Álgebra III - 2do C. 2020 - Clase 1 - 1/9/2020

1 Resolución clásica de polinomios

1.1 La ecuación cuadrática

(1) Babilonios (1700-1600 AC)

Ya tenían un algoritmo para resolver $x + y = s, xy = p$ (o sea encontrar las raíces de $X^2 - sX + p$):

- $s \mapsto s/2$
- $(s/2)^2$
- $(s/2)^2 - p$
- $\sqrt{(s/2)^2 - p}$
- $x = (s/2) + \sqrt{(s/2)^2 - p},\ y = s - x\,.$

(2) 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), del tipo

$$X^3 = a^2 b \ \Leftrightarrow\ X^2 = aY \ \text{ y } \ XY = ab.$$

Las soluciones algebraicas de cúbicas no se conocen.

(3) Hoy

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

Soluciones:

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

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

Relacionar con lo que conté en la reunión, que más que de los babilonios (me emocioné y dije cualquiera), era la forma en la que pensaron Vandermonde y Lagrange en el S. XVIII para resolver $X^2 - sX + p$, para luego intentar resolver con las mismas ideas las ecuaciones de grado 3, 4, 5, 6, etc.:

- Si conocemos $x+y$ y $x-y$ recuperamos x e y
- Conocemos $x+y=s$ pero no $x-y$... pero $(x-y)^2=(x+y)^2-4xy=s^2-4p$! O sea conocemos $x+y$ y $(x-y)^2$...

1.2 La ecuación cúbica

(1) Renacimiento italiano

Scipione del Ferro, 1515, encontró solución para cúbicas de la forma $X^3+bX=c$ con $b,c\in\mathbb{R}_{>0}$. Su estudiando Florido conocía la solución y en 1535 desafió a Niccolo Fontana (Tartaglia) a resolver 30 cúbicas. Tartaglia venció y le contó su solución a Cardano en 1539, que la publicó en Ars Magna, 1545, separando en 13 casos para mantener siempre coeficientes positivos.
La interpretación de hoy, para resolver $aX^3+bX^2+cX+d=0$ con $a\neq 0$, es la siguiente:

- Hacer mónica la ecuación: $X^3+bX^2+cX+d=0$ con $b,c,d\in\mathbb{C}$
- Hacer $Y=X+b/3$ para deshacerse del término cuadrático. Queda

$$Y^3+pY+q=0 \text{ con } p= \qquad \text{y } q= \qquad .$$

- Escribir una solución y de la forma $y=u+v$ con $3uv=-p$ ¿Por qué se puede?

- Haciendo la cuenta queda que $y^3+py+q=0$ se transforma en $u^3+v^3+q=0$ sabiendo $u^3v^3=-\frac{p^3}{27}$, o sea tenemos la suma y producto de u^3 y v^3, que son entonces las raíces de la ecuación cuadrática:

$$Z^2+qZ-\frac{p^3}{27}$$

  ¡Fijarse que aparece $\Delta=q^2+\frac{4p^3}{27}=\frac{27q^2+4p^3}{27}$! (¿relación con el discriminante?)

- Sea $\delta=\sqrt{\frac{27q^2+4p^3}{27}}$, entonces $u^3=\frac{-q+\delta}{2}$ y $v^3=\frac{-q-\delta}{2}$, y finalmente

$$y=u+v=\sqrt[3]{\frac{-q+\delta}{2}}+\sqrt[3]{\frac{-q-\delta}{2}}$$

Pregunta 1: Así pareciera haber 9 soluciones, pero hay solo 3.... ¿Cuáles son?

Pregunta 2: Resolviendo así $X^3 + X - 2$ da una raíz $\sqrt[3]{1 + \frac{2}{9}\sqrt{21}} + \sqrt[3]{1 - \frac{2}{9}\sqrt{21}}$?????

En realidad los números complejos fueron introducidos recién en 1572 por Bombelli. La ecuación de grado 4 aparece en Ars Magna. Su resolución se debe a Ludovico Ferrari.
Euler en 1749 creía que todas las ecuaciones polinomiales eran 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 cuatro operaciones vulgares, y uno puede dificilmente defender la postura que operaciones trascendentes se meten en la situación." (traducción muy libre...)

(2) Vandermonde y Lagrange $\sim$1770

Descubrieron independientemente el rol jugado por las propiedades de simetría en las soluciones de las ecuaciones:
$X^2 + aX + b = 0$

- Si conocemos $x + y$ y $x - y$ recuperamos x e y
- Conocemos $x+y = -a$ pero no $x-y$... pero $(x-y)^2 = (x+y)^2-4xy = a^2-4b$ implica $x - y = \pm\sqrt{a^2 - 4b}$! Esto implica

$$x = \frac{-a + \sqrt{a^2 - 4b}}{2} \quad \text{e} \quad y = \frac{-a - \sqrt{a^2 - 4b}}{2}.$$

Intermezzo
Teorema Fundamental de los Polinomios Simétricos Elementales, S. XIX

Se sabía desde Albert Girard (1630) e Isaac Newton (1665) que toda expresión simétrica en las raíces es una expresión en los coeficientes de la ecuación.

En lo que sigue A es un anillo conmutativo, y $X_1, \ldots, X_n$ son variables.

Definición 1.1 (Polinomio simétrico)
Un polinomio $g \in A[X_1, \ldots, X_n]$ *es* simétrico *si para toda permutación* σ *de las variables, se tiene que* $\sigma(g) = g$ *(donde* $\sigma(g) = g(\sigma(X_1), \ldots, \sigma(X_n))$*.*

Ejemplos Notemos $\mathbf{X} := (X_1, \ldots, X_n)$

- Las sumas de Newton:

$$\begin{cases} N_1(\mathbf{X}) = X_1 + \cdots + X_n \\ N_2(\mathbf{X}) = X_1^2 + \cdots + X_n^2 \\ \quad \vdots \\ N_k(\mathbf{X}) = X_1^k + \cdots + X_n^k, \quad \text{para} \;\; k \in \mathbb{N} \end{cases}$$

- Los polinomios simétricos elementales:

$$\begin{cases} s_1(\mathbf{X}) = X_1 + \cdots + X_n \\ s_2(\mathbf{X}) = X_1X_2 + \cdots + X_1X_n + X_2X_3 + \cdots + X_2X_n + \cdots + X_{n-1}X_n \\ \quad \vdots \\ s_k(\mathbf{X}) = \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \cdots X_{i_k}, \quad \text{para} \;\; 1 \le k \le n \\ \quad \vdots \\ s_n(\mathbf{X}) = X_1 \cdots X_n \\ s_k(\mathbf{X}) = 0 \quad \text{para} \;\; k > n. \end{cases}$$

(A veces se pone también por conveniencia $s_0(\mathbf{X}) = 1$.)

Observar que si $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = (X - x_1) \cdots (X - x_n)$, entonces se tiene para $\mathbf{x} = (x_1, \ldots, x_n)$

$$\begin{cases} a_{n-1} = -s_1(\mathbf{x}) \\ a_{n-2} = s_2(\mathbf{x}) \\ \quad \vdots \\ a_0 = (-1)^n s_n(\mathbf{x}). \end{cases}$$

Los polinomios de Newton y los polinomios simétricos elementales están relacionados por las fórmulas de Girard-Newton, que permiten entonces expresar recursivamente los polinomios de Newton en términos de los polinomios simétricos elementales:

$$\begin{aligned} &N_1(\mathbf{X}) = s_1(\mathbf{X}), \quad \text{i.e.} \;\; N_1(\mathbf{X}) - s_1(\mathbf{X}) = 0 \\ &N_2(\mathbf{X}) = s_1(\mathbf{X})N_1(\mathbf{X}) - 2s_2(\mathbf{X}), \quad \text{i.e.} \;\; N_2(\mathbf{X}) - s_1(\mathbf{X})N_1(\mathbf{X}) + 2s_2(\mathbf{X}) = 0 \\ &\quad \vdots \\ &N_k(\mathbf{X}) - s_1(\mathbf{X})N_{k-1}(\mathbf{X}) + s_2(\mathbf{X})N_{k-2}(\mathbf{X}) + \cdots + (-1)^k k s_k(\mathbf{X}) = 0 \end{aligned}$$

El caso $k = n$ es muy simple de probar. ¿Por qué?

El caso $k \neq n$ es bastante más engorroso y lo dejo como ejercicio de la teórica para resolver a lo largo de la materia.

Observaciones básicas

- La suma, producto y composición de polinomios simétricos es un polinomio simétrico.
- Si $f \in A[\mathbf{X}]$, entonces $f(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X}))$ es simétrico, pues para toda permutación σ se tiene

$$\sigma(f(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X}))) = f(\sigma(s_1(\mathbf{X})), \ldots, \sigma(s_n(\mathbf{X}))).$$

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

Enunciamos y probamos ahora el teorema fundamental que justifica toda esta sección.

Teorema 1.2 (Teorema fundamental de los polinomios simétricos elementales.)

Sea $g \in A[X_1, \ldots, X_n]$ un polinomio simétrico. Entonces existe un único $h \in A[X_1, \ldots, X_n]$ tal que

$$g(\mathbf{X}) = h(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X})).$$

(Todo polinomio simétrico es un polinomio en los polinomios simétricos elementales, y además esa escritura es única.)

Prueba.–

Existencia de h : La hacemos por inducción imponiendo un orden total a los monomios en las variables $X_1, \ldots, X_n$, que se llama el orden lexicográfico graduado: gana el grado y en caso de igualdad se desempata mirando quién gana de izquierda a derecha.

$$X_1^{j_1} \cdots X_n^{j_n} > X_1^{k_1} \cdots X_n^{k_n} \quad \Leftrightarrow \quad \begin{array}{l} j_1 + \cdots + j_n > k_1 + \cdots + k_n, \\ \text{o si } j_1 + \cdots + j_n = k_1 + \cdots + k_n, \text{ ent. } j_1 > k_1, \text{ etc.} \end{array}$$

Por ejemplo para dos variables:

$$X_1^2 > X_1X_2 > X_2^2 > X_1 > X_2 > 1.$$

Observar que hay solo finitos monomios menores que un monomio dado (dibujarlo para dos variables).
También que dado este orden total, todo polinomio f tiene un término principal compuesto por un coeficiente principal y su monomio principal.

Sea entonces $g \in A[\mathbf{X}]$ simétrico, y sea $c\, X_1^{j_1} \cdots X_n^{j_n}$ su término principal.
Sabiendo que g es simétrico y como es el orden entre monomios, ¿qué se puede decir de $j_1, j_2, \ldots, j_n$? (no avanzar hasta no resolver esto, y si no se le ocurre nada haga ejemplos con polinomios simétricos g chiquitos para inspirarse).

Considero entonces el polinomio $c\, s_1(\mathbf{X})^{j_1-j_2} s_2(\mathbf{X})^{j_2-j_3} \cdots s_n(\mathbf{X})^{j_n}$ y calculo su término principal. ¿Da? (¡oh casualidad!)

Así cuando hacemos $g - c\, s_1(\mathbf{X})^{j_1-j_2} s_2(\mathbf{X})^{j_2-j_3} \cdots s_n(\mathbf{X}) j_n$, se cancela el término de cabeza y el polinomio *simétrico* obtenido tiene finitos monomios más chicos para el orden.
Se repite el procedimiento, o se concluye por inducción.

Ejercicio: hacerlo para $X_1^3 + X_2^3$ en dos variables.

Unicidad de h: Qpq si $h_1(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X})) = h_2(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X}))$ entonces $h_1(\mathbf{X}) = h_2(\mathbf{X})$, o sea si $h(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X})) = 0$ entonces $h(\mathbf{X}) = 0$. Recíprocamente,

$$h(\mathbf{X}) \neq 0 \;\Rightarrow h(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X})) \neq 0,$$

es decir tiene un monomio....
La pregunta es: Si $h \neq 0$, ¿qué termino sobrevive seguro en $h(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X}))$?

■

Consecuencia esencial para nosotros:
Sea $f = a_n X^n + \cdots + a_0 \in K[X]$ con K cuerpo, con raíces $x_1, \ldots, x_n$ en algún lugar, y sea $g \in K[X_1, \ldots, X_n]$ un polinomio simétrico. Entonces $g(x_1, \ldots, x_n) \in K$.
Esto es pues existe $h \in K[X_1, \ldots, X_n]$ tal que $g = h(s_1(\mathbf{X}), \ldots, s_n(\mathbf{X}))$ y por lo tanto

$$g(x_1, \ldots, x_n) = h(s_1(\mathbf{x}), \ldots, s_n(\mathbf{x})) = h(\frac{-a_{n-1}}{a_n}, \ldots, (-1)^n \frac{a_0}{a_n}) \in K.$$

• **La resolución de la cúbica según Vandermonde**

$f = X^3 + aX^2 + bX + c$ con raíces x, y y z, ω raíz cúbica primitiva de 1

Así $1 + \omega + \omega^2 = 0$ y por lo tanto

$$x = \frac{1}{3}\big((x + y + z) + (x + \omega y + \omega^2 z) + (x + \omega^2 y + \omega z)\big)$$

donde $x+y+z$ es simétrico en x, y, z pero $(x+\omega y+\omega^2 z)$ y $(x+\omega^2 y+\omega z)$ no lo son.

Y tampoco lo son

$$u := (x + \omega y + \omega^2 z)^3 \quad \text{y} \quad v := (x + \omega^2 y + \omega z)^3$$

(para poder sacárles después las raíces cúbicas, copiando la idea de lo que hicieron en la resolución de la cuadrática).

¡Pero $u + v$ y $u\,v$ sí son simétricos en x, y, z! (verificarlo)

Con lo cual $u + v$ y $u\,v$ son expresiones A y B en los coeficientes a, b, c de la cúbica f, lo que implica que u y v son raíces de la cuadrática $X^2 - AX + B$ que se puede resolver.

• **La resolución de la cúbica según Lagrange**

Lagrange independientemente sistematizó lo de Vandermonde.

$f = X^3 + aX^2 + bX + c$ con raíces x, y y z, ω raíz cúbica primitiva de 1

Sean

$$t_1(x, y, z) := x + \omega y + \omega^2 z, \quad t_2 := \omega\, t_1, \quad t_3 := \omega^2\, t_1$$
$$t_4 := x + \omega^2 y + \omega z, \quad t_5 := \omega\, t_4, \quad t_6 := \omega^2\, t_4,$$

las 6 permutaciones de $t_1(x, y, z)$ que se obtienen al permutar por $\sigma \in S_3$ las raíces x, y, z.

Por lo tanto

$$g = (X - t_1)(X - t_2)(X - t_3)(X - t_4)(X - t_5)(X - t_6) \in \mathbb{C}[x, y, z][X]$$

es un polinomio que cuando uno le aplica σ una permutación de las raíces, se tiene

$$\sigma(g(x, y, z)(X)) = g(\sigma(x), \sigma(y), \sigma(z))[X] = (X - \sigma(t_1)) \cdots (X - \sigma(t_6)) = g(x, y, z)(X).$$

Es decir, los coeficientes de g son simétricos en x, y, z y se pueden expresar como polinomios en a, b, c, los coeficientes de f.

¡Lástima que g tiene grado 6 y no grado 2!

PEEEERO también vale ....

$$g \;=\; (X^3 - t_1^3)(X^3 - t_4^3)$$

¿Por qué?

O sea

$$g \;=\; (X^3 - t_1^3)(X^3 - t_4^3) \;=\; X^6 - (t_1^3 + t_4^3)X^3 + t_1^3 t_4^3$$

es un polinomio de grado 2 disfrazado de hecho ¿no? ¿por qué?

Y además sus coeficientes $A = t_1^3 + t_4^3$ y $B = t_1^3 t_4^3$ son simétricos, o sea son expresiones en los coeficientes de f.... (Notar que t_1^3 y t_4^3 son los u y v de Vandermonde.)

Se pueden recuperar entonces t_1^3 y t_4^3 como raíces de la cuadrática $X^2 - AX + B$ (que se llama la *resolvente*) y luego sacarles raíz cúbica, así se obtienen t_1 y t_4, y recuerdo que $x + y + z = -a$.

Concluimos $x = \frac{1}{3}((x + y + z) + t_1 + t_4)$, etc.