PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 122, Number 1, September 1994

ON CONSTRUCTING FIELDS CORRESPONDING TO THE $\tilde{A}_n$'S OF MESTRE FOR ODD n

JOHN R. SWALLOW

(Communicated by Lance W. Small)

ABSTRACT. An isomorphism is given between the trace bilinear form of Mestre's A_n extensions over $\mathbb{Q}(t)$ and a certain quadratic form over $\mathbb{Q}$ with base field lifted to $\mathbb{Q}(t)$. This reduces the problem of constructing $\tilde{A}_n$ extensions from Mestre's A_n's to that of diagonalizing certain forms over $\mathbb{Q}$. The result expands a result of Schneps.

1. INTRODUCTION

Let $n \geq 4$, and denote by $\tilde{A}_n$ the unique nonsplit double cover of the alternating group A_n. For odd n, Mestre has constructed a family of polynomials $F_t(X) \in \mathbb{Q}(t)[X]$ whose splitting fields are regular A_n extensions of $\mathbb{Q}(t)$. Many of these extensions embed in regular $\tilde{A}_n$ extensions of $\mathbb{Q}(t)$. In this note we show that one can explicitly construct all such extensions. Theorems of Crespo [1] describe how to construct such extensions given a diagonalization of the trace bilinear form, and we reduce the problem of diagonalization over $\mathbb{Q}(t)$ to that over $\mathbb{Q}$. Specifically, if one writes $F_0(X) = P(X)$ as a product of (not necessarily irreducible) polynomials $\prod_{i=1}^{s} p_i(X)$ in $\mathbb{Q}[X]$ and has bases for the trace bilinear forms T_i on $\mathbb{Q}(X)/(p_i(X))$ for each i, then a basis for the trace bilinear form T on $\mathbb{Q}(t)(X)/(F_t(X))$ can be given explicitly.

The special case of this result in which each $p_i(X)$ is linear was proved by Schneps [3]; her result allows the construction of $\tilde{A}_n$ fields associated to Mestre A_n's over $\mathbb{Q}(t)$ with the roots of $P(X)$ adjoined. Our result, on the other hand, relaxes the condition on the roots of $P(X)$; we are then able to construct all of Mestre's $\tilde{A}_n$'s over the ground field $\mathbb{Q}$, which provided the motivation for this paper. Also, Feit used these methods and the Mestre A_5 associated to $p(x) = 9x - 10x^3 + x^5$ to produce an irreducible polynomial over $\mathbb{Q}$ with Galois group $\tilde{A}_5$, whose coefficients are much smaller than any so far constructed with Schneps's earlier result. It is included in the appendix.

2. MAIN RESULT

Let K be a field of characteristic not 2. Serre has determined a necessary and sufficient condition for a Galois extension of K with Galois group A_n to

Received by the editors December 22, 1992.
1991 *Mathematics Subject Classification.* Primary 12Y05, 12F12; Secondary 11E12, 11R32.

be embedded in an $\tilde{A}_n$ extension:

Theorem 1 [4]. *Let L/K be a Galois extension of fields with group A_n, and let $f(X)$ be a monic irreducible polynomial over K of degree n with splitting field L. Set $E = K(X)/(f(X))$. Then L embeds in a Galois extension of K with group $\tilde{A}_n$ if and only if the trace bilinear form $\mathrm{Tr}_{E/K}(X^2)$ has trivial Hasse-Witt invariant.*

The determination, then, of whether or not an extension given by a Mestre polynomial with Galois group A_n lifts to an $\tilde{A}_n$ extension amounts to the computation of the Hasse-Witt invariant, and this computation is made less difficult by the fact that the trace form is independent of t and hence can be taken at $t = 0$. To use Crespo's results to construct the $\tilde{A}_n$ extension one requires an explicit isomorphism, over $\mathbb{Q}(t)$, between the trace bilinear form given in Serre's theorem and either the sum of n squares $X_1^2 + \cdots + X_n^2$ or one of the forms $X_1^2 + \cdots + X_{n-4m}^2 - X_{n-4m+1}^2 - \cdots - X_n^2$. (Her formula may require a simple transformation of this isomorphism.) We shall show that finding such an isomorphism can be reduced to finding an isomorphism at $t = 0$, i.e., between certain forms over $\mathbb{Q}$. This permits the explicit construction of $\tilde{A}_n$ extensions over $\mathbb{Q}(t)$ and hence, by Hilbert's Irreducibility Theorem, over $\mathbb{Q}$.

We first describe Mestre's construction. Let n be an odd integer ≥ 5, and let $P(X)$ be the generic monic polynomial of degree n over $\mathbb{Q}$. Mestre shows that there exist polynomials $Q(X)$ and $R(X)$, unique up to scalar multiplication and both of degree $n-1$ over $\mathbb{Q}$, such that $R(X)$ is prime to $P(X)$ and the relation $PQ' - P'Q = R^2$ is satisfied. Let $S(t) = \prod_z t - \frac{P(z)}{Q(z)}$, where z runs through the roots of $R(X)$; $S(t)$ is a polynomial in the coefficients of $P(X)$. Form the polynomial $H = l_S \Delta(S) \mathrm{res}(P, R)$, where l_S is the coefficient of the highest term of S, $\mathrm{res}(P, R)$ is the resultant of P and R, and $\Delta(S)$ is the discriminant of S. We then have

Theorem 2 [2]. *Let $p(X)$ be a specialization of P into $\mathbb{Q}$ such that H does not vanish, and let $q(X)$ be the corresponding specialization of Q. Let $x_1, x_2, \ldots, x_n$ be the roots of $f_t(X) = p(X) - tq(X)$. Let*

$$E = \mathbb{Q}(t)(x_1) \quad \text{and} \quad L = \mathbb{Q}(t)(x_1, x_2, \ldots, x_n).$$

Then if $\Delta(p)$ is a nonzero square, $\mathrm{Gal}(L/\mathbb{Q}(t))$ is isomorphic to A_n. If also the Hasse-Witt invariant of the form $\mathrm{Tr}_{E/\mathbb{Q}(t)}(X^2)$ is trivial, then L can be embedded in a regular Galois extension $L'/\mathbb{Q}(t)$ such that $\mathrm{Gal}(L'/\mathbb{Q}(t))$ is isomorphic to $\tilde{A}_n$.

We establish some notation. If $m(X) \in \mathbb{Q}[X]$ and $\{p_i\}_{i=1}^s$ is a set of fixed polynomials in $\mathbb{Q}[X]$, then let $\sigma_{p_1, \ldots, p_s}(m(X)) = \sigma(m(X))$ be the representative of smallest degree of the image of $m(X)$ under the canonical projection $\mathbb{Q}[X] \to \mathbb{Q}[X]/(\prod_{i=1}^s p_i(X))$. Our result is then

Theorem 3. *Let $p(X)$, $q(X)$, $f_t(X)$, x_j, E, and L be as in Mestre's theorem, and let $r(X)$ be the associated specialization of $R(X)$. Fix a factorization of $p(X) = \prod_{i=1}^s p_i(X)$ over $\mathbb{Q}[X]$, not necessarily of irreducibles. Then $\mathrm{Tr}_{E/\mathbb{Q}(t)}(X^2)$ is isomorphic to $\mathbb{Q}(t) \otimes_{\mathbb{Q}} (\perp_{i=1}^s \mathrm{Tr}_{V_i/\mathbb{Q}}(X^2))$, where $V_i = \mathbb{Q}(X)/(p_i(X))$, and, if we are given bases $\{g_{i1}, g_{i2}, \ldots, g_{in_i}\}$ for the V_i, a*

basis of $E/\mathbb{Q}(t)$ *which gives this isomorphism is* $\{\nu_{ij}(X)\}$, *where*

$$\nu_{ij}(X) = \frac{\sigma(g_{ij}(X)r(X)\prod_{k=1,k\neq i}^{s}(A(X)-e_k))}{r(X)\prod_{k=1,k\neq i}^{s}(e_i-e_k)},$$

the e_i *can be chosen as arbitrary distinct rationals,* $A(X) = A(X, e_1, e_2, \ldots, e_s)$ *is a polynomial over* $\mathbb{Q}$ *of degree at most* n *which takes the value* e_i *on a root of* p_i, *and the coefficients of* $A(X)$ *form a solution to an explicit system of linear equations in the coefficients of the* $p_i(X)$ *and in the* e_i.

Corollary. *If the trace form* $\mathrm{Tr}_{E/\mathbb{Q}(t)}$ *is a sum of squares and the matrix* $(\nu_{ij})+I$ *is nonsingular, then its determinant gives an element of* L *whose rational multiples are the complete set of elements whose square roots generate* $\tilde{A}_n$ *extensions over* $\mathbb{Q}(t)$ *containing* L.

Proof. We wish to find an $A(X) \in \mathbb{Q}[X]$ such that

(a) for any root ψ of $p(X)$, $A(\psi) \in \mathbb{Q}$, and
(b) if ψ and ψ' are roots of $p_i(X)$ and $p_{i'}(X)$ with $i \neq i'$, then $A(\psi) \neq A(\psi')$.

Since $\mathrm{Res}(P, R) \neq 0$, $P(X)$ has distinct roots. Choose the e_i rational and distinct. By the Chinese Remainder Theorem, there exists an $A(X) \in \mathbb{Q}[X]$ such that $A(X) \equiv e_i (p_i)$ for each i. Now $A(X)$ is defined modulo $P(X)$, so we may choose a representative with degree at most n; our conditions are then satisfied.

Now we shall show, by invoking the argument of Serre stated in Schneps's paper, that the coefficients of the trace form in the basis given above are independent of t. First we show that the coefficients are polynomials in $\mathbb{Q}[t]$. Let B be the integral closure of $\mathbb{Q}[t]$ in E. The denominator of $\nu_{ij}(X)$ lies in the fractional ideal of B generated by $r(x_1)$. It follows that $\nu_{ij} \cdot \nu_{i'j'}$ under the trace form $\mathrm{Tr}_{E/\mathbb{Q}(t)}(X^2)$ is the trace of a fraction which has for numerator an element of B (a polynomial in x_1 with coefficients in $\mathbb{Q} \subset \mathbb{Q}[t]$) and for denominator an element of the fractional ideal of B generated by $r(x_1)^2$. But $(r(x_1)^2)$ is the different of the extension E, as follows. The extension $E/\mathbb{Q}(t)$ is regular, and ramification does not occur in $\bar{\mathbb{Q}}/\mathbb{Q}$, so for the computation of the different we consider $E \otimes_{\mathbb{Q}(t)} \bar{\mathbb{Q}}(t)$. From Mestre's paper we know that $f_t(X)$ has multiple roots when $t = \frac{p(z)}{q(z)}$ for a root z of $r(X)$. When that happens, z is a triple root of $f_t(X)$ with all other roots distinct. Therefore, $(x_1 - z)^2$ divides the different for each root z of $r(X)$. Since Mestre gives the discriminant of $f_t(X)$ as $\lambda(t - \frac{p(z)}{q(z)})^2$ with $\lambda \in \bar{\mathbb{Q}}$ and z running over the roots of $r(X)$, no other primes in $\bar{\mathbb{Q}}(t)$ may ramify. We have shown then that the different D of $E \otimes_{\mathbb{Q}(t)} \bar{\mathbb{Q}}(t)$ and hence of E is $(r(x_1)^2)$. Now by definition of the different, $\mathrm{Tr}_{E/\mathbb{Q}(t)}(aD^{-1}) \in \mathbb{Q}[t]$ for any $a \in B$; since $D^{-1} = (1/r(x_1)^2)$, the coefficients of the trace form are polynomials in t.

Now we show that the coefficients of the trace form have no poles at infinity. Fix a coefficient of the form as $\nu_{ij} \cdot \nu_{i'j'}$ for some i, j, i', j'. Notice that it is a sum of fractions each with numerator and denominator in $\mathbb{Q}[x_k]$ for some k, and this sum is symmetric with respect to $x_1, x_2, \ldots, x_n$. The degree of each numerator is less than or equal to $2(n-1)$ by virtue of the action of σ, while the degree of each denominator is $2(n-1)$. Now reducing to a single fraction

with a denominator which is the product of the former denominators, we get a fraction which has as numerator a symmetric function of $x_1, x_2, \ldots, x_n$ and for denominator a constant times the norm from E to $\mathbb{Q}(t)$ of $r(x_1)^2$. Using the coefficients of $f_t(X)$ we can reduce both the numerator and denominator to polynomials in t with coefficients in $\mathbb{Q}$. The degree in t of a symmetric polynomial in the roots $x_1, x_2, \ldots, x_n$ of the Mestre polynomial $f_t(X)$ is at most the largest degree of any single x_i occurring in any term of the symmetric polynomial. Hence in our combined fraction the numerator must then have degree in t less than or equal to $2(n-1)$. Now the denominator similarly can have degree in t at most $2(n-1)$, and we know that it attains that degree, as follows. The norm of the different ideal (generated by $r(x_1)^2$) is the discriminant ideal (generated by $N_{E/\mathbb{Q}(t)}r(x_1)^2$ as well as by the discriminant of the extension), and the nonvanishing of H insures that the discriminant of the extension in fact has t-degree $2(n-1)$. Hence the combined fraction has no pole at $t=\infty$. Since we showed that it was a polynomial in t, it must be constant and we may compute it at $t=0$.

If $i \neq i'$ then $\nu_{ij} \cdot \nu_{i'j'}$ clearly is zero at every root of $p(X)$, forcing the trace to be zero. If $i = i'$ then on every root of $p(X)$ which is not a root of $p_i(X)$ the product is zero, and on the roots of $p_i(X)$ it takes the same value as $g_{ij}(X) \cdot g_{i'j'}(X)$; hence

$$\nu_{ij} \cdot \nu_{i'j'} = \sum_{p_i(\psi)=p_{i'}(\psi)=0} g_{ij}(\psi) g_{i'j'}(\psi),$$

and the isomorphism is valid.

The corollary is a direct consequence of [1].

3. Examples

Example 1 (Schneps's case). Let $p(X)$ be a product of $\mathbb{Q}$-linear terms $p_i(X) = X + a_i$ such that H does not vanish, and let $q(X)$ and $r(X)$ be the associated Mestre polynomials. The discriminant of $p(X)$ is clearly a square. Now $A(X) = X$ has the property that it is rational on every root of $p(X)$; hence if we set $e_i = -a_i$, then it takes the value e_i on a root of $p_i(X)$. Set $g_{i1}(X) = 1$ for each $i = 1, 2, \ldots, n$. From the theorem we recover

$$\nu_{i1}(X) = \left(\prod_{k \neq i} \frac{(X + a_k)}{(-a_i + a_k)} \right) \left(\frac{r(-a_i)}{r(X)} \right),$$

which is precisely Schneps's normalizing basis.

Example 2 ("Gaussian integer case"). Let $p(X) = \prod_{i=1}^{n}(X^2 + a_i^2)(X + z)$, $a_i, z \in \mathbb{Q}$. We know that $\mathrm{Tr}_{E/\mathbb{Q}(t)}(X^2)$ is isomorphic to $\sum_{j=1}^{n} X_j^2 - \sum_{j=1}^{n} X_{n+j}^2 + X_{2n+1}^2$. If $p(X)$ is H-general, we then have a basis $\{\nu_{i1}, \nu_{i2} \mid i = 1, 2, \ldots, n\} \cup \{\nu_{n+1\,1}\}$ which is orthogonal and which satisfies $\nu_{i1}(X) \cdot \nu_{i1}(X) = 2$, $\nu_{i2}(X) \cdot \nu_{i2}(X) = -2a_i^2$ for $i \leq n$, and $\nu_{n+1\,1}(X) \cdot \nu_{n+1\,1}(X) = 1$:

$$\nu_{i1}(X) = \frac{\sigma(r(X)(X^2 - z^2) \prod_{k=1, k\neq i}^{n}(X^2 + a_k^2))}{r(X)(-a_i^2 - z^2) \prod_{k=1, k\neq i}^{n}(-a_i^2 + a_k^2)},$$

$$\nu_{i2}(X) = \frac{\sigma(Xr(X)(X^2 - z^2) \prod_{k=1, k\neq i}^{n}(X^2 + a_k^2))}{r(X)(-a_i^2 - z^2) \prod_{k=1, k\neq i}^{n}(-a_i^2 + a_k^2)},$$

and

$$\nu_{n+1\ 1}(X) = \frac{\sigma(r(X)\prod_{k=1}^{n}(X^2+a_k^2))}{r(X)\prod_{k=1}^{n}(z^2+a_k^2)} = \frac{r(-z)\prod_{k=1}^{n}(X^2+a_k^2)}{r(X)\prod_{k=1}^{n}(z^2+a_k^2)}.$$

The basis required is then $\{\omega_i\}_1^{2n+1}$ defined by

$$\omega_i(X) = \frac{3}{4}\nu_{i1}(X) + \frac{1}{4a_i}\nu_{i2}(X),$$

$$\omega_{n+i}(X) = \frac{1}{4}\nu_{i1}(X) + \frac{3}{4a_i}\nu_{i2}(X)$$

for i in $\{1, 2, \ldots, n\}$, and $\omega_{2n+1}(X) = \nu_{n+1\ 1}(X)$.

Appendix

Using the theorem with $p(x) = x^5 - 10x^3 + 9x$, $s = 1$, and $p_1(x) = p$, and then substituting $t = \frac{1}{144}$, W. Feit has found that the following polynomial has Galois group SL(2, 5) over $\mathbb{Q}$.

$$\begin{aligned}
&228300570738279857690513781143310649891225600000000000\\
&\quad + 331419301185417748099709517524564596949516288000000000x^2\\
&\quad + 154911461277206970106015975305713540613852364800000x^4\\
&\quad + 643255881543805314898477939726691059779026944000x^6\\
&\quad + 679709094392899372412764801947048178090844160x^8\\
&\quad + 620463002328471734148118489880873359972352x^{10}\\
&\quad + 197615074508483992632808212362986256 00x^{12}\\
&\quad + 250387323794613562120711699282016x^{14}\\
&\quad + 10664322464389826228818973 80x^{16}\\
&\quad + 8721383239957961830 51x^{18}\\
&\quad + 237747342358746x^{20} + 26087787x^{22} + x^{24}.
\end{aligned}$$

References

1. T. Crespo, *Explicit construction of $\tilde{A}_n$ type fields*, J. Algebra **127** (1989), 452–461.
2. J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(t)$ de group de Galois $\tilde{A}_n$*, J. Algebra **131** (1990), 483–495.
3. L. Schneps, *Explicit construction of extensions of $\mathbb{Q}(t)$ of Galois group $\tilde{A}_n$ for n odd*, J. Algebra **146** (1992), 117–123.
4. J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), 651–676.

Department of Mathematics, Yale University, New Haven, Connecticut 06520
E-mail address: swallow@math.yale.edu