Pub. Mat. UAB
Vol. 30 nº 2-3 Des. 1986

SOBRE EL TEOREMA D'IRREDUCTIBILITAT DE HILBERT

Núria Vila

Aquesta nota té per objectiu presentar una demostració simplificada del teorema d'irreductibilitat de Hilbert.

Són moltes les versions i demostracions d'aquest cèlebre teorema: des de l'original de Hilbert i la de Dörge (cf. [4], [1]) emprant el llenguatge i tècniques de l'època; les de Lang, Fried i Serre (cf. [5], [2], [8]), utilitzant tècniques de geometria algebraica; fins a les de Roquette i Weissauer (cf. [7], [9]) fent servir tècniques d'anàlisi no estàndard.

La demostració que presento és elemental i inspirada, bàsicament, en les versions donades a [4], [1], [5] i [8].

Teorema d'irreductibilitat (Hilbert). Sigui $f(T,X) \in Z[T,X]$ un polinomi irreductible a $Q[T,X]$. Existeixen infinits valors de T, $t \in Z$, tals que el polinomi substituït $f(t,X) \in Z[X]$ és irreductible a $Q[X]$.

Demostració. Sense restricció, podem suposar que $f(T,X)$ és mónic en la variable X. En efecte, si $f(T,X) = a_0(T)\, X^n + a_1(T)\, X^{n-1} + \ldots + a_n(T)$, el canvi de variables $X = Y/a_0(T)$ dóna $f(T,X) = g(T,Y)/a_0(T)^{n-1}$, on $g(T,Y) \in Z[T,Y]$ és mónic en Y i irreductible a $Q[T,Y]$. És clar aleshores que, per a tot $t \in Z$ tal que $a_0(t) \neq 0$, si $g(t,Y)$ és irreductible a $Q[Y]$, aleshores $f(t,X)$ és irreductible a $Q[X]$.

Sigui $f(T,X) = X^n + a_1(T)\, X^{n-1} + \ldots + a_n(T) \in Z[T,X]$ irreductible a $Q[T,X]$. Siguin $\theta_1, \ldots, \theta_n$ les arrels de $f(T,X)$ en una clausura algebraica $\overline{Q(T)}$ de $Q(T)$. Si $t \in Z$,

siguin $\theta_{1,t}, \ldots, \theta_{n,t}$ les arrels del polinomi $f(t,X)$ en una clausura algebraica $\overline{Q}$ de Q. És clar que els $\theta_{i,t}$, $1 \le i \le n$, són enters sobre Z.

Sigui $t \in Z$, considerem l'homomorfisme d'anells especialitzar a t, $s_t : Q[T] \longrightarrow Q$, $s_t(p(T)) = p(t)$. Aquest homomorfisme s'estén a un homomorfisme d'anells

$$s_t : Q[T, \theta_1, \ldots, \theta_n] \longrightarrow Q[\theta_{1,t}, \ldots, \theta_{n,t}],$$

determinat a menys de permutacions; sigui $s_t(\theta_i) = \theta_{i,t}$, $1 \le i \le n$.

D'altra banda, si $h(T,X) \in \overline{Q(T)}[X]$ és un factor de $f(T,X)$ a $\overline{Q(T)}[X]$, clarament

$$h(T,X) = \prod_{j=1}^{r} (X - \theta_{i_j}) = X^r + b_{r-1} X^{r-1} + \ldots + b_0 ,$$

on els b_i's, $0 \le i \le r-1$, són funcions simètriques elementals en $\theta_{i_1}, \ldots, \theta_{i_r}$. Donat que $f(T,X)$ és irreductible, per a cada factorització de $f(T,X)$ a $\overline{Q(T)}[X]$ hi ha almenys un coeficient $b \in \overline{Q(T)}$ tal que $b \notin Q(T)$. Sigui B el conjunt format per un coeficient $b \in \overline{Q(T)} \setminus Q(T)$ per a cada factorització de $f(T,X)$ a $\overline{Q(T)}[X]$.

Sigui $t \in Z$; si $f(t,X)$ redueix a $Q[X]$, aleshores existeix un $b \in B$ tal que $s_t(b) \in Q$. De la integritat sobre Z de $\theta_{i,t} = s_t(\theta_i)$ es té que $s_t(b) \in Z$. Així doncs, si per a tot $b \in B$, $s_t(b) \notin Z$, el polimoni $f(t,X)$ és irreductible a $Q[X]$.

Sigui $b \in B$; designem per $S_b = \{ t \in Z : \rho < t, \ s_t(b) \in Z \}$ i per $s(N) = \max_{b \in B} \# (S_b \cap [1,N])$. Només cal provar que existeix δ, $0 \le \delta < 1$, tal que $s(N) = O(N^{\delta})$. En efecte, sigui $I = \{t \in Z : \rho < t, \ f(t,X)$ és irreductible a $Q[X]\}$, ja hem vist que $I \supset \{ t \in Z : \rho < t \} \setminus (\cup_{b \in B} S_b)$ i aleshores tindrem que

$$i(N) = \# (I \cap [1,N]) \ge N (1 - c N^{\delta - 1})$$

on $c > 0$ és una constant. Per tant $i(N)$ no estarà acotat, com es vol demostrar.

Considerem $C((1/T))_{conv}$ el cos de les sèries de Laurent en $1/T$ amb part principal finita convergents en un entorn del infinit. Pel teorema de Puiseux (cf. [3], Th. 8.14) es té que $\overline{C((T^{-1}))_{conv}} = \varinjlim C((T^{-1/n}))_{conv}$. Donat que

$b \in \overline{Q(T)} \subset \overline{C((T^{-1}))_{conv}}$, sigui $b = b(T) = \sum_{v=k}^{-\infty} c_v T^{v/n}$. Podem suposar que els $c_v \in \mathbf{R}$, per a tot v; en efecte si c_{v_0} és el primer coeficient tal que $c_{v_0} \in C \setminus \mathbf{R}$, aleshores, per a tot $t \in \mathbf{R}$ suficientment gran $b(t)$ és complex, car el terme $c_{v_0} t^{v_0/n}$ és dominant. També podem suposar que $b(T)$ no és un polinomi en T, ja que hem escollit $b \notin Q[T]$. Aleshores ens podem reduir a demostrar el següent:

Lema. Sigui $\varphi(T) = \sum_{v=k}^{-\infty} a_v T^{v/n}$, $a_v \in \mathbf{R}$, una sèrie de Laurent convergent per a $t \geq \rho > 0$. Suposem que $\varphi(T) \notin \mathbf{R}[T]$. Sigui $S_\varphi = \{t \in \mathbf{Z} : t \geq \rho \text{ i } \varphi(t) \in \mathbf{Z}\}$ i $s_\varphi(N) = \#(S_\varphi \cap [1,N])$. Existeix un δ, $0 < \delta < 1$ tal que $s_\varphi(N) = O(N^\delta)$.

Demostració (Serre [8]): Existeix un enter $m \geq 1$ tal que

$$\varphi^{(m-1)}(T) = \sum_{v=-\mu}^{-\infty} c_v T^{v/n} \quad , \quad \mu > 0, \quad c_{-\mu} \neq 0.$$

Provarem que m punts de S_φ no poden estar massa aprop. La idea és la següent: per exemple, si $m = 2$, siguin $t_1, t_2 \in S_\varphi$ suficientment grans, donat que la corba $\varphi(T)$ té una tangent amb pendent tendint a zero per t gran, la distància de t_1 a t_2 és gran, car $|\varphi(t_1) - \varphi(t_2)| \geq 1$. En general, siguin $\rho < t_1 < \ldots < t_m$ tals que $\varphi(t_i) = y_i \in Z$, $1 \leq i \leq m$. Sigui $P(T)$ el polinomi d'interpolació de Lagrange de grau $m-1$ tal que $P(t_i) = y_i$, $1 \leq i \leq m$. És a dir

$$P(T) = \sum_{i=1}^{m} \left(y_i \prod_{\substack{1 \leq j \leq m \\ i \neq j}} (T - t_j) \Big/ \prod_{\substack{1 \leq j \leq m \\ i \neq j}} (t_i - t_j) \right).$$

És clar que $\varphi - P$ s'anul·la a $t_1, \ldots, t_m$. Pel teorema de Rolle, existeix $\xi \in (t_1, t_m)$ tal que $\varphi^{(m-1)}(\xi) = P^{(m-1)}(\xi)$. Ara bé, $P^{(m-1)}(T) = (m-1)! \sum_{i=1}^{m} y_i \Big/ \prod_{\substack{1 \leq j \leq m \\ i \neq j}} (t_i - t_j)$, per tant

$|P^{(m-1)}(T)| > r^{-m(m-1)/2}$, on $r = t_m - t_1$. D'altra banda, si t_1 és prou gran tenim:

$$| \varphi^{(m-1)}(\xi) | \leq c_1 t_1^{-\mu/n}$$

És a dir, $c_1 t_1^{-\mu/n} r^{m(m-1)/2} > 1$. Per tant, existeixen dues constants, $\alpha > 0$, $c > 0$, tals que $r > c t^{\alpha}_1$. Dit d'una altra manera, en l'interval $[t, t + c t^{\alpha}]$ hi ha com a màxim m-1 enters de S_φ, si t és suficientment gran.

Sigui N un valor suficientment gran. Donat un δ, $0 < \delta < 1$, considerem la partició de l'interval [1,N] donada per $[1,N^{\delta}] \cup [N^{\delta}, N]$. Clarament podem suposar $c N^{\alpha} > 1$. Sigui $0 \leq k < \alpha$ tal que $N^k > c^{-1}$. Dividint l'interval $[N^{\delta}, N]$ en $[N^{k+1-\alpha\delta}] + 1$ parts iguals, cadascuna d'aquestes parts té longitud més petita que $c N^{\alpha\delta}$. Per tant, en cadascun d'aquests subintervals hi ha O(1) elements de S_φ. Aleshores, $s_\varphi(N) = O([N^{\delta}] + [N^{k+1-\alpha\delta}] + 1)$, i si prenem $\delta = (k+1)/(\alpha+1)$, obtenim que $s_\varphi(N) = O(N^{\delta})$.

La conseqüència més important del teorema d'irreductibilitat de Hilbert ve donada pel següent corol.lari (per a la demostració vegeu [6]).

Corol.lari. Existeixen infinits valors de T, $t \in Z$ tals que el grup de Galois de f(T,X) sobre Q(T) és isomorf al grup de Galois de f(t,X) sobre Q.

Aplicacions

1. Hilbert (cf. [4]), com aplicació d'aquest resultat, prova que el grup alternat, A_n, es realitza com a grup de Galois sobre Q. Per això, construeix, per a tot n, polinomis sobre Q(T) amb grup de Galois A_n.

   Val a dir que un error en un signe en el treball original (J. Crelle 110), apareix corregit a les obres completes. Amb les notacions de [6] els polinomis correctes són:

$$F = \begin{cases} f + (-1)^{n/2} T^2, & \text{si } n \text{ parell} \\ f + ((-1)^{(n-1)/2} T^2 - f'(a)) X, & \text{si } n \text{ imparell.} \end{cases}$$

2. Serre (cf. [8]) demostra que els grups GL(2,n), per a tot n, es realitzen com a grup de Galois sobre Q. Sobre Q(T), considera la corba el·líptica definida per

$$Y^2 + XY = X^3 - \frac{36}{T-1728} X - \frac{1}{T-1728},$$

d'invariant modular j = T. Sigui $E_n = \{ (x_1, y_1), \ldots, (x_{n^2}, y_{n^2}) \}$ el conjunt dels seus punts de n torsió i $N_n = Q(T) \{x_i, y_i\}_{1 \le i \le n^2}$, el cos obtingut al adjuntar-los. En aquest cas $G(N_n / Q(T)) = GL(2,n)$. Com a conseqüència GL(2,n), per a tot n, és grup de Galois sobre Q.

Referències

1. K. Dörge: Zum Hilbertschen Irreduzibilitätssatz, Math. Ann. 95 (1926), 84-97.

2. M. Fried: On Hilbert irreducibility theorem, J. Number Theory 6 (1974), 211-231.

3. O. Forster: Lectures on Riemann surfaces, Grad. Text in Math. Springer 1980.

4. D. Hilbert: Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, J. reine und angew. Math. 110 (1892), 104-129. Gesammelte Abhandlungen, 265-286.

5. S. Lang: Diophantine Geometry, Interscience tracs. New York 1966.

6. E. Nart, N. Vila: Sobre l'existència d'equacions que realitzen S_n i A_n com a grup de Galois d'un cos de números, Pub. Mat. U.A.B. 13 (1979), 79-87.

7. P. Roquette: Nonstandard Aspects of Hilbert's irreducibility Theorem, Lect. Notes in Math. 498 (1975), 231-275.

8. J. P. Serre: Autour du theoreme de Mordell-Weil II, Cours au College de France 1980.

9. R. Weissauer: Der Hilbertsche irreduzibilitätssatz, J. reine und angew. Math. 334 (1982), 203-220.

Rebut el dia 12 de Maig de 1986

Departament d'Algebra i Fonaments
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007-BARCELONA
ESPANYA