Resolución clásica de polinomios

ALG 3 2017. 15/8/17
CLASE 1

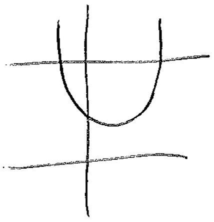
1) Ecuaciones cuadráticas

a) Babilonios (1700-1600 AC).

Tienen un algoritmo para resolver $X+Y=s$, $xy=p$
(o sea las raíces de X^2-sX+p), sin notaciones algebraicas

1) $s \mapsto s/2$
2) $(s/2)^2$
3) $(s/2)^2-p$ $(\sim \Delta)$
4) $\sqrt{(s/2)^2-p}$
5) $\frac{s}{2}+\sqrt{\left(\frac{s}{2}\right)^2-p}$ era x, $y=s-x$

b) Griegos hasta 100 DC



Resuelven cuadráticas por construcciones geométricas
No hay formulaciones algebraicas (como conocemos hoy) hasta al menos 100 DC

Diofanto en 250 DC introduce alguna notación geométrica y también métodos para resolver algunas cúbicas que involucran intersecciones de cónicas (círculos, elipses, parábolas e hipérbolas)

$$X^3=a^2b \iff X^2=aY \text{ e } XY=ab$$

Soluciones algebraicas de cúbicas desconocidas.

Hoy en día: $aX^2+bX+c=0$ con $a,b,c\in\mathbb{C}$, $a\neq 0$

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

donde $\sqrt{b^2-4ac}$ denota cualquier raíz cuadrada en $\mathbb{C}$ de
$\Delta=b^2-4ac$

2) <u>Ecuaciones cúbicas</u> (Renacimiento italiano)

Fórmulas de Cardano (Ars Magna, 1545)

Scipione del Ferro' 1515:
encontró solución para cúbicas $x^3 + bx = c$ con $b, c \in \mathbb{R}_{>0}$
Su estudiante Florido conocía la solución y en 1535 desafió a Niccolò Fontana (Tartaglia) a resolver 30 cúbicas
Tartaglia venció y le contó su solución a Cardano en 1539, que la publicó en Ars Magna en 1545. (separando en 13 casos prefiriendo siempre coeficientes positivos)

<u>Interpretación de hoy</u>:

$$aX^3 + bX^2 + cX + d = 0 \quad \text{con} \quad a \neq 0$$

$\mapsto$ $X^3 + bX^2 + cX + d = 0$; $b, c, d \in \mathbb{C}$

$\mapsto$ haciendo $Y = X + \frac{b}{3}$

$$\left(X + \frac{b}{3}\right)^3 - \frac{b^2}{3}X - \frac{b^3}{27} + cX + d = 0$$

$$\left(X + \frac{b}{3}\right)^3 + \left(c - \frac{b^2}{3}\right)\left(X + \frac{b}{3}\right) - \frac{bc}{3} + \frac{b^3}{9} - \frac{b^3}{27} + d = 0$$

$\mapsto$ $Y^3 + pY + q = 0$

con $\begin{cases} p = -\frac{b^2}{3} + c \\ q = \frac{2b^3}{27} - \frac{bc}{3} + d \end{cases}$

Por lo tanto hay que resolver

$$X^3 + pX^{\cancel{2}} + q = 0$$

<u>Cambio de variable</u>: $X = U + V$ con $3UV = -p$

(o sea U, V soluciones de $Y^2 - XY = -\frac{p}{3}$)

$\Rightarrow$

$$X^3 = (U+V)^3 = U^3 + V^3 + 3U^2V + 3UV^2$$
$$= U^3 + V^3 - p(U+V)$$
$$X^3 = U^3 + V^3 - pX$$

$\leadsto \quad X^3 + pX + q = U^3 + V^3 + q = 0$

O sea:

$$\left\{\begin{array}{l} U^3 + V^3 = -q \\ U^3V^3 = \dfrac{-p^3}{27} \end{array}\right\} \text{ suma y producto ¡}$$

U^3, V^3 son raíces de la ecuación cuadrática

$$Y^2 + qY - \frac{p^3}{27} = 0 \qquad (\text{"Resolvente"})$$

cuyo discriminante es $\Delta = q^2 + \dfrac{4p^3}{27} = \dfrac{27q^2 + 4p^3}{27}$

discriminante de la cúbica

Sea $\delta = \sqrt{\dfrac{27q^2+4p^3}{27}}$

Entonces $U^3 = \dfrac{-q+\delta}{2}$, $V^3 = \dfrac{-q-\delta}{2}$

$$\Rightarrow \quad X = U + V = \sqrt[3]{\frac{-q+\delta}{2}} + \sqrt[3]{\frac{-q-\delta}{2}}$$

Pregunta: hay así 9 soluciones pero la cúbica tiene 3.

¿Cómo se sabe cuáles son?

$UV = -\dfrac{p}{3}$ decide la elección de signos

¡Ojo que esto define las raíces en forma muy complicada!

$X^3 + X - 2 = 0 \qquad 1 = \sqrt[3]{1 + \frac{2}{9}\sqrt{21}} + \sqrt[3]{1 - \frac{2}{9}\sqrt{21}}$

En realidad los números complejos fueron introducidos por BOMBELLI (1526-1572) más tarde en 1572.

La ecuación de grado 4 aparece en ARS MAGNA. Su resolución se debe a Ludovico Ferrari.

EULER (1749): creía que todas las ecuaciones polinomiales son resolubles por radicales:
"Research on the imaginary roots of equations":
Uno puede garantizar que las expresiones para las raíces no contienen ninguna otra operación que la extracción de raíces, además de las 4 operaciones vulgares, y uno puede difícilmente defender la postura que operaciones trascendentes se metan en la situación.

Vandermonde - Lagrange ∼ 1770

descubrieron independientemente el rol jugado por propiedades de simetría en las soluciones de las ~~raíces~~ ecuaciones:

$$x^2 + ax + b = 0 \qquad a = -(\alpha+\beta)$$
$$b = \alpha\beta$$

$\alpha+\beta = -a$. $\alpha-\beta$? no simétrico pero $(\alpha-\beta)^2$ lo es:

$$(\alpha-\beta)^2 = a^2 - 4b \implies \alpha-\beta = \pm\sqrt{a^2-4b}$$

$$\implies \alpha = \frac{-a+\sqrt{a^2-4b}}{2}, \quad \beta = \frac{-a-\sqrt{a^2-4b}}{2}$$

Se sabía desde GIRARD (1630) y NEWTON (1665) que toda expresión simétrica en las raíces es una expresión en los coeficientes de la ecuación.

Teorema fundamental de los polinomios simétricos elementales (5)

(s. XIX)

A anillo conmutativo, $X_1, ., X_n$ variables

<u>Definición</u> $g \in A[X_1, ., X_n]$ es simétrica si $\forall \sigma \in S_n$ permutación (de índices, o sea de variables), se tiene $\sigma(g) = g$

donde $\sigma(g) = g(\sigma(X_1), ., \sigma(X_n))$

<u>Ejemplos</u>: 1) <u>Las sumas de Newton</u>

$$N_1 = X_1 + .. + X_n$$
$$N_2 = X_1^2 + .. + X_n^2 \qquad N_k = \sum_{i=1}^{n} X_i^k$$
$$\vdots$$
$$N_k = X_1^k + .. + X_n^k$$

2) <u>Polinomios simétricos elementales</u>

$$\begin{cases} S_1 = X_1 + .. + X_n \\ S_2 = X_1 X_2 + .. + X_1 X_n + X_2 X_3 + .. + X_{n-1} X_n \\ \vdots \\ S_k = \displaystyle\sum_{1 \le i_1 < .. < i_k \le n} X_{i_1} \cdots X_{i_k} \\ \vdots \\ S_n = X_1 \cdots X_n \end{cases} \qquad (S_k = 0 \text{ para } k > n)$$

Sabemos que si

$$f = X^n + a_{n-1} X^{n-1} + .. + a_1 X + a_0 = (X - \alpha_1) .. (X - \alpha_n)$$

entonces

$$a_{n-1} = -S_1(\alpha_1, ., \alpha_n)$$
$$a_{n-2} = S_2(\alpha_1, ., \alpha_n)$$
$$\vdots$$
$$a_0 = (-1)^n S_n(\alpha_1, ., \alpha_n)$$

Los N_k se pueden escribir en función de los S_j :

$\therefore$ $N_1 = S_1$ $\qquad\qquad$ $N_1 - S_1 = 0$

$N_2 = S_1^2 - 2S_2$ $\qquad\qquad$ $N_2 - S_1 N_1 + 2S_2 = 0$

...

$$N_k - S_1 N_{k-1} + S_2 N_{k-2} + \cdots + (-1)^k k S_k = 0 \quad \text{para } \cancel{1 \le k \le n} \ \forall k$$

(fácil para $k = n$. Ejercicio en general) $\qquad$ ($S_k = 0$ para $k > n$)

~~¿Y para k>n?~~

$$\cancel{N_k + S_1 N_{k-1} + \cdots + (-1)^{k-n-1} S_n N_{k-n} = 0}$$

~~N.B.~~

Teorema fundamental de los pols sim eltales

Sea $g \in A[X_1, .., X_n]$ simétrico. Entonces $\exists!\ h \in A[X_1, .., X_n]$ /

$$g(X_1, .., X_n) = h(s_1(X_1, .., X_n), \ldots, s_n(X_1, .., X_n))$$

Todo pol. simétrico es un pol. en los pols sim. eltales, y además la escritura es única (Caso particular de la correspondencia de Galois)

Demostración

Obs. básicas: 1 suma, prod y comp de pols simétricos es simétrico

2 $f \in A[X_1, .., X_n] \Rightarrow f(s_1, .., s_n)$ es simétrico pues

$$\sigma(f) = f(\sigma(s_1), .., \sigma(s_n))$$

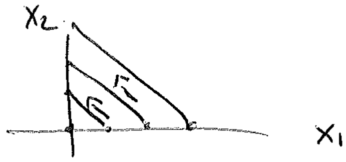
En general $\qquad \sigma(f(g_1, .., g_n)) = f(\sigma(g_1), .., \sigma(g_n))$

Le ponemos un orden total a los monomios en $A[X_1, .., X_n]$, que se llama el orden lexicográfico graduado:

$$X_1^{a_1} \cdots X_n^{a_n} > X_1^{b_1} \cdots X_n^{b_n} \iff \begin{array}{l} a_1 + \cdots + a_n > b_1 + \cdots + b_n \\ \text{ó} \\ a_1 + \cdots + a_n = b_1 + \cdots + b_n \\ \text{pero } a_1 > b_1 \\ \text{o } a_1 = b_1 \text{ pero } a_2 > b_2 \text{ etc...} \end{array}$$

$x_1 > x_2$

$x_1^2 > x_1 x_2 > x_2^2 > x_1 > x_2 > 1$



Hay sólo finitos monomios menores que un monomio fijo.

Existencia

Sea $g \in A[x_1, ., x_n]$ simétrico y sea

$c_{\underline{a}} x_1^{a_1} \cdots x_n^{a_n}$ su término "principal"

Por como es el orden y porque g es simétrico, sabemos que

se cumple $a_1 \geq a_2 \geq \cdots \geq a_n$.

Considero

$$c_{\underline{a}} \, s_1^{a_1 - a_2} \, s_2^{a_2 - a_3} \cdots s_{n-1}^{a_{n-1} - a_n} \, s_n^{a_n}$$

y calculo su coeficiente principal:

$$c_{\underline{a}} \, x_1^{a_1 - a_2} \, x_1^{a_2 - a_3} x_2^{a_2 - a_3} \cdots (x_1 \cdots x_{n-1})^{a_{n-1} - a_n} \, x_n^{a_n}$$

$$= c_{\underline{a}} \, x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} = \text{cte pcpal } (g)$$

Luego

$g - c_{\underline{a}} \, s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}$ cancela el término de cabeza

Es un pol. simétrico formado por finitos monomios cuyo cte

ppal es menor que el de g

Repitiendo el procedimiento en algún momento se agotaron

los coeftes ppales y queda

$$g - h(s_1, ., s_n) = 0$$

Ejercicio: hacerlo para $x_1^3 + x_2^3$ en 2 variables

Unicidad:

Queremos probar que si $h_1(s_1, ., s_n) = h_2(s_1, ., s_n)$

entonces $h_1 = h_2$

O sea si $h(s_1, ., s_n) = 0$, ent. $h = 0$.

o sea si $h \neq 0$, entonces $h(s_1,.., s_n) \neq 0$

$$h(x_1,.., x_n) = \sum c_{\underline{a}} x_1^{a_1} \cdots x_n^{a_n}$$

$$\Rightarrow h(s_1,.., s_n) = \sum c_{\underline{a}} s_1^{a_1} \cdots s_n^{a_n}$$

cte ppal de
$$s_1^{a_1} = x_1^{a_1}$$
$$s_2^{a_2} = x_1^{a_2} x_2^{a_2}$$
$$\vdots$$
$$s_n^{a_n} = (x_1 \cdots x_n)^{a_n}$$

$\Rightarrow$ cte ppal de $h(s_1,.., s_n)$ se elige entre los ctes ppales de

$$c_{\underline{a}} x_1^{a_1+..+a_n} x_2^{a_2+..+a_n} \cdots x_n^{a_n}$$

o eventualmente suma de ellos

pero $(a_1,.., a_n) \mapsto (a_1+..+a_n, a_2+..+a_n, .., a_n)$

es inyectiva:

2 monomios $\neq$ no aportan cancelación de coeftes ppales

luego cte ppal $(h(s_1,.., s_n)) = c_{\underline{a}} x_1^{a_1+..+a_n} \cdots x_n^{a_n}$

donde $(a_1,.., a_n)$ es tq $a_1+..+a_n$ es máximo

y entre ellos $a_2+..+a_n$ es máximo

$\vdots$

a_n es máximo

ejemplo $x_1^2 x_2 + x_1 x_2^2$

$$(x_1+x_2)^2 x_1 x_2 + (x_1+x_2)(x_1 x_2)^2$$

$\mapsto x_1^3 x_2$ ó $x_1^3 x_2^2$? gana $x_1^3 x_2^2$ ¿

$\boxtimes$

La cuadrática según Vandermonde:

$$\alpha = \frac{1}{2}\Big[(\alpha+\beta) + (\alpha-\beta)\Big]$$

$$= \frac{1}{2}\Big[\alpha+\beta + \underset{\overset{\|}{\sqrt{(\alpha-\beta)^2}}}{(\alpha+(-1)\beta)}\Big]$$

La cúbica según Vandermonde

Sea una cúbica con raíces α, β, γ, y sea ω una raíz cúbica primitiva de 1. Entonces $1+\omega+\omega^2 = 0$

y por lo tanto

$$\alpha = \frac{1}{3}\Big[(\alpha+\beta+\gamma) + (\alpha+\underbrace{\omega\beta+\omega^2\gamma}_{\text{no simétrico}}) + (\alpha+\underbrace{\omega^2\beta+\omega\gamma}_{\text{no simétrico}})\Big]$$

Queremos hacer $\sqrt[3]{(\alpha+\omega\beta+\omega^2\gamma)^3}$ y $\sqrt[3]{(\alpha+\omega^2\beta+\omega\gamma)^3}$

Pero $u = (\alpha+\omega\beta+\omega^2\gamma)^3$; $v = (\alpha+\omega^2\beta+\omega\gamma)^3$ no son simétricos. Aunque sí lo son

$u+v$ y $u \cdot v$ (en α, β, γ)

Por lo tanto $u+v$ y $u\cdot v$ son expresiones en los coeftes de los polinomios originales!

Conociendo $u+v$ y $u\cdot v$ puedo conocer u y v.

Lagrange lo sistematizó

$f \in \mathbb{C}[X]$ cúbica con raíces α, β, γ

Sea $t_1 = \alpha + \omega\beta + \omega^2\gamma$

y consideremos $t_2, .., t_6$ las otras 5 permutaciones

o sea los de la forma $\omega^i\alpha + \omega^j\beta + \omega^k\gamma$ $\quad i, j, k = 0, 1, 2$