LAGRANGE LO SISTEMATIZÓ:

LAGRANGE 1736-1813

Ecole Polytechnique (1794) Germain - Lagrange
Abierta a las mujeres en ... 1972

1) $f \in \mathbb{C}[X]$ cúbica con raíces α, β, γ; ω raíz primitiva 3 de 1

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

y consideremos $t_2 = \omega t_1$, $t_3 = \omega^2 t_1$

$t_4 = \alpha + \omega^2\beta + \omega\gamma$, $t_5 = \omega t_4$, $t_6 = \omega^2 t_4$

las otras 5 permutaciones de t_1 al aplicar $\sigma \in S_3$ a t_1.

Sea $g = (X - t_1) \cdots (X - t_6) \in \mathbb{C}(X)$

Entonces g es simétrico en α, β y γ: sus coeftes son simétricos en α, β, γ

Pero además

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

$$= X^6 - [\underbrace{t_1^3 + t_4^3}_{\text{simétrico}}] X^3 + \underbrace{t_1^3 t_4^3}_{\text{simétrico}}$$

← RESOLVENTE? de grado 6 pero de grado 2 de hecho

Se puede expresar $t_1^3 + t_4^3$ y $t_1^3 t_4^3$ en función de los coeficientes de la ecuación original

2) $t_1 = \alpha + i\beta - \gamma - i\delta$ y sus $4! = 24$ permutaciones

$$g(X) = \prod_{i=1}^{24} (X - t_i) = (X^4 - t_1^4)(X^4 - t_5^4)(X^4 - t_9^4)\cdots(X^4 - t_{21}^4)$$

(6 factores de grado 4) g igualmente se puede seguir reduciendo.

Igualmente los 2 notaron que si $t_1 = \alpha - \beta + \gamma - \delta$

Las 24 permutaciones dan 6 valores $\neq$ q' se repiten 4 veces c/uno

$\pm t_1$, $\pm t_3$ con $t_3 = \alpha + \beta - \gamma - \delta$, $\pm t_5$ con $t_5 = \alpha - \beta - \gamma + \delta$

de nuevo los coeftes son simétricos c/r a las raíces $\quad$ (2)

$$g(x) = (x-t_1)^4 (x+t_1)^4 (x-t_3)^4 (x+t_3)^4 (x-t_5)^4 (x+t_5)^4$$
$$= (x^2-t_1^2)^4 (x^2-t_3^2)^4 (x^2-t_5^2)^4$$
$$= \left[(x^2-t_1^2)(x^2-t_3^2)(x^2-t_5^2) \right]^4$$

t_1^2, t_2^2 y t_3^2 se obtienen como raíces de una cúbica que se puede calcular

Luego: se calcula t_1, t_2, t_3

y luego $\alpha = \frac{1}{4}\left[(\overbrace{\alpha+\beta+\gamma+\delta}^{\text{sim}}) + t_1 + t_2 + t_3 \right]$ etc.

Sólo hay que asignar signos...

<u>Ec de grado 5</u>: No hay truco semejante, llega a 24 factores de grado 5 de la forma $x^5 - t^5$?

<u>Problemas</u>

(1) Asume existencia de raíces

(2) Trata a las raíces (desconocidas) como si fueran variables independientes

¿Raíces?

1. $X^n - 1$ tiene todas sus raíces en $\mathbb{C}$ (ecuaciones ciclotómicas)

2. $X^2 + aX + b$ tiene sus dos raíces en $\mathbb{C}$

<u>Teorema</u>: $\mathbb{C}$ es algebraicamente cerrado

Girard 1629
Euler 1719 Laplace 1791
D'Alembert 1796
Gauss: 1797/99 - 1816 - 1849

· Consecuencia del teo de Liouville (Cauchy 1844)
"toda función holomorfa en $\mathbb{C}$ y acotada es cte"
· Una demo de AL

<u>Ingredientes</u>:

1. $f \in \mathbb{R}[X]$ de grado impar tiene raíz en $\mathbb{R}$ (Bolzano)
2. $f \in \mathbb{C}[X]$ de grado 2 tiene raíces en $\mathbb{C}$
3. TFPSE

<u>Demostración</u> (Euler - Laplace)

1. Spg podemos suponer $f \in \mathbb{R}[X]$ pues para $f \in (\mathbb{C}-\mathbb{R})[X]$

Se considera

$$f \cdot \overline{f} = \left(\sum_i a_i X^i\right)\left(\sum_j \overline{a}_j X^j\right) = \sum \left(\sum_{i+j=k} a_i \overline{a}_j\right) X^k \in \mathbb{R}[X]$$

Y si $z \in \mathbb{C}$ es raíz de $f \cdot \overline{f}$, o bien es raíz de f o bien es raíz de $\overline{f}$ en cuyo caso $\overline{z}$ es raíz de f.

Luego: $f \in \mathbb{R}[X]$, $gr(f) = n = 2^k q$ con q impar.

Dem por inducción en k:

1) $k=0 \Rightarrow gr(f)$ impar $\Rightarrow f$ tiene raíz real

2) $k>0$

$f(x)=(x-\alpha_1)\dots(x-\alpha_n)$. Qpq $\exists\, \alpha_i \in \mathbb{C}$

Dado $c \in \mathbb{R}$, $\beta_{ij} = \alpha_i+\alpha_j + c\,\alpha_i\alpha_j \quad (i<j)$

$\Rightarrow \exists \binom{n}{2} = \frac{n(n-1)}{2} = \frac{2^k q\,(2^k q-1)}{2} = 2^{k-1} q\,(2^k q-1)$ tales β_{ij}

$= 2^{k-1} m$ con m impar

Defino

$$g(x) = \prod (x-\beta_{ij})$$

<u>Afirmación</u>: $g \in \mathbb{R}[x]$:

$\sigma(g(x)) = \prod(x-\sigma(\beta_{ij}))$ Pero $\sigma(\beta_{ij}) = \beta_{i'j'}$ en forma

biyectiva $\Rightarrow \sigma(g(x)) = g(x) \;\forall \sigma \in S_n$

$$g(x) = x^N + b_{n-1}x^{N-1} + \dots + b_0$$

$$\sigma(g(x)) = x^N + \underbrace{\sigma(b_{n-1})} x^{N-1} + \dots + \sigma(b_0)$$

σ(coefics) = coefics que son expresiones en los α_i

Por lo tanto g tiene alguna raíz en $\mathbb{C}$

Para cada elección de c en $\mathbb{R}$, tenemos algún $\beta_{ij} \in \mathbb{C}$:

$\alpha_{i(c)} + \alpha_{j(c)} + c\,\alpha_{i(c)}\alpha_{j(c)} \in \mathbb{C}$ ~~pa~~

Pero hay finitos α_i e infinitos c: Para dos valores $\neq$ de c

tienen que coincidir i y j:

$$\begin{cases} \alpha_i+\alpha_j + c\,\alpha_i\alpha_j \in \mathbb{C} \\ \alpha_i+\alpha_j + c'\,\alpha_i\alpha_j \in \mathbb{C} \end{cases} \Rightarrow \begin{cases} \alpha_i+\alpha_j \in \mathbb{C} \\ \alpha_i\alpha_j \in \mathbb{C} \end{cases}$$

$\Rightarrow$ Sols de una cuadrática

$\Rightarrow \alpha_i, \alpha_j \in \mathbb{C}$ $\boxtimes$

CUERPOS

1. Axiomas: $(K,+,\cdot)$ $\quad 1\neq 0$

   $+,\cdot$ $\quad (K,+)$ grupo abeliano

   $\quad (K^{\times},\cdot)$ " "

   Distributivas $\qquad$ Ejemplos

2. K cpo $\Rightarrow$ K dom. íntegro

3. A anillo conmutativo, I ideal

   A/I cuerpo $\Leftrightarrow$ I ideal maximal

   $$I\subseteq J\subsetneq A \Rightarrow I=J$$

4. Característica de un cuerpo

$$car(K)=\begin{cases}\min\{n\in\mathbb{N} : n1=\underbrace{1+\dots+1}_{n}=0 \text{ en } K\} & \text{si existe}\\ 0 & \text{si no}\end{cases}$$

Se tiene $car(K)=0$ ó $car(K)=p$ con p primo pues

$$\phi: \mathbb{Z}\longrightarrow K$$
$$1_{\mathbb{Z}}\longmapsto 1_K$$

homomorfismo de anillos:

$$\begin{cases}\phi(a+b)=\phi(a)+\phi(b)\\ \phi(ab)=\phi(a)\phi(b)\\ \phi(1)=1\end{cases}$$

$$\phi(m)=\underbrace{1+\dots+1}_{m}, \quad \phi(-m)=\underbrace{-1-\dots-1}_{m}$$

Ker ϕ es un ideal de $\mathbb{Z}$: $\quad$ Ker $\phi=\{0\}$ o Ker $\phi=n\mathbb{Z}$

e $\mathrm{Im}\,\phi\simeq \mathbb{Z}/\mathrm{Ker}\,\phi=\mathbb{Z}$ ó $\mathbb{Z}/n\mathbb{Z}$

Pero $\mathrm{Im}\,\phi$ subanillo de K que es íntegro

$\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ íntegro, i.e $n=p$.

Si $car(K)=0$, $\mathrm{Im}\,\phi\simeq\mathbb{Z}$ $\Rightarrow$ K contiene a $\mathbb{Q}$ como subcuerpo

Si $car(K)=p$, $\mathrm{Im}\,\phi\simeq\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$ Cuerpo finito con p eltos

Se dice que $\mathbb{Q}$ o $\mathbb{F}_p$ son los cuerpos primos de K y K es un espacio vectorial (vía la inclusión) sobre su cuerpo primo

5 Extensiones de cuerpos

Definición: Sean E, K cuerpos. Se dice que E es una extensión de K si $\exists \varphi : K \to E$ homomorfismo de cuerpos (de anillos)

Pero todo homomorfismo de cuerpos es un monomorfismo pues $Ker(\varphi)$ ideal de K, o sea $Ker(\varphi) = \{0\}$ o $\underbrace{Ker(\varphi) = K}_{\text{No pues } \varphi(1_K) = 1_E}$

O sea φ es un homomorfismo inyectivo:

$$\varphi(K) \subset E. \qquad \text{con } \varphi(K) \simeq K.$$

Decimos directamente $K \subset E$ (modulo el isomorfismo / $Im(\varphi)$)

y notamos E/K. (Identificamos K con $\varphi(K)$, o sea podemos suponer $K \subseteq E$)

Observación: Sea E/K una extensión de cuerpos. Entonces E es un K-e.v (vía φ) y por lo tanto tiene dimensión (finita o infinita) como K-e.v.

Ejemplos

Definición: (grado) Sea E/K una extensión de cuerpos.

Entonces $[E:K] =:$ grado de E sobre K

$$[E:K] = \dim_K E$$

Se dice que E/K es una extensión finita cuando $[E:K] < \infty$ e infinita sino

$[E:K] = 1 \iff E = K$ $(E \simeq K)$

Ejemplo: $\mathbb{C}/\mathbb{R}$ satisface $[\mathbb{C}:\mathbb{R}] = 2$

$\mathbb{R}/\mathbb{Q}$? $[\mathbb{R}:\mathbb{Q}] = \infty$ ...

(tendrían el mismo cardinal y no lo tienen)

Proposición: Sea $E/F/K$ una torre

(a) $[E:K] < \infty \iff [E:F]$ y $[F:K] < \infty$

y en ese caso vale $[E:K] = [E:F][F:K]$

Demostración

($\Rightarrow$) Sea $\{u_1, .., u_s\}$ base de E/K

ent $\{u_1, .., u_s\}$ genera E/F $\Big\}$ finitos
y F/K subespacio de E/K

($\Leftarrow$) Sean $\{v_1, .., v_n\}$ base de F/K y $\{w_1, .., w_m\}$ base de E/F

Entonces $\{v_i w_j,\ 1 \le i \le n,\ 1 \le j \le m\}$ es base de E/K:

$$\alpha = b_1 w_1 + \dots + b_m w_m \quad \text{~~son~~ con } b_i \in F$$

y $$b_j = a_{j1} v_1 + .. + a_{jn} v_n \quad \text{con } a_{ji} \in K$$

entonces $$\alpha = (a_{11} v_1 + \dots + a_{1n} v_n) w_1 + .. + (a_{m1} v_1 + .. + a_{mn} v_n) w_m$$

$$= \sum a_{ji} v_i w_j \qquad \underline{\text{generan}}$$

$\boxtimes$

li: Usando que los 2 cjtos son li.

$[E:F] \mid [E:K]$
$[F:K] \mid [E:K]$

Consecuencias

F/K subextensión de E/K $\Rightarrow$

$K \cong \psi(K) \subset E$
$F \cong \psi(F) \subset E$
$K \cong \phi(K) \subset F$

$$\begin{tikzcd}
 & & E \\
F \arrow[r] & \psi(F) & \psi(F) \arrow[u, phantom, "\cup"] \\
\phi(K) \arrow[u, phantom, "\cup"] & & \\
K \arrow[u, phantom] \arrow[r, "\phi"'] \arrow[rr, bend right] & \phi(K) & \psi(K) \arrow[uu, dash]
\end{tikzcd}$$

$$\psi \circ \phi(K) \cong K$$

$$\psi \circ \phi(K) \subseteq \psi(F) \subset E$$

$$\begin{array}{c} E \\ | \\ \psi(F) \\ | \\ \psi \circ \phi(K) \end{array}$$

Podemos obviar las inclusiones:

Definición (cuerpo generado por)

(1) Sea E/K extensión de cuerpos y sea $\alpha \in E$

$K[\alpha] := \{ f(\alpha),\ f \in K[X] \} \subseteq E$ anillo

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)},\ f, g \in K[X],\ g(\alpha) \neq 0 \right\} \text{ cuerpo}$$

(cuerpo cociente del dominio íntegro $K[\alpha]$)

$K(\alpha)$ es el menor cuerpo que contiene a K y a α

$K(\alpha) = \bigcap \{ F :\ F \subseteq E,\ F \text{ cuerpo},\ K \subset F,\ \alpha \in F \}$

(cuerpo generado por α) $\uparrow$ 18/8/17

---

(2) Sean $\alpha_1, .., \alpha_n \in E$

$K[\alpha_1, .., \alpha_n] := \{ f(\alpha_1, .., \alpha_n),\ f \in K[X_1, .., X_n] \} \subseteq E$ d.i

$$K(\alpha_1, .., \alpha_n) = \left\{ \frac{\beta}{\gamma};\ \beta, \gamma \in K[\alpha_1, .., \alpha_n],\ \beta \neq 0 \right\}$$
$$= \left\{ \frac{f(\alpha_1, .., \alpha_n)}{g(\alpha_1, .., \alpha_n)},\ f, g \in K[X],\ g(\alpha_1, .., \alpha_n) \neq 0 \right\}$$

Se tiene $K(\alpha_1, .., \alpha_n) = K(\alpha_1, .., \alpha_s)(\alpha_{s+1}, .., \alpha_n)$

(Lo podemos pensar como una torre)

(3) $S \subseteq E$

$K[S] = \{$ expresiones polinomiales evaluadas en eltos de $S \}$

$K(S) = \bigcap \{ F,\ F \subseteq E,\ K, S \subseteq F \}$

$$= \left\{ \frac{f(s_1, .., s_n)}{g(t_1, .., t_m)},\ f, g \text{ pols},\ s_i, t_j \in S,\ g(\underline{t}) \neq 0 \right\}$$

$$K(S \cup T) = K(S)(T) = K(T)(S)$$