Available at WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE DIRECT

Journal of Algebra 266 (2003) 27–33

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Tame A_n-extensions of $\mathbb{Q}$ ☆

Bernat Plans [a] and Núria Vila [b,*]

[a] *Dept. de Matemàtica Aplicada I, Universitat Politècnica de Catalunya, Av. Diagonal, 647, 08028 Barcelona, Spain*

[b] *Dept. d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007 Barcelona, Spain*

Received 10 July 2001

Communicated by Michel Broué

Abstract

For every positive integer n and every finite set S of prime numbers, we construct A_n-extensions of $\mathbb{Q}$ unramified at all primes in $S \cup \{\infty\}$; moreover, these extensions are obtained as splitting fields of totally real monic polynomials in $\mathbb{Z}[X]$ of degree n whose discriminant is not divisible by any prime number p in S. As a corollary, we obtain that there exist infinitely many linearly disjoint tamely ramified A_n-extensions of $\mathbb{Q}$.

1. Introduction

With regard to the Inverse Galois Problem with prescribed ramification behaviour, B. Birch posed the following question [1]:

Problem. Given a finite group G, is there a tamely ramified normal extension $F/\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) \cong G$?

In this paper we consider the above question for $G = A_n$, the alternating group. We obtain an affirmative answer in this case, as a consequence of our main result:

☆ Research partially supported by MCYT grant BFM2000-0794-C02-01.

* Corresponding author.
E-mail addresses: bernat.plans@upc.es (B. Plans), vila@mat.ub.es (N. Vila).

0021-8693/03/$ – see front matter
doi:10.1016/S0021-8693(03)00380-6

Theorem 1.1. *For every positive integer n and every finite set S of prime numbers, there exist infinitely many linearly disjoint extensions of $\mathbb{Q}$, each one obtained as the splitting field over $\mathbb{Q}$ of a totally real monic polynomial $f(X) \in \mathbb{Z}[X]$ of degree n such that*:

(1) *The discriminant of $f(X)$ is not divisible by any prime number of S.*
(2) *$f(X)$ has Galois group A_n over $\mathbb{Q}$.*

It is well known that, given a monic polynomial $f(X)$ in $\mathbb{Z}[X]$ of degree n and a prime number p not dividing its discriminant, the decomposition type of $f(X) \pmod p$ coincides with the permutation type of any Frobenius element over p in the Galois group of a splitting field of $f(X)$ over $\mathbb{Q}$, $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \subseteq S_n$. One can ensure that $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong S_n$ just by requiring the reductions of $f(X)$ modulo some prime numbers to have some well-chosen decomposition types. Moreover, by Tchebotarev's Density Theorem, this finite set of primes can be assumed to be disjoint with any finite set S given in advance. It follows that there exist S_n-extensions of $\mathbb{Q}$ unramified at all primes in a fixed arbitrary finite set.

In the case of the alternating group, the local conditions on $f(X)$ (at S) must be compatible with a global one that guarantees $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \subseteq A_n$: the discriminant of $f(X)$ must be a square in $\mathbb{Q}$. This can be achieved by requiring that $f(X)$ arises by suitable specialization of a certain well-chosen polynomial in $\mathbb{Q}(T)[X]$ with Galois group over $\mathbb{Q}(T)$ isomorphic to A_n.

We first construct a polynomial $P(X)$ of degree n with well-chosen local behaviour; we force $P(X)$ to satisfy some extra conditions which enables us to apply a result of J.F. Mestre [2] in order to obtain a regular A_n-extension of $\mathbb{Q}(T)$ defined by a polynomial of type $P(X) - TQ(X)$. Applying Hilbert's Irreducibility Theorem to $P(X) - TQ(X)$ we obtain the desired A_n-extensions of $\mathbb{Q}$ by suitable specialization of T.

We can argue as above only for odd n. As noticed in [2], from a regular A_n-extension of $\mathbb{Q}(T)$ of type $P(X) - TQ(X)$ we can always obtain a regular A_{n-1}-extension of some $\mathbb{Q}(U)$. We can then deduce the main result for even n from the odd n case provided $P(X)$ is chosen carefully enough.

2. Previous results

We first recall Mestre's result [2, Proposition 2].

Proposition 2.1. *Let $P(X)$ be a monic polynomial in $\mathbb{Z}[X]$ of odd degree $n \geqslant 3$ such that*

(i) *$P(X)$ has square integer discriminant,*
(ii) *$P(X) \equiv X^n - X \pmod l$ for some prime l not dividing $n(n-1)(n-2)$.*

There exists a polynomial $Q(X) \in \mathbb{Z}[X]$ of degree at most $n-1$ such that $P(X) - TQ(X)$ defines a regular A_n-extension of $\mathbb{Q}(T)$.

Note that, using Mestre's terminology, assumption (ii) ensures $P(X)$ being H-general (cf. [2, Proposition 4]).

Let S be a finite set of prime numbers.

Our purpose is to apply Proposition 2.1 to a polynomial of type $P(X) = Xg(X)h(X)$; we first prove the existence of $h(X)$ and $g(X)$ with suitable local properties, in particular at all primes in $S \cup \{\infty\}$, and such that the polynomial $h(X)g(X)$ has square integer discriminant.

$D(f(X))$ will denote the discriminant of a polynomial $f(X)$; the resultant of $f_1(X)$ and $f_2(X)$ will be denoted by $R(f_1, f_2)$.

Lemma 2.2. *Let $n \geqslant 7$ be an odd integer. Given a prime number $l \notin S$ such that $l \equiv 1 \pmod{n-1}$, there exist monic polynomials $h(X)$ in $\mathbb{Z}[X]$ of degree $n-3$ satisfying the following conditions*:

(i) *$h(X)$ divides $X^{n-1} - 1$ in $\mathbb{F}_l[X]$,*
(ii) *$h(X)$ is irreducible in $\mathbb{F}_p[X]$ for every $p \in S$, $p \neq 2$,*
(iii) *$h(X)$ does not have irreducible factors of degree less than* 3 *in $\mathbb{F}_2[X]$ and $D(h(X)) \equiv 5 \pmod 8$,*
(iv) *all roots of $h(X)$ are real.*

Proof. By the Chinese Remainder Theorem, the existence of $h(X)$ satisfying conditions (i), (ii), (iii) together is equivalent to the existence of three polynomials satisfying them separately. Since $X^{n-1} - 1$ has $n-1$ distinct roots in $\mathbb{F}_l$, condition (i) is clear. Condition (ii) can certainly be satisfied. We check condition (iii) by giving explicit polynomials satisfying it.

Note that $D(X^m + X^k + 1) \equiv (-1)^{m/2}(1 - km) \pmod 8$ for even $m \geqslant 4$ and odd $k < m$ such that $m \neq 2k$. Since $X^m + X^k + 1$ has no roots in $\mathbb{F}_2$, $X^2 + X + 1$ is its only possible irreducible factor in $\mathbb{F}_2[X]$ of degree less than 3. Let $m = n - 3$.

(1) For $m \equiv 2, 4 \pmod 8$, take $h(X) = X^m + X^3 + 1$.
(2) For $m \equiv 6 \pmod 8$, the polynomials $X^m + X + 1$ and $X^m + X^5 + 1$ have no common factors in $\mathbb{F}_2[X]$; at least one of them satisfies (iii).
(3) For $m \equiv 0 \pmod 8$ and $m - 6 > 9$, the polynomials $h_1(X) = X^{m-6} + X + 1$, $h_2(X) = X^{m-6} + X^5 + 1$ and $h_3(X) = X^{m-6} + X^9 + 1$ are pairwise coprime in $\mathbb{F}_2[X]$; at least one of the polynomials $(X^6 + X + 1)h_i(X)$, $i \in \{1, 2, 3\}$, satisfies (iii).
For $m = 8$, take $h(X) = X^8 + X^4 + X^3 + X + 1$.

At this point, we have proved the existence of a polynomial $h_0(X)$ satisfying conditions (i), (ii) and (iii).

Let $h_M(X) = h_\infty(X) + \frac{1}{M}(h_0(X) - h_\infty(X))$, where $h_\infty(X)$ is any separable monic polynomial in $\mathbb{Z}[X]$ of degree $n-3$ without nonreal roots; for $1/M$ small enough all roots of $h_M(X)$ must be real (cf., for example, [4, Lemma 2.1]). Taking $M \equiv 1 \pmod{8l \prod_{p \in S} p}$ large enough, the polynomial $h(X) = M^{n-3} h_M(\frac{X}{M})$ satisfies all desired conditions since all its roots are real, $h(X) \equiv h_0(X) \pmod 8$ and $h(X) \equiv h_0(X) \pmod p$ for every $p \in S \cup \{l\}$. $\square$

Lemma 2.3. *Let $n \geqslant 7$ be an odd integer and let $l \notin S$ be a prime number such that $l \equiv 1 \pmod{n-1}$. Given $h(X)$ as in Lemma 2.2, there exist monic polynomials $g(X)$ in $\mathbb{Z}[X]$ of degree 2 satisfying the following conditions*:

(i) $g(X)h(X) \equiv X^{n-1} - 1 \pmod{l}$,
(ii) $g(X)$ *is irreducible in* $\mathbb{F}_p[X]$ *for every* $p \in S \cup \{2\}$,
(iii) $g(X)h(X)$ *has square integer discriminant.*

Proof. Since $h(X)$ divides $X^{n-1} - 1$ in $\mathbb{F}_l[X]$ there exists $g_0(X) = X^2 + a_0 X + b_0 \in \mathbb{Z}[X]$ satisfying conditions (i) and (ii).

The coefficients a_0, b_0 being odd integers, we have $D(g_0(X)) \equiv 5 \pmod{8}$; from condition (iii) of Lemma 2.2 we obtain $D(g_0(X)) \equiv D(h(X)) \pmod{8}$.

In addition, conditions (i), (ii) on $g_0(X)$ and conditions (i), (ii) of Lemma 2.2 on $h(X)$ guarantee that, for every odd $p \in S \cup \{l\}$ we have

$$\left(\frac{D(g_0(X))}{p}\right) = \left(\frac{D(h(X))}{p}\right) \neq 0.$$

Thus $D(g_0(X)) \equiv q^2 D(h(X)) \pmod{8l \prod_{p\in S} p}$ for some prime number $q \notin S \cup \{2, l\}$; hence $q^2 D(h(X)) = a_0{}^2 - 4b$ for some integer $b \equiv b_0 \pmod{2l \prod_{p\in S} p}$.

The polynomial $g(X) = X^2 + a_0 X + b$ in $\mathbb{Z}[X]$ satisfies conditions (i), (ii) and (iii) since $D(g(X)h(X)) = (q D(h(X)) R(g,h))^2$ and $g(X) \equiv g_0(X) \pmod{p}$ for every $p \in S \cup \{2, l\}$. □

3. Proof of Theorem 1.1

Let S be a finite set of prime numbers.

We will prove the existence of a polynomial $f(T, X)$ in $\mathbb{Q}(T)[X]$ such that:

(i) $f(T, X)$ is a monic polynomial of degree n in the variable X,
(ii) the splitting field of $f(T, X)$ is a regular A_n-extension of $\mathbb{Q}(T)$,
(iii) for some $t_0 \in \mathbb{Q}$, $f(t_0, X)$ is a well-defined polynomial in $\mathbb{Z}[X]$ without nonreal roots and discriminant not divisible by any $p \in S$.

Theorem 1.1 can be obtained from this in the following way.

Hilbert's Irreducibility Theorem applied to a polynomial $f(T, X)$ satisfying condition (ii) guarantees that the set

$$H_1 = \left\{t \in \mathbb{Q} \text{ such that } f(t, X) \in \mathbb{Q}[X] \text{ and } \mathrm{Gal}_{\mathbb{Q}}\big(f(t, X)\big) \cong A_n\right\}$$

is non-empty; it contains a Hilbert subset of $\mathbb{Q}$. Moreover, H_1 is dense in $\mathbb{R} \times \prod_{p\in S} \mathbb{Q}_p$ (cf., for example, [3]). Condition (iii) ensures that, taking $t_1 \in H_1$ near enough to t_0 in $\mathbb{R} \times \prod_{p\in S} \mathbb{Q}_p$, all roots of the polynomial $f(t_1, X) \in \mathbb{Q}[X]$ are real and $f(t_1, X) \equiv f(t_0, X) \pmod{p}$ for every $p \in S$. Fix such a t_1 and let K_1 be the splitting field of $f(t_1, X)$

over $\mathbb{Q}$; it is an A_n-extension of $\mathbb{Q}$ unramified at all primes in $S \cup \{\infty\}$. For a suitable integer M, $M^n f(t_1, \frac{X}{M})$ is a totally real monic polynomial in $\mathbb{Z}[X]$ with discriminant not divisible by any $p \in S$.

The regularity hypothesis (ii) on $f(T, X)$ ensures that the set

$$H_2 = \left\{ t \in H_1 \text{ such that } \mathrm{Gal}_{K_1}\big(f(t, X)\big) \cong A_n \right\}$$

contains a Hilbert subset of $\mathbb{Q}$. Taking $t_2 \in H_2$ near enough to t_0, the splitting field of $f(t_2, X)$ over $\mathbb{Q}$ must be an A_n-extension of $\mathbb{Q}$ unramified at all primes in $S \cup \{\infty\}$ and linearly disjoint from K_1. As above, this extension is the splitting field of a totally real monic polynomial in $\mathbb{Z}[X]$ with discriminant not divisible by any $p \in S$. Repeating this argument successively we obtain Theorem 1.1.

It remains to prove the existence of a polynomial $f(T, X)$ in $\mathbb{Q}(T)[X]$ satisfying conditions (i), (ii) and (iii). For each odd n, we choose a prime number $l \notin S$ such that $l \equiv 1 \pmod{n-1}$ and $l \neq n$.

Case odd $n \geqslant 7$

Take $P(X) = Xg(X)h(X)$, where $h(X)$ and $g(X)$ are polynomials satisfying the conditions in Lemmas 2.2 and 2.3. We have:

(1) $P(X)$ satisfies the hypothesis of Proposition 2.1, because of (i), (iii) in Lemma 2.3,
(2) $D(P(X))$ is not divisible by any $p \in S \cup \{2\}$, since the polynomials X, $g(X)$ and $h(X)$ are separable and pairwise coprime in $\mathbb{F}_p[X]$,
(3) all roots of $P(X)$ are real, because of (iv) in Lemma 2.2 and (iii) in Lemma 2.3.

It follows from Proposition 2.1 that $F(T, X) = P(X) - TQ(X)$ defines a regular A_n-extension of $\mathbb{Q}(T)$ for some polynomial $Q(X)$ in $\mathbb{Z}[X]$ of degree at most $n-1$. Hence, $F(T, X)$ is a polynomial in $\mathbb{Q}(T)[X]$ satisfying conditions (i), (ii) and (iii) (with $t_0 = 0$).

For $n = 3, 5$ we cannot apply the results of Section 2; we perform a specific construction in order to obtain these cases.

Case $n = 5$

Recall that $D(X^3 + AX + AB) = A^2(-27B^2 - 4A)$.

Choose a polynomial $g_0(X) = X^3 + a_0X + a_0b_0$ in $\mathbb{Z}[X]$ such that

$$g_0(X) \equiv \begin{cases} X^3 - X + 1 \pmod{6}, \\ X^3 - X \pmod{p} \quad \text{for all } p \in S \cup \{l\},\ p \neq 2, 3. \end{cases}$$

Since $D(g_0(X)) \equiv 1 \pmod{8}$ and $\left(\frac{D(g_0(X))}{p}\right) = 1$ for every odd $p \in S \cup \{3, l\}$, we can find a prime number $q \notin S \cup \{2, 3, l\}$ such that $q^2 = -27b_0{}^2 - 4a$, for some integer $a \equiv a_0 \pmod{p}$ for every $p \in S \cup \{2, 3, l\}$.

The polynomial $g(X) = X^3 + aX + ab_0$ has square integer discriminant $D(g(X)) = (qa)^2$ and all its roots are real.

Since $l \equiv 1 \pmod 4$, -1 is a square modulo l and there exist integers $c, d \in \mathbb{Z}$ such that

$$(X-c)(X-d) \equiv \begin{cases} X(X+1) \pmod 6, \\ X^2+1 \pmod l, \\ (X-2)(X+2) \pmod p \quad \text{for all } p \in S,\ p \neq 2, 3. \end{cases}$$

Take $P(X) = (X-c)(X-d)g(X)$; it follows that:

(1) $P(X)$ satisfies the hypothesis of Proposition 2.1,
(2) $D(P(X))$ is not divisible by any $p \in S \cup \{2, 3\}$,
(3) all roots of $P(X)$ are real.

From Proposition 2.1 we obtain a polynomial $F(T, X) = P(X) - TQ(X)$ satisfying conditions (i), (ii) and (iii) (with $t_0 = 0$).

Case $n = 3$

Argue as in case $n = 5$ and take $P(X) = g(X)$.

Case even $n \geqslant 4$

From the odd cases applied to the odd integer $n + 1 \geqslant 5$ we obtain polynomials $P(X)$, $Q(X)$ in $\mathbb{Z}[X]$ such that $F(T, X) = P(X) - TQ(X)$ defines a regular A_{n+1}-extension of $\mathbb{Q}(T)$.

Let $U \in \overline{\mathbb{Q}(T)}$ be a root of $F(T, X) \in \mathbb{Q}(T)[X]$ as a polynomial in X. Since $T = \frac{P(U)}{Q(U)}$ it follows that $\mathbb{Q}(T, U) = \mathbb{Q}(U)$; this is the fixed field by some $A_n \subset A_{n+1}$ in the splitting field of $F(T, X)$ over $\mathbb{Q}(T)$. Hence

$$G(U, X) = \frac{F\left(\frac{P(U)}{Q(U)}, X\right)}{X - U} = \frac{P(X) - \frac{P(U)}{Q(U)} Q(X)}{X - U}$$

defines a regular A_n-extension of $\mathbb{Q}(U)$.

The polynomial $P(X)$ has a degree 1 factor $(X - u_0)$ in $\mathbb{Q}[X]$ ($u_0 = 0$ for $n + 1 \geqslant 7$, and $u_0 = c$ for $n + 1 = 5$). Since the polynomials $P(X)$, $Q(X)$ are coprime in $\mathbb{Q}[X]$, we have $P(u_0) = 0$ and $Q(u_0) \neq 0$; so $G(u_0, X) = \frac{P(X)}{X - u_0}$.

As a consequence, the polynomial $G(T, X)$ in $\mathbb{Q}(T)[X]$ satisfies conditions (i), (ii) and (iii) (with $t_0 = u_0$).

This concludes the proof of Theorem 1.1.

Corollary 3.1. *For every positive integer n and every finite set S of prime numbers, there exist infinitely many linearly disjoint A_n-extensions of $\mathbb{Q}$ unramified at all primes in $S \cup \{\infty\}$. In particular, there exist infinitely many linearly disjoint tamely ramified A_n-extensions of $\mathbb{Q}$.*

References

[1] B. Birch, Noncongruence subgroups, covers and drawings, in: L. Schneps (Ed.), The Grothendieck Theory of Dessins d'Enfants, Cambridge Univ. Press, Cambridge, 1994, pp. 25–46.
[2] J.-F. Mestre, Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A}_n$, J. Algebra 131 (1990) 483–495.
[3] Y. Morita, A Note on the Hilbert irreducibility theorem, Proc. Japan Acad. Ser. A Math. Sci. 66 (1990) 101–104.
[4] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 2nd Edition, Springer, PWN—Polish Scientific Publishers, 1990.