Pub. Mat. UAB
Vol. 27 Nº 3 Des. 1983

SOBRE LA REALITZACIÓ DE LES EXTENSIONS CENTRALS DEL GRUP ALTERNAT COM A GRUP DE GALOIS SOBRE EL COS DELS RACIONALS*

Núria Vila i Oliva

ÍNDEX

*Memòria presentada a la Secció de Matemàtiques de la Universitat Autònoma de Barcelona per optar al títol de Doctor en Ciències Matemàtiques, realitzada sota la direcció de la Doctora Pilar Bayer i Isant.

Introducció

L'anomenat problema invers de la teoria de Galois pregunta si, donat un grup finit G, existeix una extensió galoisiana N del cos dels racionals Q que tingui G per grup de Galois.

Hilbert (1892) prova que els grups simètric i alternat es realitzen com a grup de Galois sobre Q. Scholz (1937), Reichard (1937) i Šafarevič (1947), en una sèrie de treballs, resolen el problema per als p-grups. Aquests esforços tenen el seu punt culminant en el célebre resultat de Šafarevič (1954) segons el qual tot grup resoluble es realitza com a grup de Galois sobre Q. Neukirch ha clarificat els mètodes de Šafarevič, donant recentment (1979) una demostració molt entenedora en el cas resoluble d'ordre imparell.

Després del resultat de Šafarevič, hom es concentrà en la realització de certes famílies de grups no resolubles. Shimura (1966) inicia el cas dels grups GL(2,p), resolent el problema invers per als primers p, $7 \leqslant p \leqslant 97$ i Serre (1972) el resol completament per a tot valor de p primer. Macbeath (1969) demostra que els grups PGL(2,n) es realitzen tots com a grup de Galois sobre Q, generalitzant un resultat de Weber (1908) per a n primer. Shih (1974) prova que els grups PSL(2,p) es realitzen quan $p \neq 2$ és un primer tal que 2,3 ó 7 no és un residu quadràtic mòdul p. Sonn(1980) realitza $SL(2,5)=\hat{A}_5$ sobre Q com un pas previ que li permet assegurar que tot grup de Frobenius és grup de Galois sobre Q. Final-

ment Matzat, a la seva tesi doctoral (1980), dóna equacions explícites sobre $\mathbb{Q}(T)$ amb grups de Galois: $P\Gamma L(2,8)$, $P\Gamma L(2,9)$, $PSL(2,8)$, $PGL(2,9)$. Per al primer dels grups esporàdics simples, el grup de Mathieu M_{11}, hom disposa únicament d'una realització sobre $\mathbb{Q}(\sqrt{-11})$, deguda també a Matzat.

En aquesta memòria tractem el problema de la realització de les extensions centrals del grup alternat A_n com a grup de Galois. Aquestes són les extensions més "tractables" dels grups simples (no abelians) més "senzills". Provem que tota extensió central de A_n es realitza com a grup de Galois sobre $\mathbb{Q}(i)$. Sobre $\mathbb{Q}$, demostrem que el problema té resposta afirmativa per a gairabé la meitat dels valors de n.

La memòria està subdividida en cinc capítols. En el capítol I es revisen els conceptes de teoría de grups necessaris pel tractament del problema; en particular estudiem l'extensió central universal $\hat{A}_n$ del grup alternat, de la que donem dues presentacions.

En el capítol II es dóna un teorema de reducció que permet assegurar que n'hi ha prou en realitzar $\hat{A}_n$ per tenir resolt el problema de realitzar tota extensió central de A_n com a grup de Galois. La realització de $\hat{A}_n$ l'abordem com un problema d'immersió galoisiana. Donem també un criteri que permet fer una primera "tria" d'equacions que realitzen A_n, a fi que el problema d'immersió esmentat tingui solució.

En el capítol III presentem un resultat molt recent de J. P. Serre, comunicat a Martinet, encara no publicat. En el nostre context, Serre calcula l'obstrucció que presenta el problema d'immersió a $\hat{A}_n$ en termes d'un invariant de Hasse-Witt. Com una primera aplicació, utilitzant les realitzacions de A_n sobre Q donades pels polinomis que vàrem construir a [17], donem una resposta afirmativa al problema per a $n \equiv 0$ (mòd. 8), i $n \equiv 2$ (mòd. 8) i suma de dos quadrats.

En el capítol IV es tracta el problema de la Q-definició d'extensions galoisianas de $\bar{Q}(T)$. Provem que tot grup complet que admeti "bones" presentacions és grup de Galois sobre Q(T) i, per tant, sobre Q. Donem també un mètode per obtenir equacions sobre Q(T) amb grup de Galois grups complets per als que hom disposa d'una "bona" presentació. En un apèndix demostrem que hi ha extensions de $\bar{Q}(T)$ amb grup de Galois $\hat{A}_n$ i tals que el polinomi definidor de l'extensió té els coeficients a Q(T).

En el capítol V, utilitzant els mètodes del capítol IV, construïm noves famílies d'equacions que realitzen A_n. L'obstrucció que aquestes equacions presenten al problema d'immersió galoisiana a $\hat{A}_n$ és calculable. Demostrem que és nul.la per a tot valor de n sobre Q(i) i que, sobre Q, és nul.la si $n \equiv 0,1$ (mòd. 8); $n \equiv 2$ (mòd. 8) i n és suma de dos quadrats; $n \equiv 3$ (mòd. 8) i satisfent la propietat (N) (cf. Cap.V, §5). Com a conseqüència queda demostrat que tota extensió central de A_n es realitza com a grup de Galois sobre Q, per als darrers valors de n.

Si un resultat utilitzat es troba a la literatura, en donem una referència explícita.

Finalment, vull expressar el meu agraïment a la Dra. Pilar Bayer per l'estímul i confiança que m'ha donat en tot moment i per la seva valuosa ajuda en la realització d'aquest treball. També voldria agrair al Professor J. P. Serre la seva gentilesa en comunicarme el resultat, ja esmentat, i per l'atenció que m'ha dispensat.

Capítol I. Extensions centrals

Al tractar de realitzar com a grup de Galois totes les extensions centrals del grup alternat o, més generalment, d'un grup perfecte qualsevol, hi ha una extensió central que juga un paper molt destacat: l'extensió central universal. L'objecte d'aquest capítol és estudiar aquesta extensió en el cas del grup alternat.

§1. Extensions centrals. Extensió central universal

Sigui G un grup. Un grup E es diu que és una *extensió central* de G, si existeix una successió exacta de grups

$$1 \to A \to E \xrightarrow{p} G \to 1,$$

tal que la imatge de A a E està continguda en el centre de E.

Una extensió central $\hat{G}$ de G es diu *universal* si, per a tota extensió central E de G, existeix un únic homomorfisme de grups $h:\hat{G} \to E$, tal que el diagrama

$$\begin{array}{ccccccccc} 1 & \to & \ker\pi & \to & \hat{G} & \xrightarrow{\pi} & G & \to & 1 \\ & & & & \downarrow h & & \| \mathrm{id} & & \\ 1 & \to & \ker p & \to & E & \xrightarrow{p} & G & \to & 1 \end{array}$$

és commutatiu.

És clar que si una extensió central universal existeix, és única a menys d'isomorfismes sobre G.

Esmentem, tot seguit, els resultats fonamentals sobre les extensions centrals universals.

Teorema 1.1. ([16], Th. 5.3) Una extensió central E de G és universal si i només si E és perfecte i tota extensió central de E descompon. #

Recordem que un grup es diu perfecte quan coincideix amb el seu commutador.

Teorema 1.2. ([16], Th. 5.7) Un grup G admet una extensió central universal si i només si G és perfecte. #

Remarca. La noció d'extensió central universal va ésser introduïda per primera vegada per Schur ([25], 1904), per als grups finits. Veiem ara com es lliga aquesta noció amb les definicions clàssiques.

S'anomena *grup dels multiplicadors de Schur* de G el grup de cohomologia $H^2(G,C^*)$.

Proposició 1.3. Si G és un grup finit perfecte, l'extensió central universal $\hat{G}$ de G té nucli isomorf al grup dels multiplicadors de Schur de G. A més, $\hat{G}$ és el grup de representacions *(Darstellungsgruppe)* de G.

Demostració. En la demostració del teorema 1.2, ([16], pàg.45) es prova que, escollit un homomorfisme d'un grup lliure F sobre G de nucli R, aleshores

$$\hat{G} = F'/_{[R,F]} \quad \text{i} \quad \ker\pi = R \cap F'/_{[R,F]} ,$$

on F' és el commutador de F i π la projecció induïda per $F/[R,F] \to F/R \simeq G$. D'altra banda, $\ker\pi \simeq H^2(G,C^*)$ per [10], V, 23.5c). Per tant, $\hat{G}$ és el grup de representacions de G, que és únic per ésser G perfecte ([10], V, 23.4, 23.6). #

§2. Extensió central universal del grup alternat: $\hat{A}_n$

El primer que cal determinar per estudiar l'extensió central universal del grup alternat A_n, com s'ha vist a la proposició 1.3, és el grup dels seus multiplicadors. Això ho féu el propi Schur el 1911 ([26]).

Teorema 1.4. ([35], 3, 2.22) El grup dels multiplicadors de Schur de $A_n (n \geqslant 4)$ té ordre 2, si $n \neq 6,7$. Per $n=6$ ó 7 és d'ordre 6. #

D'ara endavant suposarem sempre $n \neq 6,7$. Així doncs, l'extensió central universal $\hat{A}_n$ de A_n és una extensió central de A_n amb nucli $Z/2$.

Teorema 1.5. (Schur). El grup $\hat{A}_n$ està definit pels generadors $c, x_1, \ldots, x_{n-2}$, i les relacions

$$c^2 = x_1^3 = (x_{j-1}x_j)^3 = 1, \qquad 1 < j \leqslant n-2,$$

$$[x_i, c] = 1, \qquad 1 \leqslant i \leqslant n-2,$$

$$x_j^2 = (x_i x_j)^2 = c, \qquad 1 < j \leqslant n-2,\ 1 \leqslant i < j-1.$$

Demostració. Provarem que només hi ha dues extensions de A_n amb nucli $Z/2$: la trivial i la donada pels generadors i relacions del teorema. Aquest quedarà demostrat, car és immediat veure que una extensió trivial no pot ésser universal.

Considerem la presentació de A_n donada per Moore (1897) (cf. [4], pàg. 66), de generadors $s_1, \ldots, s_{n-2}$ i relacions

$$s_1^3 = s_j^2 = (s_{j-1}s_j)^3 = (s_i s_j)^2 = 1, \qquad 1 \leqslant j \leqslant n-2,\ 1 \leqslant i < j-1.$$

Sigui G una extensió de A_n per $Z/2$ donada per la successió exacta,

$$1 \to \mathbb{Z}/2 \xrightarrow{f} G \xrightarrow{g} A_n \to 1.$$

Si $f(\mathbb{Z}/2)=\langle c\rangle \subset G$, és clar que $c^2=1$, $c\in Z(G)$ i $g(c)=1$, on $Z(G)$ denota el centre de G.

D'altra banda, existeix $x_1\in g^{-1}(s_1)$ tal que $x_1^3=1$, ja que si $x_1^3=c$, aleshores $(x_1c)^3 = x_1^3c^3 = 1$ i $x_1c\in g^{-1}(s_1)$. Anàlogament, es prova que existeixen elements $x_j\in G$ tals que

$$x_j\in g^{-1}(s_j) \quad \text{i} \quad (x_{j-1}x_j)^3=1, \quad \text{per a tot } 1<j\leqslant n-2.$$

Per tant, G és el grup generat per $x_1,\dots,x_{n-2}$, c amb primers lligams

$$c^2=x_1^3=(x_{j-1}x_j)^3=1, \qquad 1<j\leqslant n-2,$$

$$x_j^2,(x_ix_j)^2\in\langle c\rangle, \qquad 1<j\leqslant n-2,\ 1\leqslant i<j-1.$$

Vegem que les darreres relacions no poden ésser tan arbitràries. Provem primerament que $x_j^2=x_{j-1}^2$, per a tot $j>2$. En efecte, com que $(x_{j-1}\ x_j)^3=1$, aleshores $x_{j-1}x_jx_{j-1}x_jx_{j-1}=x_j^{-1}$. Elevant al quadrat aquesta expressió,

$$x_{j-1}^4x_j^4x_{j-1}^2=(x_j^{-1})^2.$$

Provem ara que $(x_{i-1}x_j)^2=(x_ix_j)^2$, per a tot $j>3$, $1<i<j-1$. Es satisfan les identitats,

$$x_jx_{i-1}x_ix_j^{-1}=x_{i-1}^{-1}x_j^{-1}x_ix_j^{-1}(x_{i-1}x_j)^2=x_{i-1}^{-1}x_jx_ix_j^{-1}(x_{i-1}x_j)^2x_j^2 =$$

$$=x_{i-1}^{-1}x_i^{-1}x_j^2(x_{i-1}x_j)^2(x_ix_j)^2x_j^2=x_{i-1}^{-1}x_i^{-1}(x_{i-1}x_j)^2(x_ix_j)^2.$$

Elevant al cub, obtenim

$$x_j(x_{i-1}x_i)^3x_j^{-1}=(x_{i-1}^{-1}x_i^{-1})^3(x_{i-1}x_j)^2(x_ix_j)^2.$$

Per tant $(x_{i-1}x_j)^2=(x_ix_j)^2$, per a tot $j>3$, $1<i<j-1$. Finalment elevant al cub l'expressió, $x_jx_1x_j=(x_1x_j)^2x_1^2$, es té que $(x_1x_j)^2=x_j^2$, per a tot $2<j\leqslant n-2$.

Veiem doncs que el grup G, generat per $x_1,\ldots,x_{n-2},c$, satisfà les relacions

$$c^2=x_1^3=(x_{j-1}x_j)^3=1, \qquad 1<j\leqslant n-2$$

$$(x_ix_j)^2=x_j^2=x_{j-1}^2\in\langle c\rangle, \qquad 1\leqslant i<j-1,\ 2<j<n-2.$$

Per tant hi ha dues possibles extensions de A_n per $Z/2$:

$$G_1=Z/2\times A_n \quad \text{i} \quad G_2=\hat{A}_n. \qquad \#$$

§3. Segona presentació de $\hat{A}_n$

Aquest paràgraf està dedicat a donar una presentació de $\hat{A}_n$ amb únicament dos generadors, que serà utilitzada en el capítol IV.

Teorema 1.6. Existeixen elements $x,y,c\in\hat{A}_n$ tals que x,y generen $\hat{A}_n$ i satisfan les relacions:

$$x^3=1,$$

$$(x^{(-1)^{(n-1)r}}y^{-r}xy^r)^2 = c\ , \qquad 1\leqslant r\leqslant [(n-2)/2],$$

$$c^2=[x,c] = [y,c] = 1,$$

$$y^{n-2}= c^{n(n-2)(n-3)(n-7)/8},$$

$$(yx)^n=1, \text{ si és } n \text{ imparell}, \qquad (yx)^{n-1}=1, \text{ si és } n \text{ parell}.$$

Per demostrar aquest teorema, cal determinar l'ordre de

$x_{n-2}\cdots x_2$, $x_{n-2}\cdots x_1$, on $\{x_i\}_{1\leqslant i\leqslant n-2}$ són els generadors de $\hat{A}_n$ satisfent les relacions del teorema 1.5. Per fer això provarem una sèrie de lemes previs, cada un dels quals és de fàcil demostració.

Anotem algunes relacions entre els elements x_i's, deduïdes immediatament de les relacions definidores de $\hat{A}_n$, que convé tenir present, car les utilitzem constantment.

Per $j>2$, $(x_{j-1}x_j)^3=1 \Rightarrow x_{j-1}x_jx_{j-1}=cx_jx_{j-1}x_j$.

Per $j=2$, $(x_1x_2)^3=1 \Rightarrow x_1x_2x_1=x_2x_1^2x_2$, $x_2x_1x_2=cx_1^2x_2x_1^2$.

Per $1<j\leqslant n-2$, $1<i<j-1$, $(x_ix_j)^2=c \Rightarrow x_ix_j=cx_jx_i$, $x_jx_ix_j=x_i$.

Per $2<j\leqslant n-2$, $(x_1x_j)^2=c \Rightarrow x_1x_j=x_jx_1^{-1}$, $x_jx_1x_j=cx_1^{-1}$, $x_1^2x_jx_1^2=x_j$.

En tot el que segueix, k és un enter positiu, $1\leqslant k\leqslant n-2$. Els elements $x_1,\ldots,x_k$ són els k-primers generadors de $\hat{A}_n$ per la presentació del teorema 1.5.

<u>Lema 1.7.</u> Si $k>r\geqslant 2$,

$$(x_k\cdots x_r)(x_k\cdots x_2)=c^{(k-2)(k-r)-1}(x_{k-1}\cdots x_2)(x_k\cdots x_{r+1}).$$

<u>Demostració.</u> Per inducció sobre k. Si $k=r+1$,

$$x_{r+1}x_rx_{r+1}x_r\cdots x_2=x_rx_{r+1}x_{r-1}\cdots x_2=c^{r-2}(x_r\cdots x_2)x_{r+1}.$$

Suposem-ho cert per a $k-1$,

$$(x_k\cdots x_r)(x_k\cdots x_2)=c^{k-r-1}(x_kx_{k-1}x_kx_{k-2}\cdots x_r)(x_{k-1}\cdots x_2)=$$

$$=c^{k-r}x_{k-1}x_kx_{k-1}x_{k-2}\cdots x_r\,x_{k-1}\cdots x_2\ .$$

Per hipòtesi d'inducció,

$$(x_k\cdots x_r)(x_k\cdots x_2)=c^{k-r}x_{k-1}x_k c^{(k-3)(k-r-1)-1}(x_{k-2}\cdots x_2)(x_{k-1}\cdots x_{r+1})$$

$$=c^{(k-2)(k-r)-1}(x_{k-1}\cdots x_2)(x_k\cdots x_{r+1}). \quad \#$$

<u>Lema 1.8.</u> Si $k>r\geqslant 2$,

$$(x_k\cdots x_2)^r=c^{(r-1)((k-2)(2k-r-2)-2)/2}(x_{k-1}\cdots x_2)^{r-1}(x_k\cdots x_{r+1}).$$

<u>Demostració.</u> Per inducció sobre r. El cas r=2 s'ha provat ja en el lema 1.7. Suposem-ho cert per a r-1.

$$(x_k\cdots x_2)^r=c^{(r-2)((k-2)(2k-r-1)-2)/2}(x_{r-1}\cdots x_2)^{r-2}(x_k\cdots x_r)(x_r\cdots x_2).$$

Pel lema 1.7

$$(x_k\cdots x_2)^r=c^{(r-2)((k-2)(2k-r-1)-2)/2}(x_{k-1}\cdots x_2)^{r-2}c^{(k-2)(k-r)-1}(x_{k-1}\cdots x_2)(x_k\cdots x_{r+1})$$

$$=c^{(r-1)((k-2)(2k-r-2)-2)/2}(x_{k-1}\cdots x_2)^{r-1}(x_k\cdots x_{r+1}). \quad \#$$

<u>Proposició 1.9.</u> $(x_k\cdots x_2)^k=c^{k(k-1)(k-3)(k-6)/8}$.

<u>Demostració.</u> Pel lema 1.8,

$$(x_k\cdots x_2)^k=c^{(k-2)((k-2)(2k-k-1)-2)/2}(x_{k-1}\cdots x_2)^{k-2}x_k x_k\cdots x_2$$

$$=c^{(k(k-2)(k-3)+1)/2}(x_{k-1}\cdots x_2)^{k-1}.$$

El resultat s'obté per inducció sobre k. #

<u>Lema 1.10.</u> Si $1<r<k$,

$$x_2x_3\cdots x_r x_{r+1}x_r\cdots x_3x_2=c^{r-1}x_{r+1}x_r\cdots x_3x_2x_3\cdots x_r x_{r+1}.$$

<u>Demostració.</u> Per inducció sobre r. Per r=2 és immediat. Supo-

sem-ho cert per r-1. Aleshores,

$$x_2\cdots x_r x_{r+1} x_r\cdots x_2 = c\ x_2\cdots x_{r-1} x_{r+1} x_r x_{r+1} x_{r-1}\cdots x_2$$

$$= c\ x_{r+1} x_2\cdots x_{r-1} x_r\cdots x_2 x_{r+1} = c^{r-1} x_{r+1} x_r\cdots x_3 x_2 x_3\cdots x_r x_{r+1}. \#$$

<u>Lema 1.11.</u> Si $r \leqslant k$ i k és parell,

$$(x_k\cdots x_1)^r = c^{(r-1)(r-2)/2} (x_k\cdots x_2)^r x_1^{(-1)^{r-1}} x_2\cdots x_r.$$

<u>Demostració.</u> Per inducció sobre r. Si r=2,

$$(x_k\cdots x_1)^2 = x_k\cdots x_2 x_k\cdots x_1 x_2 x_1 = (x_k\cdots x_2)^2 x_1^2 x_2.$$

Suposem-ho cert per r-1. Aleshores,

$$(x_k\cdots x_1)^r = (x_k\cdots x_1)^{r-1} x_k\cdots x_1 = c^{(r-2)(r-3)/2} (x_k\cdots x_2)^{r-1} x_1^{(-1)^{r-2}} x_2\cdots x_{r-1} x_k\cdots x_1.$$

Utilitzant el lema 1.10 obtenim,

$$x_1^{(-1)^{r-2}} x_2\cdots x_{r-1} x_k\cdots x_1 = c^{(k-r)(r-2)} x_1^{(-1)^{r-2}} x_k\cdots x_{r+1} c^{r-2} x_r\cdots x_3 x_2 x_3\cdots x_r x_1$$

$$= c^{(k-r+1)(r-2)} x_1^{(-1)^{r-2}} x_k\cdots x_3 x_2 x_3\cdots x_r x_1$$

$$= c^{(k-r+1)(r-2)} x_k\cdots x_3 x_1^{(-1)^{r-2}} x_2 x_1^{(-1)^{r-2}} x_3\cdots x_r$$

$$= c^{r-2} x_k\cdots x_3 x_2 x_1^{(-1)^{r-1}} x_2\cdots x_r. \quad \#$$

<u>Proposició 1.12.</u> Sigui k parell,

$$(x_k\cdots x_1)^{k+1} = c^{k(k-2)/8}.$$

<u>Demostració.</u> Pel lema 1.11,

$$(x_k\cdots x_1)^k=c^{(k-2)(k-1)/2}(x_k\cdots x_2)^k x_1^2x_2\cdots x_k.$$

Per tant,

$$(x_k\cdots x_1)^{k+1}=c^{(k-2)/2}(x_k\cdots x_2)^k x_1^2x_2\cdots x_kx_k\cdots x_2x_1$$
$$=c^{(k-2)/2}\ c(x_k\cdots x_2)^k,$$

i aplicant la proposició 1.9, obtenim el resultat. #

<u>Lema 1.13.</u> Si $3\leqslant r<k$ i k és imparell,

$$(x_1x_2x_1^2x_3x_2\cdots x_rx_{r-1})(x_k\cdots x_1)=x_k\cdots x_2x_1x_2x_1^2x_3x_2\cdots x_{r+1}x_r.$$

<u>Demostració.</u> És fàcil veure que

$$x_1x_2x_1^2x_k\cdots x_1=x_k\cdots x_2x_1x_2x_1^2x_3x_2.$$

Provem el lema per inducció sobre r. Si $r=3$,

$$x_1x_2x_1^2x_3x_2x_k\cdots x_1=x_1x_2x_1^2x_3x_k\cdots x_4x_2x_3x_2x_1$$
$$=cx_1x_2x_1^2x_3x_k\cdots x_4x_3x_2x_3x_1$$
$$=x_1x_2x_1^2x_k\cdots x_5x_3x_4x_3x_2x_1^2x_3$$
$$=cx_1x_2x_1^2x_k\cdots x_5x_4x_3x_4x_2x_1^2x_3$$
$$=x_1x_2x_1^2x_k\cdots x_2x_1x_4x_3=x_k\cdots x_3x_2x_1x_2x_1^2x_3x_2x_4x_3.$$

Suposem-ho cert per $r-1$. Aleshores,

$$x_1x_2x_1^2x_3x_2\cdots x_rx_{r-1}x_k\cdots x_1=c^{k-r}x_1x_2x_1^2\cdots x_rx_k\cdots x_{r+1}x_{r-1}x_rx_{r-1}\cdots x_2x_1$$

$$=c^{k-r+1}x_1x_2x_1^2\cdots x_rx_k\cdots x_{r+1}x_rx_{r-1}x_r\cdots x_2x_1$$

$$=c^{k}x_1x_2x_1^2\cdots x_rx_k\cdots x_2x_1^2x_r$$

$$=c^{k-r}x_1x_2x_1^2\cdots x_{r-1}x_{r-2}x_k\cdots x_{r+2}x_rx_{r+1}x_r\cdots x_2x_1^2x_r$$

$$=c^{k-r+1}x_1x_2x_1^2\cdots x_{r-1}x_{r-2}x_k\cdots x_{r+2}x_{r+1}x_rx_{r+1}\cdots x_2x_1^2x_r$$

$$=x_1x_2x_1^2\cdots x_{r-1}x_{r-2}x_k\cdots x_2x_1x_{r+1}x_r$$

$$=x_k\cdots x_2x_1x_2x_1^2x_3x_2\cdots x_rx_{r-1}x_{r+1}x_r. \quad \#$$

<u>Lema 1.14.</u> Si $r\leqslant k$ i k és imparell,

$$(x_k\cdots x_1)^r=c(x_k\cdots x_2)^r x_1x_2x_1^2x_3x_2\cdots x_rx_{r-1}.$$

<u>Demostració.</u> Per inducció sobre r. Si $r=2$, és una comprovació. Suposem-ho cert per $r-1$. Aleshores,

$$(x_k\cdots x_1)^r=c(x_k\cdots x_2)^{r-1}x_1x_2x_1^2x_3x_2\cdots x_{r-1}x_{r-2}x_k\cdots x_1,$$

i utilitzant el lema 1.13, acabem la demostració. #

<u>Lema 1.15.</u> Si $r\geqslant 3$,

$$x_1x_2x_1^2x_3x_2\cdots x_rx_{r-1}x_rx_{r-1}\cdots x_1=c^{(r-2)(r-3)/2}x_1^2x_2x_3\cdots x_rx_1^{(-1)^r+1}.$$

<u>Demostració.</u> Per inducció sobre r. Per $r=3$ és una comprovació. Suposem-ho cert per $r-1$. Aleshores,

$$x_1x_2x_1^2\cdots x_{r-1}x_{r-2}x_rx_{r-1}x_rx_{r-1}\cdots x_1=x_1x_2x_1^2\cdots x_{r-1}x_{r-2}x_{r-1}x_rx_{r-2}\cdots x_1$$

$$=c^{r-3}x_1x_2x_1^2\cdots x_{r-1}x_{r-2}x_{r-1}x_{r-2}\cdots x_1^2x_r$$

$$=c^{(r-3)(r-2)/2}\ x_1^2x_2\cdots x_rx_1^{1+(-1)^r}. \quad \#$$

<u>Proposició 1.16.</u> Si k és imparell,

$$(x_k\cdots x_1)^{k+2}=c^{(k-1)(k-7)/8}.$$

<u>Demostració.</u> Pels lemes 1.14, 1.15 tenim,

$$(x_k\cdots x_1)^{k+2}=c(x_k\cdots x_2)^kx_1x_2x_1^2\cdots x_kx_{k-1}(x_k\cdots x_1)^2$$

$$=c(x_k\cdots x_2)^kc^{(k-2)(k-3)/2}x_1^2x_2x_3\cdots x_kx_k\cdots x_1=c^{(k-3)/2}c(x_k\cdots x_2)^k.$$

Utilitzant la proposició 1.9, obtenim el resultat. #

<u>Lema 1.17.</u> Si $1\leqslant r<k$,

$$(x_k\cdots x_2)^{-r}x_1(x_k\cdots x_2)^r=c^rx_{r+1}x_r\cdots x_2x_1^{(-1)^{(k-2)r}}x_2x_3\cdots x_rx_{r+1}.$$

<u>Demostració.</u> Per inducció sobre r. Si r=1,

$$(x_k\cdots x_2)^{-1}x_1(x_k\cdots x_2)=c^{k-1}x_2\cdots x_kx_1x_k\cdots x_2$$

$$=c^{k-1}x_2\cdots x_kx_k\cdots x_3x_1^{(-1)^{k-2}}x_2$$

$$=c^{k-1}c^{k-2}x_2x_1^{(-1)^{k-2}}x_2=c\ x_2x_1^{(-1)^{k-2}}x_2.$$

Suposem-ho cert per r-1. Aleshores,

$$(x_k\cdots x_2)^{-r}x_1(x_k\cdots x_2)^r=(x_k\cdots x_2)^{-1}c^{r-1}x_rx_{r-1}\cdots x_2x_1^{(-1)^{(k-2)(k-r)}}x_2\cdots x_{r-1}x_rx_k\cdots x_2$$

$$=c^{k+r-2}x_2\cdots x_{r+1}x_rx_{r-1}\cdots x_2x_{r+2}\cdots x_kx_1^{(-1)^{(k-2)(r-1)}}x_k\cdots x_{k+2}x_2\cdots x_{r-1}x_rx_{r+1}\cdots x_2,$$

Pel lema 1.10,

$$=c^{r+k-2}x_{r+1}\cdots x_3x_2x_3\cdots x_kx_k\cdots x_3x_1^{(-1)^{(k-2)(r-1)+r-2}}x_2x_3\cdots x_{r+1}$$

$$=c^rx_{r+1}\cdots x_3x_2x_1^{(-1)^{(k-2)r}}x_2\cdots x_{r+1}. \quad \#$$

<u>Proposició 1.18.</u> Si $1\leqslant r<k$,

$$(x_1^{(-1)^{r(k-1)}}(x_k\cdots x_2)^{-r}x_1(x_k\cdots x_2)^r)^2=c.$$

<u>Demostració.</u> Pel lema 1.17,

$$(x_1^{(-1)^{r(k-1)}}(x_k\cdots x_2)^{-r}x_1(x_k\cdots x_2)^r)^2=(c^rx_1^{(-1)^{r(k-1)}}x_{r+1}\cdots x_2x_1^{(-1)^{(k-2)r}}x_2\cdots x_rx_{r+1})^2$$

$$=x_1^{(-1)^{r(k-1)}}x_{r+1}\cdots x_2x_1^{(-1)^{r(k-2)}}x_2\cdots x_rx_{r+1}x_1^{(-1)^{r(k-1)}}x_{r+1}\cdots x_2x_1^{(-1)^{r(k-2)}}x_2\cdots x_rx_{r+1}=c. \quad \#$$

<u>Demostració del teorema 1.6.</u>

Sigui $x=x_1$, $y=c^{(n-1)(n-2)(n-3)(n-4)/2}x_{n-2}\cdots x_2$.
Per les proposicions 1.9, 1.18, 1.12 i 1.16, x,y satisfan les relacions del teorema. D'altra banda x,y generen $\hat{A}_n$, ja que $g(x),g(y)$ generen A_n ([4], pàg. 66). #

Capítol II. El problema d'immersió

El problema de la realització de les extensions centrals de A_n l'abordem com un problema d'immersió galoisiana. Per veure que tota extensió central de A_n és grup de Galois, provem primerament que n'hi ha prou en realitzar la seva extensió central universal $\hat{A}_n$. Seguidament donem un criteri, pel qual, hom pot saber si, per a una equació amb grup de Galois A_n, el problema d'immersió local per al primer de l'infinit té solució. En cas negatiu, pel principi local-global, podrem ja desestimar l'equació en qüestió com a possible candidata a ésser solució del problema d'immersió global plantejat.

§1. Immersions galoisianas

Sigui K un cos (commutatiu) i $\bar{K}$ una clausura separable. Denotem per G_K el grup de Galois absolut de K, és a dir, el grup de Galois de $\bar{K}$ sobre K.

Sigui G un grup finit. Sigui L/K una extensió galoisiana finita amb grup de Galois G(L/K) isomorf a G. Sigui $h:G_K \to G$ l'epimorfisme de grups induït per la projecció canònica $G_K \to G(L/K)$.

Sigui E un grup finit, extensió del grup G, donat per la successió exacta

$$1 \to A \to E \xrightarrow{j} G \to 1. \qquad (1)$$

Es diu que l'extensió L/K admet una *immersió galoisiana* a E quan existeix un homomorfisme

$$f:G_K \to E,$$

tal que el diagrama següent

$$\begin{tikzcd} & & & G_K \arrow[dl, "f"'] \arrow[d, "h"] & \\ 1 \arrow[r] & A \arrow[r] & E \arrow[r, "j"] & G \arrow[r] & 1 \end{tikzcd}$$

és commutatiu.

Sigui $N=\bar{K}^{\ker(f)}$ el cos fix del nucli de f. Si f és epijectiu, es té que $G(N/K)\simeq E$ i $N \supset L \supset K$. En identificar $G(N/K)$ amb E i $G(L/K)$ amb G, la projecció canònica $G(N/K) \to G(L/K)$ és aleshores l'homomorfisme donat j. Si f no és epijectiu, s'obté únicament una àlgebra galoisiana amb grup de Galois E. Ikeda [12] demostrà que si el nucli A és abelià, i K un cos de nombres, aleshores un problema d'immersió galoisiana que tingui una àlgebra per solució, té també un cos com a solució.

Suposem d'ara endavant que el nucli A és un grup abelià. La successió (1) dóna a A estructura de G-modul i determina un element $a\in H^2(G,A)$. Mitjançant l'homomorfisme d'inflació definit per h,

$$\inf: H^2(G,A) \to H^2(G_K,A),$$

tenim la següent caracterització cohomològica de l'existència d'immersions galoisianes.

<u>Teorema 2.1.</u> ([9],1.1) L'extensió galosiana L/K admet una immersió galoisiana a E si i només si $\inf(a)=0$. #

En particular, si (1) descompon, el problema d'immersió té solució.

Suposem ara que K és un cos de nombres. El problema d'immersió galoisiana dóna lloc en aquest cas a un problema

d'immersió galoisiana local. Per a cada primer $\mathfrak{p}$ de K, sigui $K_{\mathfrak{p}}$ la seva completació, $\bar{K}_{\mathfrak{p}}$ una clausura algebraica i $G_{K_{\mathfrak{p}}}=G(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$. Una inclusió (fixada) de K a $K_{\mathfrak{p}}$ es pot estendre a una de $\bar{K}$ a $\bar{K}_{\mathfrak{p}}$ de manera que, aleshores, $\bar{K}_{\mathfrak{p}}=\bar{K}.K_{\mathfrak{p}}$ i $G_{K_{\mathfrak{p}}}$ es pot identificar amb un grup de descomposició de $\mathfrak{p}$ a $\bar{K}/K$. Per tant $G_{K_{\mathfrak{p}}}$ és un subgrup de G_K (determinat a menys de automorfismes interns). Siguin $G_{\mathfrak{p}}=h(G_{K_{\mathfrak{p}}})$, $h_{\mathfrak{p}}=h|G_{K_{\mathfrak{p}}}$, $E_{\mathfrak{p}}=j^{-1}(G_{\mathfrak{p}})$ i $j_{\mathfrak{p}}=j|E_{\mathfrak{p}}$. La successió exacta (1) origina la successió exacta

$$1 \to A \to E_{\mathfrak{p}} \xrightarrow{j_{\mathfrak{p}}} G_{\mathfrak{p}} \to 1 \ . \qquad (2)$$

Una solució global f restringeix a una solució local $f_{\mathfrak{p}}$. És a dir, si $f_{\mathfrak{p}}=f|G_{K_{\mathfrak{p}}}$, el diagrama

$$\begin{tikzcd} & & G_{K_{\mathfrak{p}}} \arrow[dl, "f_{\mathfrak{p}}"'] \arrow[d, "h_{\mathfrak{p}}"] & \\ 1 \arrow[r] & A \arrow[r] & E_{\mathfrak{p}} \arrow[r, "j_{\mathfrak{p}}"] & G_{\mathfrak{p}} \arrow[r] & 1 \end{tikzcd}$$

és commutatiu. És vàlid l'important principi local-global següent.

<u>Teorema 2.2.</u> ([18], 2.2, 4.7) Si A és un G_K-mòdul trivial finit, l'aplicació

$$H^2(G_K,A) \xrightarrow{\Pi \mathrm{res}_{\mathfrak{p}}} \prod_{\mathfrak{p}} H^2(G_{K_{\mathfrak{p}}},A)$$

és injectiva. En conseqüència, en aquest cas, el problema d'immersió galoisiana global té solució si i només si el corresponent problema d'immersió galoisiana local té solució per a tot primer $\mathfrak{p}$ de K. #

§2. Teorema de reducció

El resultat següent és conegut (cf.[34]). Aci, però, en donem una demostració diferent, a la vegada més natural.

Teorema 2.3. Sigui K un cos de nombres, G un grup finit perfecte. Sigui $\hat{G}$ l'extensió central universal de G. Si $\hat{G}$ es realitza com a grup de Galois sobre K, aleshores tota extensió central finita de G també és grup de Galois sobre K.

Demostració. Sigui E una extensió central finita de G. Sigui $a \in H^2(G, \ker e)$ l'element que determina la successió exacta

$$1 \to \ker e \to E \xrightarrow{e} G \to 1.$$

Sigui $u \in H^2(G, \ker \pi)$ l'element associat a la successió exacta

$$1 \to \ker \pi \to \hat{G} \xrightarrow{\pi} G \to 1.$$

Per ésser $\hat{G}$ extensió universal, existeix un homomorfisme $g: \hat{G} \to E$, tal que el diagrama

$$\begin{array}{ccccccccc} 1 & \to & \ker \pi & \to & \hat{G} & \to & G & \to & 1 \\ & & & & \downarrow g & & \| \mathrm{id} & & \\ 1 & \to & \ker e & \to & E & \to & G & \to & 1 \end{array}$$

és commutatiu. Per tant, g indueix un homomorfisme $g: \ker \pi \to \ker e$. Sigui h la composició dels homomorfismes $G_K \to \hat{G} \xrightarrow{\pi} G$. El diagrama de parelles

$$\begin{array}{ccc} (G_K, \ker \pi) & \xrightarrow{(h,\mathrm{id})} & (G, \ker \pi) \\ \downarrow (\mathrm{id}, g) & & \downarrow (\mathrm{id}, g) \\ (G_K, \ker e) & \xrightarrow{(h,\mathrm{id})} & (G, \ker e) \end{array}$$

és commutatiu, car ker π, ker e, són G-mòduls i G_K-mòduls trivials. A nivel de cohomologia això dóna lloc al diagrama commutatiu següent

$$\begin{array}{ccc} H^2(G,\ker\pi) & \xrightarrow{(h,id)^*} & H^2(G_K,\ker\pi) \\ \downarrow{\scriptstyle (id,g)^*} & & \downarrow{\scriptstyle (id,g)^*} \\ H^2(G,\ker e) & \xrightarrow{(h,id)^*} & H^2(G_K,\ker e). \end{array}$$

Així si

$$0 = \inf(u) = (h,id)^*(u) \ ,$$

tindrem que

$$\inf(a)=(h,id)^*(a)=(h,id)^*((id,g)^*(u))=(id,g)^*((h,id)^*(u))=0. \ \#$$

§3. Principi local-global per a $\hat{A}_n$

El nostre problema ha quedat reduït a la realització com a grup de Galois sobre $\mathbb{Q}$, de l'extensió central universal $\hat{A}_n$. Afrontem aquest problema des del punt de vista de les immersions galoisianes.

Sigui $K/\mathbb{Q}$ una extensió de Galois amb grup de Galois isomorf a A_n. Sigui $a_n \in H^2(A_n,\mathbb{Z}/2)$ l'element corresponent a la successió exacta

$$1 \to \mathbb{Z}/2 \to \hat{A}_n \xrightarrow{\pi} A_n \to 1 \qquad (3)$$

construïda a 1.5.

Sigui $h:G_{\mathbb{Q}} \to A_n$ l'epimorfisme que defineix $K/\mathbb{Q}$. Considerem l'homomorfisme d'inflació

$$\inf: H^2(A_n, \mathbb{Z}/2) \to H^2(G_{\mathbb{Q}}, \mathbb{Z}/2).$$

L'extensió $K/\mathbb{Q}$ admet una immersió galoisiana a $\hat{A}_n$ si i només si $\inf(a_n)=0$. Per tant, donada una extensió $K/\mathbb{Q}$ que realitzi A_n, podem dir que *l'obstrucció* al problema d'immersió galoisiana a $\hat{A}_n$ és $\inf(a_n)=b_n$.

D'altra banda, resulta del §1 que aquest problema d'immersió galoisiana localitza. Sigui p un primer de $\mathbb{Q}$ (finit o no), sigui

$$\mathrm{res}_p: H^2(G\ , \mathbb{Z}/2) \to H^2(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$$

l'homomorfisme de restricció. Pel principi local-global, $b_n=0$ si i només si $\mathrm{res}_p(b_n)=(b_n)_p=0$, per a tot p primer de $\mathbb{Q}$.

A continuació fem algunes consideracions de caràcter general sobre aquesta obstrucció local. Sigui p un primer de $\mathbb{Q}$ fix. Tenim el següent diagrama commutatiu

$$\begin{array}{ccc} H^2(A_n, \mathbb{Z}/2) & \xrightarrow{\inf} & H^2(G_{\mathbb{Q}}, \mathbb{Z}/2) \\ \downarrow \mathrm{res}_p & & \downarrow \mathrm{res}_p \\ H^2(G_p, \mathbb{Z}/2) & \xrightarrow{\inf_p} & H^2(G_{\mathbb{Q}_p}, \mathbb{Z}/2), \end{array}$$

on $G_p=h(G_{\mathbb{Q}_p})$.

És clar que $(b_n)_p=0$ si i només si el problema d'immersió galoisiana donat per

$$1 \to \mathbb{Z}/2 \to \hat{G}_p \xrightarrow{\pi} G_p \to 1, \qquad (4)$$

on $\hat{G}_p=\pi^{-1}(G_p)$, té solució.

Si la successió exacta (4) descompon, aleshores $(b_n)_p=0$. En particular si $H^2(G_p, \mathbb{Z}/2)=0$, es té que $(b_n)_p=0$.

Tenint en compte [29], cap. VIII, §2, §4 i cap. IX, th. 4, hom demostra fàcilment

<u>Proposició 2.4.</u> Sigui G un grup finit. Es compleix

a) Si $2 \nmid \#G$, aleshores $H^q(G,Z/2)=0$, per a tot q.

b) Si G és cíclic i $2|\#G$, aleshores $H^q(G,Z/2)\simeq Z/2$, per a tot q.

c) Si $2|\#G$, aleshores $H^q(G,Z/2)_p=0$, per a tot primer $p|\#G, p\neq 2$. A més, l'homomorfisme

$$H^q(G,Z/2)\xrightarrow{res} H^q(S^{(2)},Z/2)$$

és injectiu, on $S^{(2)}$ és el 2-subgrup de Sylow de G. #

Retornant a la nostra situació, si p és un primer de Q, és clar que G_p és isomorf a un grup de descomposició de p a K/Q. Ara, si l'ordre de G_p és imparell, $(b_n)_p=0$. Si $G_p\neq 0$ té ordre parell, $H^2(G_p,Z/2)\neq 0$, car la seva 2-component és no nul.la ([28], I, 4.3).

§4. L'obstrucció local a l'infinit

En aquest paràgraf estudiem el problema d'immersió local a $\hat{A}_n$ en el cas del primer de l'infinit.

Sigui K/Q una extensió galosiana amb grup de Galois A_n.

Si el primer de l'infinit, p_∞, no ramifica a $K/\mathbb{Q}$, aleshores $(b_n)_{p_\infty}=0$.

Suposem d'ara endavant que p_∞ ramifica a $K/\mathbb{Q}$. És clar que $G_{p_\infty}=G(\mathbb{C}/\mathbb{R})=\{id,\gamma\}$, on γ és la conjugació complexa. Per tant, $H^2(G_{p_\infty},\mathbb{Z}/2)\simeq\mathbb{Z}/2$. D'altra banda, $\hat{G}_{p_\infty}$ ve determinat per $\hat{\gamma}\in\pi^{-1}(\gamma)$, on π és l'homomorfisme $\hat{A}_n\to A_n$.

Si $\hat{\gamma}^2=1$, aleshores $\hat{G}_{p_\infty}\simeq\mathbb{Z}/2\times\mathbb{Z}/2$ i (4) descompon. Per tant, tenim que $(b_n)_{p_\infty}=0$.

Si $\hat{\gamma}^4=1$, aleshores, $\hat{G}_{p_\infty}\simeq\mathbb{Z}/4$ i, en conseqüència, $res_{p_\infty}(a_n)\neq 0$. Com que, en aquest cas, $G_{\mathbb{Q}_{p_\infty}}\simeq G(\mathbb{C}/\mathbb{R})\simeq G_{p_\infty}$, tenim que $inf_{p_\infty}=id$. Aleshores

$$(b_n)_{p_\infty}=inf_{p_\infty}\,res_{p_\infty}(a_n)\neq 0$$

Hem demostrat així el resultat següent.

<u>Proposició 2.5.</u> Donada una extensió galosiana $K/\mathbb{Q}$ amb grup de Galois A_n, l'obstrucció local a l'infinit per $\hat{A}_n$ és nul.la, si i només si hi ha un element d'ordre 2 a l'antiimatge de γ pel homomorfisme $\pi:\hat{A}_n\to A_n$. #

Sigui $f(X)\in\mathbb{Q}[X]$ un polinomi irreduïble de grau n tal que el seu grup de Galois G_f és isomorf a A_n. Direm que $f(X)$ admet una immersió galoisiana a $\hat{A}_n$ (resp. una immersió galoisiana local per a p_∞ a $\hat{A}_n$), quan això succeeixi per la clausura normal de $f(X)$.

Donem tot seguit condicions sobre el nombre d'arrels reals del polinomi perquè la seva obstrucció local a l'infinit sigui nul.la.

Proposició 2.6. Sigui $f(X)$ un polinomi irreduïble de grau n amb grup de Galois isomorf a A_n. Si el polinomi $f(X)$ té exactament r_1 arrels reals, aleshores $n\equiv r_1$ (mòd. 4).

Demostració. Siguin $\theta_1,\ldots,\theta_{n-r_1}$, les $n-r_1$ arrels complexes no reals de $f(X)$. Aleshores, $\gamma\in G_{p_\infty}\subset G_f$, pensat com a permutació de les arrels de $f(X)$, ve donat per

$$\gamma=(12)(34)\ldots(n-r_1-1\ \ n-r_1).$$

Com que per hipòtesi $G_f\simeq A_n$, tindrem que

$$\gamma\in G_f \text{ si i només si } (n-r_1)/2 \text{ és parell. } \#$$

Teorema 2.7. Sigui $f(X)\in\mathbb{Q}[X]$ un polinomi irreduïble de grau n amb grup de Galois isomorf a A_n. Suposem que $f(X)$ té exactament r_1 zeros reals. L'obstrucció local de $f(X)$ a l'infinit és zero si i només si $n\equiv r_1$ (mòd. 8).

Demostració. Per la proposició 2.6,

$$r_1 \equiv n \pmod{4} \quad \text{i} \quad \gamma=(12)(34)\ldots(n-r_1-1\ n-r_1)\in G_{p_\infty}.$$

Per la proposició 2.5, tot està en provar que $\hat{\gamma}^2=1$, on $\hat{\gamma}\in\pi^{-1}(\gamma)$. D'altra banda, tenim les identitats

$$\begin{aligned}\gamma&=(12)(34)\ldots(n-r_1-1\ n-r_1)\\ &=(12)(34)(12)(56)\ldots(12)(n-r_1-1\ n-r_1)(12)^{(n-r_1-4)/2}\\ &=s_2\ s_4\ldots s_{n-r_1-2}\ ,\end{aligned}$$

on $s_i=(12)(i+1\ i+2)$. Per ([4], pàg. 66), $s_1,\ldots,s_{n-2}$ generen A_n. En el teorema 1.5, s'ha provat que existeixen elements $x_i\in\hat{A}_n$ que generen $\hat{A}_n$ i satisfan les relacions de 1.5, tals que $\pi(x_i)=s_i$ per a tot $1\leqslant i\leqslant n-2$, on $\pi:\hat{A}_n\to A_n$. Aleshores,

$$\begin{aligned}\hat{\gamma}^2&=x_2x_4\ldots x_{n-r_1-2}\ x_2x_4\ldots x_{n-r_1-2}\\ &=c^{(n-r_1-2)/2}c^{(n-r_1-4)/2}\ldots c^2c\\ &=c^{(n-r_1)/4}\ .\end{aligned}$$

Per tant,

$$\hat{\gamma}^2=1 \text{ si i només si } (n-r_1)/4 \text{ és parell. } \#$$

Corol.lari 2.8. Sigui $f(X)\in Q[X]$ un polinomi irreduïble de grau n amb grup de Galois isomorf a A_n. Si el nombre d'arrels reals de $f(X)$ és $r_1\not\equiv n$ (mòd. 8), aleshores $f(X)$ no admet una immersió galoisiana a $\hat{A}_n$. #

Així doncs, a través d'una condició "fàcil" de computar sobre una equació que realitzi A_n, sabrem si el problema d'immersió plantejat no té solució per a aquesta equació. Això ens permet fer una primera tria de les equacions que realitzen A_n. Aplicant el teorema de Descartes, veiem que per a polinomis del tipus X^n+aX+b l'immersió galoisiana no sera *mai* possible si $n\equiv 4,6,5$, ó 7 (mòdul 8). El mateix es pot dir per a polinomis del tipus X^n+aX^2+bX+c, si $n\equiv 5,6$, ó 7 (mòdul 8).

En el treball [17] vàrem construir explícitament, per a cada valor de n, equacions sobre Q amb grup de Galois A_n (cf. cap. III, §3). Anotem ara el següent

Corol.lari 2.9. Les equacions del teorema 2.1 de [17] admeten una immersió galoisiana a $\hat{A}_n$ local a l'infinit si i només si $n\equiv 0$ ó 2 (mòd. 8). #

Capítol III. El teorema de Serre

Donat el problema d'immersió galoisiana

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow & & \\ 1 & \to & \mathbb{Z}/2 & \to & \hat{A}_n & \to & A_n & \to & 1, \end{array}$$

en un resultat recent [31], Serre calcula l'obstrucció $\inf(a_n) \in H^2(G_K, \mathbb{Z}/2)$ en termes d'un invariant de Hasse-Witt.

En aquest capítol presentem aquest resultat i en donem una primera aplicació: Les realitzacions de A_n sobre $\mathbb{Q}$, donades pels polinomis que construírem a [17], Th 2.1, admeten una immersió galoisiana a $\hat{A}_n$ per a $n \equiv 0 \pmod 8$, $n \equiv 2 \pmod 8$ i suma de dos quadrats. En conseqüència, per a aquests valors de n, tota extensió central de A_n es realitza com a grup de Galois sobre $\mathbb{Q}$.

§1. L'invariant de Hasse-Witt d'una extensió.

Sigui K un cos de característica $\neq 2$, $\bar{K}$ una clausura separable i $G_K = G(\bar{K}/K)$.

Denotem per Br(K) el grup de Brauer de K, és a dir, el conjunt de les classes d'equivalència de K-àlgebres centrals simples i de dimensió finita sobre K, dotat del producte tensorial de K-àlgebres.

Donat que Br(K) és isomorf a $H^2(G_K, \bar{K}^*)$ ([29], X, Prop.9), és fàcil veure que la 2-component del grup de Brauer, $Br_2(K)$ és isomorfa a $H^2(G_K, \mathbb{Z}/2)$. En efecte, la successió exacta

$$1 \to \mu_2 \to \bar{K}^* \xrightarrow{\cdot 2} \bar{K}^* \to 1,$$

dóna lloc a la següent successió exacta de cohomologia

$$\ldots \to H^1(G_K,\bar{K}^*) \to H^2(G_K,\mu_2) \to H^2(G_K,\bar{K}^*) \xrightarrow{\cdot 2} H^2(G_K,\bar{K}^*) \to \ldots .$$

Pel teorema 90 de Hilbert, $H^1(G_K,\bar{K}^*)=0$, d'on s'obté el resultat.

Remarca. Com que l'obstrucció $\inf(a_n)\in H^2(G_Q,Z/2)$, definida a II, §3, és un element de $Br_2(Q)$, hi ha una extensió quadràtica on descompon ([1], X, Th 5).

Denotem per (a,b), $a,b\in K$, la K-àlgebra de quaternions de generadors 1, x_1,x_2, amb l'estructura de K-àlgebra donada per

$$x_1^2=a,\ x_2^2=b \quad \text{i} \quad x_1x_2=-x_2x_1.$$

(a,b) és una K-àlgebra central i simple, que defineix un element de $Br_2(K)$. És sabut que sobre un cos de nombres, $Br_2(K)$ està generada per les àlgebres de quaternions.

Recordem ara algunes propietats de les àlgebres de quaternions ([20], 57:10), que utilitzarem més endavant. Siguin $a,b,c,d\in K^*$. En el grup de Brauer de K són vàlides les igualtats:

1. $(1,a)=(1,-1)=(a,-a)=(a,1-a)=M_2(K)=1$.

2. $(b,a)=(a,b)=(ac^2,bd^2)$.

3. $(a,b)\otimes(a,c)=(a,bc)$.

Sigui L/K una extensió separable de grau n. La forma quadràtica $Tr_{L/K}(X^2)$, no degenerada, dota a L d'una estruc-

tura d'espai quadràtic. El seu discriminant, $d(L)$, i el discriminant de l'extensió, $\delta_{L/K}$, defineixen el mateix element de K^*/K^{*2}.

Anomenem *invariant de Hasse-Witt* de l'extensió L/K l'invariant de Hasse-Witt de l'espai quadràtic $(L, Tr_{L/K}(X^2))$. Si, en una base ortogonal de L/K, $Tr_{L/K}(X^2)=a_1X_1^2+..+a_nX_n^2$, aleshores l'invariant de Hasse-Witt $w(L/K)$, com element del grup de Brauer, és

$$w(L/K) = \bigotimes_{1\leqslant i<j\leqslant h} (a_i, a_j).$$

Recordem que si un espai quadràtic descompon $U=V_1 \perp V_2$, l'invariant de Hasse-Witt de U és

$$w(U)=w(V_1) \otimes w(V_2) \otimes (d(V_1), d(V_2)),$$

on $d(V_i)$ és el discriminant de V_i. En conseqüència si $V \simeq rH$, on H és un pla hiperbòlic,

$$w(V)=(-1,-1)^{r(r-1)/2}.$$

§2. L'obstrucció global: Teorema de Serre

Sigui L/K una extensió separable de grau n i N/K la seva clausura normal. El grup de Galois de N/K és un subgrup del grup simètric S_n. La projecció natural $G_K \to G(N/K)$ dóna lloc a l'homomorfisme

$$g: G_K \to S_n.$$

A nivell de cohomologia, g indueix, en particular, un homomorfisme

$$g^*: H^2(S_n, \mathbb{Z}/2) \to H^2(G_K, \mathbb{Z}/2).$$

Sigui $\tilde{S}_n$ el grup generat pels elements $\tilde{t}_i$, $1 \leqslant i \leqslant n-1, \varepsilon$, satisfent les relacions

$$\varepsilon^2 = [\varepsilon, \tilde{t}_i] = \tilde{t}_i^2 = (\tilde{t}_i \tilde{t}_{i+1})^3 = 1, \qquad 1 \leqslant i \leqslant n-1,$$

$$(\tilde{t}_i \tilde{t}_j)^2 = \varepsilon, \qquad |j-i| \geqslant 2.$$

Definim $\pi: \tilde{S}_n \to S_n$ per

$$\pi(\tilde{t}_i) = t_i, \ \pi(\varepsilon) = 1,$$

on t_i són generadors de S_n satisfent les relacions

$$t_i^2 = (t_i t_{i+1})^3 = (t_i t_j)^2 = 1, \quad \text{si } |j-i| \geqslant 2$$

([4], pàg. 63).

És clar que la successió

$$1 \to \mathbb{Z}/2 \to \tilde{S}_n \xrightarrow{\pi} S_n \to 1,$$

és exacta. Sigui $s_n \in H^2(S_n, \mathbb{Z}/2)$ l'element que determina aquesta successió.

<u>Teorema 3.1.</u> (Serre [31]) $w(L/K) = g^*(s_n) \otimes (2, d(L))$. #

Com a conseqüència immediata d'aquest teorema tenim

Proposició 3.2. Sigui L/K una extensió separable de grau n N/K la seva clausura normal. Suposem que $G(N/K)\simeq A_n$. Sigui $a_n\in H^2(A_n,\mathbb{Z}/2)$ l'element associat a la successió exacta

$$1 \to \mathbb{Z}/2 \to \hat{A}_n \to A_n \to 1.$$

Aleshores,

$$w(L/K)=\inf(a_n)\in H^2(G_K,\mathbb{Z}/2).$$

És a dir, l'obstrucció perquè N/K admeti una immersió galoisiana a $\hat{A}_n$ és $w(L/K)$.

Demostració. Sigui $h:G_K \to A_n$ l'epimorfisme definit per l'extensió galoisiana N/K. Tenim que $g=ioh$, on $i:A_n \to S_n$ és la inclusió canònica. És clar que $g^*=h^*oi^*$ i que $i^*(s_n)\in H^2(A_n,\mathbb{Z}/2)$ és no trivial; és a dir, $i^*(s_n)=a_n$. D'altra banda, $d(L)\in K^{*2}$ ja que $G(N/K)\simeq A_n$. Per tant, pel teorema 3.1,

$$w(L/K)=h^*(i^*(s_n)) \otimes (2,d(L))=h^*(a_n)=\inf(a_n). \ \#$$

Observació. Després d'aquest resultat, el problema de realitzar $\hat{A}_n$ com a grup de Galois sobre $\mathbb{Q}$ ha quedat centrat en resoldre les qüestions següents:

a) Trobar polinomis $f(X)\in\mathbb{Q}[X]$ irreduïbles, de grau n, tals que $G_f\simeq A_n$.

b) Calcular $w(L/\mathbb{Q})$, on $L=\mathbb{Q}(\theta)$, θ arrel de $f(X)$.

c) Donar condicions sobre $f(X)$ a fi que $w(L/Q)=1$.

Cap d'aquestes qüestions no té una resposta fàcil. Voldria destacar ara, les dificultats que hom troba en tractar de resoldre b). Sigui $L=Q(\theta)$, on θ és una arrel del polinomi irreduïble $f(X)=X^n+a_{n-1}X^{n-1}+\ldots+a_o\in Q[X]$. La matriu definidora de $Tr_{L/Q}(X^2)$ és la matriu formada per $Tr_{L/Q}(\theta^{i+j})$, $0\leqslant i,j\leqslant n-1$. Per les fòrmules de Newton ([2],V, App.I), $Tr_{L/Q}(\theta^i)$ són polinomis isobàrics de pes i en $a_o,\ldots,a_{n-1}$. El primer problema es troba en diagonalitzar $Tr_{L/Q}(X^2)$. A la vista de les expresions de $Tr_{L/Q}(\theta^i)$, la tasca es simplifica si el polinomi $f(X)$ és de la forma $X^n+p(X)$, on $p(X)$ té grau petit.

Així els polinomis donats per Hilbert [8] sobre $Q(T)$ i per Schur [27] sobre Q (quan $n\not\equiv 2$ (mòd. 4)), no són escaients per al nostre problema, car es tracta de polinomis complets.

§3. Primers resultats sobre Q

En un treball en col.laboració amb E. Nart, [17], vàrem donar criteris perquè polinomis del tipus $X^n+aX^3+bX^2+cX+d$ tinguin grup de Galois isomorf a A_n. Utilitzant aquests criteris construirem, per a tot valor de n, infinits polinomis amb grup de Galois sobre Q isomorf a A_n. Esmentem els resultats que fan referència al cas n parell, car els utilitzarem tot seguit.

Teorema 3.3. ([17], Th.1.1) Sigui n un enter parell, $n>2$. Sigui $f(X)=X^n+bX^2+cX+d\in\mathbb{Z}[X]$, $b,d\neq 0$ un polinomi satisfent les condicions

1) $f(X)$ és irreduïble i primitiu.

2) $c^2(n-1)^2=4bdn(n-2)$.

3) $(-1)^{n/2}d$ és un quadrat.

4) Si $u=-c(n-1)/2(n-2)b$, existeix un primer p de $\mathbb{Z}$ tal que

   4a) $p\mid f(u)$ i $p\nmid c(n-1)$.

   4b) $3\nmid v_p(f(u))$.

Aleshores, el grup de Galois de $f(X)$ sobre $\mathbb{Q}$ és isomorf a A_n. #

Teorema 3.4. ([17], Th. 2.1) Sigui n un enter parell, $n>2$. Sigui q un factor primer de $n-1$ i $A\in\mathbb{Z}$ tal que $2q\nmid A$ i l'expressió

$$1+(-1)^{n/2}2^3n^n(n-1)^{n-1}(n-2)^{n-1}A^2/q^{n-2} \text{ no és un cub.}$$

Si posem

$$b = (-1)^{n/2}2^2n^3(n-1)^2(n-2)A^2,$$

$$c = (-1)^{n/2}2^3n^2(n-2)qA^2,$$

$$d = (-1)^{n/2}(2qA)^2,$$

el grup de Galois de $f(X)=X^n+bX^2+cX+d$ sobre $\mathbb{Q}$ és isomorf a A_n. #

<u>Teorema 3.5.</u> Sigui n un enter parell, $n>4$. Sigui $f(X)=X^n+bX^2+cX+d\in\mathbb{Z}[X]$ un polinomi satisfent les condicions del teorema 3.3 (p.e. els polinomis donats en el teorema 3.4).

Els polinomis $f(X)$ admeten immersió galosiana a $\hat{A}_n$ sobre $\mathbb{Q}$ si i només si

$n\equiv 0$ (mòd. 8) o $n\equiv 2$ (mòd. 8) i suma de dos quadrats.

<u>Demostració.</u> Sigui $L=\mathbb{Q}(\theta)$, on θ és una arrel de $f(X)$. Volem calcular el valor de l'invariant de Hasse-Witt de $L/\mathbb{Q}$, $w(L/\mathbb{Q})$. $1,\theta,\ldots,\theta^{n-1}$ és una base de $L/\mathbb{Q}$. Els valors de $Tr(\theta^i)$, $1\leqslant i\leqslant n-1$, són:

$$Tr(1)=n \qquad Tr(\theta^{n-2})= -(n-2)b$$

$$Tr(\theta^i)=0,\ 1\leqslant i\leqslant n-3 \qquad Tr(\theta^{n-1})= -(n-1)c.$$

Sigui $m=n/2$. És clar que $1,\theta,\ldots,\theta^{m-1}$ són vectors dos a dos ortogonals i que $\theta,\ldots,\theta^{m-2}$ són vectors isòtrops. Per tant l'espai quadràtic L descompon en la forma

$$L=V_1\perp V_2\perp \langle 1,\theta^{m-1}\rangle,$$

on $V_1 \simeq (m-2)H$, i H és un pla hiperbòlic.

Calculem el discriminant de l'espai V_2 ;

$$d(L)=(-1)^{m-2}d(V_2)n(-(n-2)b)=d(V_2)\ (-1)^{m-1}n(n-2)b.$$

Com que $G_f \simeq A_n$, tenim que $d(L)=1 \in Q^*/Q^{*2}$. És a dir,

$$d(V_2)=(-1)^{m-1}n(n-2)b \in Q^*/Q^{*2}.$$

Per les condicions 2), 3) del teorema 3.3, $(-1)^{m-2}n(n-2)b \in Q^{*2}$, per tant $d(V_2)=-1 \in Q^*/Q^{*2}$, és a dir, V_2 és un pla hiperbòlic. Així doncs l'espai L descompon en la forma

$$L=V_3 \perp \langle 1,\theta^{m-1}\rangle,$$

on $V_3 \simeq (m-1)H$. Aleshores,

$$\begin{aligned} w(L/Q) &= w(V_3) \otimes w(\langle -1,\theta^{m-1}\rangle) \otimes ((-1)^{m-1},(-1)^{m-1}) \\ &= (-1,-1)^{(m-1)(m-2)/2} \otimes (n,-(n-2)b) \otimes (-1,-1)^{m-1} \\ &= (-1,-1)^{(m-1)m/2} \otimes (n,(-1)^m) = \\ &= (-1,-1)^{n(n-2)/8} \otimes (n,(-1)^{n/2}). \end{aligned}$$

Per tant, si $n \equiv 0 \pmod{8}$, $w(L/Q)=1$ (*)

si $n \equiv 2 \pmod{8}$, $w(L/Q)=(n,-1)$

si $n \equiv 4 \pmod{8}$, $w(L/Q)=(-1,-1) \neq 1$

si $n \equiv 6 \pmod{8}$, $w(L/Q)=(-1,-n) \neq 1$

En conseqüència, $w(L/Q)=1$ si i només si

$n \equiv 0 \pmod{8}$ ó $n \equiv 2 \pmod{8}$ i n suma de dos quadrats. #

(*) El resultat en aquest cas em va ésser indicat per J.P.Serre.

Corol.lari 3.6. Tota extensió central de A_n es realitza com a grup de Galois sobre $\mathbb{Q}$ per $n\equiv 0$ (mòd. 8), $n\equiv 2$ (mòd. 8) i suma de dos quadrats.

Remarca. Pel comportament local en el primer de l'infinit, (corol.lari 2.9), ja sabiem que per a $n\equiv 4$ ó 6 (mòd. 8) no seria possible l'immersió galoisiana a $\hat{A}_n$ per aquestes equacions. D'altra banda, pel cas n imparell, únicament disposem de polinomis del tipus X^n+bX^2+cX+d que realitzin A_n, si n és un quadrat imparell ([17], Th. 1.6). Hom pot provar que, en aquest cas, $w(L/\mathbb{Q})=1$. Per tant $\hat{A}_n$ es realitza també si n és un quadrat imparell. Observem, però, que un quadrat imparell és sempre de la forma $1+8\lambda$. El cas $n\equiv 1$ (mòd. 8) serà resolt completament en el capítol V.

Capítol IV. El mètode de les superfícies de Riemann

Pel teorema d'existència de Riemann, tot grup finit G és grup de Galois sobre $\mathbb{C}(T)$. Hom es pot preguntar si hi ha una equació definidora de l'extensió de $\mathbb{C}(T)$ amb coeficients racionals, de manera que sobre $\mathbb{Q}(T)$ sigui normal, amb grup de Galois isomorf a G. Aquesta és una qüestió difícil, no resolta en general. D'altra banda, com és ben conegut, si hom realitza un grup G com a grup de Galois sobre $\mathbb{Q}(T)$, pel teorema d'irreduïbilitat de Hilbert, aquest grup és realitzable sobre $\mathbb{Q}$.

En aquest capítol donem condicions perquè, per a grups complets amb bones presentacions, la qüestió abans esmentada tingui solució. Aquests mètodes serán aplicats en el capítol següent per obtenir noves equacions sobre $\mathbb{Q}(T)$ amb grups de Galois isomorfs a S_n i a A_n, respectivament.

§1. Cossos de definició

Sigui F un cos de funcions algebraiques d'una variable amb cos de constants k. El problema de classificar les extensions finites de F està completament resolt en el cas $k=\mathbb{C}$, via el teorema d'existència de Riemann. Sigui $\mathcal{R}$ la superfície de Riemann associada a F. Sigui F'/F una extensió finita de cossos. La superfície de Riemann $\mathcal{R}'$ associada a F',és un recobriment de $\mathcal{R}$ amb un nombre finit de punts de ramificació. El teorema d'existència de Riemann ens diu que hi ha una correspondència bijectiva entre les extensions finites de F i els recobriments ramificats de grau finit de $\mathcal{R}$. Per

tant, el problema de classificar les extensions finites de F, queda reduït a un problema topològic de solució ben coneguda. Sigui $S=\{\mathcal{P}_1,\ldots,\mathcal{P}_r\}$ un nombre finit de punts de la superfície de Riemann $\mathcal{R}$. Els recobriments de grau finit de $\mathcal{R}$ que no ramifiquen fora de S, es corresponen bijectivament amb els recobriments no ramificats de la superfície $\mathcal{R}$-S. Aquests es corresponen bijectivament amb els subgrups d'índex finit del grup fonamental, $\pi_1(\mathcal{R}-S)$, de la superfície $\mathcal{R}$-S. El grup $\pi_1(\mathcal{R}-S)$ té r+2g generadors, $u_1,\ldots,u_r,x_1,y_1,\ldots,x_g,y_g$, satisfent una única relació

$$u_1\ldots u_r[x_1,y_1]\ldots[x_g,y_g]=1, \qquad (1)$$

on g és el gènere de $\mathcal{R}$.

Sigui F^S la màxima extensió galoisiana de F que no ramifica fora de S. El seu grup de Galois $G^S=G(F^S/F)$ és la completació profinita del grup $\pi_1(\mathcal{R}-S)$, és a dir, el completat per la topologia definida pels subgrups normals d'índex finit.

Si el cos de constants k és algebraicament tancat de característica zero, tot el dit fins ara és vàlid (principi de Lefschetz). El grup de Galois G^S és doncs el grup profinit amb r+2g generadors amb l'única relació (1) (cf.[5]).

D'ara endavant suposarem que el cos de constants k és $\bar{Q}$, la clausura algebracia de Q, i que $F=\bar{Q}(T)$. Sigui $k_o\subset\bar{Q}$ un subcos, suposem que els primers $\mathcal{P}_1,\ldots,\mathcal{P}_r$ de F són k_o-definits, és a dir, $(\mathcal{P}_i\cap k_o[T])\bar{Q}[T]=\mathcal{P}_i$, per $1\leqslant i\leqslant r$ finit. Denotem $S=\{\mathcal{P}_1,\ldots,\mathcal{P}_r\}$ i F^S la màxima extensió galoisiana de F no ramificada fora de S. En aquest cas hom té que g=0 i $G^S=G(F^S/F)$ és el grup profinit generat pels r elements de G^S, $u_1,\ldots,u_r$ amb la relació $u_1\ldots u_r=1$. Els subgrups generats pels elements

u_i, i els seus conjugats, són els grups d'inèrcia dels primers de F^S sobre els $\mathfrak{p}_i$, $1\leqslant i\leqslant r$.

Sigui $\alpha\in G(\bar{Q}/k_o)$. És clar que, en ésser els primer $\mathfrak{p}_i$ k_o-definits α es pot estendre a un automorfisme $\tilde{\alpha}\in G(F^S/F_o)$, on $F_o=k_o(T)$. Cada element $\tilde{\alpha}$ defineix a la vegada l'automorfisme de $G^S=G(F^S/F)$ següent

$$\begin{aligned} G^S &\to G^S \\ u &\mapsto u^{\tilde{\alpha}}=\tilde{\alpha}u\tilde{\alpha}^{-1}. \end{aligned}$$

<u>Lema 4.1.</u> Amb aquestes notacions, els subgrups generats pels elements u_i i $u_i^{\tilde{\alpha}}$ són conjugats a G^S, $1\leqslant i\leqslant r$.

<u>Demostració.</u> Sigui $\mathfrak{P}_i$ un primer de F^S sobre $\mathfrak{p}_i$, tal que $T_{\mathfrak{P}_i}(F^S/F)=\langle u_i\rangle$, on $T_{\mathfrak{P}_i}(F^S/F)$ denota el grup d'inèrcia de $\mathfrak{P}_i$ a F^S/F. És clar que $u_i^{\tilde{\alpha}}\in T_{\tilde{\alpha}(\mathfrak{P}_i)}(F^S/F)$, ja que per ésser $\bar{Q}$ algebraicament tancat, els grups d'inèrcia coincideixen amb els de descomposició i

$$u_i^{\tilde{\alpha}}(\tilde{\alpha}(\mathfrak{P}_i))=\tilde{\alpha}u_i\tilde{\alpha}^{-1}(\tilde{\alpha}(\mathfrak{P}_i))=\tilde{\alpha}u_i(\mathfrak{P}_i)=\tilde{\alpha}(\mathfrak{P}_i).$$

D'altra banda, si $u\in T_{\tilde{\alpha}(\mathfrak{P}_i)}(F^S/F)$, tenim que $u(\tilde{\alpha}(\mathfrak{P}_i))=\tilde{\alpha}(\mathfrak{P}_i)$ i, per tant, $\tilde{\alpha}^{-1}u\tilde{\alpha}\in T_{\mathfrak{P}_i}(F^S/F)=\langle u_i\rangle$. Així doncs, $\langle u_i^{\tilde{\alpha}}\rangle=T_{\tilde{\alpha}(\mathfrak{P}_i)}(F^S/F)$.

Donat que $\mathfrak{p}_i$ és k_o-definit i que $\tilde{\alpha}\in G(F^S/F_o)$, $\tilde{\alpha}(\mathfrak{P}_i)$ està també sobre $\mathfrak{p}_i$. Per tant $T_{\tilde{\alpha}(\mathfrak{P}_i)}(F^S/F)$ i $T_{\mathfrak{P}_i}(F^S/F)$ són conju-

gats a G^S. #

<u>Definició.</u> Sigui G un grup finit. Direm que una r-pla $(t_1,\ldots,t_r)$ és una *r-presentació de Hurwitz* de G, si els elements $t_1,\ldots,t_r$ generen G i satisfan la relació

$$t_1\ldots t_r = 1.$$

El conjunt de r-presentacions de Hurwitz de G el denotem $\mathcal{H}_r(G)$.

Donada $(t_1,\ldots,t_r)\in\mathcal{H}_r(G)$, denotem per $\mathcal{H}(t_1,\ldots,t_r)$ el conjunt de r-presentacions de Hurwitz $(s_1,\ldots,s_r)\in\mathcal{H}_r G)$ tals que $\langle s_i\rangle$, $\langle t_i\rangle$ són subgrups conjugats a G, per a tot $1\leqslant i\leqslant r$.

Dos elements $(s_1,\ldots,s_r),(s'_1,\ldots,s'_r)\in\mathcal{H}(t_1,\ldots,t_r)$ direm que són equivalents si existeix un automorfisme $g\in Aut(G)$ tal que

$$g(s_i)=s'_i\ ,\quad 1\leqslant i\leqslant r.$$

Anomenem *nombre de Hurwitz* $h(t_1,\ldots,t_r)$ de $(t_1,\ldots,t_r)\in\mathcal{H}_r(G)$ el cardinal del conjunt de classes d'equivalència de $\mathcal{H}(t_1,\ldots,t_r)$.

És a dir

$$h(t_1,\ldots,t_r)= \#\ \mathcal{H}(t_1,\ldots,t_r)/Aut\ G.$$

Sigui N/F una extensió galoisiana finita tal que $N\subset F^S$, és a dir, tal que l'extensió N/F no ramifica fora de S. Sigui G=G(N/F) el seu grup de Galois i $\pi:G^S\to G$ la projecció canònica. És clar que $(\pi(u_1),\ldots,\pi(u_r))$ és una r-presenta-

ció de Hurwitz de G i que els subgrups generats pels elements $\pi(u_i)$ a G, i els seus conjugats, són els grups d'inèrcia dels primers de N sobre $\mathcal{P}_i$.

Sigui $\alpha\in G(\bar{Q}/k_o)=G(F/F_o)$, α s'estén a un F_o-homomorfisme $\tilde{\alpha}$ de N en una clausura algebraica de N. Hi ha $[N:F]$ extensions de α, però en ésser N/F normal, les imatges de N per les diferents extensions de α coincideixen. Sigui $N^{\alpha}=\tilde{\alpha}(N)$ la la imatge de N per les extensions de α.

<u>Proposició 4.2.</u> Si $h(\pi(u_1),\ldots,\pi(u_r))=1$, aleshores $N^{\alpha}=N$, per a tot $\alpha\in G(\bar{Q}/k_o)$.

<u>Demostració.</u> Donat que els primers $\mathcal{P}_i$ són k_o-definits, $N^{\alpha}\subset F^S$. Sigui $G_{\alpha}=G(N^{\alpha}/F)$ i $\pi_{\alpha}:G^S\to G_{\alpha}$ la projecció natural. Pel lema 4.1, tenim que $\pi(u_i)$ i $\pi(u_i^{\tilde{\alpha}})$ generen subgrups conjugats de G. Per tant $(\pi(u_1^{\tilde{\alpha}}),\ldots,\pi(u_r^{\tilde{\alpha}}))\in\mathcal{H}(\pi(u_1),\ldots,\pi(u_r))$. Com que per hipòtesi $h(\pi(u_1),\ldots,\pi(u_r))=1$, existeix $g\in Aut(G)$ tal que

$$g(\pi(u_i^{\tilde{\alpha}}))=(\pi(u_i)),\quad 1\leqslant i\leqslant r.$$

Un element $u\in G^S$, $u=u_{i_1}\ldots u_{i_s}$, és $u\in\ker(\pi)$ si i només si

$$1=\pi(u)=\pi(u_{i_1}\ldots u_{i_s})=g(\pi(u_{i_1}^{\tilde{\alpha}})\ldots\pi(u_{i_s}^{\tilde{\alpha}}))=g(\pi(u^{\tilde{\alpha}}))\ .$$

Per tant, $u\in\ker(\pi)$ si i només si $u^{\tilde{\alpha}}\in\ker(\pi)$.

D'altra banda, és clar que $u\in\ker(\pi_{\alpha})$ si i només si $u^{\tilde{\alpha}^{-1}}\in\ker(\pi))$. En conseqüència $\ker(\pi)=\ker(\pi_{\alpha})$ i, per tant, $N^{\alpha}=N$, per a tot $\alpha\in G(\bar{Q}/k_o)$. #

Definició. Una extensió de Galois N/F diem que és *galoisiana* k_o-*definida*, on $k_o \subset \bar{\mathbb{Q}}$ és un subcos, quan existeix una extensió N_o/F_o de Galois, $F_o = k_o(T)$, tal que

$$N_o\bar{\mathbb{Q}} = N \quad \text{i} \quad G(N_o/F_o) \simeq G(N/F).$$

En general és un problema difícil trobar els subcossos de definició d'una extensió galoisiana N/F (cf.[37]). Donem a continuació un criteri per calcular cossos de definició quan el grup de Galois és complet.

Recordem que un grup G es diu complet si té centre trivial i tot automorfisme de G és intern.

Teorema 4.3. Sigui G un grup finit complet. Sigui $(t_1,\ldots,t_r)$ una r-presentació de Hurwitz de G tal que $h(t_1,\ldots,t_r)=1$. Sigui $k_o \subset \bar{\mathbb{Q}}$ i $S=\{\mathcal{P}_1,\ldots,\mathcal{P}_r\}$ una família de primers de F k_o-definits. Aleshores, existeix una extensió galoisiana N/F amb grup de Galois G, $N \subset F^S$ i tal que N/F és galoisiana k_o-definida.

Demostració. Siguin $u_1,\ldots,u_r$ els generadors del grup profinit G^S satisfent $u_1 \ldots u_r = 1$. Sigui $\pi: G^S \to G$ l'homorfisme definit per $\pi(u_i)=t_i$. Sigui $N=(F^S)^{\ker(\pi)}$; provarem que N/F és galoisiana k_o-definida. Per la proposició 4.2 tenim que $N^\alpha = N$, per a tot $\alpha \in G(\bar{\mathbb{Q}}/k_o)$. Com a conseqüència és fàcil veure que N/F_o és normal, on $F_o = k_o(T)$. Sigui $\Gamma = G(N/F_o)$, és clar que $G=G(N/F)$ és un subgrup normal de Γ; per tant Γ actúa sobre G per conjugació. És a dir, per a cada $a \in \Gamma$, sigui $\varphi_a \in \mathrm{Aut}(G)$ definit per $\varphi_a(s) = asa^{-1}$, $s \in G$. Per ésser G complet, existeix un únic $s_a \in G$ tal que $\varphi_a(s) = asa^{-1} = s_a s\, s_a^{-1}$, per a

tot $s \in G$. Podem doncs definir un homomorfisme de grups

$$j : \Gamma \to G ,$$

on $j(a)=s_a$ per a tot $a \in \Gamma$. Clarament la successió

$$1 \to H \to \Gamma \xrightarrow{j} G \to 1$$

és exacta, on $H=C_\Gamma(G)$ és el centralitzador de G a Γ. Per tant $G=G(N/F) \simeq \Gamma/H$. Com que la inclusió de G a Γ és una secció de j, tenim que

$$\Gamma = G.H .$$

Sigui $N_o=N^H$, és clar que N_o/F_o és galoisiana, i que $G(N_o/F_o) \simeq G=G(N/F)$. Com que $N_o \cap F=N^H \cap N^G=N^\Gamma=F_o$, tenim que $N_o\bar{Q}=N$. Per tant, N/F és galoisiana k_o-definida. #

Remarca. Si un grup finit G és complet i admet una presentació de Hurwitz amb nombre de Hurwitz 1, G es realitza com a grup de Galois sobre Q(T). Per tant, pel teorema d'irreduïbilitat de Hilbert, G també és grup de Galois sobre Q.

§2. Un criteri de racionalitat.

En aquest paràgraf donem un criteri que ens permeterà construir polinomis sobre Q(T) amb grup de Galois certs grups complets prefixats.

En tot el que segueix, F i F_o denotaran $\bar{Q}(T)$ i Q(T), respectivament.

En primer lloc estudiem la ramificació de les extensions finites de $F=\bar{\mathbb{Q}}(T)$.

Sigui L/K una extensió finita i separable de cossos de grau n, N/K la seva clausura galoisiana i $G=G(N/K)$. Anomenem *representació per permutacions* de G associada a L/K la representació fidel i transitiva de G com a permutació de les n arrels del polinomi $\mathrm{Irr}(\theta,K)\in K[X]$, on θ és un element primitiu de L/K.

És clar que aquesta representació no depend de l'element primitiu escollit.

<u>Teorema 4.4.</u> Sigui L/F una extensió finita, N/F la seva clausura galoisiana i $G=G(N/F)$ el seu grup de Galois. Sigui $\mathfrak{q}$ un primer de F i $\bar{\mathfrak{p}}$ un primer de N sobre $\mathfrak{q}$. Si un generador del grup d'inèrcia $T_{\bar{\mathfrak{p}}/\mathfrak{q}}$, en la representació de G per permutacions associada a L/F, descompon en producte de g cicles disjunts de longitud e_i, $1\leqslant i\leqslant g$, aleshores

$$\mathfrak{q}=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g},$$

on $\mathfrak{p}_i$ són primers de L, $1\leqslant i\leqslant g$.

<u>Demostració.</u> Sigui $L=F(\theta)$, $f(X)=\mathrm{Irr}(\theta,F)$, $n=\mathrm{gr}(f(X))$. Suposem que

$$f(X)=f_1(X)\cdots f_{g'}(X)$$

és la descomposició de $f(X)$ en factors irreduïbles a $F_{\mathfrak{q}}$, on $F_{\mathfrak{q}}$ és el completat de F a $\mathfrak{q}$. Si $e'_i=\mathrm{gr}(f_i(X))$, aleshores

$$\mathfrak{p} = \mathfrak{P}_1^{e'_1} \cdots \mathfrak{P}_{g'}^{e'_{g'}} ,$$

on $\mathfrak{P}_i$ són primers de L.

Siguin $x_1,\ldots,x_n$ les arrels de $f(X)$ en una clausura algebraica de $F_{\mathfrak{p}}$. Sigui $s \in G$ un generador de $T_{\mathfrak{P}}(N/F)$. És fàcil veure que la representació de s com a permutació de $x_1,\ldots,x_n$ és la mateixa que la associada a L/F. Aleshores, donat que $T_{\mathfrak{P}}(N/F) \simeq G(F_{\mathfrak{p}}(x_1,\ldots,x_n)/F_{\mathfrak{p}})$, s permuta les arrels de cada $f_i(X)$ entre elles. Per tant, podem descompondre $s = s_1 \cdots s_{g'}$, on els s_i's són dos a dos disjunts. Cada s_i és un cicle. En efecte, si no fos així podriem descompondre $s_i = s_{i,1} \cdots s_{i,r_i}$ en cicles disjunts. Si $x_{i,1},\ldots,x_{i,k_{ij}}$ són les arrels que permuta $s_{i,j}$ i $g_{i,j}(X) = \prod_{r=1}^{k_{ij}} (X - x_{i,r})$, és clar que $g_{i,j}(X)$ és invariant per s_i i, per tant, també per s. En conseqüència, $g_{i,j}(X) \in F_{\mathfrak{p}}[X]$ i $g_{i,j}(X) \mid f_i(X)$. Això està en contra de la irreduïbilitat de $f_i(X)$. Així doncs els s_i són cicles disjunts i aleshores $g' = g$ i $e'_i = e_i$. #

<u>Corol.lari 4.5.</u> Sigui L/F una extensió finita, N/F la seva clausura galoisiana. Sigui $\mathfrak{p}$ un ideal primer de F tal que

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} ,$$

on $\mathfrak{P}_i$'s són primers de L. Aleshores, l'index de ramificació de $\mathfrak{p}$ a N/F és el $\mathrm{mcm}(e_1,\ldots,e_g)$. A més, el generador del

grup d'inèrcia de $\mathfrak{p}$ a N/F, en la representació de G per permutacions associada a L/F, descompon en g cicles disjunts de longitut e_i, $1 \leqslant i \leqslant g$. #

Sigui N/K una extensió de Galois finita, G=G(N/K) el seu grup de Galois i π una representació per permutacions fidel i transitiva de G, de grau n. Direm que L és el *cos associat* a π si

$$L = N^H ,$$

on H és el subgrup de G associat a la representació π ([6], Th.5.3.1). Aleshores la representació per permutacions associada a L/K és equivalent a π.

<u>Observació.</u> Sigui N/F una extensió galoisiana, G=G(N/F) el seu grup de Galois i π una representació per permutacions, de grau n, fidel i transitiva de G. Sigui L el cos associat a π, aleshores la ramificació a L/F está totalment determinada per la de N/F. En efecte, si $\mathfrak{p}$ no ramifica a N, $\mathfrak{p}$ no ramifica a L. Si $\mathfrak{p}$ ramifica a N, s és un generador de $T_{\mathfrak{p}}(N/F)$ i $\pi(s)$ descompon en g cicles disjunts de longitut e_i, $1 \leqslant i \leqslant g$, aleshores

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \quad \text{a} \quad L.$$

Finalment, donem el resultat que serà clau per a la construcció de polinomis amb coeficients a $F_o = Q(T)$ de grup de Galois un grup complet admetent una bona presentació de Hurwitz.

Teorema 4.6. Sigui G un grup finit complet, π una representació per permutacions fidel i transitiva de grau n, de G. Sigui $(t_1,\ldots,t_r)$ una r-presentació de Hurwitz de G amb nombre de Hurwitz $h(t_1,\ldots,t_r)=1$. Siguin $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ primers de F Q-definits. Suposem que hi ha una única extensió K/F_o de grau n, a menys de F_o-isomorfismes, amb ramificació únicament a $\mathfrak{p}_i$, $1\leqslant i\leqslant r$, i del tipus

$$\mathfrak{p}_i = \mathfrak{A}_{i,1}^{e_{i,1}} \ldots \mathfrak{A}_{i,k}^{e_{i,k}} \mathfrak{A}_{i,0} ,$$

on els $\mathfrak{A}_{i,j}$, $0\leqslant j\leqslant k$ són divisors de K, no ramificats; $e_{i,j}$ són les diferents longituts, més grans que 1, dels cicles disjunts en que descompon $\pi(t_i)$, $0<j\leqslant k$ i $e_{i,0}=1$; gr $\mathfrak{A}_{i,j}$ és el numero de cicles disjunts a $\pi(t_i)$ de longitut $e_{i,j}$, $0\leqslant j\leqslant k$. Aleshores, el grup de Galois de la clausura galoisiana de K/F_o és isomorf a G.

Demostració. Sigui $S=\{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}$. Sigui N l'únic subcos de F^S tal que $G=G(N/F)$ i $T_{\mathfrak{p}_i}(N/F)=\langle t_i\rangle$, $1\leqslant i\leqslant r$. Pel Teorema 4.3, N és galoisiana Q-definida, és a dir, existeix N_o/F_o extensió de Galois tal que

$$N_o\bar{Q} = N \quad \text{i} \quad G(N_o/F_o)=G.$$

Sigui H el subgrup de G associat a π ([6], Th. 5.3.1) i $L=N^H$ el cos fix. Ja hem observat que la ramificació a L/F està completament determinada. Sigui $L_o=N_o^H$, és clar que $L_o\bar{Q}=L$. Per ésser L/L_o no ramificada, la ramificació de

L_o/F_o és del mateix tipus que la de K/F_o. A més, $[L_o:F_o]=(G:H)=n$. Per la unicitat de K, tenim que $L_o=K$. #

Apèndix. Nombre de Hurwitz de $\hat{A}_n$

Ja hem esmentat que el problema de la definició d'extensions galoisianas de $\bar{Q}(T)$ és, en general, un problema difícil. No sempre una extensió galoisiana de $\bar{Q}(T)$ és galoisiana Q-definida. En certs casos , però, és pot assegurar que prové d'una de Q (no necessàriament galoisiana) (cf.[32],[37]).

Definició. Una extensió finita N/F, $F=\bar{Q}(T)$, es diu que és k_o-*definida*, $k_o \subset \bar{Q}$, si existeix una extensió $N_o|F_o$, on $F_o=k_o(T)$, tal que

$$N_o\bar{Q}=N \ , \quad [N:F]=[N_o:F_o] \ .$$

Això ens diu que existeix un element $\theta \in N$ tal que $N=F(\theta)$ i $Irr(\theta,F) \in F_o[X]$. L'extensió $F_o(\theta)|F_o$ no serà en general normal.

De manera semblant a la emprada a [15] provem el següent

Teorema 4.7. Sigui G un grup finit, $(t_1,\ldots,t_r)$ una r-presentació de Hurwitz de G tal que $h(t_1,\ldots,t_r)=1$. Sigui $S=\{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}$ una família de primers de F, k_o-definits, $k_o \subset \bar{Q}$. Aleshores existeix una extensió galoisiana N/F, $F \subset F^s$, amb grup de Galois G, tal que N/F és k_o-definida.

Demostració. Siguin $u_1,\ldots,u_r$ generadors del grup profinit $G^S=G(F^S/F)$ satisfent la relació $u_1\ldots u_r=1$. Sigui $\pi:G^S \to G$ l'homomorfisme definit per

$$\pi(u_i)=t_i.$$

Sigui $N=(F^S)^{\ker(\pi)}$ el cos fix per $\ker(\pi)$. És clar que N/F és galoisiana, $N\subset F^S$ i $G(N/F)=G$. Provarem que N/F és k_o-definida.

Per la proposició 4.2, per a tot automorfisme $\alpha\in G(\bar{Q}/k_o)$ és $N^\alpha=N$. En conseqüència, N/F_o és normal, on $F_o=k_o(T)$.

Sigui $r:G(N/F_o) \to G(F/F_o)$ l'epimorfisme de restricció definit per

$$r(a)=a_{|F}\in G(F/F_o) \quad ,$$

on $a\in G(N/F_o)$. És clar que la successió

$$1 \to G \to G(N/F_o) \xrightarrow{r} G(F/F_o) \to 1$$

és exacta. Construirem una secció de l'homomorfisme r.

Sigui $\mathfrak{q}_o=(T-x_o)$, $x_o\in F_o$, un primer de F_o tal que a N/F descompongui completament. Sigui $\mathfrak{p}$ un primer de N sobre $\mathfrak{q}_o$. Si $\alpha\in G(\bar{Q}/k_o)$, les diferents extensions $\tilde{\alpha}\in G(N/F_o)$ de α están caracteritzades per les seves imatges sobre $\mathfrak{p}$. En efecte,

$$\tilde{\alpha}(\mathfrak{p})=\tilde{\alpha}'(\mathfrak{p}) \text{ si i només si } \tilde{\alpha}^{-1}\tilde{\alpha}'(\mathfrak{p}) = \mathfrak{p}.$$

És a dir, si i només si $\tilde{\alpha}^{-1}\tilde{\alpha}' \in D_{\mathfrak{P}}(N/F)=\{1\}$. Per tant,

$$\tilde{\alpha}(\mathfrak{P})=\tilde{\alpha}'(\mathfrak{P}) \text{ si i només si } \tilde{\alpha}=\tilde{\alpha}'.$$

Aleshores, per a cada $\alpha\in G(\bar{Q}/k_o)$ existeix una única extensió $\tilde{\alpha}\in G(N/F_o)$ tal que

$$\tilde{\alpha}(\mathfrak{P})=\mathfrak{P}.$$

Sigui $H=\{a\in G(N/F_o)$, tals que $a(\mathfrak{P})=\mathfrak{P}\}$; acabem de provar que

$$\mathrm{Aut}(\bar{Q}/k_o)\simeq H .$$

Aquest isomorfisme dóna lloc, òbviament, a una secció del epimorfisme r. Sigui $N_o=N^H$ el cos fix pel subgrup $H\subset G(N/F_o)$. Aleshores

$$N_o\cap F=N^H\cap N^G=N^{G(N/F_o)}=F_o .$$

Per tant, N_oF/N_o és galoisiana amb grup de Galois isomorf a $G(F/F_o)\simeq G(\bar{Q}/k_o)$. Com que, per construcció, $G(N/N_o)=H\simeq G(\bar{Q}/k_o)$, tenim que $N_oF=N$. #

Utilitzant aquest resultat, provarem que hi ha extensions galoisianes de $\bar{Q}(T)$ amb grup de Galois $\hat{A}_n$, Q-definides. Pel teorema 4.7, només cal trobar una r-presentació de Hurwitz de $\hat{A}_n$ amb nombre de Hurwitz 1. Provarem que la presentació de $\hat{A}_n$ donada al Capítol I, §3 satisfà aquestes condicions.

En primer lloc, cal conèixer com són els automorfismes de $\hat{A}_n$.

<u>Lema 4.8.</u> Hi ha correspondencia bijectiva entre $Aut(A_n)$ i $Aut(\hat{A}_n)$.

<u>Demostració.</u> Siguin $c,x_1,\ldots,x_{n-2}$ els generadors de $\hat{A}_n$ donats al teorema 1.5. Sigui $\pi:\hat{A}_n \to A_n$ tal que

$$\pi(c)=1 \ ,\pi(x_i)=s_i, \quad 1\leqslant i\leqslant n-2 \ ,$$

on s_i $1\leqslant i\leqslant n-2$ generen A_n.

Sigui $\hat{f}\in Aut(\hat{A}_n)$; és clar que $\hat{f}(c)=c$, ja que el subgrup generat per c és el centre de $\hat{A}_n$. $\hat{f}$ dóna lloc a un homomorfisme $\varphi(\hat{f}):A_n \to A_n$ definit per

$$\varphi(\hat{f})(s)=\pi(\hat{f}(x)),$$

on $s\in A_n$ i $x\in\pi^{-1}(s)$. És clar que $\varphi(\hat{f})$ està ben definida i pel lema de la serp és un automorfisme de A_n. Acabem doncs de definir $\varphi:Aut(\hat{A}_n) \to Aut(A_n)$.

Sigui $f\in Aut(A_n)$; si $f(s_i)=s_i'$, $1\leqslant i\leqslant n-2$, s_i' generen A_n i satisfan les mateixes relacions que els elements s_i. De la demostració del teorema 1.5, es segueix que existeixen $x_i'\in\hat{A}_n$ tals que $\pi(x_i')=s_i'$, $1\leqslant i\leqslant n-2$, satisfent les mateixes relacions que els elements x_i. Sigui $\psi(f):\hat{A}_n \to \hat{A}_n$ definit per

$$\psi(f)(x_i)=x_i' \ , \quad 1 \leqslant i \leqslant n-2,$$

És clar que $\psi(f)(c)=c$, que $\psi(f)\in Aut(\hat{A}_n)$ i que $\pi(\psi(f)(x)=f(\pi(x))$. D'altra banda és clar també que φ, ψ són correspondències inverses l'una de l'altra. #

Recordem que tot automorfisme de A_n s'obté per conjugació per elements de S_n. Per tant $Aut(A_n)\simeq S_n$. ([35],3,2.17).

Sigui $t_1=y$, $t_2=x$, $t_3=(yx)^{-1}$, on x,y són els generadors de $\hat{A}_n$ donats en el teorema 1.6. És clar que (t_1,t_2,t_3) és una 3-presentació de Hurwitz de $\hat{A}_n$. Recordem que

$$\#t_1=2^{n(n-2)(n-3)(n-7)/8}(n-2),$$

$$\#t_2=3,$$

$$\#t_3=\begin{cases} n, \text{ si } n \text{ és imparell,} \\ n-1, \text{ si } n \text{ és parell.} \end{cases}$$

D'altra banda, podem suposar que

$$\pi(t_1)=(12)^{n-1}(34\ldots n),$$

$$\pi(t_2)=(123),$$

i, per tant, $\pi(t_3)=(12\ldots n)^{-1}$, si n és imparell; $\pi(t_3)=(134\ldots n)^{-1}$, si n és parell.

<u>Teorema 4.9.</u> $h(t_1,t_2,t_3)=1$.

Demostració. Sigui $(r_1,r_2,r_3)\in \mathcal{H}(t_1,t_2,t_3)$. Suposem que n és imparell. Existeix $x\in\hat{A}_n$ tal que $r_3=xt_3^k\,x^{-1}$. Com que $\#\langle r_3\rangle=\#\langle t_3\rangle = n$, tenim que $(k,n)=1$, i $\pi(t_3^k)=(12\ldots n)^{-k}$ és un n-cicle. Existeix $a\in S_n$ tal que

$$\varphi_a(\pi(t_3^k))=a(\pi(t_3^k))a^{-1}=\pi(t_3).$$

Pel lema 4.8, existeix $\hat{\varphi}_a\in \mathrm{Aut}(\hat{A}_n)$ tal que

$$\hat{\varphi}_a(t_3^k)=t_3 \ .$$

Per tant, mòdul $\mathrm{Aut}(\hat{A}_n)$, (r_1,r_2,r_3) és equivalent a (r_1',r_2',t_3), on $\pi(r_2')$ és un 3-cicle.

És clar que conjugant per potències de $(12\ldots n)$ podem aconseguir que $\pi(r_2')$ sigui del tipus $(1ij)$. Per tant, mòdul $\mathrm{Aut}(\hat{A}_n)$, (r_1',r_2',t_3) és equivalent a (r_1'',r_2'',t_3), on $\pi(r_2'')=(1ij)$.

D'altra banda,

$$\pi(r_1'')=\pi(t_3)^{-1}\pi(r_2'')^{-1}=(12\ldots n)(1ji) =$$

$$=\begin{cases} (12\ldots j-1\,i\,i+1\ldots n\,j\,j+1\ldots i-1), & \text{si } j<i \\ (12\ldots i-1)(i\,i+1\ldots j-1)(j\,j+1\ldots n), & \text{si } j>i. \end{cases}$$

Com que $\pi(r_1'')$ és conjugat d'una potència de $\pi(r_1)$ a S_n, i $\#\pi(r_1'')=n-2$, la primera possibilitat no es pot donar. Puix

que $\pi(r_1)$ no conté els digits 1 i 2, ha d'ésser i=2, j=3, en la segona possibilitat. És a dir,

$$\pi(r_1'')=(34\ldots n) \text{ i } \pi(r_2'')=(123).$$

Per tant $r_2''=t_3$, ja que ambdós tenen ordre 3. En conseqüència, també $r_1''=t_1$.

El cas n parell es demostra de manera semblant. #

Capítol V. La realització de $\hat{A}_n$

En aquest darrer capítol donem solucions al problema que ens hem plantejat: La realització de les extensions centrals del grup alternat com a grup de Galois.

Provarem que tota extensió central de A_n és grup de Galois sobre $\mathbb{Q}(i)$ i que, per a gairabé la meitat dels valors de n, també ho és sobre $\mathbb{Q}$. Més concretament, demostrem que per als valors de n següents:

$n \equiv 0$ ó 1 (mòd. 8),

$n \equiv 2$ (mòd. 8) i suma de dos quadrats,

$n \equiv 3$ (mòd. 8) i satisfent la propietat (N) (cf. §5),

tota extensió central de A_n és grup de Galois sobre $\mathbb{Q}$.

Per fer això, construirem primer noves equacions amb grup de Galois S_n sobre $\mathbb{Q}(T)$, utilitzant les tècniques donades en el capítol anterior. Aquestes equacions de S_n ens permeten, a la vegada, obtenir noves famílies d'equacions amb grup de Galois A_n, tals que l'obstrucció al problema d'immersió a $\hat{A}_n$ és calculable. La resta del capítol està destinada a diagonalitzar la forma quadràtica traça associada a aquestes equacions i al càlcul del seu invariant de Hasse-Witt.

§1. Noves equacions per als grups S_n, A_n

Donat que el grup simètric S_n és complet, podem aplicar els mètodes del capítol anterior per construir equacions sobre $\mathbb{Q}(T)$ amb grup de Galois isomorf a S_n. Per això, trobarem primerament una 3-presentació de Hurwitz de S_n amb nombre de Hurwitz 1.

Proposició 5.1. Siguin n,k enters positius, primers entre si, $k \leqslant n$. Considerem les permutacions següents

$$s_1=(n\ n-1\ldots 321),$$

$$s_2=(12\ldots k)(k+1\ldots n),$$

$$s_3=(1\ k).$$

Aleshores (s_1,s_2,s_3) és una 3-presentació de Hurwitz de S_n.

Demostració. És clar que $s_3=s_1s_2$, per tant $s_1s_2s_3=1$. Sigui G el subgrup generat per s_1,s_2. Provarem que $G=S_n$. És clar que $s_2^{n-k}=(12\ldots k)^{n-k}\in G$. Per tant $(12\ldots k)\in G$, ja que $(k,n-k)=1$. En conseqüència $(k+1\ k+2\ldots n)\in G$. És una comprovació que

$$s_1(k+1\ldots n)s_3(12\ldots k)s_3 = (12).$$

Aleshores $(12)\in G$ i $G=S_n$. #

<u>Proposició 5.2.</u> $h(s_1,s_2,s_3)=1$, on (s_1,s_2,s_3) és la 3-presentació de Hurwitz de la proposició anterior.

<u>Demostració.</u> Sigui $(t_1,t_2,t_3)\in\mathcal{H}(s_1,s_2,s_3)$. Existeix $a\in S_n$ tal que $t_1=a\ s_1^i\ a^{-1}$. Com que $\#t_1=n$, tenim que $(n,i)=1$ i t_1 és un n-cicle. Per tant, existeix $b\in S_n$ i $bt_1b^{-1}=s_1$. Així doncs, mòdul $\mathrm{Aut}(S_n)=S_n$, (t_1,t_2,t_3) és equivalent a (s_1,t_2',t_3'), on $t_i'=bt_ib^{-1}$, $i=2$ ó 3. És clar que t_3' és una trasposició, ja que $\langle t_3'\rangle$ és conjugat de $\langle s_3\rangle$. És fàcil veure que existeix un enter k tal que $s_1^{-k}t_3'\ s_1^k=(1\ j)$, on $j\leqslant(n+1)/2$. Per tant, mòdul $\mathrm{Aut}(S_n)$, (s_1,t_2',t_3') és equivalent a $(s_1,t_2'',(1j))$ on $t_2''=s_1^{-k}\ t_2'\ s_1^k$. D'altra banda,

$$t_2''=s_1^{-1}(1\ j)=(12\ldots j-1)(j\ j+1\ldots n).$$

Però, $\langle t_2''\rangle,\langle s_2\rangle$ són subgrups conjugats, és a dir

$$t_2''\text{ és conjugat de }((12\ldots k)(k+1\ldots n))^r.$$

Per tant, ha de ésser $j=k+1$. #

Teorema 5.3. Siguin n,k enters positius, primers entre si, $k \leqslant n$. El polinomi

$$G(X,T)=X^{n-k}(X-\frac{n}{n-k})^k-(\frac{-k}{n-k})^k\ T \qquad (1)$$

té grup de Galois sobre $Q(T)$ isomorf a S_n.

Demostració. Considerem els primers $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\infty$ de $\bar{Q}(T)$ donats per les igualtats

$$\mathrm{div}(T)=\mathfrak{p}_0\ \mathfrak{p}_\infty^{-1}\ ,\ \mathrm{div}(T-1)=\mathfrak{p}_1\ \mathfrak{p}_\infty^{-1}.$$

És clar que $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\infty$ són primers Q-definits. Provarem que hi ha una única extensió $K/Q(T)$, de grau n, ramificant únicament a $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$ amb tipus de ramificació

$$\mathfrak{p}_\infty=\mathfrak{P}_\infty^n\ ,\ \mathfrak{p}_0=\mathfrak{P}_{00}^{n-k}\mathfrak{P}_{01}^k,\ \mathfrak{p}_1=\mathfrak{P}_1^2\ \mathfrak{a}, \qquad (2)$$

on $\mathfrak{P}_\infty, \mathfrak{P}_{00}, \mathfrak{P}_{01}, \mathfrak{P}_1$ són primers de grau 1 de K i $\mathfrak{a}$ és un divisor no ramificat de grau n-2. Aleshores, pel teorema 4.6, tindrem que el grup de Galois sobre $Q(T)$ de la clausura galoisiana de K és S_n.

Suposem que existís una extensió $K/Q(T)$ amb l'estruc-

tura de ramificació donada a (2). Per la fórmula del gènere de Hurwitz ([7], IV, 2.4), tenim que

$$2g_K-2 = -2n+n-1+n-k-1+k-1+1 = -2,$$

per tant el gènere g_K de K és igual a zero. D'altra banda K té primers de grau 1, per tant K és un cos de funcions racionals ([3], pàg. 23).

Podem escollir la variable x de manera que $K=Q(x)$ i

$$\mathrm{div}(x)=\mathfrak{p}_{00}\,\mathfrak{p}_\infty^{-1}, \quad \mathrm{div}(x-1)=\mathfrak{p}_1\,\mathfrak{p}_\infty^{-1},$$

$$\mathrm{div}(x-a)=\mathfrak{p}_{01}\,\mathfrak{p}_\infty^{-1}, \mathrm{div}(x^{n-2}+a_{n-3}x^{n-3}+\ldots+a_0)=\mathfrak{a}\,\mathfrak{p}_\infty^{-1},$$

on $a, a_0, \ldots, a_{n-3} \in Q$.

Aleshores, tenim que

$$\mathrm{div}(T)=\mathfrak{q}_0\,\mathfrak{q}_\infty^{-1}=\mathfrak{p}_{00}^{n-k}\mathfrak{p}_{01}^{k}\,\mathfrak{p}_\infty^{-n}=\mathrm{div}(x^{n-k}(x-a)^k),$$

$$\mathrm{div}(T-1)=\mathfrak{q}_1\,\mathfrak{q}_\infty^{-1}=\mathfrak{p}_1^2\,\mathfrak{a}\,\mathfrak{p}_\infty^{n}=\mathrm{div}((x-1)^2(x^{n-2}+a_{n-3}x^{n-3}+\ldots+a_0)).$$

Per tant, existeixen $b, b' \in Q$ tals que

$$x^{n-k}(x-a)^k = bT,$$

$$(x-1)^2(x^{n-2}+a_{n-3}x^{n-3}+\ldots+a_1x+a_0)=b'(T-1) .$$

És immediat veure que b=b' i que

$$x^{n-k}(x-a)^k-b=(x-1)^2(x^{n-2}+a_{n-3}x^{n-3}+\ldots+a_o).$$

Això és equivalent a dir que $g(x)=x^{n-k}(x-a)^k-b$, té exactament una arrel doble, x=1. Per tant ha d'ésser

$$a=n/(n-k) \quad , \quad b=(-k/(n-k))^k.$$

Com a conseqüència, hi ha com a màxim un únic cos, a menys de Q(T) isomorfismes, amb ramificació nomes a $\mathfrak{p}_\infty, \mathfrak{p}_0, \mathfrak{p}_1$ i del tipus (2).

D'altra banda, ara és immediat provar que si K=Q(x), on x és una arrel del polinomi irreduïble

$$G(X,T)=X^{n-k}(X-\frac{n}{n-k})^k-(\frac{-k}{n-k})^k T\in Q(T)[X],$$

K té l'estructura de ramificació desitjada. #

<u>Lema 5.4.</u> El polinomi $G(X,T)=X^{n-k}(X-\frac{n}{n-k})^k-(\frac{-k}{n-k})^k T$ té discriminant

$$D(G)=(-1)^{(n-1)(n-2)/2}n^n(-k/(n-k))^{k(n-1)}T^{n-2}(T-1).$$

Demostració. Denotem per $R(G,G')$ la resultant de G,G', on G' és el polinomi derivat de G respecte de la variable X. Es compleix

$$D(G)=(-1)^{n(n-1)/2}\ R(G,G')$$

$$=(-1)^{n(n-1)/2}n^n(-(\frac{-k}{n-k})^k T)^{k-1}(-\frac{(-k)^k}{(n-k)^k}T)^{n-k-1}((1-\frac{n}{n-k})^k-\frac{(-k)^k}{(n-k)^k}T)$$

$$=(-1)^{(n-1)(n-2)/2}n^n(\frac{-k}{n-k})^{k(n-1)}T^{n-2}(T-1).\ \#$$

A continuació, utilitzant aquests polinomis obtindrem polinomis amb grup de Galois A_n, per a cada valor de n.

Teorema 5.5. Siguin k,n enters positius, primers entre si, $k\leqslant n/2$. El polinomis

$$F_{n,k}(X,T)=X^n-A(nX-k(n-k))^k,$$

si n és imparell, on $A=k^{n-2k}(1-(-1)^{(n-1)/2}nT^2)$;

$$F_{n,k}(X,T)=X^n+k^{n-2k}B^{n-k-1}(nX+(n-k)kB)^k,$$

si n és parell, on $B=((-1)^{n/2}k(n-k)T^2+1)$,

tenen grup de Galois A_n sobre $Q(T)$.

Demostració. Sigui N el cos de descomposició del polinomi (1), obtingut en el teorema 5.3. Sigui $L=N^{A_n}$ el cos fix per A_n; aleshores $Q(T)\subset L\subset N$. Estudiant l'extensió $L/Q(T)$, obtindrem els polinomis $F_{n,k}(X,T)$ amb grup de Galois A_n.

Cas n imparell. És clar que

$$T_{\mathfrak{p}_\infty}(N/Q(T))\subset A_n,$$

$$T_{\mathfrak{p}_0}(N/Q(T)),\ T_{\mathfrak{p}_1}(N/Q(T))\not\subset A_n.$$

Per tant, $\mathfrak{p}_\infty$ no ramifica a $L/Q(T)$ i $\mathfrak{p}_0,\mathfrak{p}_1$ ramifiquen a $L/Q(T)$.

Sigui

$$\mathfrak{p}_0=\bar{\mathfrak{p}}_0^2\ ,\quad \mathfrak{p}_1=\bar{\mathfrak{p}}_1^2$$

on $\bar{\mathfrak{p}}_0$, $\bar{\mathfrak{p}}_1$ són primers de L de grau 1.

Mitjançant la fórmula del gènere de Hurwitz, obtenim que el gènere de L és zero. Per tant L és un cos de funcions racionals. Escollim la funció y de manera que $L=Q(y)$, i

$$\mathrm{div}(y)=\bar{\mathfrak{p}}_0\,\bar{\mathfrak{p}}_1^{-1}.$$

És compleix que

$$\mathrm{div}(T(T-1)^{-1})=\mathfrak{p}_0\,\mathfrak{p}_1^{-1}=\bar{\mathfrak{p}}_0^2\,\bar{\mathfrak{p}}_1^{-2}=\mathrm{div}(y^2).$$

Per tant, existeix $\lambda \in Q$ tal que $T(T-1)^{-1}=\lambda y^2$. Pel lema 5.4 tenim que, en aquest cas,

$$D(G) \in L^{*2} \text{ si i només si } \lambda=(-1)^{(n-2)/2} n \in L^*/L^{*2} .$$

En conseqüència, com que $G(N/L) \simeq A_n$,

$$T=(1-((-1)^{(n-1)/2} n y^2)^{-1})^{-1} .$$

Substituint a $G(X,T)$ i fent els canvis de variable

$$\tilde{y}=y^{-1}((-1)^{n/2} n)^{-1}, \quad \tilde{X}=k\ X^{-1} ,$$

obtenim

$$F(\tilde{X},\tilde{Y})=\tilde{X}^n-k^{n-2k}(1-(-1)^{(n-1)/2} n \tilde{y}^2)(n\tilde{X}-k(n-k))^k .$$

<u>Cas n parell.</u> De manera semblant al cas anterior obtenim que, a $L/Q(T)$, $\mathfrak{p}_0$ no ramifica i $\mathfrak{p}_1, \mathfrak{p}_\infty$ ramifiquen. Sigui

$$\mathfrak{p}_\infty = \bar{\mathfrak{p}}_\infty^2 , \quad \mathfrak{p}_1=\bar{\mathfrak{p}}_1^2,$$

on $\bar{\mathfrak{p}}_1, \bar{\mathfrak{p}}_\infty$ són primers de L de grau 1. Igual que abans, L és un cos de funcions racionals i escollim la variable y, de manera que $L=Q(y)$ i

$$\mathrm{div}(y)=\bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_\infty^{-1} .$$

Aleshores,

$$\mathrm{div}(T-1)=\mathfrak{p}_1\mathfrak{p}_\infty^{-1}=\mathfrak{P}_1^2\mathfrak{P}_\infty^{-2}=\mathrm{div}(y^2).$$

Sigui $\lambda\in\mathbb{Q}$ tal que $T-1=\lambda y^2$. Pel lema 5.4,

$$D(G)\in L^* \text{ si i només si } \lambda=(-1)^{n/2}k/(n-k)\in L^*/L^{*2}.$$

En conseqüència,

$$T=1+(-1)^{n/2}k\ y^2/(n-k).$$

Substituint a $G(X,T)$ i fent els canvis de variable

$$y=(n-k)\tilde{y},\ X=(-k)((-1)^{n/2}k(n-k)\tilde{y}^2+1)\tilde{X}^{-1},$$

obtenim el resultat. #

<u>Observació.</u> Aquestes equacions, en el cas $k=1$, foren obtingudes per Matzat ([15]).

<u>Corol.lari 5.6.</u> El grup de Galois de $F_{n,k}(X,T)$ sobre $\mathbb{Q}(i)(T)$ és isomorf a A_n, $n\geqslant 5$.

<u>Demostració.</u> Sigui N el cos de descomposició de $F_{n,k}(X,T)\in\mathbb{Q}(T)$. És clar que $i\notin N$. En efecte, si $i\in N$ aleshores

$$Q(T) \subset Q(i)(T) \subset N,$$

i $G(N/Q(T)) \simeq A_n$ tindria un subgrup d'índex 2, la qual cosa no és possible. En conseqüència $G(N(\imath)/Q(\imath)(T)) \simeq A_n$. #

Remarca. Pel teorema d'irreduïbilitat de Hilbert existeixen infinits valors de $T=t$, $t \in \mathbb{Z}$, tals que els polinomis $F_{n,k}(X,t)$ tenen grup de Galois isomorf a A_n, sobre $\mathbb{Q}$ i també sobre $\mathbb{Q}(i)$.

§2. El lema fonamental

Sigui $f(X)=X^n+a_kX^k+\ldots+a_0 \in K[X]$ un polinomi irreduïble amb coeficients a un cos K de característica zero. Sigui θ una arrel de $f(X)$ i $E=K(\theta)$.

Aquest apartat està enterament dedicat a l'estudi de l'espai quadràtic $(E, Tr_{E/K}(X^2))$. El resultat més interessant és el càlcul de $Tr_{E/K}$ restringida a cert subespai de E, que, d'altra banda, és fonamental per determinar l'invariant de Hasse-Witt de les equacions del teorema 5.5.

La forma quadràtica $Tr_{E/K}(X^2)$ està determinada pels valors $Tr(\theta^i)$, on $0 \leqslant i \leqslant 2n-2$, ja que $1,\theta,\ldots,\theta^{n-1}$ és una base de E com K-espai vectorial.

Es comprova sense dificultat, bé per un càlcul directe, bé utilitzant les fórmules de Newton ([2], V, App I), que si $k<n/2$,

$Tr(1)=n,$

$Tr(\theta^i)=0, \qquad 1\leqslant i\leqslant n-k-1,$

$Tr(\theta^i)=-i\ a_{n-i}, \qquad n-k\leqslant i\leqslant n.$

Si $k\leqslant \frac{n+1}{3}$,

$Tr(\theta^{n+i})=0, \qquad 1\leqslant i\leqslant n-2k-1,$

$$Tr(\theta^{n+i})=\sum_{j=\max\{n-k-i,0\}}^{\min\{k,n-i\}}(i+j)a_j\ a_{n-(i+j)}, \qquad n-2k\leqslant i\leqslant n-2.$$

La diagonalització de $Tr_{E/K}(X^2)$, depèn de la paritat de n-k.

<u>Cas n-k parell.</u> Els vectors $1,\theta,\ldots,\theta^{(n-k)/2}$ són ortogonals dos a dos i $\theta,\ldots,\theta^{(n-k-2)/2}$ són vectors isòtrops. Per tant l'espai E descompon de la manera següent

$$E=\langle 1\rangle \perp \langle\theta^{(n-k)/2}\rangle \perp E' \perp E'' ,$$

on $E'\simeq(n-k-2)/2\ H$, H és un pla hiperbòlic, i E" és un subespai de dimensió k, contingut en un suplementari de $\langle\theta,\ldots,\theta^{(n-k-2)/2}\rangle a \langle 1,\theta,\ldots,\theta^{(n-k)/2}\rangle^{\perp}$.

Cas n-k imparell. Els vectors $1,\theta,\ldots,\theta^{(n-k-1)/2}$ són dos a dos ortogonals i $\theta,\ldots,\theta^{(n-k-1)/2}$ són vectors isòtrops. Per tant l'espai E descompon de la manera següent

$$E=\langle 1\rangle \perp E' \perp E'',$$

on $E'\simeq(n-k-1)/2\ H$, H és un pla hiperbòlic, i E" és un subespai de dimensió k contingut en un suplementari de $\langle\theta,\ldots,\theta^{(n-k-1)/2}\rangle$ a $\langle 1,\theta,\ldots,\theta^{(n-k-1)/2}\rangle^{\perp}$.

Per acabar l'estudi de l'espai quadràtic E, hauriem de classificar l'espai E". Per tal fí, calcularem el valor de la forma quadràtica restringida al subespai $\langle 1,\theta,\ldots,\theta^{[(n-k)/2]}\rangle^{\perp}$.

Lema fonamental 5.7. Siguin $e,v\in\langle 1,\theta,\ldots,\theta^{m}\rangle^{\perp}$, on $m=[(n-k)/2]$. Suposem que

$$e=\sum_{i=0}^{n-1}\lambda_i\theta^i\ ,\qquad v=\sum_{i=0}^{n-1}\mu_i\theta^i\ .$$

Aleshores, si n-k és imparell,

$$Tr_{E/K}(ev)=\sum_{j=1}^{k}-\mu_{m+j}\Big(\sum_{i=1}^{k+1-j}\lambda_{m+i}(n-k-1+i+j)a_{k+1-i-j}\Big)+A;$$

Si n-k és parell,

$$Tr_{E/K}(ev)=\lambda_m\mu_m(n-k)a_k+\sum_{j=1}^{k-1}-\mu_{m+j}\left(\sum_{i=1}^{k-j}\lambda_{m+i}(n-k+i+j)a_{k-i-j}\right)+A\,.$$

On

$$A=\frac{1}{n}\left[\sum_{1\leqslant i\leqslant j\leqslant k}\delta_{ij}(\lambda_{n-i}\mu_{n-j}+\lambda_{n-j}\mu_{n-i})\left(\sum_{r=1}^{\min\{k-j,i\}}-a_{j+r}a_{i-r}n(j-i+2r)+a_ia_ji(n-j)\right)\right]$$

i $\delta_{ij}=\begin{cases}1, & \text{si } i\neq j\\ 1/2, & \text{si } i=j.\end{cases}$

<u>Demostració.</u> Un vector $e=\sum_{i=0}^{n-1}\lambda_i\theta^i$ pertany a $<1,\theta,\ldots,\theta^m>^{\perp}$ si i només si

$$Tr(e)=\lambda_0 n-\sum_{i=n-k}^{n-1}\lambda_i \quad \text{i} \quad a_{n-i}=0,$$

i (3)

$$Tr(e\theta^j)=-\sum_{i=n-k-j}^{n-j}\lambda_i(i+j)a_{n-(i+j)}=0,\quad 1\leqslant j\leqslant m.$$

Anotem els altres valors de $Tr(\theta^j e)$, per a $j>m$,

$$Tr(\theta^j e)=-\sum_{i=n-k-j}^{n-j}\lambda_i(i+j)a_{n-(i+j)},$$

si $m<j\leqslant n-2k$.

$$Tr(\theta^j e) = -\sum_{i=\max\{0,n-k-j\}}^{n-j} \lambda_i (i+j) a_{n-(i+j)} + \sum_{i=2n-2k-j}^{n-1} \lambda_i Tr(\theta^{i+j}),$$

si $n-2k+1 \leqslant j \leqslant n-1$.

Per tant,

$$Tr_{E/K}(ev) = Tr((\sum_{i=0}^{n-1} \lambda_i \theta^i) v) = \sum_{i=m+1}^{n-1} \lambda_i \; Tr(\theta^i v)$$

$$= \sum_{i=m+1}^{n-2k} \lambda_i (-\sum_{j=n-k-i}^{n-i} \mu_i (i+j) a_{n-(i+j)}) +$$

$$+ \sum_{i=n-2k+1}^{n-1} \lambda_i (-\sum_{j=\max\{0,n-k-i\}}^{n-i} \mu_i (i+j) a_{n-(i+j)} + \sum_{j=2n-2k-i}^{n-1} \mu_j Tr(\theta^{i+j}))$$

$$= -\mu_0 (\sum_{i=n-k}^{n-1} \lambda_i i a_{n-i}) + \sum_{j=1}^{m-1} \mu_j (-\sum_{i=n-k-j}^{n-j} \lambda_i (i+j) a_{n-(i+j)}) +$$

$$+ \sum_{j=0}^{k} \mu_{m+j} (-\sum_{i=m+1}^{n-m-j} \lambda_i (i+j+m) a_{n-(i+j+m)}) +$$

$$+ \sum_{j=1}^{2k-1} \mu_{n-j} (\sum_{i=j}^{2k-1} \lambda_{n-2k+i} \; Tr(\theta^{2n-2k-i-j})).$$

Si denotem per

$$A'=-\lambda_0\mu_0 n+\sum_{j=1}^{2k-1}\mu_{n-j}\left(\sum_{i=j}^{2k-1}\lambda_{n-2k+i}\ Tr(\theta^{2n-2k+i-j})\right),$$

Tenim que

$$Tr_{E/K}(ev)=T'+\sum_{j=1}^{m-1}-\mu_j Tr(\theta^j e)+\sum_{j=0}^{k}\mu_{m+j}\left(-\sum_{i=m+1}^{n-m-j}\lambda_i(i+j+m)a_{n-(i+j+m)}\right)$$

$$=T'+\sum_{j=0}^{k}\mu_{m+j}\left(-\sum_{i=m+1}^{n-m-j}\lambda_i(i+j+m)a_{n-(i+j+m)}\right).$$

Provarem que A'=A. Aleshores ja és fàcil acabar la demostració del lema. N'hi ha prou en observar que:

Si n-k és parell, $m=(n-k)/2$ i aleshores, $Tr(\theta^m e)=0$

ens diu que

$$\lambda_m(n-k)a_k=-\sum_{i=m+1}^{n-m}\lambda_i(i+m)a_{n-(i+m)}.$$

Si n-k és imparell, $m=(n-k-1)/2$ i aleshores,

$$0=Tr(\theta^m e)=-\sum_{i=m+1}^{n-m}\lambda_i(i+m)a_{n-i-m}.$$

Per demostrar que A'=A fem un càlcul previ del valor de A'.

Lema 5.8. Per a tot $1 \leqslant q \leqslant k-1$ és compleix

$$A'+n\lambda_0\mu_0 = \sum_{s=1}^{q} -\left(\left(\sum_{i=1}^{s} \lambda_{n-i} a_{k-(s-i)}\right)\left(\sum_{i=q-s+1}^{k} \mu_{n-2k+s+i}(n-k+i)a_{k-i}\right)\right)+$$

$$+\sum_{s=1}^{q} -\left(\left(\sum_{i=1}^{s} \mu_{n-i} a_{k-(s-i)}\right)\left(\sum_{i=q-s+1}^{k} \lambda_{n-2k+s+i}(n-k-i)a_{k-i}\right)\right)+$$

$$+\sum_{t=2k-q-1}^{q+2} \mu_{n-t}\left(\sum_{i=1}^{2k-t} \lambda_{n-i} Tr(\theta^{2n-t-i})\right)+\sum_{r=1}^{q+1} \mu_{n-r}\left(\sum_{i=1}^{2k-(q+1)} \lambda_{n-i} Tr(\theta^{2n-i-r})\right)$$

Demostració. Per inducció sobre q. Si q=1, tenint en compte que $Tr(\theta^{2n-2k})=(n-k)a_k^2$ i que $Tr(e.\theta^{k-1})=Tr(v.\theta^{k-1})=0$, car $1 \leqslant k \leqslant m$, s'obté el resultat.

Suposem-ho cert per q-1, anem a provar-ho per q. Sigui R_λ el terme següent

$$\sum_{i=1}^{q} \lambda_{n-i} Tr(\theta^{2n-2k+q-i})+\sum_{s=1}^{q-1}\left(-\sum_{i=1}^{s} \lambda_{n-i} a_{k-(s-i)}\right)(n-k+q-s)a_{k-q+s}.$$

R_λ és el coeficient de μ_{n-2k+q} en l'expressió de $A'+n\lambda_0\mu_0$ vàlida per q-1. Un terme semblant en funció dels paràmetres μ_i que denotem R_μ, és el coeficient de λ_{n-2k+q} en la citada expressió de $A'+n\lambda_0\mu_0$.

Afirmació

$$R_\lambda=\left(\sum_{i=1}^{q}\lambda_{n-i}\ a_{k-(q-i)}\right)\ a_k(n-k),$$

$$R_\mu=\left(\sum_{i=1}^{q}\mu_{n-i}\ a_{k-(q-i)}\right)\ a_k(n-k).$$

Suposant certa l'afirmació i tenint en compte que

$$Tr(\theta^{k-q}e)=Tr(\theta^{k-q}v)=0,$$

obtenim

$$A'+n\lambda_0\,\mu_0=\left(\sum_{i=1}^{q}\lambda_{n-i}a_{k-(q-i)}\right)\left(-\sum_{i=1}^{k}\mu_{n-2k+q+i}(n-k+i)a_{k-i}\right)+$$

$$+\left(\sum_{i=1}^{q}\mu_{n-i}a_{k-(q-i)}\right)\left(-\sum_{i=1}^{k}\lambda_{n-2k+q+i}(n-k+i)a_{k-i}\right)+$$

$$+\sum_{s=1}^{q-1}\left(\left(\sum_{i=1}^{s}\lambda_{n-i}a_{k-(s-i)}\right)\left(-\sum_{i=q-s+1}^{k}\mu_{n-2k+s+i}(n-k+i)a_{k-i}\right)\right)+$$

$$+\sum_{s=1}^{q-1}\left(\left(\sum_{i=1}^{s}\mu_{n-i}a_{k-(s-i)}\right)\left(-\sum_{i=q-s+1}^{k}\lambda_{n-2k+s-i}(n-k+i)a_{k-i}\right)\right)+$$

$$+\sum_{t=2k-q-1}^{q+2}\mu_{n-t}\left(\sum_{i=1}^{2k-t}\lambda_{n-i}\ Tr(\theta^{2n-t-i})\right)+$$

$$+\sum_{r=1}^{q+1}\mu_{n-r}\Big(\sum_{i=q+1}^{2k-1}\lambda_{n-2k+i}\ \mathrm{Tr}(\theta^{2n-2k+i-r})\Big).$$

D'on s'obté el resultat. Per tant, només tenim que provar l'afirmació.

Substituint $\mathrm{Tr}(\theta^{2n-2k+q-i})$ pel seu valor, tenim

$$R_\lambda=\sum_{i=1}^{q}\lambda_{n-i}\Big(\sum_{j=\max\{0,k-q+i\}}^{\min\{k,2k-q+i\}}a_j(n-2k+q-i+j)a_{2k-(q-i+j)}\Big)-$$

$$-\sum_{s=1}^{q-1}\Big(\sum_{i=1}^{s}\lambda_{n-i}a_{k-(s-i)}\Big)(n-k+q-s)a_{k-q+s}.$$

Observem que, per ésser $1\leqslant q\leqslant k-1$, aleshores $\max\{0,k-q+i\}=k-q+i$ i que això passa si i només si $\min\{k,2k-q+i\}=k$. Per tant,

$$R_\lambda=\lambda_{n-q}(a_k^2(n-k))+\sum_{i=1}^{q-1}\lambda_{n-i}\Big(\sum_{j=k-q+i}^{k}a_j(n-2k+q-i+j)a_{2k-(q-i-j)}\Big)$$

$$-\sum_{i=1}^{q-1}\sum_{s=i}^{q-1}\lambda_{n-i}\ a_{k-(s-i)}(n-k+q-s)a_{k-q+s}$$

$$=\Big(\sum_{i=1}^{q}\lambda_{n-i}\ a_{k-q+i}\Big)a_k(n-k).\quad\#$$

Acabem ara la demostració del lema fonamental. Pel lema 5.8 aplicat en el cas $q=k-1$ i pel fet de que $Tr(e)=Tr(v)=0$, obtenim

$$A'=\sum_{s=1}^{k-1} -\left(\left(\sum_{i=1}^{s} \lambda_{n-i}a_{k-(s-i)}\right)\left(\sum_{i=k-s}^{k} \mu_{n-2k+s+i}(n-k+i)a_{k-i}\right)\right) +$$

$$+\sum_{s=1}^{k-1} -\left(\left(\sum_{i=1}^{s} \mu_{n-i}a_{k-(s-i)}\right)\left(\sum_{i=k-s}^{k} \lambda_{n-2k+s+i}(n-k+i)a_{k-i}\right)\right) +$$

$$+\sum_{r=1}^{k} \mu_{n-r}\left(\sum_{i=k}^{2k-1} \lambda_{n-2k+i}\ Tr(\theta^{2n-2k+i-r}\right) -$$

$$-\frac{1}{n}\left(\sum_{i=0}^{k-1} \lambda_{n-k+i}(n-k+i)a_{k-i}\right)\left(\sum_{i=0}^{k-1} \mu_{n-k+i}(n-k+i)a_{k-i}\right) .$$

Sigui $c_{x,y}$ el coeficient de $\lambda_{n-x}\mu_{n-y}$, $1\leqslant x\leqslant y\leqslant k$ en l'expressió anterior de A'. Aleshores

$$c_{x,y}=Tr(\theta^{2n-x-y})-\frac{1}{n}((n-x)a_x a_y(n-y)) +$$

$$+\sum_{s=\max\{k-y,x\}}^{k-1} -a_{k-s+x}a_{y+s-k}(n+k-y-s) +$$

$$+\sum_{s=\max\{y,k-x\}}^{k-1} -a_{k-s+y}(n+k-s-x)a_{-k+s+x}.$$

Substituint $Tr(\theta^{2n-x-y})$ pel seu valor i suposant que $x \leqslant k-y$, obtenim

$$c_{x,y} = \sum_{i=0}^{x+y} a_i (n+i-x-y) a_{x+y-i} - \frac{1}{n}(n-x)(n-y) a_x a_y -$$

$$- \sum_{i=x+1}^{x+y} a_i a_{x+y-i} (n+i-x-y) - \sum_{i=y+1}^{x+y} a_i a_{x+y-i} \ (n-x-y+i)$$

$$= \sum_{i=0}^{x-1} a_i (n+i-x-y) a_{x+y-i} + (n-y) a_x a_y + \sum_{i=x+1}^{x+y} a_i a_{x+y-i} (n+i-x-y) -$$

$$-\frac{1}{n}(n-x)(n-y) a_x a_y - \sum_{i=x+1}^{x+y} a_i a_{x+y-i} (n+i-x-y) - \sum_{i=y+1}^{x+y} a_i a_{x+y-i} (n-x-y+i) =$$

$$= \frac{1}{n} a_x a_y (n-y) x + \sum_{i=0}^{x-1} a_i (n+i-x-y) a_{x+y-i} - \sum_{j=0}^{x-1} a_j a_{x+y-j} (n-j) =$$

$$= \frac{1}{n}\left(a_x a_y (n-y) x - \sum_{r=1}^{x} a_{x-r} a_{y+r} n (y-x+2r)\right).$$

Fent un càlcul anàleg, si $x>k-y$, obtenim el mateix resultat. #

§3. Càlcul efectiu de l'obstrucció global

Siguin n,k enters positius, k imparell i $k \leqslant (n+1)/3$. Considerem el polinomi irreduïble de $K[X]$ donat per

$$F_k(X)=X^n+a(bX+c)^k, \qquad (4)$$

on

$$a=\begin{cases} -k^{n-2k}(1-(-1)^{(n-1)/2}nT^2) & , \text{ si } n \text{ és imparell} \\ k^{n-2k}\ ((-1)^{n/2}k(n-k)T^2+1)^{n-k-1}, & \text{si } n \text{ és parell,} \end{cases}$$

$b=n$

$$c=\begin{cases} -k(n-k) & , \text{ si } n \text{ és imparell} \\ (n-k)k((-1)^{n/2}k(n-k)T^2+1) & , \text{ si } n \text{ és parell,} \end{cases}$$

i $T \in K$.

Suposem que el grup de Galois de $F_k(X)$ sobre K és isomorf a A_n. Pel teorema 5.5 i pel corol.lari 5.6, sabem que això passa si $K=\mathbb{Q}(T)$ o bé si $K=\mathbb{Q}(i,T)$.

Sigui N el cos de descomposició de $F_k(X)$. En aquest apartat calcularem el valor de l'obstrucció global al problema d'immersió galoisiana de N/K a $\hat{A}_n$. Pel teorema de Serre, 3.1, el valor de l'obstrucció ve donat per l'invariant

de Hasse-Witt de la forma quadràtica $Tr_{E/K}(X^2)$, on $E=K(\theta)$, θ una arrel de $F_k(X)$.

<u>Proposició 5.9.</u> Siguin $e,v\in\langle 1,\theta,\ldots,\theta^m\rangle^{\perp}$, on $m=[(n-k)/2]$. Suposem que

$$e=\sum_{i=0}^{n-1}\lambda_i\theta^i \quad \text{i} \quad v=\sum_{i=0}^{n-1}\mu_i\theta^i .$$

Aleshores,

$$Tr_{E/K}(ev)=\sum_{j=1}^{k}-a\mu_{n-m-j}\Big(\sum_{i=k+1-j}^{k}\lambda_{n-m-i}(n+k+1-i-j)\binom{k}{i+j-k-1}b^{i+j-k-1}c^{2k+1-i-j}\Big)+A ,$$

si n és parell. I

$$Tr_{E/K}(ev)=\sum_{j=1}^{k-1}\mu_{n-m-j}a\Big(\sum_{i=k-j}^{k-1}\lambda_{n-m-i}(n+k-i-j)\binom{k}{i+j-k}b^{i+j-k}c^{2k-i-j}\Big)+$$

$$+\lambda_{n-m-k}\mu_{n-m-k}(n-k)ab^k+A,$$

si n és imparell. On

$$A=a^2nk(n-k)\Big(\sum_{i=1}^{k}\lambda_{n-i}\binom{k-1}{i-1}c^{k-i}b^{i-1}\Big)\Big(\sum_{i=1}^{k}\mu_{n-i}\binom{k-1}{i-1}c^{k-i}b^{i-1}\Big).$$

Abans de provar aquesta proposició donem un resultat que necesitarem sobre nombres combinatoris.

<u>Lema 5.10.</u> Si i,j,k són enters positius, $i+j \leqslant k$, es compleix

$$\sum_{r=1}^{i} \binom{k}{j+r}\binom{k}{i-r}(j-i+2r)=k\binom{k-1}{j}\binom{k-1}{i-1}.$$

<u>Demostració.</u>

$$\sum_{r=1}^{i} \binom{k}{j+1}\binom{k}{i-r}(j-i+2r)=\binom{k}{j+1}\left(\binom{k}{i-1}(j-i+2)+S\right)$$

on

$$S=\sum_{r=2}^{i} \binom{k}{i-r}(j-i+2r)\,\frac{(k-j-1)\dots(k-j-r+1)}{(j+2)\dots(j+r)}\ .$$

Afirmem que, per a tot $2 \leqslant t \leqslant i-1$, es compleix

$$S=\sum_{r=2}^{i-t} \binom{k}{i-r}(j-i+2r)\frac{(k-j-1)\dots(k-j-r+1)}{(j+2)\dots(j+r)}+\frac{(k-j-1)\dots(k-j-i+t)(k-1)\dots(k-(t-1))}{(j+2)\dots(j+i-t)\cdot(t-1)!}.$$

Ho provem per inducció sobre t. Per t=2 és una comprovació. Suposem-ho cert per t-1, sigui

$$S'=\sum_{r=2}^{i-t} \binom{k}{i-r}(j-i+2r)\frac{(k-j-1)\dots(k-j-r+1)}{(j+2)\dots(j+r)}\ .$$

Aleshores

$$S=S'+\binom{k}{t-1}(j+i-2t+2)\ \frac{(k-j-1)\dots(k-j-i+t)}{(j+2)\dots(j+i-t+1)}\ +$$

$$+\ \frac{(k-j-1)\dots(k-j-i+t-1)(k-1)\dots(k-(t-2))}{(j+2)\dots(j+i-t+1)(t-2)!}$$

$$=S'+\frac{(k-1)\dots(k-t+2)(k-j-1)(k-j-i+t)}{(t-1)!\ \ (j+2)\dots(j+i-t+1)}(j+i-t+1)(k-t+1).$$

Per tant, si t=i-1 tenim que

$$S=\ \frac{(k-1)\dots(k-i+2)(k-j-1)}{(i-2)!}\ .$$

Aleshores

$$\sum_{r=1}^{i}\binom{k}{j+r}\binom{k}{i-r}(j-i+2r)=\binom{k}{j+1}\left(\binom{k}{i-1}(j-i+2)+\frac{(k-1)\dots(k-i+2)(k-j-1)}{(i-2)!}\right)$$

$$=\binom{k}{j+1}\ \frac{(k-1)\dots(k-i+2)}{(i-1)!}((k-i+1)(j+1))$$

$$=\binom{k-1}{j}\binom{k-1}{i-1}k.\quad \#$$

Demostració de la proposició 5.9. Substituint en les expressions de les traces del lema fonamental 5.7 el coeficient a_i pel seu valor en aquest cas, $0 \leqslant i \leqslant k$, s'obté, directament, la primera part de l'expressió de $Tr_{E/K}(ev)$.

El valor de A, substituint i aplicant el lema 5.10, és

$$A=\frac{a^2}{n}\sum_{1\leqslant i\leqslant j\leqslant k}\delta_{ij}(\lambda_{n-i}\mu_{n-j}+\lambda_{n-j}\mu_{n-i})b^{i+j}c^{2k-i-j}\left(-nk\binom{k-1}{i-1}\binom{k-1}{j}+i(n-j)\binom{k}{i}\binom{k}{j}\right)$$

$$=\frac{a^2(n-k)k}{n}\sum_{1\leqslant i\leqslant j\leqslant k}\delta_{ij}(\lambda_{n-1}\mu_{n-j}+\lambda_{n-j}\mu_{n-i})b^{i+j}c^{2k-i-j}\binom{k-1}{i-1}\binom{k-1}{j-1}$$

$$=\frac{a^2(n-k)k}{n}\left(\sum_{i=1}^{k}\lambda_{n-i}b^ic^{k-i}\binom{k-1}{i-1}\right)\left(\sum_{i=1}^{k}\mu_{n-i}b^ic^{k-i}\binom{k-1}{i-1}\right). \quad \#$$

Estem ja en disposició de classificar completament l'espai quadràtic E, en aquest cas.

Teorema 5.11. Si $E=K(\theta)$, on θ és una arrel del polinomi (4). Aleshores

$$E=\langle 1\rangle \perp E' \perp \langle v\rangle ,$$

$$\text{on } E' \simeq \begin{cases} \langle \theta^{(n-k)/2}\rangle \perp ((n-3)/2)H, & \text{si } n \text{ és imparell,} \\ ((n-2)/2)H, & \text{si } n \text{ és parell,} \end{cases}$$

éssent H un pla hiperbòlic.

<u>Demostració.</u> El polinomi $F_k(X)$, veure (4), és un cas particular dels tractats al §2. Per tant, si $m=[(n-k)/2]$, l'espai quadràtic E descompon en la forma:

Si n és imparell,

$$E=\langle 1\rangle \perp \langle \theta^m\rangle \perp E' \perp E'' ,$$

on $E'\simeq(m-1)H$, H és un pla hiperbòlic, i E" és un subespai de dimensió k contingut en un suplementari de $\langle\theta,\ldots,\theta^{m-1}\rangle$ a $\langle 1,\theta,\ldots,\theta^m\rangle^{\perp}$.

Si n és parell,

$$E=\langle 1\rangle \perp E' \perp E'' ,$$

on $E'\simeq mH$ i E" és un subespai de dimensió k contingut en un suplementari de $\langle\theta,\ldots,\theta^m\rangle$ a $\langle 1,\theta,\ldots,\theta^m\rangle^{\perp}$.

El coneixement de la traça restringida a $\langle 1,\theta,\ldots,\theta^m\rangle^{\perp}$, proposició 5.9, ens permetrà construir efectivament suficients vectors isòtrops per classificar completament l'espai E".

En primer lloc observem que si $e=\sum_{i=0}^{n-1}\lambda_i\theta^i\in E''$, aleshores a la vista de les fòrmules (3) del §2, deduïm que $\lambda_{n-m},\ldots,\lambda_{n-1}$, λ_0 són funció lineal de $\lambda_{n-m-1},\ldots,\lambda_{n-m-k}$, mentre que aquests darrers paràmetres són lliures. Per tant,

existeixen constants $A_1,\dots,A_k\in K$ tals que

$$\sum_{i=1}^{k}\lambda_{n-i}b^i c^{k-i}\binom{k-1}{i-1}=A_1\lambda_{n-m-1}+\dots+A_k\lambda_{n-m-k}.$$

Suposem primer que les constants $A_i=0$ per a tot $1\leqslant i<(k+1)/2$. Aleshores definim els vectors $e_i=\sum_{j=0}^{n-1}\lambda_j^i\theta^j$, $1\leqslant i\leqslant(k-1)/2$, de manera que

$$\lambda_j^i=0,\quad \text{per a tot } j\neq n-m-i,\ 0\leqslant j\leqslant n-1;$$

$$\lambda_{n-m-i}^i\neq 0\ .$$

Tenim doncs $(k-1)/2$ vectors linealment independents tals que

$$Tr(e_i^2)=Tr(e_ie_j)=0,\quad 1\leqslant i,j\leqslant(k-1)/2,$$

per la proposició 5.9. En conseqüència,

$$E''=E_1\perp\langle v\rangle,$$

on $E_1\simeq((k-1)/2)H$.

Suposem ara que existeix un r, $1\leqslant r\leqslant(k-1)/2$ tal que $A_r\neq 0$. Considerem els vectors $e_i=\sum_{j=0}^{n-1}\lambda_j^i\theta^j$, on

$\lambda^i_j=0$, per a tot $j\neq n-m-r$, $j\neq n-m-i$, $0\leqslant j\leqslant n-1$,

$\lambda^i_{n-m-i}\neq 0$ i λ^i_{n-m-r} tals que $A_1\lambda^i_{n-m-1}+\ldots+A_k\lambda^i_{n-m-k}=0$,

per a tot $i\neq r$, $1\leqslant i\leqslant (k-1)/2$. És clar que els vectors $\{\theta^i, e_j\}$, $0\leqslant i\leqslant m$, $1\leqslant j\leqslant (k-1)/2, j\neq r$, són linealment independents i que

$$Tr(e_i^2)=Tr(e_ie_j)=0,\ 1\leqslant i,j\leqslant (k-1)/2 \quad i,j\neq r,$$

per la proposició 5.9. Tenim doncs,

$$E''=E_1\perp E_2 \ ,$$

on $E_1\simeq((k-3)/2)H$, dim $E_2=3$.

Tenim que acabar de classificar aquest espai E_2. Distingim ara segons la paritat de n. Sigui $m=[(n-k)/2]$.

Si n és parell, sigui $v=\sum_{i=0}^{n-1}\mu_ie_i$, on

$\mu_i=0$ per a tot $i\neq n/2$, $i\neq n-m-r$, $1\leqslant i\leqslant n-1$,

$\mu_{n/2}\neq 0$ i μ_{n-m-r} tal que $A_1\mu_{n-m-1}+\ldots+A_k\mu_{n-m-k}\neq 0$.

Observem que $n/2=n-m-(k+1)/2$. És clar que $v\in E_2$ i que per a un $\mu_{n/2}$ convenient ,

$$\mathrm{Tr}\ v^2=-a\mu_{n/2}^2 nc^k+\frac{a^2k(n-k)}{n}(A_1\mu_{n-m-1}+\ldots+A_k\mu_{n-m-k})^2$$

$$=-(n-k)k((-1)^{n/2}k(n-k)T^2+1)n+k(n-k)n$$

$$=n(n-k)^2k^2(-1)^{n/2}T^2=(-1)^{(n-2)/2}n\in K^*/K^{*2}.$$

D'altra banda, és fàcil comprovar que

$$d(E_2)=n(-1)^{n/2}\in K^*/K^{*2}\ .$$

Per tant tenim que E_2 descompon

$$E_2=\langle v\rangle\perp E_3,$$

on E_3 és un pla hiperbòlic.

Suposem ara que n és imparell. Sigui $v=\sum_{i=0}^{n-1}\mu_i\theta^i$, on

$\mu_i=0$, per a tot $i\neq m$, $i\neq m+r$, $0\leqslant i\leqslant n-1$,

$\mu_m\neq 0$ i μ_{m+r} tal que $A_1\mu_{n-m-1}+\ldots+A_k\mu_{n-m-k}\neq 0$.

És clar que $v\in E_2$ i que per a un μ_m convenient,

$$\mathrm{Tr}v^2=\mu_m^2(n-k)ab^k+a^2k(n-k)(A_1\mu_{n-m-1}+\ldots+A_k\mu_{n-m-k})^2/n$$

$$=a(n-k)\,(\mu_m^2nb^k+ak(A_1\mu_{n-m-1}+\ldots+A_k\mu_{n-m-k})^2)\,/n$$

$$=a(n-k)(1-(1-(-1)^{(n-1)/2}nT^2)\,/\,n=a(n-k)(-1)^{(n-1)/2}T^2$$

$$=-k(n-k)(-1)^{(n-1)/2}(1-(-1)^{(n-1)/2}nT^2)\in K^*/K^{*2}.$$

D'altra banda, és fàcil comprovar que

$$d(E_2)=(n-k)k(-1)^{(n-1)/2}(1-(-1)^{(n-1)/2}nT^2).$$

Per tant tenim que E_2 descompon

$$E_2=\langle v\rangle\perp E_3,$$

on E_3 és un pla hiperbòlic. #

<u>Observació.</u> La proposició 5.9 és certa per a tot polinomi irreduïble del tipus $X^n+a(bX+c)^k$. La descomposició de l'espai E donada al teorema 5.11 només és vàlida per als valors de a,b,c de (4). De fet, però, aquests valors únicament s'han utilitzat en el últim pas, és a dir, en la classificació del subespai E_2 de dimensió 3.

Ara ja estem en condicions de calcular l'invariant de Hasse-Witt dels polinomis $F_k(X)$ donats a (4).

Teorema 5.12. Sigui $\theta\in\bar{K}$ una arrel del polinomi $F_k(X)=X^n+a(bX+c)^k$ donat a (4). Sigui $E=K(\theta)$. L'invariant de Hasse-Witt de l'extensió E/K és

$$w(E)=\begin{cases}(-(n-k)k,(-1)^{(n-1)/2}n)\otimes(-1,-1)^{(n+1)(n-1)/8}, & \text{si } n \text{ és imparell,}\\ (n,(-1)^{n/2})\otimes(-1,-1)^{n(n-2)/8}, & \text{si } n \text{ és parell.}\end{cases}$$

Demostració. Suposem primer que n és imparell. Pel teorema anterior, E descompon

$$E=\langle 1\rangle\perp\langle\theta^{(n-k)/2}\rangle\perp\langle v\rangle\perp E',$$

on $E'\simeq((n-3)/2)H$, H pla hiperbòlic. Recordem que

$$Tr(\theta^{n-k})=-(n-k)ab^k.$$

Aleshores, utilitzant les propietats esmentades en el capítol I, §1, tenim que

$$w(E)=w(\langle 1\rangle\perp\langle\theta^{(n-k)/2}\rangle\perp\langle v\rangle)\otimes((-1)^{(n-3)/2},-1)\otimes(-1,-1)^{(n-3)(n-5)/8}$$

$$=w(\langle 1\rangle\perp\langle\theta^{(n-k)/2}\rangle)\otimes(-n(n-k)ab^k,-(-1)^{(n-3)/2})\otimes(-1,-1)^{(n-3)(n-1)/8}$$

$$=(n,-(n-k)ab^k)\otimes(-n(n-k)ab^k,(-1)^{(n-1)/2})\otimes(-1,-1)^{(n-1)(n-3)/8}$$

$$=((-1)^{(n-1)/2}n,n(n-k)ab^k)\otimes(-1,-1)^{(n-1)/2}\otimes(-1,-1)^{(n-1)(n-3)/8}$$

$$=((-1)^{(n-1)/2}n,-n(n-k)k^{n-2k}(1-(-1)^{(n-1)/2}nT^2)n^k)\otimes(-1,-1)^{(n-1)(n+1)/8}$$

$$=((-1)^{(n-1)/2}n,-k(n-k)(1-(-1)^{(n-1)/2}nT^2)\otimes(-1,-1)^{(n-1)(n+1)/8}$$

$$=((-1)^{(n-1)/2}n,-k(n-k))\otimes((-1)^{(n-1)/2}n,1-(-1)^{(n-1)/2}nT^2)\otimes(-1,-1)^{(n-1)(n+1)/8}$$

$$=((-1)^{(n-1)/2}n,-k(n-k))\otimes(-1,-1)^{(n-1)(n+1)/8}.$$

Suposem ara que n és parell. Pel teorema anterior tenim que en aquest cas E descompon

$$E=\langle 1\rangle\perp\langle v\rangle\perp E' ,$$

on $E'\simeq((n-2)/2)H$, H pla hiperbòlic.

Aleshores,

$$w(E)=w(\langle 1\rangle\perp\langle v\rangle)\otimes(-1,-1)^{(n-2)(n-4)/8}\otimes((-1)^{(n-2)/2},-1)$$

$$=(n,n(-1)^{(n-2)/2})\otimes(-1,-1)^{n(n-2)/8}$$

$$=(n,(-1)^{n/2})\otimes(-1,-1)^{n(n-2)/8}. \quad \#$$

§4. Resolució del problema sobre Q(i)

Provarem a continuació que per als polinomis $F_{n,k}(X,T)$ construïts al teorema 5.5 existeixen infinites especialitzacions $T=t$, $t\in\mathbb{Z}$, de manera que els polinomis resultants $F_{n,k}(X,t)$, sobre $\mathbb{Q}(i)$, admeten una immersió galoisiana a $\hat{A}_n$. Tenim així, per tant, per a cada valor de n, families

infinites de polinomis que resolen el problema d'immersió sobre una *mateixa* extensió quadràtica, $Q(i)$.

<u>Teorema 5.13.</u> Siguin n,k enters positius primers entre si. Sigui k imparell, $k \leqslant (n+1)/3$. Sigui $F_{n,k}(X,T)$ el polinomi construit al teorema 5.5 i N el seu cos de descomposició. L'extensió $N/Q(i,T)$ admet una immersió galoisiana a $\hat{A}_n$ per a tot valor de k, si n és parell i per a tot valor de k quadrat, si n és imparell.

<u>Demostració.</u> Pel corol.lari 5.6, el polinomi $F_{n,k}(X,T)$ té grup de Galois isomorf a A_n sobre $Q(i,T)$. Sigui θ una arrel de $F_{n,k}(X,T)$ i $E=Q(i,T)(\theta)$. Pel teorema 5.12, tenim els següents valors per l'invariant de Hasse-Witt,

$$w(E/Q(i,T)) = \begin{cases} 1, & \text{si } n \text{ és parell,} \\ (-(n-k),n)=1, & \text{si } n \text{ és imparell i } k \text{ és un quadrat.} \end{cases}$$

Per tant, per la proposició 3.2, l'obstrucció perquè $F_{n,k}(X,T)$ admeti una immersió galoisiana a $\hat{A}_n$ sobre $Q(i,T)$ és nul.la. En conseqüència, per a tot valor de n, $n \neq 6$ ó 7, $\hat{A}_n$ és grup de Galois sobre $Q(i,T)$. #

Fent ús del teorema d'irreduïbilitat de Hilbert s'obté

Corol.lari 5.14. El problema d'immersió galoisiana a $\hat{A}_n$ sobre $\mathbb{Q}(i)$ té solució per a tot n, $n\neq 6$ ó 7.

Corol.lari 5.15. Tota extensió central de A_n es realitza com a grup de Galois sobre $\mathbb{Q}(i)$ per a tot n, $n\neq 6$ ó 7.

§5. Solucions sobre Q

En aquest darrer paràgraf donem les solucions obtingudes sobre Q del problema invers de la Teoria de Galois que ens hem plantejat.

Definició. Direm que un enter n ($n\neq 4$ m, $n\neq 8m+7$) té la *propietat* (N) si existeixen enters k_1,k_2,k_3 tals que $n=k_1^2+k_2^2+k_3^2$ i, per algun i, $1\leqslant i\leqslant 3$, $(k_i,n)=1$ i $k_i^2\leqslant (n+1)/3$.

Teorema 5.16. Siguin n,k enters positius primers entre si. Sigui k imparell, $k\leqslant (n+1)/3$. Sigui $F_{n,k}(X,T)$ el polinomi construït al teorema 5.5 i N el seu cos de descomposició. L'extensió $N/\mathbb{Q}(T)$ admet immersió galoisiana a $\hat{A}_n$ en els casos següents

$n\equiv 0$ (mòd. 8) , $k>0$

$n\equiv 1$ (mòd. 8) , k un quadrat

$n\equiv 2$ (mòd. 8) i n suma de dos quadrats, $k>0$

$n\equiv 3$ (mòd. 8) i n satisfent (N), $k=k_i^2$.

Demostració. Sigui θ una arrel del polinomi $F_{n,k}(X,T)$ i $E=\mathbb{Q}(T,\theta)$.

Si n és parell, pel teorema 5.12, tenim que

$$w(E)=(-n,(-1)^{n/2})\otimes(-1,-1)^{n(n-2)/8}.$$

Per tant,

Si $n\equiv 0$ (mòd. 8), $w(E)=1$.

Si $n\equiv 2$ (mòd. 8), $w(E)=(n,-1)$.

Si $n\equiv 4$ (mòd. 8), $w(E)=(-1,-1)\neq 1$.

Si $n\equiv 6$ (mòd. 8), $w(E)=(-n,-1)\neq 1$.

És clar que, $(n,-1)=1$ si i només si n és suma de dos quadrats.

Si n és imparell, pel teorema 5.12, tenim que

$$w(E)=(-(n-k)k,(-1)^{(n-1)/2}n)\otimes(-1,-1)^{(n+1)(n-1)/8}.$$

Per tant,

Si $n\equiv 1$ (mòd. 8), $w(E)=(-(n-k)k,n)$.

Si $n\equiv 3$ (mòd. 8), $w(E)=(-(n-k)k,-n)\otimes(-1,-1)$.

Si $n\equiv 5$ (mòd. 8), $w(E)=(-(n-k)k,n)\otimes(-1,-1)$.

Si $n\equiv 7$ (mòd. 8), $w(E)=(-(n-k)k,-n)$.

En conseqüència, si $n\equiv 1$ (mòd. 8), l'extensió $N/\mathbb{Q}(T)$ admet una immersió galoisiana a $\hat{A}_n$, per a tot enter k quadrat.

En efecte,

$$w(E)=(-(n-k)k,n)=(-(n-k),n)=1.$$

Si $n\equiv 3$ (mòd. 8) i n satisfà la propietat (N), aleshores existeix un valor de k tal que $N/\mathbb{Q}(T)$ admet una immersió galoisiana a $\hat{A}_n$. En efecte, donat que n satisfà la propietat (N), existeix una descomposició de n en suma de tres quadrats satisfent:

$$n=k_1^2+k_2^2+k_3^2,$$

$$(k_i,n)=1,\ k_i^2 \leqslant (n+1)/3 \text{ per algun } 1\leqslant i\leqslant 3.$$

Sigui $k=k_i^2$, aleshores

$$\begin{aligned} w(E) &= (-(n-k)k,-n) \otimes (-1,-1) \\ &= (-(n-k),-n) \otimes (-1,-1) \\ &= ((n-k),-1) \otimes (-(n-k),n). \end{aligned}$$

Ara, $(n-k,-1)=1$, car $n-k$ és suma de dos quadrats. D'altra banda és immediat que $(-(n-k),n)=1$. #

Pel teorema d'irreduïbilitat de Hilbert, hi ha infinits valors de $T=t$, $t\in\mathbb{Z}$ tals que $F_{n,k}(X,t)$ admet una immersió galoisiana a $\hat{A}_n$ sobre $\mathbb{Q}$, pels valors de n donats al teorema anterior. Si $n\equiv 4,5,6$ ó 7 (mòd. 8) aquests polinomis no admeten una immersió galoisiana a $\hat{A}_n$, per a cap valor de k.

Remarca. Tot enter $n\equiv 3$ (mod. 8) és suma de tres quadrats i admet descomposicions primitives. Mitjançant l'ordinador hem comprovat que tot enter $n\leqslant 600.000$, $n\equiv 3$ (mòd. 8), té la propietat (N). Sembla ésser, per tant, que la propietat (N) *no* és restrictiva.

D'altra banda, A. Arenas ha provat: Tot nombre de la forma q^t, on q és un primer, $q\equiv 3$ (mòd. 8) té la propietat (N). Si $n=p_1^{a_1}p_2^{a_2}q_1^{b_1}\ldots q_s^{b_s}$, on els primers $p_i\equiv 1$ (mòd. 4) i els $q_j\equiv 3$ (mòd. 4), $1\leqslant j\leqslant s$, tota descomposició primitiva de n en suma de tres quadrats té un sumand primer amb n.

Corol.lari 5.17. El problema d'immersió galoisiana a $\hat{A}_n$ sobre Q té solució si

$n\equiv 0, 1$ (mòd. 8),

$n\equiv 2$ (mòd. 8) i n és suma de dos quadrats,

$n\equiv 3$ (mòd. 8) i n satisfà la propietat (N). #

Corol.lari 5.18. Per a aquests valors de n, tota extensió central de A_n es realitza com a grup de Galois sobre Q. #

Índex terminològic

Bibliografia

1. E. Artin, J. Tate; Class field theory. Benjamin, 1967.

2. N. Bourbaki; Éléments des mathématique, Algèbre Chap. 5. Hermann, 1967.

3. C. Chevalley; Introduction to the theory of algebraic functions of one variable. Amer. Math. Soc. Surveys, n° 6, 1951.

4. H.S.M. Coxeter, W. J. Moser; Generators and relations for discrete groups. Ergeb. der Math. 14, Springer, 1965.

5. A. Grothendieck; Géométrie formelle et géométrie algebrique. Séminaire Bourbaki. May 1959, 182, 1-28.

6. M. Hall; The theory of groups. The Macmillan Cy., 1959.

7. R. Hartshorne; Algebraic Geometry. Graduate Texts in Math. 52, Springer, 1977.

8. D. Hilbert; Ueber die irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. J. Reine Angew. Math. 110 (1892), 104-129.

9. K. Hoechsmann; Zum Einbettungsproblem. J. Reine Angew. Math. 229 (1968), 81-106.

10. B. Huppert; Endliche Gruppen I. Die Grund. der Math. Wiss. 134, Springer, 1967.

11. A. Hurwitz; Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten. Math. Ann. 39 (1891), 1-61. Math. Werke I, 321-383.

12. M. Ikeda; Zum Existenz eigentlicher galoisscher Körper beim Einbettungsproblem. Hamb. Abh. 24 (1960) 126-131.

13. A. M. Macbeath; Extensions of the rationals with Galois Group PGL $(2,Z_n)$. Bull. London Math. Soc., 1 (1969), 332-338.

14. B.H. Matzat; Konstruktion von Zahlkörpen mit der Galois gruppe M_{11} über $Q(\sqrt{-11})$. Manuscripta Math. 26 (1979), 103-111.

15. B.H. Matzat, Zur konstruktion von Zahl-und Funktionen-Körpern mit vorgegebener Galoisgruppe. Karlsruhe , 1980.

16. J. Milnor; Introduction to algebraic K-theory. Princeton University Press, 1971.

17. E. Nart , N. Vila; Equations with Absolute Galois group isomorphic to A_n. J. Number Theory, 16 (1983), 6-13.

18. J. Neukirch; Über das Einbettungsproblem der algebraischen Zahlentheorie. Invent. Math. 21 (1973), 59-116.

19. J. Neukirch; On solvable Number Fields. Invent. Math 53 (1979), 135-164.

20. O. T. O'Meara; Introduction to quadratic forms. Die Grund. der Math. Wiss. 117, Springer, 1963.

21. H. Reichardt; Konstruktion von Zahlkörper mit gegebener Galoisgruppe von Primzahlpotenzordnung. J. Reine Angew. Math. 177 (1937), 1-15.

22. I. R. Šafarevič; On p-extensions. Math. Sbornik 20 (1947), 351-363. Amer. Math. Soc. Transl. 4 (1960), 59-79.

23. I. R. Šafarevič; Construction of fields of algebraic numbers with given solvable Galois group. Izv. Akad. Nauk SSSR Ser. Mat. 18 (1954), 525-578. Amer. Math. Soc. Transl. 4 (1960), 185-237.

24. A. Scholz; Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I. Math. Z 42 (1937), 161-188.

25. I. Schur; Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. J. Mat. 127 (1904), 20-50.

26. I. Schur; Über die Darstellungen der symmetrischen und alternierender Gruppen durch gebrochene lineare Substitutionen. J. Math. 139 (1911), 155-250.

27. I. Schur; Affektlose Gleichungen in der theorie der Laguerreschen und Hermiteschen Polynome. J. Reine Angew. Math. 165 (1931), 52-58.

28. J. P. Serre; Cohomologie Galoisienne. Lecture Notes in Math. 5, Springer, 1965.

29. J. P. Serre; Corps Locaux. Hermann,1968.

30. J. P. Serre; Propiétés galoisiennes de points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 259-331.

31. J. P. Serre; Carta a Martinet, Febrer 1982. (Publicació en preparació).

32. K. Y. Shih; On the construction of Galois extensions of function fields and number fields. Math. Ann. 207 (1974), 99-120.

33. G. Shimura; A reciprocity law in non-solvable extensions. J. Reine Angew. Math. 221 (1966), 209-220.

34. J. Sonn; SL(2,5) and Frobenius Galois groups over Q. Cand. J. Math. XXXII (1980), 281-293.

35. M. Suzuki; Group Theory I. Die Grund. der Math. Wiss. 247, Springer, 1963.

36. H. Weber; Lehrbuch der Algebra. Chelsea, 1a. ed. 1894-96.

37. A. Weil; The field of definition of a variety. Amer J. of Math. 78 (1956), 509-524.

Rebut el 20 de juliol del 1983

Departament d'Àlgebra i Fonaments.
Facultat de Matemàtiques
Universitat de Barcelona
ESPANYA