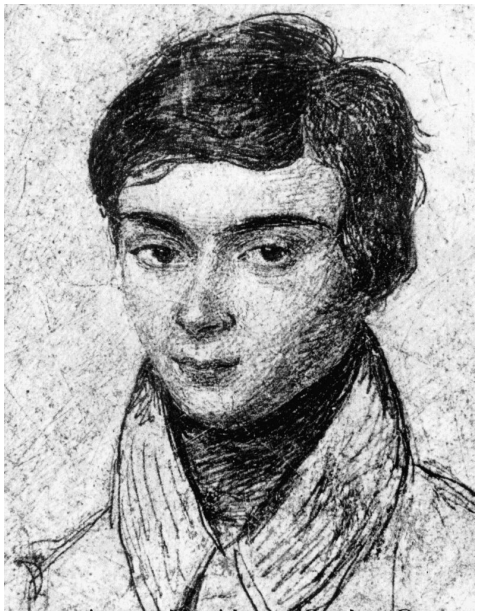
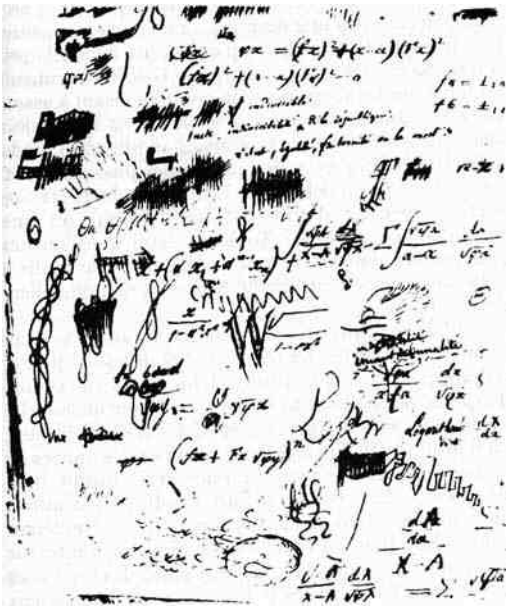
Galois y los polinomios

TIMM, 25 de octubre de 2025





Este es Évariste Galois y eso de ahí sus apuntes de mates.

Galois nació el 25 de octubre de 1811 en Bourg-la-Reine, a pocos kilómetros de París. Hoy cumpliría 214 años.

Hasta los 12 años fue educado por su madre en casa, igual que su hermana Nathalie y su hermano Alfred. Después entró en el Liceu Louis-le-Grand de París. Al principio no parecía un estudiante brillante, aunque obtuvo algunos premios en latín y griego, pues su madre le había proporcionado una sólida formación en lenguas clásicas. El tercer año suspendió un trabajo de retórica y tuvo que repetir curso. Fue entonces cuando descubrió el amplio mundo de las matemáticas, gracias al profesor Vernier, que le instó a leer obras de los mejores matemáticos de la época, como los Elementos de Geometría de Legendre y las memorias de Lagrange sobre cálculo de funciones y resolución algebraica de ecuaciones. Galois tenía entonces 15 años.

Si os apetece echar un vistazo a las lecturas de Galois, podéis encontrar aquí la menoria de Lagrange sobre resolución de ecuaciones algebraicas y aquí el libro de Legendre. Pero si os ponéis a leer estas cosas, tened cuidadito y no descuidéis otras materias, no os vaya a pasar como a Galois, que no tenía contentos a sus profesores de humanidades. Tampoco convencía del todo a los de mates porque era algo desorganizado... Si queréis saber algo más sobre la vida y la obra de Galois, está bien este artículo.

1 Expresiones por radicales de números algebraicos

A Galois le interesó especialmente el trabajo de Lagrange sobre resolución de ecuaciones algebraicas por radicales. Como seguramente sabéis, las ecuaciones algebraicas (en una variable) se pueden expresar en la forma

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0,$$

donde x es una variable o indeterminada y los a_i son números a los que llamamos coeficientes del polinomio $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$. Cuando a_n es distinto de cero, decimos que el grado del polinomio (y de la ecuación) es n.

Todos conocemos una fórmula general para la solución de la ecuación $ax^2 + bx + c = 0$ de grado 2:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Decimos que es una fórmula general porque es válida para cualesquiera valores de los coeficientes a, b, c. También decimos, aunque igual esto lo usáis menos, que es una expresión por radicales de las raíces del polinomio (o de las soluciones de la ecuación) porque se realiza operando, a partir de los coeficientes del polinomio, con sumas, restas, multiplicaciones, divisiones y raíces (en este caso raíces cuadradas, aunque en las expresiones por radicales se admiten raíces de cualquier orden).

Esta solución se conoce, al menos, desde tiempos de Al-Juarizmi, allá por el siglo VIII. En el siglo XVI, Tartaglia, Cardano y Ferrari encontraron fórmulas generales para las ecuaciones de grados 3 y 4, también expresadas por radicales. Está muy bien este libro para aprender más sobre esta historia. Del mismo autor tenéis un texto más cortito sobre la ecuación cúbica aquí.

Lagrange, en el siglo XVIII, estudió con detalle los desarrollos de las fórmulas generales de las ecuaciones de grados 2, 3 y 4 con la intención de descubrir patrones que le permitieran generalizar la solución a grados mayores. Y sí que encontró patrones, pero en lugar de ayudarle a resolver la ecuación quíntica, le hicieron sospechar que no podía existir una fórmula general que se expresara por radicales. Un década después de la muerte de Lagrange, cuando Galois tenía 13 años, Abel, un joven matemático noruego, demostró que, efectivamente, no existen tales fórmulas generales para ecuaciones de grado mayor que 4.

Galois, que también leyó ese trabajo de Abel (lo enlazamos aquí por curiosidad, pero es aún más difícil de entender que los anteriores, especialmente si no se ha estudiado bien la obra de Lagrange y de Gauss), aprendió rápidamente de los patrones, técnicas, herramientas e ideas de Lagrange y Abel y se afanó en el estudio de la resolubilidad por radicales de las ecuaciones de cualquier grado, pues el hecho de que no haya una fórmula general no implica que no puedan resolverse por radicales algunas ecuaciones concretas de grado mayor que 4. Comprobadlo resolviendo el siguiente ejercicio:

Ejercicio 1 *A las raíces de un polinomio con coeficientes racionales se les llama números algebraicos. Prueba que* $\sqrt{2} + \sqrt[3]{2}$ *es un número algebraico.*

Seguramente, en el ejercicio anterior, habéis encontrado un polinomio de grado 6 que, además, se puede comprobar (aunque igual es un poco pesado) que es irreducible, es decir, que no se puede escribir como el producto de dos polinomios no constantes. Con un poco más de esfuerzo también se puede ver que sus otras 5 raíces son

$$-\sqrt{2}+\sqrt[3]{2},\ \sqrt{2}+\zeta_3\sqrt[3]{2},\ -\sqrt{2}+\zeta_3\sqrt[3]{2},\ \sqrt{2}+\zeta_3^2\sqrt[3]{2},\ -\sqrt{2}+\zeta_3^2\sqrt[3]{2},$$

donde

$$\zeta_3=\frac{-1+\sqrt{-3}}{2}.$$

Pues Galois se empeñó en descubrir qué polinomios cumplen esta propiedad de que todas sus raíces se puedan expresar por radicales y cuáles no, y lo consiguió. Luego veremos a qué conclusión llegó, aunque es un poquito complicada. Antes, vamos a dedicar un rato a descubrir algunas de esas cosillas que Galois aprendió entre los 15 y los 20 años. Lo haremos resolviendo unos cuantos problemas. ¡Quién sabe! A lo mejor Galois también pasó una mañana enfrascado en problemas como estos.

Lo primero que aprendió Galois de Lagrange fue el Teorema Fundamental de Álgebra[1], que dice que un polinomio de grado n con coeficientes racionales (o en general reales, o complejos)

$$a_nx^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0$$

se puede factorizar así:

$$a_n(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),$$

donde $\alpha_1,\alpha_2,\ldots,\alpha_n$ son números complejos.

En particular, un polinomio de grado 2 cumple

$$ax^2+bx+c=a(x-\alpha)(x-\beta)$$

y si multiplicamos la parte de la derecha de la igualdad resulta que

$$\alpha+\beta=-b/a,$$

$$\alpha\beta=c/a.$$

Esta propiedad, que es posible que la conozcáis como "relaciones de Cardano-Vieta", es útil para resolver muchos problemas, como este:

Ejercicio 2 *Comprueba que*

$$\sqrt[3]{20+14\sqrt{2}}+\sqrt[3]{20-14\sqrt{2}}=4.$$

Pista: Multiplica los dos sumandos de la izquierda de la igualdad.

[1] A Gauss no le convenció del todo la demostración de Lagrange, le pareció incompleta, así que dedicó su tesis doctoral a dar una demostración mejor del Teorema fundamental del álgebra.

2 División de polinomios

Ni a Lagrange ni a Gauss se les hubiera podido ocurrir una demostración del Teorema Fundamental del Álgebra si no hubieran sabido dividir polinomios.

Es importante recordar que dados dos polinomios $P_1(x), P_2(x)$ con coeficientes racionales, podemos dividir $P_1(x)$ entre $P_2(x)$, es decir, existen otros dos polinomios con coeficientes racionales[2], $Q(x)$, al que llamamos cociente, y $R(x)$, el resto, de modo que

$$P_1(x) = P_2(x)Q(x) + R(x)$$

y el grado del resto es menor que el grado del divisor, $P_2(x)$.

Ejercicio 3 (Fase local, 2024) *Sea $P(x)$ un polinomio de grado 5 y sean a, b números reales distintos de cero. Supongamos que el resto de dividirlo por $x^3 + ax^2 + b$ es igual al resto de dividirlo por $x^3 + ax + b$. Determinar $a + b$.*

Pongamos que tenemos un polinomio $P(x)$ de grado n y que tiene una raíz α. Si dividimos por $x - \alpha$, nos tendrá que quedar un resto de grado 0, es decir, una constante:

$$P(x) = (x - \alpha)Q(x) + r.$$

Al evaluar $x = \alpha$, resulta que $0 = P(\alpha) = (\alpha - \alpha)Q(\alpha) + r = 0 + r = r$. Así que

$$P(x) = (x - \alpha)Q(x).$$

Si encontramos otra raíz β de $P(x)$, tendrá que ser una raíz de $Q(x)$, ¿verdad? Y entonces

$$P(x) = (x - \alpha)(x - \beta)Q_2(x).$$

¿Y si encontramos otra raíz más? ¿Puede tener $P(x)$ más de n raíces distintas?

Ejercicio 4 *Encuentra todos los polinomios $P(x)$ con coeficientes reales tales que*

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

para todo x y $P(1) = 1$.
Pista: Da valores enteros a x y observa qué ocurre.

Teniendo en cuenta las ideas anteriores, se puede resolver en pocas líneas los siguientes problemas:

Ejercicio 5 (Fase local, 2024) *Sea $P(x)$ un polinomio de grado n tal que*

$$P(i) = \frac{1}{i} \quad \text{para todo } i = 1, 2, \ldots, n + 1.$$

Determinar $P(n + 2)$.

Ejercicio 6 *Sea $P(x)$ un polinomio con coeficientes enteros. Supongamos que hay 3 enteros diferentes a, b, c tales que $P(a) = P(b) = P(c) = -1$. Probar que no existe ningún entero k tal que $P(k) = 0$.*

[2]Si partimos de dos polinomios con coeficientes reales, el cociente y el resto tendrán coeficientes reales.

3 Relaciones entre las raíces de un polinomio

En la sección anterior hemos manejado un polinomio del que conocíamos, al menos, una raíz. A menudo tendremos un polinomio $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ de grado n de cuyas raíces no sabemos nada.

Como, para resolver la ecuación $P(x) = 0$, podemos dividir todo por a_n y las raíces no cambian, vamos a suponer a partir de ahora que nuestro polinomio es mónico, es decir, que $a_n = 1$. Así nos quedarán más sencillas algunas fórmulas que vamos a obtener.

Estábamos diciendo que no sabemos nada de las raíces de $P(x)$ ... Bueno, siempre sabremos algo, porque el Teorema Fundamental del Álgebra dice que van a existir tantas raíces como el grado del polinomio (aunque pueden estar repetidas) y que

$$P(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n).$$

Esto da más información de lo que puede parecer, porque si multiplicamos la parte derecha de la igualdad como hicimos con las ecuaciones de grado 2, nos salen una relaciones entre las raíces y los coeficientes del polinomio, estas que a veces se conocen como relaciones de Cardano-Vieta:

$$\begin{aligned}
a_{n-1} &= -(\alpha_1 + \alpha_2 + \ldots + \alpha_n) \\
a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n \\
a_{n-3} &= -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n) \\
&\ldots \\
a_0 &= (-1)^n \alpha_1\alpha_2\ldots\alpha_n
\end{aligned}$$

Escribid estas relaciones en los casos $n = 3, 4$ y usadlas para pensar los siguientes problemas:

Ejercicio 7 (Fase local, 2011) *Si las 3 raíces reales del polinomio (en la variable x)*

$$x^3 - 7x^2 + ax - 8$$

están en progresión geométrica, ¿cuáles son todos los posibles valores de a?

Ejercicio 8 *Halla para qué valores reales de a todas las raíces de*

$$x^3 - 2x^2 - 25x + a$$

son números enteros.
Pista: Llama α, β y γ a las raíces del polinomio e intenta calcular $\alpha^2 + \beta^2 + \gamma^2$.

Si el siguiente problema se resiste, puede ser útil echar un vistazo a la sección siguiente:

Ejercicio 9 (HMMT 2007) *Sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ las cuatro raíces complejas de*

$$x^4 + 2x^3 + 2 = 0.$$

Determinar

$$\{\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3\}$$

4 Polinomios simétricos

El problema anterior es muy interesante porque la clave para encontrar los valores de esas expresiones de las raíces del polinomio de grado 4 está en construir uno de grado 3 que las tiene como raíces. Si conseguimos resolver la ecuación de grado 3, tendremos los valores de estas expresiones. Además, a partir de los tres valores obtenidos, se pueden calcular las raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

Eso es, de hecho, la idea de Lagrange para explicar la resolución de la ecuación cuártica: dada una ecuación de grado 4, se construye una de grado 3 (a la que llamamos resolvente), de tal modo que la solución de esta última ecuación proporciona fácilmente la de la ecuación inicial. El proceso completo está muy bien explicado en la página 3 de este documento.

Y este es el patrón que encontró Lagrange, pues para resolver las ecuaciones cúbicas construía un resolvente de grado 2. Si este procedimiento se hubiera podido repetir con ecuaciones de grado superior habría sido estupendo. En cualquier caso, Galois explotó estas ideas de Lagrange y sus resolventes para demostrar su precioso teorema.

Pero vamos al lío. ¿Cómo calculamos ese polinomio de grado 3 que tiene unas raíces que no sabemos muy bien quiénes son? Pues Lagrange se basaba en la teoría de los polinomios simétricos.

Un polinomio simétrico en n variables $x_1, x_2, \ldots, x_n$ es una suma finita de términos de la forma

$$a x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n},$$

con a un coeficiente y los exponentes e_i enteros no negativos, que queda invariante cuando permutamos las variables. Por ejemplo,

$$xy^2 - 5x^3y^5 + y^7$$

es un polinomio en dos variables, x, y, pero no es simétrico, porque si permuto x con y me queda un polinomio diferente:

$$x^2y - 5x^5y^3 + x^7.$$

El polinomio $x + y + z$ sí que es simétrico y $x_1^2 + x_2^2 + x_3^2 + x_4^2$ también lo es.

¿Os acordáis de las relaciones de Cardano-Vieta? Sí, estas:

$$a_{n-1} = -(\alpha_1 + \alpha_2 + \ldots + \alpha_n)$$

$$a_{n-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n$$

$$a_{n-3} = -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n)$$

$$\ldots$$

$$a_0 = (-1)^n \alpha_1\alpha_2 \ldots \alpha_n$$

Pues observad que si cambiamos α por x y nos olvidamos del signo que aparece a la derecha de las igualdades, conseguimos n polinomios simétricos en n variables:

$$x_1 + x_2 + \ldots + x_n$$

$$x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n$$

$$x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n$$

$$\ldots$$

$$x_1x_2 \ldots x_n$$

Estos polinomios tienen nombre. Se llaman polinomios simétricos elementales en n variables. Que son simétricos está bastante claro, pero si no lo veis bien porque hay muchos puntos suspensivos, escribidlos en los casos $n = 2, 3$ y 4. ¿Y por qué se llaman elementales? Pues por un teorema muy bonito que Lagrange usaba todo el tiempo y Galois se aprendió muy bien. Lo enunciaremos sin muchos formalismos:

Teorema 1 (Teorema fundamental de los polinomios simétricos) *Todo polinomio simétrico en n variables se escribe en función de las funciones simétricas elementales.*

¿Os atrevéis a expresar los polinomios simétricos del siguiente ejercicios en función de las tres funciones simétricas elementales en tres variables?

Ejercicio 10 *Sean x, y, z números reales tales que $x + y + z = 2, xy + yz + xz = 1, xyz = 2$. Hallar el valor de las siguientes expresiones:*

1. $x^2 + y^2 + z^2$
2. $x^3 + y^3 + z^3$
3. $x^4 + y^4 + z^4$

Las sumas de potencias, como las del ejercicio anterior, siempre pueden escribirse en función de las funciones simétricas elementales, independientemente del valor del exponente y del número de variables. Sus relaciones con las funciones simétricas elementales se conocen con el nombre de "identidades de Newton" (con que el teorema debía de ser conocido mcuho antes de Lagrange). Podéis encontrar más información, por ejemplo, aquí.

Y ahora viene la parte más emocionante de todo esto: cuando evaluamos las funciones simétricas elementales en las raíces de una polinomio (o sea, si volvamos a cambiar x por α), resulta que obtenemos (con el signo que corresponda) los coeficientes del polinomio. Y entonces... tachán... cuando tenemos un polinomio simétrico $F(x_1, x_2, \ldots, x_n)$ en n variables y lo evaluamos en las raíces de un polinomio $P(x)$ de grado n, el valor obtenido, $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, se puede calcular a partir de los coeficientes de $P(x)$. Por ejemplo:

Ejercicio 11 *¿Cuánto vale el polinomio $x^2y + xy^2 + x^2z + xz^2 + y^2z + yz^2$ cuando lo evaluamos en las raíces de $x^3 - x^2 + 2x + 5$?*

Aquí tenéis dos versiones de un problema de la fase local de la OME en 2013:

Ejercicio 12 (Fase local, 2013) *Prueba que las sumas de las primeras, segundas y terceras potencias de las raíces del polinomio $p(x) = x^3 + 2x^2 + 3x + 4$ valen lo mismo.*

Ejercicio 13 (Fase local, 2013) *Busca un polinomio de grado 3 cuyas raíces sean precisamente el cuadrado de las raíces del polinomio*

$$p(x) = x^3 + 2x^2 + 3x + 4.$$

Para conseguir una solución sencilla al siguiente problema, probad a usar lo que habéis aprendido de la sumas de tres cubos:

Ejercicio 14 *Demuestra que si x, y, z son números reales distintos entonces*

$$\sqrt[3]{x-y} + \sqrt[3]{y-z} + \sqrt[3]{z-x} \neq 0.$$

5 Un final de duelo

En 1831, cuando solo tenía 20 años, Galois ya había encontrado una solución al problema de la resolución de ecuaciones por radicales. Fue una solución un poco extraña que sus contemporáneos no recibieron con entusiasmo. Ahora lo enunciamos así:

Teorema 2 (Galois) *Una ecuación es resoluble por radicales si y solamente si el grupo de la ecuación es resoluble.*

El grupo de la ecuación, definido por Galois en su manuscrito, es un cierto grupo de permutaciones de las raíces del polinomio. La estructura de grupo es un concepto algebraico muy importante en la actualidad, pero no existía en la época de Galois. Su trabajo, de hecho, supuso un impresionante impulso al desarrollo del álgebra moderna. Los estudiantes del Grado en Matemáticas de la Universidad de Málaga aprenden la teoría de grupos (y descubren qué es eso de un grupo resoluble) y la teoría de Galois entre el primer y el segundo curso. Cuando se aprende todo eso, se puede apreciar mejor el alcance y la importancia del teorema de Galois.

Lamentablemente, Galois no pudo disfrutar del éxito de su trabajo. En 1832, antes de que se lo aceptaran para su publicación, tuvo la extravagante ocurrencia de aceptar un reto a un duelo con pistolas y no salió bien parado.

Ojalá solo se hubiera entregado a un duelo como el que os proponemos a continuación:

Ejercicio 15 (Fase local, 2010) *Consideramos un polinomio mónico de grado 4 cuyos coeficientes colocaremos dentro de los cuadrados siguiendo ciertas reglas:*

$$P(x) = x^4 + \square\, x^3 + \square\, x^2 + \square\, x + \square$$

1. *Juegan dos personas.*
2. *Por turnos, eligen un hueco y colocan en él un entero no nulo.*

Gana el segundo jugador si $P(x)$ tiene al menos dos raíces enteras distintas. Si no, gana el primero.
Demuestra que hay una estrategia ganadora para el primer jugador. Cuando la hayas encontrado, piensa cuál sería la estrategia ganadora del primer jugador si las dos raíces pueden ser iguales, es decir, si el segundo jugador también gana cuando $P(x)$ tiene una raíz entera múltiple.

Podéis encontrar muchos más problemas sobre polinomios en el capítulo 7 del libro Modern Olympiad Number Theory.