Grups de Galois a la Galois

Joan-C. Lario

31 Gener 2013

Griselda Pascual

Grups de Galois

L'experiència (sigui com a docents o com a discents) ens diu que després de fer un curs –de mesos de feina!– en Teoria de Galois, hom acaba sovint calculant grups de Galois de:

- polinomis de grau 1;

Grups de Galois

L'experiència (sigui com a docents o com a discents) ens diu que després de fer un curs –de mesos de feina!– en Teoria de Galois, hom acaba sovint calculant grups de Galois de:

- polinomis de grau 1;
- polinomis de grau 2;

Grups de Galois

L'experiència (sigui com a docents o com a discents) ens diu que després de fer un curs –de mesos de feina!– en Teoria de Galois, hom acaba sovint calculant grups de Galois de:

- polinomis de grau 1;
- polinomis de grau 2;
- polinomis de grau 3;

Grups de Galois

L'experiència (sigui com a docents o com a discents) ens diu que després de fer un curs –de mesos de feina!– en Teoria de Galois, hom acaba sovint calculant grups de Galois de:

- polinomis de grau 1;
- polinomis de grau 2;
- polinomis de grau 3;
- polinomis de grau 4;

Grups de Galois

L'experiència (sigui com a docents o com a discents) ens diu que després de fer un curs –de mesos de feina!– en Teoria de Galois, hom acaba sovint calculant grups de Galois de:

- polinomis de grau 1;
- polinomis de grau 2;
- polinomis de grau 3;
- polinomis de grau 4;

i poca cosa més.

Grups de Galois

L'experiència (sigui com a docents o com a discents) ens diu que després de fer un curs –de mesos de feina!– en Teoria de Galois, hom acaba sovint calculant grups de Galois de:

- polinomis de grau 1;
- polinomis de grau 2;
- polinomis de grau 3;
- polinomis de grau 4;

i poca cosa més. Com Galois calculava els grups de Galois?

Premier Mémoire

Presentada i rebutjada (amb raons de pes) a l'Acadèmia de Ciències de Paris el gener de 1831.

- F. Xavier Labrador (2011), imatges digitals a http://www.bibliotheque-institutdefrance.fr/numerisation/
- Peter M. Neumann (2011), The Mathematical Writings of Évariste Galois.
- Harold M. Edwards (2012), Galois for 21st-Century Readers.

La Premier Mémoire conté 3 lemes i 8 proposicions.

Premier Mémoire

Presentada i rebutjada (amb raons de pes) a l'Acadèmia de Ciències de Paris el gener de 1831.

- F. Xavier Labrador (2011), imatges digitals a http://www.bibliotheque-institutdefrance.fr/numerisation/
- Peter M. Neumann (2011), The Mathematical Writings of Évariste Galois.
- Harold M. Edwards (2012), Galois for 21st-Century Readers.

La Premier Mémoire conté 3 lemes i 8 proposicions. Ara repassarem els tres lemes i la Proposició 1. Es busquen voluntaris per tal d'estudiar les altres set proposicions en dues sessions de treball.

Premier Mémoire: Lema 1

Lemma 1

Sigui $f \in K[x]$ irreductible. Si $g \in K[x]$ té una arrel en comú amb f en alguna extensió de K, aleshores f divideix g.

Galois es ventila la demostració amb mitja frase tot esmentant que el màxim comú divisor de ambdós polinomis té coeficients al cos K.

Premier Mémoire: Lema 1

Lemma 1

Sigui $f \in K[x]$ irreductible. Si $g \in K[x]$ té una arrel en comú amb f en alguna extensió de K, aleshores f divideix g.

Galois es ventila la demostració amb mitja frase tot esmentant que el màxim comú divisor de ambdós polinomis té coeficients al cos K.

Els lemes 2 i 3 serveixen per construir el cos de descomposició d'un polinomi qualsevol (irreductible o no) $f \in K[x]$.

Galois no assumeix l'existència del cos de descomposició; simplement ensenya que, en cas d'existir, ell sap com operar amb els seus elements de manera pràctica i canònica. Kronecker és el primer que mostra l'existència del cos de descomposició.

Premier Mémoire: Lema 2

Lemma 2

Si $f \in K[x]$ no té arrels múltiples, aleshores existeix una combinació lineal entera de les arrels de f

$$V = A_1\alpha_1 + A_2\alpha_2 + \cdots + A_m\alpha_m, \quad A_i \in \mathbb{Z},$$

tal que $\#\{V^\sigma : \sigma \in \mathscr{S}_m\} = m!$.

Prova. Galois no dóna cap demostració. Considerem el polinomi lineal

$$V(x_1, \ldots, x_m) = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m$$

Tenim $m!$ polinomis V^σ en permutar les arrels α_i. Aleshores

$$\Delta = \prod_{\sigma \neq \tau} V^\sigma - V^\tau \in K[x_1, \ldots, x_m] \setminus \{0\}$$

Per inducció sobre m, tot polinomi no nul en m variables sobre un cos K admet una substitució entera donant una avaluació no nula.

Premier Mémoire: Lema 3

Lemma 3

Siguin $f \in K[x]$ i $V = A_1\alpha_1 + A_2\alpha_2 + \cdots + A_m\alpha_m$ com abans. Aleshores, per a totes les arrels es té

$$\alpha_i \in K(V).$$

És a dir, $K(\alpha_1, \ldots, \alpha_m) = K(V)$.

Prova. Galois dóna un sketch de la demostració. Considerem

$$G(X) := \prod_{\sigma \in \mathscr{S}_m} X - V^\sigma = \prod_{j=1}^{m} F(X, \alpha_j) \in K[X]$$

per cert $F(X, Y) \in K[X, Y]$ amb $F(X, \alpha_i) = \prod_{\sigma(i)=i} X - V^\sigma$. Aleshores

$$\varphi(V) + x\psi(V) = \gcd(F(V, x), f(x)) \in K(V)[x].$$

De manera que $\alpha_i = -\psi(V)/\varphi(V)$.

Exemple $m = 3$

Sigui $f(x) = (x-\alpha_1)(x-\alpha_1)(x-\alpha_1) \in K[x]$. Triem A, B, $C \in \mathbb{Z}$ tals que

$$V = A\alpha_1 + B\alpha_2 + C\alpha_3 \quad \text{dóna 6 valors diferents per permutació.}$$

$$G(X) = F(X,\alpha_1)F(X,\alpha_2)F(X,\alpha_3)$$

$$F(X,\alpha_1) = (X-(A\alpha_1+B\alpha_2+C\alpha_3))(X-(A\alpha_1+B\alpha_3+C\alpha_2)) \in K[X,\alpha_1]$$

$$\gcd(F(V,x),f(x)) = \varphi(V)x + \psi(V)$$

$$\alpha_1 = -\psi(V)/\varphi(V).$$

El grup de Galois

Prenen $f \in K[x]$ i $V = A_1\alpha_1 + A_2\alpha_2 + \cdots + A_m\alpha_m$ com abans. Tenim $K(\alpha_1, \ldots, \alpha_m) = K(V)$. Factoritzem en irreductibles a $K[X]$:

$$G(X) = \prod_{\sigma \in \mathscr{S}_m} X - V^\sigma = G_0(X)G_1(X)G_2(X)\ldots$$

Siguin V, V', V'', $\ldots$, $V^{(n-1)}$ les arrels de $G_0(X)$. El grup de Galois $\mathrm{Gal}(f)$ ve donat per:

$$V \mapsto V^{(i)} \in K(V)$$

Són els automorfismes de $K(V)$. Galois s'ho mira com una matriu $n \times m$:

$$\begin{array}{llll}
(V) & \phi(V) & \phi_1(V) & \ldots \quad \phi_{m-1}(V) \\
(V') & \phi(V') & \phi_1(V') & \ldots \quad \phi_{m-1}(V') \\
(V'') & \phi(V'') & \phi_1(V'') & \ldots \quad \phi_{m-1}(V'') \\
 & & \ldots & \\
(V^{(n-1)}) & \phi(V^{(n-1)}) & \phi_1(V^{(n-1)}) & \ldots \quad \phi_{m-1}(V^{(n-1)})
\end{array}$$

Premier Mémoir: Proposició 1

Proposició 1

Donat un polinomi $f \in K[x]$ amb arrels $\alpha_1, \ldots, \alpha_m$, sempre existirà un grup de permutacions de les arrels tal que:

- *Si $F(\alpha_1, \ldots, \alpha_m) \in K$, per cert $F \in K[x_1, \ldots, x_m]$, aleshores $F(\alpha_1, \ldots, \alpha_m) = F^\sigma(\alpha_1, \ldots, \alpha_m)$ per a tota permutació del grup;*
- *i recíprocament, si $F(\alpha_1, \ldots, \alpha_m) = F^\sigma(\alpha_1, \ldots, \alpha_m)$ per tota permutació del grup, aleshores $F(\alpha_1, \ldots, \alpha_m) \in K$.*

En d'altres paraules, $K(\alpha_1, \ldots, \alpha_m)^{\mathrm{Gal}(f)} = K$.

Premier Mémoir: Proposició 1

Prova. En virtut del Lema 3 sabem que $K(\alpha_1, \ldots, \alpha_m) = K(V)$ i les permutacions corresponen a $V \mapsto V^{(i)}$, on V, V', V'', $\ldots$, $V^{(n-1)}$ són les arrels de $G_0(X)$.

De manera canònica, escrivim $F(\alpha_1, \ldots, \alpha_m) = \phi(V)$, on $\phi \in K[X]$ és un polinomi de grau $\leq n-1$.

Si $F(\alpha_1, \ldots, \alpha_m) = \phi(V) \in K$, vol dir que ϕ és de grau zero, i aleshores $\phi(V^{(i)})$ dóna el mateix valor per a tot i.

Recíprocament, si tots els $\phi(V^{(i)})$ donen el mateix valor aleshores

$$\phi(V) = \frac{1}{n} \sum_{i=0}^{n-1} \phi(V^{(i)}).$$

I clarament pertany a K doncs és una expressió simètrica en els $V^{(i)}$.