Annales de l'institut Fourier

Nuria Vila

Polynomials over Q solving an embedding problem

Annales de l'institut Fourier, tome 35, nº 2 (1985), p. 79-82
<http://www.numdam.org/item?id=AIF_1985__35_2_79_0>

© Annales de l'institut Fourier, 1985, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
35, 2 (1985), 79-82.

POLYNOMIALS OVER Q SOLVING AN EMBEDDING PROBLEM

par Núria VILA

In 1980 we have constructed infinitely many polynomials with coefficients in **Q** having absolute Galois group the alternating group A_n (cf. [2]). Recently, J.-P. Serre (cf. [4]) has described the obstruction to a certain embedding problem as the Hasse-Witt invariant of an associated quadratic form.

In this note, using Serre's result, we see that the fields defined by the equations of [2], Th. 2.1, can be embedded in a Galois extension with Galois group $\hat{A}_n$, the representation group of A_n, if and only if $n \equiv 0 \pmod 8$ or $n \equiv 2 \pmod 8$ and n sum of two squares. Then, for theses values of n, every central extension of A_n occurs as Galois group over **Q**.

I would like to thank Professor J.-P. Serre for communicating to me the results of [2] and for pointing out to me the case $n \equiv 0 \pmod 8$.

Let K be a number field and R its ring of integers. Let

$$F(X) = X^n + aX^2 + bX + c, \qquad ac \neq 0,$$

be a polynomial of R[X] satisfying the following conditions:

(i) F(X) is irreducible and primitive.

(ii) $b^2(n-1)^2 = 4acn(n-2)$.

(iii) $(-1)^{n/2}c$ is a square.

(iv) If $u = -b(n-1)/2(n-2)a$, there exists a prime ideal $\mathfrak{p}$ of R such that

$$c(n-1) \notin \mathfrak{p}, \quad f(u) \in \mathfrak{p} \qquad \text{and} \qquad 3 \nmid v_{\mathfrak{p}}(f(u)).$$

In [2], Th. 1.1, we have proved that if n is an even integer, $n > 2$, the Galois group of F(X) over K is isomorphic to the alternating group A_n.

Key-words : Algebraic Number theory - Field theory and polynomials - Inverse problem of Galois theorem.

The main result of this note is

THEOREM. — *Suppose that* n *is an even integer,* $n > 6$. *Let* N *be the splitting field of the polynomial* F(X). *The extension* N/K *can be embedded in a Galois extension with Galois group a given central extension of* A_n *if and only if*

$$\begin{array}{lll} n \equiv 0 \ (mod.\ 8), & or & \\ n \equiv 2 \ (mod.\ 8) & and & n \text{ is a sum of two squares.} \end{array}$$

Since for n even, we have constructed infinitely many polynomials with coefficients in $\mathbf{Q}$ satisfying the condition (i), (ii), (iii), (iv) (cf. [2], Th. 2.1), we have:

COROLLARY. — *Every central extension of* A_n *appears as Galois group over* $\mathbf{Q}$ *if*

$$\begin{array}{lll} n \equiv 0 \ (mod.\ 8), & or & \\ n \equiv 2 \ (mod.\ 8) & and & n \text{ is a sum of two squares.} \end{array}$$

Other values of n are considered in [5].

First of all, we prove the following

LEMMA. — *Let* $f(X) = X^n + aX^2 + bX + c \in R[X]$ *be an irreducible polynomial such that* $b^2(n-1)^2 = 4acn(n-2)$. *Let* $E = K(\theta)$, *where* θ *is a root of* $f(X)$. *The quadratic form* $\mathrm{Tr}_{E/K}(X^2)$ *diagonalizes as follows:*

$$\mathrm{Tr}_{E/K}(X^2) \sim \begin{cases} nX_1^2 - (n-2)aX_2^2 + X_3X_4 + \cdots + X_{n-1}X_n, & \text{if } n \text{ is even,} \\ nX_1^2 + X_2X_3 + \cdots + X_{n-1}X_n, & \text{if } n \text{ is odd.} \end{cases}$$

Proof. — Easy computations give:

$$\begin{array}{ll} \mathrm{Tr}(1) = n, & \mathrm{Tr}(\theta^i) \ \ = 0, \quad 1 \leqslant i \leqslant n-3, \\ \mathrm{Tr}(\theta^{n-2}) = -(n-2)a, & \mathrm{Tr}(\theta^{n-1}) = -(n-1)b. \end{array}$$

Suppose that n is even; let $m = n/2$. Clearly $1, \theta, \ldots, \theta^{m-1}$ are pairwise orthogonal vectors of E and $\theta, \ldots, \theta^{m-2}$ are isotropic vectors of E. Then the quadratic space E splits:

$$E \sim \langle 1 \rangle \perp \langle \theta^{m-1} \rangle \perp (m-2)H \perp E',$$

where H is a hyperbolic plane and E′ is a quadratic plane.

Since $b^2(n-1)^2 = 4ac(n-2)$, the polynomial

$$g(X) = nf(X) - Xf'(X)$$

has a double root u. Hence the discriminant of $f(X)$ is

$$\begin{aligned} d &= (-1)^{n(n-1)/2}R(f,f') \\ &= (-1)^{n(n-1)/2}R(g,f')/n \\ &= (-1)^{n(n-1)/2}(n-2)^{n-1}b^{n-1}f'(u)^2/n, \end{aligned}$$

where $R(f,f')$ is the resultant of f and f'.

Consequently, the discriminant of E' in K^*/K^{*2} is -1. Thus, E' is a hyperbolic plane.

The proof in the case n odd runs in an analogous way.

Proof of the Theorem. – Let $\hat{A}_n$ be the representation group *(Darstellungsgruppe)* of A_n (cf. [1]). The group $\hat{A}_n$ is the only non-trivial extension of A_n with kernel $\mathbf{Z}/2$ (cf. [3]).

Let $0 \neq a_n \in H^2(A_n, \mathbf{Z}/2)$ be the cohomological class associated to $\hat{A}_n$. It is easy to see (cf. [5], Th. 1.1) that our embedding problem is reduced to embed N/K in a Galois extension with Galois group $\hat{A}_n$. As it is well-known, the obstruction to this embedding problem is $\inf(a_n)$, where

$$\inf : H^2(A_n, \mathbf{Z}/2) \to H^2(G_K, \mathbf{Z}/2)$$

is the homomorphism associated to the epimorphism $p: G_K \to A_n$. Let θ be a root of $F(X)$ and $L = \mathbf{Q}(\theta)$. By [4], Th. 1,

$$\inf(a_n) = w(L/K),$$

where $w(L/K)$ denote the Hasse-Witt invariant of the quadratic form $\mathrm{Tr}_{L/K}(X^2)$. By the Lemma, we have

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

Therefore, $w(L/K) = 1$ if and only if $n \equiv 0 \pmod{8}$, or $n \equiv 2 \pmod{8}$ and n is a sum of two squares.

Remark. – If n is an odd square and $f(X) \in R[X]$ is a polynomial satisfying the conditions (i), (ii) and (iv), the Galois group of $f(X)$ is also isomorphic to A_n (cf. [2], Th. 1.6). Then, we can proceed as in the

Theorem to prove that, in this case, the splitting field of $f(X)$ can be embedded in a Galois extension with Galois group any central extension of A_n.

BIBLIOGRAPHY

[1] B. HUPPERT, Endliche Gruppen I, *Die Grund. der Math. Wiss.*, 134, Springer, 1967.

[2] E. NART and N. VILA, Equations with absolute Galois group isomorphic to A_n, *J. Number Th.*, 16 (1983), 6-13.

[3] I. SCHUR, Über die Darstellungen der symmetrischen und alternierender Gruppen durch gebrochene lineare Substitutionen, *J. reine angew. Math.*, 139 (1911), 155-250.

[4] J.-P. SERRE, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Com. Math. Helv.*, to appear.

[5] N. VILA, On central extensions of A_n as Galois group over $\mathbf{Q}$, to appear.

Manuscrit reçu le 26 avril 1984.

Núria VILA,

Departament d'Algebra i Fonaments
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via, 585
08007 Barcelona (Espanya).