Una lectura comentada de la «*Mémoire*» de Galois

JOSEP PLA I CARRERA

Professor emèrit de la UB
jpla@ub.edu
Facultat de Matemàtiques de la UB

Jornada Galois

Sala d'actes
Facultat de Matemàtiques i Estadística [UPC]
Dimecres, 6 de març de 2013

Una lectura comentada de la «Mémoire» de Galois

Índex

Évariste Galois

Dibuix d'Évariste amb l'abric escolar nou,
fet per la seva germana Antoine-Marie.
Évariste tenia quinze anys.
Moriria, en un duel, cinc anys més tard.

ÉVARISTE GALOIS

Bourg-la-Reine (França), 5 d'octubre de 1811
Paris (França), 31 de maig de 1832

Nitens lux,
horrenda procella,
tenebris æternis involuta.

El paper de Liouville

Évariste Galois redactà la «Mémoire sur les conditions de résolubilité des équations par radicaux», que comentarem en aquesta xerrada, la nit abans del duel —el 29 de maig de 1832— i l'envia al seu amic Auguste Chevalier.

Joseph Liouville [1802-1882] la va publicar, per primera vegada, amb d'altres textos, l'any 1846, a la revista *Journal de Mathématiques Pures et Appliées*, p 417–433.

La *Mémoire* de Galois

La ≪Mémoire≫ consta de tres parts ben diferenciades:

1. **Els principis**: [tres] definicions i quatre lemes.
2. **La teoria**: cinc proposicions.
3. **Una aplicació**: tres proposicions.

Els Principis

Primera part

Els principis

Definicions i Lemes

Els Principis: les definicions

Les definicions:

1. L'*adjunció* d'elements a un *cos*.
2. Els elements *racionals* i *irracionals*.
3. Les *substitucions* ***actuen*** sobre les *permutacions*.

   Diu textualment:

   ≪Les substitucions són el **pas** d'una permutació a una altra.≫
   ≪Quan les agrupem, totes les farem provenir de la **mateixa** permutació≫.
4. Una idea [molt informal] de *grup*, però diu:≪és **tancat** per composició≫.

◀ 8

El text de Galois suggereix, doncs, els conceptes de *grup* i d'*extensió algèbrica d'un cos*.

Serien desenvolupats, respectivament, per Arthur Cayley [1821-1895] i Camille Jordan [1838-1922], el primer, i per Richard Dedekind [1831-1916], el segon.

Els Principis: lemes I i II

Lema I. Una equació racional irreductible no pot tenir una arrel en comú amb una equació racional sense dividir-la.

[És un corol·lari de l'algorisme màxim comú divisor d'Euclides per a polinomis.]

Lema II. Donada una equació $f(X) = 0$, amb els coeficients en el cos K_0 i amb les arrels $\xi_1, \ldots, \xi_n$, totes diferents, sempre podrem formar una funció racional de les arrels

$$V = V(\xi_1, \ldots, \xi_n)$$

que, quan permutem les arrels $\xi_1, \ldots, \xi_n$, de totes les maneres possibles, prengui valors diferents.

[Galois suggereix agafar $V(\xi_1, \ldots, \xi_n) := a_1\,\xi_1 + a_2\,\xi_2 + \cdots + a_n\,\xi_n$, amb $a_1, a_2, \ldots, a_n$, enters convenients.

Els valors diferents $v_i = a_1\,\xi_{\sigma_i(1)} + \cdots + a_n\,\xi_{\sigma_i(n)}$, amb $\sigma_i \in \mathfrak{S}_n$, $\sigma_1 = \mathrm{Id}$, i $i = 1, 2, \ldots, n!$, són les arrels de l'equació [de grau $n!$]

$$F(V) = (V - v_1)\,(V - v_2)\cdots(V - v_{n!-1})\,(V - v_{n!}) \overset{\text{t.f.s.}}{\in} K_0[V].$$ ◀ 4 ◀ 5 ◀ 7]

Els Principis: el lema III

Lema III. Si V és una funció com la del lema II, aleshores **totes** les arrels $\xi_1, \ldots, \xi_n$, de l'equació inicial es poden expressar en funció d'un valor fix v_1 de V: $\xi_i = \ell_i(v_1)$.

[La funció $V(\xi_1, \ldots, \xi_n)$ s'anomena una resolvent de l'equació $f(X) = 0$.

De fet, els valors $v_j, j = 1, \ldots, n!$, són elements primitius de $K_1 := K_0(\xi_1, \ldots, \xi_n) = K_0(v_j)$.

És un cas particular d'un teorema general de la secció §100 del treball de Lagrange de 1770 sobre les equacions polinòmiques.]

Demostració. Sigui el factor $F_1(V)$ de $F(V)$ definit per $F_1(V) = (V - v_1) \cdots (V - v_{(n-1)!})$, on les $v_i, i = 1, \ldots, (n-1)!$, s'obtenen de $V(\xi_1, \xi_2, \xi_3, \ldots, \xi_n)$ permutant $\xi_1, \xi_2, \xi_3, \ldots, \xi_n$ amb totes les permutacions $\sigma \in \mathfrak{S}_n$ que $\sigma(\xi_1) = \xi_1$ —les que deixen fixa l'arrel ξ_1. ▶ 3

1. $F_1(V)$ s'escriu $F(V, \xi_1)$ amb coeficients en el cos K_0 **(??????)**.
2. És fàcil veure que $F(v_1, X) = 0$ i $f(X) = 0$ solament tenen en comú l'arrel ξ_1.
3. Per tant, $g(X) = \text{mcd}(F(v_1, X), f(x)) \in K_0(v_1)[X]$ i és de primer grau en X. O sigui, $g(X) = \text{mcd}(F(v_1, X), f(x)) = \alpha(v_1)\, X + \beta(v_1)$.
4. A més, $\alpha(v_1)\, \xi_1 + \beta(v_1) = 0$. D'on $\xi_1 = -\dfrac{\beta(v_1)}{\alpha(v_1)}$. ■

Els Principis: el lema IV

Lema IV. Sigui $G(V)$ un polinomi minimal de V. Si hom té $\xi_i = \ell_i(v_1)$ i v_k és una altra arrel de $G(V)$, aleshores $\ell_i(v_k)$ també és una arrel de l'equació inicial.

◀ 7

Una anàlisi. Siguin $v_1, v_2, \ldots, v_r$ les arrels del polinomi minimal $G(V)$ (irreductible en el cos K_0) de la resolvent V i sigui r el seu grau. Considerem la taula

		ξ_1	ξ_2	$\ldots$	ξ_i	$\ldots$	ξ_n
$\leftarrow-$							
$\vert$	v_1	$\ell_1(v_1)$	$\ell_2(v_1)$	$\ldots$	$\ell_i(v_1)$	$\ldots$	$\ell_n(v_1)$
$\downarrow$	v_2	$\ell_1(v_2)$	$\ell_2(v_2)$	$\ldots$	$\ell_i(v_2)$	$\ldots$	$\ell_n(v_2)$
	$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
σ_k							
$\vert$	v_j	$\ell_1(v_j)$	$\ell_2(v_j)$	$\ldots$	$\ell_i(v_j)$	$\ldots$	$\ell_n(v_j)$
	$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\downarrow$							
$-\rightarrow$	v_k	$\ell_1(v_k)$	$\ell_2(v_k)$	$\ldots$	$\ell_i(v_k)$	$\ldots$	$\ell_n(v_k)$
	$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
	v_r	$\ell_1(v_r)$	$\ell_2(v_r)$	$\ldots$	$\ell_i(v_r)$	$\ldots$	$\ell_n(v_r)$

Segons el lema IV els elements de cada fila són arrels de l'equació polinòmica inicial $f(X) = 0$.

Aquestes arrels són diferents? **Sí!!!!!** [pel lema I].

▶ 2

Les Proposicions

Segona part

Les Proposicions

La proposició I

Proposició I. *Teorema*. Considerem una equació donada les m arrels de la qual són $a, b, c, \ldots$ Sempre **existeix** un grup de permutacions de les lletres $a, b, c, \ldots$ que té la propietat següent:

Tota funció de les arrels

1. **invariant** per les substitucions del grup, és racionalment coneguda.
2. [Recíprocament,] **determinable racionalment**, és invariant per les substitucions [del grup].

[La demostració de Galois és la que trobem en els textos actuals.

Hi ha autors que donen aquesta propietat com a definició del grup de Galois.

En una nota a peu de pàgina, Galois precisa que el seu concepte d'**invariància** és numèric i no pas formal com en Lagrange.

En el text, ho concreta amb dos exemples:

—el cas formal general de grau n —de grup $\mathfrak{S}_n$;

—el cas ciclotòmic de grau primer p —de grup generat per un cicle d'ordre p.]

◀ ??

La proposició II

Proposició II. *Teorema*. Suposem que, a una equació, se li adjunta l'arrel r d'una equació auxiliar **irreductible**.

1. Aleshores, tindrà lloc una d'ambdues situacions:
   1. o bé el grup de l'equació no canviarà,
   2. o bé el dividirà en p **grups** cada un d'ells pertanyent a l'equació proposada quan se li adjunta respectivament cada una de les arrels de l'equació auxiliar.
2. Aquests grups tenen la següent propietat remarcable

   Es passa de l'un a l'altre operant totes les permutacions del primer **una mateixa substitució** de les lletres.

Qui és i com és p?

Demostració de la proposició II

Demostració.

1. Sigui $f(X) = 0$ l'equació que volem resoldre, on $f(X) \in K_0[V]$.
2. Considerem $F(V) = (V - v_1)(V - v_2) \cdots (V - v_{n!-1})(V - v_{n!}) \in K_0[V]$. ▶ 3
3. Sigui $G_1(V) \in K_0[V]$ el factor irreductible que $G_1(v_1) = 0$, on $v_1 = a_1\,\xi_1 + \cdots + a_n\,\xi_n$ és una resolvent de $f(X)$. ▶ 5
4. Adjuntem una de les arrels $\eta_1, \ldots, \eta_m$ d'una equació auxiliar $g(Y) = 0$, on $g(Y) \in K_0[Y]$.
5. $G_1(V)$ pot factoritzar a $K_1 := K_0(\eta_1)$. Sigui $H_1(V)$ el factor irreductible de $G_1(V)$ a K_1 que té com arrel v_1: $H_1(v_1) = 0$. **(??????)**.
6. $H_1(V)$ és un polinomi mònic $H(V, \eta_1)$ de V i η_1, amb coeficients en K_0, irreductible.
   Li corresponen les permutacions —**totes diferents**— v_j per a les que $H(v_j, \eta_1) = 0$.
7. Treballem amb el polinomi $L(V) := H(V, \eta_1) \times H(V, \eta_2) \times \cdots \times H(V, \eta_m) \overset{\text{t.f.s.}}{\in} K_0(V)$.
8. Els ≪conjunts≫ $H(V, \eta_1), \cdots, H(V, \eta_m)$ són ≪disjunts≫ o ≪iguals≫ pel que fa a les v_j.
9. D'una banda $G_1(V) \big| L(V)$ i, de retruc, $L(V) = G_1(V)^k$ per a un cert k [LEMA I].
10. Les arrels d'$L(V)$ tenen, doncs, multiplicitat k. Hi ha k ≪conjunts≫ $H(V, \eta_j)$ repetits. N'agafem un de cada; en total $p = \frac{m}{k}$.
11. En resulta que $G_1(V) = P(V) = \prod_{p=\frac{m}{k}} H(V, \eta_s)$, on els factors $H(V, \eta_s)$ són diferents dos a dos que proporcionen els p grups de l'enunciat. ■

Comentari a la proposició II

Hem partit, doncs, les substitucions del grup inicial de Galois $\mathcal{G}$ en $p := \frac{m}{k}$ grups **diferents**.

Galois s'adona, a més, del fet següent:

> Si $v, \omega(v)$ són **dues arrels** de $H_1(V, \eta_1)$, i v' és **una arrel** de $H_1(V, \eta_2)$, aleshores $\omega(v')$ en serà **una altra**.

Hom passa, doncs, d'un ≪conjunt≫ a l'altre amb una mateixa ≪substitució≫.

La proposició II: una anàlisi

Ara considerem el que Galois anomena grups [exemple de la proposició V].

$\mathcal{H}$	$\mathcal{H}_1$	$\mathcal{H}_2$
$\xi_1\ \xi_2\ \xi_3\ \xi_4$;	$\xi_1\ \xi_3\ \xi_4\ \xi_2$;	$\xi_1\ \xi_4\ \xi_2\ \xi_3$;
$\xi_2\ \xi_1\ \xi_4\ \xi_3$;	$\xi_3\ \xi_1\ \xi_2\ \xi_4$;	$\xi_4\ \xi_1\ \xi_3\ \xi_2$;
$\xi_3\ \xi_4\ \xi_1\ \xi_2$;	$\xi_4\ \xi_2\ \xi_1\ \xi_3$;	$\xi_2\ \xi_3\ \xi_1\ \xi_4$;
$\xi_4\ \xi_3\ \xi_2\ \xi_1$;	$\xi_2\ \xi_4\ \xi_3\ \xi_1$;	$\xi_3\ \xi_2\ \xi_4\ \xi_1$.

I mirem quines substitucions **proporcionen** cada columna i quines **passen** dels elements d'una columna a l'altra.

Comencem amb la primera columna. És una columna de ≪permutacions≫. Seguint la presentació de Galois, les ≪substitucions≫ passen de la permutació bàsica 1 2 3 4 a la permutació de cada fila.

fila 0:	1	2	3	4	subst.
fila 1:	1	2	3	4	σ_0
fila 2:	2	1	4	3	σ_1
fila 3:	3	4	1	2	σ_2
fila 4:	4	3	2	1	σ_4

O sigui tenim les substitucions:

$$\sigma_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\ \sigma_4=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

El conjunt $\mathcal{H}:=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ conté Id —és σ_1— i és tancat per la composició $\circ$.

És un grup, tant en la nomenclatura galoisiana com en la nostra.

La proposició II: una anàlisi

Ara bé, si apliquem el mateix criteri amb les altres dues columnes obtenim, respectivament, el conjunt $\mathcal{H}_1$ de les τ_i i el conjunt $\mathcal{H}_2$ de les υ_i, $i = 1, 2, 3, 4$.

$$\tau_1 = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,4\,2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,1\,2\,4 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,2\,1\,3 \end{pmatrix}, \tau_4 = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,4\,3\,1 \end{pmatrix}.$$

$$\upsilon_1 = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,2\,3 \end{pmatrix}, \upsilon_2 = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,1\,3\,2 \end{pmatrix}, \upsilon_3 = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix}, \upsilon_4 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,4\,1 \end{pmatrix}.$$

Fixem-nos que

$$\begin{aligned} \tau_1 \circ \mathcal{H} &= \{\tau_1 \circ \sigma_1, \tau_1 \circ \sigma_2, \tau_1 \circ \sigma_3, \tau_1 \circ \sigma_4\} = \{\tau_1, \tau_2, \tau_3, \tau_4\} = \mathcal{H}_1, \\ \upsilon_1 \circ \mathcal{H} &= \{\upsilon_1 \circ \sigma_1, \upsilon_1 \circ \sigma_2, \upsilon_1 \circ \sigma_3, \upsilon_1 \circ \sigma_4\} = \{\upsilon_1, \upsilon_2, \upsilon_3, \upsilon_4\} = \mathcal{H}_2. \end{aligned}$$

Els conjunts $\mathcal{H}_1$ i $\mathcal{H}_2$ **no** contenen la substitució unitat **ni** són tancats per $\circ$.
Galois en diu grups però els grups han d'estar tancats per $\circ$. ▶ 1

fila 0:	1	4	2	3	subst.
fila 1:	1	4	2	3	σ_0
fila 2:	4	1	3	2	σ_4
fila 3:	2	3	1	4	σ_2
fila 4:	3	2	4	1	σ_3

fila 0:	1	3	4	2	subst.
fila 1:	1	3	4	2	σ_0
fila 2:	3	1	2	4	σ_3
fila 3:	4	2	1	3	σ_4
fila 4:	2	4	3	1	σ_2

De fet, hem de tirar enrere amb τ_1^{-1} i amb υ_1^{-1}, respectivament.

Obtenim, doncs, $\mathcal{H}_1 \circ \tau_1^{-1} = \tau_1 \circ \mathcal{H} \circ \tau_1^{-1} [= \mathcal{H}]$ i $\mathcal{H}_2 \circ \upsilon_1^{-1} = \upsilon_1 \circ \mathcal{H} \circ \upsilon_1^{-1} [= \mathcal{H}]$.

Les proposicions III i IV

Proposició III. *Teorema*. Si a una equació li adjuntem totes les arrels d'una equació auxiliar, els grups dels que es parla en el teorema II tenen, a més, aquesta propietat: en cada un dels grups les substitucions són les mateixes.

[Com en l'exemple anterior. Si tenim en compte, l'observació anterior, ens adonarem que Galois introdueix el concepte de [sub]grup normal o invariant.]

Proposició IV. *Teorema*. Si hom adjunta a una equació el valor numèric d'una certa funció de les seves arrels, el grup de l'equació s'abaixarà de manera que no contingui d'altres permutacions que aquelles per a les quals aquesta funció és invariant.

[Són dos corol·laris de la proposició II, importants per al desenvolupament ulterior de Galois.]

Proposició V. *Problema*. Galois explica el lligam que hi ha entre les dues torres, la d'extensions dels cossos —ascendent— i la dels grups associats —descendent.

[Mentre l'explica, l'exemplifica amb el cas de la resolució de la quàrtica.]

Tercera part

Tercera part

Aplicació dels resultats

Les proposicions VI, VII i VIII

Aplicació a les equacions polinòmiques de grau **primer** *p*

Proposició VI. *Lema*. Una equació irreductible de grau **primer** *p*, **no pot** esdevenir reductible per l'adjunció d'un radical l'índex del qual sigui diferent del propi grau de l'equació.

[M'ha costat molt trobar-ne una demostració adequada.]

Proposició VII. *Problema*. Quin és el grup d'una equació irreductible d'un grau **primer** *p*, resoluble per radicals?.

[És el grup generat per un cicle d'ordre *p*.]

Proposició VIII. *Teorema*. Per tal que una equació irreductible de grau primer *p* sigui resoluble per radicals, **és necessari i suficient** que dues qualssevol de les arrels siguin conegudes, i les altre se'n dedueixin racionalment.

[És un corol·lari [delicat] del teorema anterior.
És el resultat que Galois posa de manifest a la introducció.]

Comentari a la proposició VII

El grup penúltim $\mathcal{G}_1$ —l'últim és $\mathcal{G}_0 = \{\mathrm{Id}\}$— el genera un cicle com ara $\sigma := (1\ 2\ \cdots\ p)$, o sigui $\mathcal{G} = \{\mathrm{Id} = \sigma^0, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$ que s'obté per adjuncions d'equacions auxiliars binòmiques.

Com són els grups que el precedeixen i ell mateix?

Les **úniques** substitucions del grup de Galois $\mathcal{G}$ són de la forma

$$x_k \mapsto x_{\alpha\, k+\beta},$$

on α i β són elements de $\mathbb{Z}_p$.

Com exemple, mostra que la quíntica general és **no és** resoluble per radicals: Si $p = 5$, el grup $\mathcal{G}$ serà el següent:

	a b c d e	a c e b d	a e d c b	a d b e c
	b c d e a	c e b d a	e d c b a	d e a b c
	c d e a b	e b d a c	d c b a e	b e c a d
	d e a b c	b d a c e	c b a e d	e c a d b
	e a b c d	d a c e b	b a e d c	c a d b e

	$\alpha k + \beta$			
	$\alpha = 1$	$\alpha = 2$	$\alpha = 4$	$\alpha = 3$
k	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
	0 : 1 2 3 4 5	4 : 1 3 5 2 4	2 : 1 5 4 3 2	3 : 1 4 2 5 3
	1 : 2 3 4 5 1	1 : 3 5 2 4 1	1 : 5 4 3 2 1	1 : 4 2 5 3 1
β	2 : 3 4 5 1 2	3 : 5 2 4 1 3	0 : 4 3 2 1 5	4 : 2 5 3 1 4
	3 : 4 5 1 2 3	0 : 2 4 1 3 5	4 : 3 2 1 5 4	2 : 5 3 1 4 2
	4 : 5 4 3 2 1	2 : 4 1 3 5 2	3 : 2 1 5 4 3	0 : 3 1 4 2 5

El grup de Galois $\mathcal{G}$ té 20 elements i n'hauria de tenir, segons ens ha dit abans [▶ 6], 120.