galois fue el primero que usó el término <<grupo>>, en el desarrollo de su teoría de ecuaciones y cuerpos, (que en la actualidad conocemos con el nombre de <<Teoría de Galois>>). En los artículos de Cauchy, durante el período 1840 - 1850 empieza el estudio de los grupos en sí, aunque se trataba aún de grupos de permutaciones. Sin embargo, el teorema de Lagrange apareció por primera vez, en una forma limitada y difícil de reconocer en el artículo <<Reflexiones sur La Resolution des Equations Algebriques>> de Joseph-Louis Lagrange (1736-1813) publicado en dos partes por la academia de Berlín en los años 1770-1771.

En esta obra de 200 páginas no se mencionan los grupos ni los cuerpos; sin embargo, fue una de las bases más importantes para el desarrollo del álgebra moderna en el siglo XIX. Los matemáticos que vinie ron después, como Galois y Abel, estudiaron mucho esta obra para sus propias investigaciones.

El tema de la obra es el problema de buscar soluciones generales de las ecuaciones. El gran problema del algebra de aquella época era hallar una solución general para ecuaciones de quinto grado (y más alto) por medio de radicales. Por ejemplo, la ecuación general de segundo grado $ax^2 + 6x + c = 0$ tiene como solución los números $(-6 + \sqrt{6^2-4ac})/2a$. Las ecuaciones de tercer y cuarto grado fueron resueltas por los matemáticos italianos ya en el siglo 16 y en la promera parte del artículo de Lagrange se estudian los diferentes métodos conocidos para resolver las ecuaciones de tercer y cuarto grado. Lagrange busca los principios básicos (<< ... la vraie metaphysique>>) de estos métodos y guarda la esperanza de usarlos para encontrar soluciones semejantes por radicales de las ecuaciones de mayor grado (posteriormente a comienzos del siglo XIX, Ruffini y Abel basándose en estas ideas de Lagrange demostraron que eso era imposible.)

En general uno quiere sustituir una ecuación de alto grado por otra que sea de menor grado. Lo que Lagrange halla es que se trata siempre de la existencia de <<funciones>> resolventes de las raices y que las funciones mismas son raices de ecuaciones de grados más bajos.

Conviene exhibir un ejemplo y este no es más que uno de los muchos que se discuten en el artículo. Tomemos la ecuación general de cuarto grado (se verifica que se puede omitir el término en x^3) :

(1) $X^4 + n X^2 + p X + q = 0$

Siguiendo el método de Cardano, sea << y >> otro número desconocido. Podemos reemplazar la ecuación (1) por

(2) $X^4 + 2y X + y^2 = n X^2 - pX - q + 2y X^2 + y^2$

$= (2y - n) X^2 - pX + (y^2 - q)$

Si escogemos <<y>> de la manera correcta, la ecuación (2) se convertirá en una de la forma

$$(3) \qquad (X^2 + y)^2 = (A\,x + B)^2$$

donde A, B dependen de y, n, p, q.

De (3) se obtiene entonces la ecuación de segundo grado

$$X^2 - AX + y - B = 0.$$

La elección de << y >> debe hacerse de tal manera que

$$(4) \qquad y^3 - \frac{n}{2}\, y^2 - qy + \frac{4nq - p^2}{8} = 0$$

y esta es una ecuación de tercer grado.

Supongamos que a, b, c, d son las cuatro raices de la ecuación original (1). Entonces Lagrange muestra que una raiz de la ecuación (3) es de la forma, $(ab + cd)/2$. Buscando la razón de por qué es esta expresión raiz de una ecuación de grado tres, observa que las cuatro raices deben entrar de una manera simétrica y si se permutan de todas las maneras posibles (24 permutaciones) existen exactamente 3 valores distintos:

$$\frac{ab + cd}{2}, \quad \frac{ac + bd}{2}, \quad \frac{ad + bc}{2}$$

(Nótese, por ejemplo que $\frac{ab + cd}{2} = \frac{ba + dc}{2} = \frac{cd + ab}{2}$, etc.)

Concluye pues que, $(ab + cd)/2$ debe ser raiz de una ecuación de tercer grado con coeficientes que dependen de n, p, q. (La demostración de Lagrange no parece en la actualidad muy rigurosa; pero usando teoremas de la teoría de Galois se puede demostrar que el resultado es correcto.)

Entonces, en general la ecuación de grado u

$$X^u + m\,X^{u-1} + nX^{u-2} + \dots = 0$$

sean $X', X'', \dots X^{(u)}$ las raices. El problema es buscar <<funciones>> (funciones racionales) de las raices que sean ellas mismas raices de ecuaciones de grado más bajo. Sea $f(X', X'', \dots, X^{(u)})$ una función de las raices. Operamos en la función permutando los símbolos $X', X'', \dots X^{(u)}$ de u! maneras. Si $f(x'x'', \dots x^{(u)}), f(x'', x', \dots, x^{(u)}), \dots$

$f\,(x', x'', \ldots, x^{(u-1)})$ son los $u!$ resultados de estas operaciones, entonces el polinomio

$$\theta = (t - f(x', x'', \ldots, x^{(u)})\,(t - f(x'', x', \ldots, x^{(u)}))\ldots(t-f(x', x'', \ldots, x^{(u-1)}))$$

es de grado $u!$. Si f queda fija bajo ciertas permutaciones y

$$\theta = (t-f\,(x', \ldots))\,(t-f(x'', \ldots)) \ldots$$

donde solo aparecen las funciones diferentes entonces θ es un polinomio de grado r = número de funciones diferentes. Con referencia a esto, en la sección 99 de la obra se puede leer lo siguiente: << 2o, que ce degré sera toujours egal au nombre 1.2.3... u (u étant le degré de l'equeation donnde) ov a un Sous multiple de ce nombre >>. <<ce degré >> se refiere a r, el grado de θ. De manera que, el <<Teorema de Lagrange>> en su forma primitiva se puede enunciar de la manera siguiente:

Si $f(x', x'', \ldots, x^{(u)})$ es una función de u variables y si bajo las $u!$ posibles permutaciones de las variables aparecen r <<funciones>> distintas, entonces r es divisor de $u!$.

Para ver mejor la relación de este teorema con el teorema que conocemos hoy, es fácil demostrar el siguiente lema : Si la función $f(x', x'', \ldots, x^{(u)})$ se convierte en r funciones distintas cuando operamos con las permutaciones de S_u entonces $r = [S_u : H]$, donde H es el subgrupo de permutaciones que dejan fija f. Según esto, el teorema de Lagrange en su forma original equivale a decir que el índice del subgrupo H de S_u es divisor del orden de S_u.

La demostración comienza en la sección 97. El demuestra que si

$f\,(x', x'', x''', x^{IV}, \ldots) = f(x^{IV}, x''', x', x'', \ldots)$ entonces $f(x'', x''', x', x^{IV}, \ldots) = f(x''', x', x^{IV}, x'', \ldots)$ (permutando siempre en orden ciclico las tres primeras variables.) De esto concluye que las funciones se distribuyen en pares iguales; esta afirmación no es correcta pues con una permutación de orden 3, se dividen en grupos de tres. Sin embargo, la idea de la demostración es completamente clara :

Si operamos con todas las permutaciones posibles y si f se encuentra S veces en la lista, entonces cada otra función diferente ocurre s veces en la lista. Así pues, el número de funciones diferentes (o el grado de θ) tiene que ser $u!/s$.

De manera que, el teorema que llamamos teorema de Lagrange fué enumerado por él en forma restringida y en un lenguaje completamente diferente al que usamos hoy. Sin embargo, pasando los años, con el desarrollo gradual de la idea de grupo se mejoró y clarificó el teorema. La idea de grupo de permutaciones fue formulada mas precisamente por Galois 50 años después; pero las semillas del concepto se encuentran en este trabajo de Lagrange, no solo en las secciones discutidas, sino en otros apartes del artículo.

B I B L I O G R A F I A

Lagrange, Joseph - Louis; Reflexions sur la Resolution Algebrique des Equations, Nouveaux Memories de lAcademie Royale des Sciences et Belles Lettres de Berlin, 1770 - 1771.

Mathematical Departament
Colorado University

(Recibido en Julio de 1.969)