Pub. Mat. UAB
Nº 13, Juliol 1979

SOBRE L'EXISTÈNCIA D'EQUACIONS QUE REALITZEN S_n I A_n COM A GRUPS DE GALOIS D'UN COS DE NÚMEROS.

E.Nart i N.Vila
Secció de Matemàtiques de la Universidad Autònoma de Barcelona

El problema invers de la teoria de Galois consisteix en determinar l'existència d'extensions de Galois d'un cos donat amb grup de Galois un grup finit donat.

Hilbert,a l'any 1892, al mateix treball on demostra el seu teorema d'irreduïbilitat [3], resol el problema per als cossos de números i per als grups simètric S_n i alternat A_n, per a tot $n \geq 1$.

El mètode de Hilbert consisteix en construir un polinomi amb coeficients a una extensió $K = k(T_1,\ldots,T_r)$ purament transcendent del cos de números donat k, que resolgui el problema sobre K i provar després que existeixen substitucions $T_i = t_i$, $i=1,..,r$ per elements de k que fan que el polinomi amb coeficients a k que així s'obté continui complint que el seu grup de Galois (ara sobre k) és el desitjat.

En el cas del grup simètric S_n, l'equació general de grau n ja resol el problema. En el cas del grup alternat A_n, Hilbert construeix les equacions explícitament i per demostrar que resolen el problema a K es basa en un article

de Hurwitz [4], on per mètodes purament analítics s'estudien condicions perquè el grup de monodromia de la superfície de Riemann associada a aquestes equacions, (que és isomorf de manera natural al grup de Galois que s'està tractant (vegis [8],pàg.101)) sigui el grup alternat A_n.

En aquesta nota presentem aquests resultats actualitzant les demostracions i tot el llenguatge en general, fent-ho de la manera més algebraica possible.

Donat un cos M i un polinomi $h \in M[X]$ denotarem per $G_M(h)$ el grup de Galois de h sobre M.

En primer lloc recordem el teorema d'irreduïbilitat de Hilbert (per la demostració vegis [3] o bé [2]).

Teorema (d'irreduïbilitat de Hilbert) 1. Sigui k un cos de números i $F \in k[T_1,..,T_r;X_1,..,X_s]$, $r,s \geq 1$ un polinomi irreduïble. Aleshores existeixen infinites r-tuples $(t_1,..,t_r) \in \mathbb{Z}^r$ tals que el polinomi $F(t_1,..,t_r;X_1,..,X_s) \in k[X_1,..,X_s]$ és encara irreduïble. &&

Veiem a continuació que aquest teorema és l'eina clau que permet traslladar el problema a una extensió purament transcendent del cos donat.

Corol.lari 2. Sigui k un cos de números i $K = k(T_1,..,T_r)$, $r \geq 1$, una extensió purament transcendent de k. Donat un polinomi $F \in K[X]$, existeixen infinites r-tuples $t=(t_1,..,t_r) \in \mathbb{Z}^r$ tals que el polinomi $F_t(X) := F(t_1,..,t_r;X)$ de $k[X]$ satisfà

$G_K(F) \simeq G_k(F_t)$.

Demostració.

Sigui N el cos de descomposició de F sobre K, sigui $A = k[T_1,..,T_r]$ i B la clausura entera de A dins N. Siguin $b \in B$ un element tal que $N=K(b)$ i $H \in A[X]$ el polinomi minimal de b sobre K.

Pel teorema d'irreduïbilitat podem prendre una r-tupla $t=(t_1,..,t_r) \in \mathbb{Z}^r$ tal que el polinomi $H_t(X) \in k[X]$ sigui irreduïble.

Considerem l'ideal primer de A $\mathfrak{p} = (T_1-t_1,..,T_r-t_r)$ i siguin e,f,g l'índex de ramificació, grau residual i número d'ideals primers de B sobre $\mathfrak{p}$ a N/K respectivament.

Sigui $\mathfrak{P}$ un ideal primer de B sobre $\mathfrak{p}$ i siguin $D_{\mathfrak{P}}, I_{\mathfrak{P}} \subset G_K(F)$ els grups de descomposició i d'inèrcia corresponents. Siguin $\bar{K}=A/\mathfrak{p}$, $\bar{N}=B/\mathfrak{P}$ els respectius cossos residuals. Clarament $\bar{K}=k$, per tant el cos $\bar{K}$ té característica 0 i l'extensió $\bar{N}/\bar{K}$ és separable. Es té doncs que $\bar{N}/\bar{K}$ és de Galois i $G(\bar{N}/\bar{K}) \simeq D_{\mathfrak{P}}/I_{\mathfrak{P}}$ (vegis [7],prop.20,Cap.I).

Com que $H \equiv H_t$ (mòd.$\mathfrak{p}$) es té que H és irreduïble mòdul $\mathfrak{p}$, per tant $f \geq n$, on $n=[N:K]$. De la relació efg=n s'obté que f=n i e=g=1, d'on $D_{\mathfrak{P}} = G(N/K)$ i $I_{\mathfrak{P}}=1$. Per tant:

$$G_K(F) = G(N/K) \simeq G(\bar{N}/\bar{K}) = G_k(F_t). \qquad \&\&$$

Aplicant aquest resultat a l'equació general de grau n s'obté el següent:

Teorema 3. Sobre qualsevol cos de números existeixen infinites extensions de Galois de grup de Galois isomorf a S_n. &&

Per tenir el mateix resultat per al grup alternat A_n s'ha de construir un polinomi de $K[X]$, K purament transcendent sobre el cos de números donat k, de grup de Galois A_n sobre K.

La idea de Hilbert consisteix en construir un polinomi $F \in \mathbb{Q}(T)[X]$ que satisfaci les dues condicions:

$$(1) \qquad \sqrt{D(F)} \in \mathbb{Q}(T),$$

$$(2) \qquad G_{\mathbb{C}(T)}(F) \simeq A_n,$$

on D(F) és el discriminant de F, és a dir $D(F) = \prod_{i<j} (x_i - x_j)^2$, sent $x_1,..,x_n$ les arrels de F a una clausura algebraica de $\mathbb{Q}(T)$.

La condició (1) és equivalent a que $G_{k(T)}(F) \subset A_n$, degut a que una permutació de les x_i's deixa invariant $\sqrt{D(F)} = \prod_{i<j} (x_i - x_j)$ si i només si és una permutació parella.

La condició (2) ens dóna l'altra inclusió ja que trivialment $G_{\mathbb{C}(T)}(F) \subset G_{k(T)}(F)$.

La construcció d'aquest polinomi F varia segons la paritat de n.

Cas n parell

Siguin $r=(n-2)/2$ $(n>2)$ i $a_1,..,a_r$ enters positius diferents entre si. Sigui $f \in \mathbb{Q}[X]$ l'únic polinomi satisfent $f(0)=0$ i tenint per derivada:

$$f' = n\,X\,(X-a_1)^2 \cdot \ldots \cdot (X-a_r)^2.$$

Per $x>0$, $f'(x)$ és positiu, és a dir que f és estrictament

creixent i per tant es té:

$$f(a_i)\neq 0, \text{ per } i=1,..,r; \qquad f(a_i)\neq f(a_j), \text{ per } i\neq j.$$

Considerem el polinomi $F=f+T^2 \in \mathbb{Q}(T)[X]$. Utilitzant el conegut fet de que la resultant de dos polinomis es pot expressar en termes del producte dels valors que pren un qualsevol d'ells a les arrels de l'altre (vegis [9],sec.28) es té en aquest cas:

$$D(F) = R(F,F') = n^n F(0)\cdot F(a_1)^2\cdot\ldots\cdot F(a_r)^2,$$

és a dir,

$$D(F) = n^n T^2 \prod_{i=1}^{r} (T^2+f(a_i))^2,$$

i per tant $\sqrt{D(F)}\in \mathbb{Q}(T)$.

Així doncs, el polinomi F satisfà (1). Per veure que satisfà (2) utilitzarem el següent lema:

Lema 4. Sigui G un subgrup transitiu de A_n, és a dir, un subgrup de A_n que opera transitivament en el conjunt d'índexs $X=\{1,2,..,n\}$ sobre el qual actua A_n. Si G està generat per 3-cicles, aleshores $G=A_n$.

Demostració.

Si $Y\subset X$ denotem per A(Y) el subgrup de A_n de les permutacions que deixen els elements de Y-X fixos.

Si $(1,2,3)\in G$ és un dels generadors $A(\{1,2,3\})\subset G$. Així doncs, existeix un subconjunt $Y\subset X$ contenint al menys tres elements tal que $A(Y)\subset G$. Si $Y=X$ ja hem acabat. Si $Y\subsetneq X$ existeix un 3-cicle $(i,j,k)\in G$ tal que $i\in Y$, $j\notin Y$, ja que en cas contrari, com que G està generat per 3-cicles permutaria

els elements de Y entre ells mateixos i els de X-Y també entre ells, en contra de la transitivitat.

Siguin $r,s\in Y$, $r\neq i,k$, $s\neq i,k$; tenim la relació:

$$(i,r,s)(i,j,k)(i,s,r) = (r,j,k),$$

i per tant $(r,j,k)\in G$, $\forall\ r\in Y-\{k\}$. D'aquí deduïm que $A(Y\cup\{j,k\})\subset G$ ja que els elements (r,j,k) variant $r\in Y-\{k\}$ generen $A(Y\cup\{j,k\})$. Repetint l'argument es té que $G=A(X)$. &&

Veiem finalment que $G_{\mathbb{C}(T)}(F) \simeq A_n$.

Denotem $L=\mathbb{C}(T)$, $A=\mathbb{C}[T]$, $G=G_L(F)$. Es té $G\subset G_{k(T)}(F)\subset A_n$. Sigui b una arrel de F a una clausura algebraica Ω de L i sigui $N\subset\Omega$ el cos de descomposició de F.

Proposició 5. Siguin B,C la clausura entera de A dins L(b), N respectivament. Aleshores els grups d'inèrcia de l'extensió N/L relatius als ideals primers de C són o bé trivials o bé generats per un 3-cicle.

Demostració.

Considerem els següents ideals primers de A:

$$\mathfrak{p}_0 = (T);\quad \mathfrak{p}_j = (T+\sqrt{-f(a_j)}),\quad \mathfrak{p}_{j+r} = (T-\sqrt{-f(a_j)}),\ j=1,..,r.$$

Aquests són tots els ideals primers de A que divideixen el discriminant de F, per tant són els únics ideals primers de A que poden ramificar a B i per tant (vegis [6],pàg.217) són els únics que poden ramificar a C.

Per tot ideal primer $\mathfrak{p}$ de A, el cos residual $A/\mathfrak{p}$ és isomorf a $\mathbb{C}$ i per tant els graus residuals són sempre iguals a 1.

Per $i\neq 0$, la imatge de F a $A/\mathfrak{p}_i[X]$ és el polinomi $f-f(a_i)$ que té a_i com arrel triple i totes les altres simples, ja que per a tot $a_j\neq a_i$ és $f(a_j)-f(a_i)\neq 0$ i també és $f(0)-f(a_i)\neq 0$.

Per $i=0$, la imatge de F a $A/\mathfrak{p}_0[X]$ és f, que té $x=0$ com arrel doble i totes les altres simples.

Pel lema de Hensel ([1],Cap.4,sec.3,t.2) tenim que F descomposa al completat de L respecte de $\mathfrak{p}_i$, que el denotarem $L_{\mathfrak{p}_i}$, de la manera següent:

per $i\neq 0$, $F=g_{i,0}\cdot\ldots\cdot g_{i,n-3}$, $gr(g_{i,0})=3$, $gr(g_{i,j})=1$ per $j>0$,

per $i=0$, $F=h_0\cdot\ldots\cdot h_{n-2}$, $gr(h_0)=2$, $gr(h_j)=1$ per $j>0$.

Siguin $\mathfrak{p}$ un qualsevol dels $\mathfrak{p}_i$'s per $i=0,1,..,2r$ i $\mathfrak{P}$ un ideal primer de C sobre $\mathfrak{p}$. Siguin $b_1,\ldots,b_n$ les arrels de F a una clausura algebraica de $L_{\mathfrak{p}}$. Aleshores:

$$N_{\mathfrak{P}}\simeq NL_{\mathfrak{p}}\simeq L_{\mathfrak{p}}(b_1,\ldots,b_n).$$ (vegis [7],Cap.II,sec.3).

Com que en el nostre cas $b_i\in L$ per $i\geq 4$, es té $N_{\mathfrak{P}}\simeq L_{\mathfrak{p}}(b_1,b_2,b_3)$, per tant $I_{\mathfrak{P}}\subset S_3$ i com que d'altra banda $I_{\mathfrak{P}}\subset G\subset A_n$, tenim que $I_{\mathfrak{P}}\subset A_3$ i per tant és o bé trivial o bé generat per un 3-cicle. &&

Sigui I el subgrup de G generat per tots els grups d'inèrcia i M el cos fix per I. Clarament M és la màxima subextensió n0-ramificada de N/L. Ara bé, la fórmula del gènere de Hurwitz ([5],pàg.25):

$$2g_M-2 = [M:L](2g_L-2) + \sum_{\mathfrak{P}} (e_{\mathfrak{P}}-1)$$

on g_M i g_L són els gèneres de M i L respectivament, en ... que $L=\mathbb{C}(T)$ no admet extensions no-ramificades. Per tant $M=L$, és a dir $I=G$. En consequència G està generat per 3-cicles.

D'altra banda, pensant $F = T^2+f$ com un element de $\mathbb{C}[X][T]$ es veu clar que F és irreduïble ja que -f no és un quadrat a $\mathbb{C}[X]$. En consequència G és transitiu. Aplicant el lema 4, s'obté que $G=A_n$.

Cas n imparell

Siguin $r=(n-1)/2$, $a_1,..,a_r$ enters positius diferents entre si i $a = -1/2 \sum_{i=1}^{r} (1/a_i)^2$. Considerem el polinomi:

$$g = (n-1)(X-a) \prod_{i=1}^{r} (X-a_i)^2.$$

El coeficient de X és zero i això és condició necessària i suficient perquè existeixi un polinomi $f\in\mathbb{Q}[X]$ de grau n satisfent $g = Xf'-f$. Doncs bé, si considerem $F=f+(T^2-f'(a))X$ utilitzant la mateixa fórmula de la resultant del cas parell i tenint en compte que $R(u-Xv,v)=R(u,v)$ s'obté que:

$$D(F) = (n-1)^{n-1} T^2 \prod_{i=1}^{r} (T^2+f'(a_i)-f'(a))^2.$$

Per tant F satisfà (1). I que satisfà $G_{\mathbb{C}(T)}(F)\simeq A_n$ es demostra de manera idèntica al cas n parell.

Hem construit equacions que realitzen A_n com a grup de Galois sobre $\mathbb{Q}(T)$ per a tot $n\geq 1$. Aplicant el corol.lari

2 queda provat el següent:

Teorema 6. Sobre qualsevol cos de números existeixen infinites extensions de Galois de grup de Galois isomorf a A_n.&&

REFERÈNCIES

[1] Borevich-Shafarevich "Number Theory" Ac.Press 1966.

[2] M.Fried "On Hilbert's irreducibility theorem" J.Number Theory 6,211-231 (1974).

[3] D.Hilbert "Ueber die irreduzibilität ganzer rationalen Funktionen mit ganzzahligen Coefficienten" J.Reine und angew. Math. 110 (1892), Sn.104-129.

[4] A.Hurwitz "Ueber Riemann'sche Flächen mit gegebenen Verzweigungpunkten" Math.Ann. Bd.39 (1891) S.1.

[5] S.Lang "Introduction to Algebraic and Abelian Functions" Addison Wesley 1972.

[6] P.Ribenboim "Algebraic Numbers" Wiley Interscience, New York 1972.

[7] J.P.Serre "Corps Locaux" Hermann, Paris 1968.

[8] C.L.Siegel "Topics in Complex Function Theory" Vol.1 John Wiley & Sons, Inc. 1969.

[9] B.L.Van der Waerden "Modern Algebra" Vol.1 Ungar, New York 1953.