

$$y_2 = \omega^2 u + \omega v = \omega^2 \sqrt[3]{\frac{q}{2} + \sqrt{R}} + \omega \sqrt[3]{\frac{q}{2} - \sqrt{R}}$$

$$y_3 = \omega u + \omega^2 v = \omega \sqrt[3]{\frac{q}{2} + \sqrt{R}} + \omega^2 \sqrt[3]{\frac{q}{2} - \sqrt{R}}$$

Estas fórmulas son conocidas como las fórmulas de Cardano.

Para encontrar las raíces x_1, x_2, x_3 de la cúbica general, solo tenemos que sumar $\frac{b}{3}$ a los y_i encontrados; por tanto en las expresiones para x_i no habrá más radicales que aquellos contenidos en las expresiones para y_i .

Aquí viene el descubrimiento de Lagrange:

Lagrange observó que para el caso de la ecuación cuadrática:

$$x^2 - c_1 x + c_2 = 0,$$

las raíces x_1, x_2 , siendo $x_1 = \frac{c_1 + \sqrt{c_1^2 - 4c_2}}{2}$, $x_2 = \frac{c_1 - \sqrt{c_1^2 - 4c_2}}{2}$

eran tales que: $c_1 = x_1 + x_2$,

$$c_2 = x_1 \cdot x_2, \text{ y}$$

$$\sqrt{c_1^2 - 4c_2} = x_1 - x_2.$$

Lagrange investiga estas relaciones para la ecuación cúbica ($x^3 - bx^2 + cx - d = 0$)

encontrando que: $b = x_1 + x_2 + x_3$

$$c = x_1 x_2 + x_1 x_3 + x_2 x_3$$

$$d = x_1 x_2 x_3$$

(Intercambiando las letras x_1, x_2, x_3 en todas las formas posibles no se altera el valor de los coeficientes).

$$\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \frac{1}{3} (x_1 + \omega x_2 + \omega^2 x_3)$$

$$\sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \frac{1}{3} (x_1 + \omega x_3 + \omega^2 x_2)$$

$$\sqrt{\frac{q^2}{4} + \frac{43}{27}} = \frac{\sqrt{-3}}{18} (x_1 - x_2)(x_1 - x_3)(x_2 - x_3),$$

y finalmente las 6 raíces de la ecuación (5) de grado 6, pueden expresarse como funciones de las mismas raíces x_1, x_2 y x_3 de la cúbica:

$$u = \frac{1}{3} (x_1 + \omega x_2 + \omega^2 x_3), \quad v = \frac{1}{3} (x_1 + \omega x_3 + \omega^2 x_2)$$

$$\omega u = \frac{1}{3} (x_3 + \omega x_1 + \omega^2 x_2), \quad \omega v = \frac{1}{3} (x_2 + \omega x_1 + \omega^2 x_3)$$

$$\omega^2 u = \frac{1}{3} (x_2 + \omega x_3 + \omega^2 x_1), \quad \omega^2 v = \frac{1}{3} (x_3 + \omega x_2 + \omega^2 x_1)$$

Examinando estas expresiones observa que todas pueden obtenerse a partir de una de ellas permutando en todas las formas posibles las letras x_1, x_2 y x_3 .

En cambio al aplicar al radical:

$$\sqrt{R} = \frac{\sqrt{-3}}{18} (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

todas las $3! = 6$ permutaciones de x_1, x_2 y x_3 obtenemos justamente los valores \sqrt{R} y $-\sqrt{R}$.

Lagrange observa que las 6 permutaciones de los x_i se dividen en dos conjuntos: en uno las que dejan invariante a \sqrt{R} , y en otros las que envían \sqrt{R} en $-\sqrt{R}$.

Lagrange investigó también estas relaciones en la ecuación de cuarto grado encontrando relaciones semejantes.

CAPITULO II : GRUPOS

INTRODUCCION. La noción de grupo está estrechamente ligada al nombre del genio francés Evariste Galois (1811-1832). Se considera a Evariste Galois como el iniciador de la teoría de grupos. Galois asoció a cada ecuación algebraica un conjunto de permutaciones de sus raíces al que llamó Grupo; de esta forma realizó importantes descubrimientos tanto en la teoría de grupos como en la de ecuaciones. Su teoría perfeccionó las ideas de Joseph Louis Lagrange (1736-1813), Paolo Ruffini (1765-1822) y Niels Henrik Abel (1802-1829) en relación con la resolución de ecuaciones algebraicas por radicales.

La teoría de grupos se llamó "Teoría de Sustituciones" hasta 1854, cuando el matemático inglés Arthur Cayley (1821-1895) introdujo el concepto de grupo abstracto. En 1872 Felix Klein (1849-1925) puso en evidencia el papel central de los grupos en el estudio de la geometría.

- REFERENCIAS :
- (1) LA EVOLUCION del algebra. IN: BOURBAKI, Nicolas. Elementos de historia de las matemáticas. 2ed. Madrid, Alianza Editorial, 1976. PP. 74-84.
 - (2) CLARK, A. Elementos de algebra abstracta. Madrid, Alhambra, 1974. PP. 1-11.
 - (3) LA TEORIA de grupos. Galois. IN: BABINI, José. Historia de las ideas modernas en matemática. 2ed. Washington, Unión Panamericana, O.E.A., 1974. PP. 25-29.

DEFINICION. Sea G un conjunto no vacío (finito o infinito) y $*$ una ley de composición interna binaria en G . El par $(G, *)$ se dice un grupo si $*$ satisface:

G1) PROPIEDAD ASOCIATIVA.- Si a, b y c son elementos cualesquiera de G , $(a*b)*c = a*(b*c)$.

G2) EXISTENCIA DE ELEMENTO NEUTRO.- Existe un elemento $e \in G$ tal que para todo $a \in G$, $a*e = a = e*a$.

(e se dice un elemento neutro o módulo o identidad para $*$ en G).

G3) EXISTENCIA DE INVERSO DE CADA ELEMENTO.- Para cada elemento $a \in G$, existe un elemento $a' \in G$ tal que $a*a' = e = a'*a$.

(a' se dice un inverso, recíproco, opuesto o simétrico de a con respecto a $*$).

Si $(G, *)$ es un grupo, diremos también que G es un grupo con respecto a la operación $*$. Cuando $*$ se sobreentienda se puede hablar del grupo G en vez de $(G, *)$; también llamaremos elementos del grupo $(G, *)$ a los elementos del conjunto G . Así por ejemplo diremos, el elemento neutro de G en vez del elemento neutro de $(G, *)$.

Las condiciones G1, G2 y G3 reciben el nombre de Axiomas de Grupo.

Si un grupo $(G, *)$ además de satisfacer sus tres axiomas de definición satisface la condición:

PROPIEDAD CONMUTATIVA.- $a*b = b*a$ para todo par de elementos a y b de G , entonces el grupo se dice ABELIANO o conmutativo.

Si existen un par de elementos $a, b \in G$ tales que $a*b \neq b*a$ decimos

que G es no-conmutativo o no abeliano. Cuando $a*b = b*a$ decimos que los elementos a y b conmutan o permutan.

El nombre ABELIANO es en honor del matemático Noruego, Niels Henrik Abel (1802-1829). Abel en 1824 mostró la imposibilidad de resolver, en general, ecuaciones de quinto grado por radicales (es decir valiéndose únicamente de las operaciones aritméticas elementales (suma, resta, multiplicación, división) y de la extracción de raíces). En sus investigaciones posteriores se interesó en la solución de ecuaciones por radicales para aquellas ecuaciones a las que se les pueda asociar un grupo conmutativo de permutaciones de sus raíces. Por eso, el nombre ABELIANO es uno de los apropiados para los grupos conmutativos.

DEFINICION.- Se dice que un grupo $(G, *)$ es finito, si el conjunto G tiene un número finito de elementos; en caso contrario se dice que es un grupo infinito. Si un grupo $(G, *)$ es finito y G tiene exactamente n elementos decimos que el orden de G es n y escribimos $|G| = n$ ó $O(G) = n$. Si G es infinito escribimos $|G| = \infty$.

Los axiomas G_2 y G_3 hablan de la existencia de un módulo y un inverso, en la proposición siguiente veremos que estos elementos son únicos en un grupo.

PROPOSICION 1.- Si $(G, *)$ es un grupo, entonces existe un único elemento $e \in G$ tal que $e*a = a = a*e$ para todo $a \in G$.

De la misma manera, para cada $a \in G$ existe un único elemento $a' \in G$ tal que $a'*a = e = a*a'$.

Demost. Sean $e_1, e_2 \in G$ ambos modulos, entonces:

$$e_1 = e_1 * e_2 = e_2$$

\uparrow porque e_2 es modulo \uparrow porque e_1 es modulo.

Luego la identidad en un grupo es única, la notaremos siempre e .

Sea ahora $a \in G$ y supongamos que $a', a'' \in G$ son inversos de a .

Entonces:

$$a'' = a'' * e = a'' * (a * a') = (a'' * a) * a' = e * a' = a'$$

\uparrow porque $a * a' = e$ \uparrow porque $*$ es asociativa \uparrow porque $a'' * a = e$

Luego el inverso de a es único, lo notaremos a^{-1} .

Si $(G, *)$ es un grupo finito, con pocos elementos, digamos que

$G = \{a_1 = e, a_2, \dots, a_n\}$ ($|G| = n$), se acostumbra describir el grupo mediante una tabla de composición, llamada tabla de Cayley del grupo, de la siguiente forma:

$*$	$e = a_1$	a_2	\dots	a_j	\dots	a_n	
$e = a_1$	e	a_2	\dots	a_j	\dots	a_n	← FILA 1
a_2	a_2	$a_2 * a_2$	\dots	$a_2 * a_j$	\dots	$a_2 * a_n$	← FILA 2
\dots	\dots	\dots	\dots	\dots	\dots	\dots	
a_i	a_i	$a_i * a_2$	\dots	$a_i * a_j$	\dots	$a_i * a_n$	← FILA i
\dots	\dots	\dots	\dots	\dots	\dots	\dots	
a_n	a_n	$a_n * a_2$	\dots	$a_n * a_j$	\dots	$a_n * a_n$	← FILA n .
	\uparrow	\uparrow		\uparrow		\uparrow	
	COLUMNA 1	COLUMNA 2		COLUMNA j		COLUMNA n	

En la intersección de la fila i y la columna j , de acuerdo a como está marcada la tabla, es decir en la posición (i, j) está el elemento del grupo $a_i * a_j$.

EJEMPLOS

- 1.- El conjunto \mathbb{Z} de los números enteros es un grupo conmutativo con respecto a la suma usual de números, es decir $(\mathbb{Z}, +)$ es un grupo conmutativo. En efecto, $+$ es ley de composición interna binaria en \mathbb{Z} , que es asociativa y conmutativa; hay un elemento neutro 0 para $+$ en \mathbb{Z} ; y cada elemento $a \in \mathbb{Z}$ tiene su opuesto $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$. En cambio \mathbb{Z} no es un grupo con respecto a la multiplicación usual entre números, o sea que (\mathbb{Z}, \cdot) no es un grupo, ya que no todo elemento de \mathbb{Z} tiene inverso respecto a la multiplicación. En efecto, por ejemplo, $4 \in \mathbb{Z}$ pero no existe $b \in \mathbb{Z}$ tal que $4b = 1$; observe que 1 es módulo para el producto y que los únicos elementos de \mathbb{Z} que tienen inverso respecto al producto son 1 y -1 .
- 2.- El conjunto \mathbb{Q} de los números racionales es un grupo con respecto a la suma, o sea $(\mathbb{Q}, +)$ es un grupo.
- 3.- El conjunto $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ es un grupo con respecto a la multiplicación, o sea (\mathbb{Q}^*, \cdot) es un grupo; también lo son (\mathbb{R}^*, \cdot) y (\mathbb{C}^*, \cdot) . En cambio no son grupos respecto a la multiplicación, ni el conjunto \mathbb{Q} de los números racionales, ni el conjunto \mathbb{R} de los números reales, ni el conjunto \mathbb{C} de los números complejos. El elemento 0 no tiene inverso multiplicativo, $0 \in \mathbb{Q}$, $0 \in \mathbb{R}$, $0 \in \mathbb{C}$.

4.- Consideremos el conjunto $\mathbb{Q} - \{-1\}$ y la operación $*$ definida en $\mathbb{Q} - \{-1\}$ así:
 $a * b = a + b + ab$, donde $+$ y \cdot son la suma y el producto usuales
 entre números racionales. Veamos si el par $(\mathbb{Q} - \{-1\}, *)$ es un grupo.

Primero que todo veamos si $*$ es ley de composición interna en $\mathbb{Q} - \{-1\}$; para esto basta ver que si $a, b \in \mathbb{Q} - \{-1\}$, entonces $a * b \in \mathbb{Q} - \{-1\}$ (ya que la unicidad de la imagen es consecuencia de que $+$ y \cdot son leyes de composición internas en \mathbb{Q}).

$$\begin{aligned} \text{Observemos que: } a * b = -1 &\iff a + b + ab = -1 \\ &\iff a + 1 + b + ab = 0 \\ &\iff (a + 1) + b(a + 1) = 0 \\ &\iff (a + 1)(b + 1) = 0 \\ &\iff a = -1 \text{ o } b = -1 \end{aligned}$$

Pues si $a, b \in \mathbb{Q} - \{-1\}$, entonces $a, b \in \mathbb{Q}$ y $a \neq -1$ y $b \neq -1$, entonces $a * b \neq -1$, $a * b \in \mathbb{Q}$, entonces $a * b \in \mathbb{Q} - \{-1\}$, así que $*$ es operación binaria en $\mathbb{Q} - \{-1\}$.

G₁) ASOCIATIVIDAD.- Sean $a, b, c \in \mathbb{Q} - \{-1\}$. Entonces:

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \\ &= a + b + c + ab + ac + bc + abc. \\ a * (b * c) &= a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \\ &= a + b + c + ab + ac + bc + abc. \end{aligned}$$

Si se comparan los resultados de $(a * b) * c$ y $a * (b * c)$ vemos que son iguales, así que $*$ es asociativa.

G2) EXISTENCIA DE ELEMENTO NEUTRO... Sea $a \in \mathbb{Q} - \{-1\}$, veamos si existe $e \in \mathbb{Q} - \{-1\}$ tal que $a * e = a = e * a$.

$$a * e = a \iff a + e + ae = a$$

$$\iff e(1+a) = 0$$

$$\iff e = 0, \text{ porque } 1+a \neq 0.$$

Luego $e=0$ es la única solución en $\mathbb{Q} - \{-1\}$ de la ecuación $a * e = a$.

Veamos que $e=0$ también satisface $e * a = a$.

$$0 * a = 0 + a + 0a = a.$$

Luego $e=0 \in \mathbb{Q} - \{-1\}$ es el elemento neutro para $*$.

G3) EXISTENCIA DE INVERSO DE CADA ELEMENTO... Sea $a \in \mathbb{Q} - \{-1\}$. Veamos si existe $a' \in \mathbb{Q} - \{-1\}$ tal que $a * a' = 0 = a' * a$.

Para esto, resolvamos para a' la ecuación $a * a' = 0$.

$$a * a' = 0 \iff a + a' + aa' = 0$$

$$\iff a + a'(1+a) = 0$$

$$\iff a'(1+a) = -a$$

$$\iff a' = -\frac{a}{1+a}, \text{ porque } 1+a \neq 0.$$

Luego $a' = -\frac{a}{1+a}$ es solución de $a * a' = 0$, pero no sabemos si

$-\frac{a}{1+a} \in \mathbb{Q} - \{-1\}$. Para esto, observemos que:

$$-\frac{a}{1+a} = -1 \iff \frac{a}{1+a} = 1$$

$$\iff a = 1+a$$

$$\iff 0 = 1.$$

Como $1 \neq 0$, entonces $-\frac{a}{1+a} \neq -1$ cualquiera sea $a \in \mathbb{Q} - \{-1\}$, y ha-

bemos que $-\frac{a}{1+a} \in \mathbb{Q}$, así que $a' = -\frac{a}{1+a}$ es solución de $a * a' = 0$,

y está en $\mathbb{Q} - \{-1\}$.