JOURNAL OF ALGEBRA **146**, 117–123 (1992)

Explicit Construction of Extensions of $\mathbb{Q}(t)$ of Galois Group $\tilde{A}_n$ for n Odd

LEILA SCHNEPS

URA 741 du CNRS, Laboratoire de Mathématiques,
Faculté des Sciences de Besançon, Besançon, France

Communicated by Walter Feit

Received March 13, 1990

Let H be a finite group, and G a non-split central extension of H by C_2, the multiplicative group of order 2. The group G satisfies

$$1 \to C_2 \to G \to H \to 1.$$

Let F be a field of characteristic different from 2, and let L be a Galois extension of F having Galois group H. Let $E(H, G, F, L)$ be the set of fields L' which are quadratic extensions of L, Galois over F, and such that the diagram

$$\begin{tikzcd} \mathrm{Gal}(L'/F) \arrow[r] \arrow[d] & \mathrm{Gal}(L/F) \arrow[d] \\ G \arrow[r] & H \end{tikzcd}$$

commutes.

Let $\{v_\sigma \mid \sigma \in H\}$ be a set of representatives of G modulo C_2. Then we have a factor system $\{\zeta_{\sigma,\tau} \mid \sigma, \tau \in H\}$ such that $v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma\tau}$ for all σ, τ in H. Let T be the crossed-product algebra $(L/F, \zeta_{\sigma,\tau})$. It is well known that $E(H, G, F, L) \neq \varnothing$ if and only if the algebra T splits. However, in general, even when it is known that $E(H, G, F, L) \neq \varnothing$, it is not known how to construct it explicitly. The goal of this article is to construct $E(A_n, \tilde{A}_n, K(t), L)$ where n is an odd integer $n \geqslant 5$, K is any field of characteristic 0, and the L are certain special extensions of $K(t)$ constructed by Mestre, and to explicitly give the subset $E^{\mathrm{unr}}(A_n, \tilde{A}_n, K(t), L)$ consisting of fields L' which are geometrically unramified over L.

From now on, we let $H = A_n$, $G = \tilde{A}_n$, the only non-trivial extension of A_n by C_2, and let n be an odd integer, $n \geqslant 5$. Let K be a field of characteristic 0, and $\bar{K}$ the algebraic closure of K. For all $n \geqslant 5$, Mestre (cf. [M]) has constructed polynomials $\mathscr{F}_t(X)$ defined over $K(t)$, having Galois group

0021-8693/92 $3.00

A_n, and possessing the following property. Let $x_1, ..., x_n$ be the roots of $\mathscr{F}_t(X)$, and let $E = K(t)(x_1)$. Then

$$Tr_{E/K(t)}(x^2) \simeq X_1^2 + \cdots + X_n^2$$

over K, i.e., the two quadratic forms are K-isomorphic. This condition implies that the associated algebra T splits by the following theorem of Serre, valid over any field F of characteristic different from 2:

THEOREM 1 (Serre, cf. [S]). *Let $\mathscr{F}(X)$ be a polynomial defined over F having Galois group A_n, and let $x_1, ..., x_n$ be the roots of $\mathscr{F}(X)$. Let $E = F(x_1)$. Then the algebra T is equivalent to the Witt invariant of the quadratic form $Tr_{E/F}(x^2)$ in $Br_2(F)$, the kernel of multiplication by 2 in the Brauer group of F.*

If n is odd, Mestre proceeds as follows. Let $\mathscr{P}(X)$ be the generic polynomial of degree n. Then one can associate to $\mathscr{P}(X)$ polynomials $\mathscr{Q}(X)$ and $\mathscr{R}(X)$, unique up to multiplication by a constant, both of degree $n-1$, such that $\mathscr{R}(X)$ is prime to $\mathscr{P}(X)$ and we have:

$$\mathscr{P}'\mathscr{Q} - \mathscr{P}\mathscr{Q}' = \mathscr{R}^2.$$

Let $y_1, ..., y_n$ be the roots of $\mathscr{P}(X)$. Then the coefficients of $\mathscr{Q}(X)$ and $\mathscr{R}(X)$ are polynomials in the y_i (cf. [M]). Let $\mathscr{S}(t) = l_{\mathscr{S}} \prod_v (t - \mathscr{P}(v)/\mathscr{Q}(v))$, where $l_{\mathscr{S}}$ is such that the constant coefficient of $\mathscr{S}(t)$ is equal to 1, and the product is over the roots of $\mathscr{R}(X)$. Let $H_0(y_1, ..., y_n) =^{\mathrm{def}} l_{\mathscr{S}}\, \Delta(\mathscr{S}) \operatorname{res}(\mathscr{P}, \mathscr{R})$. Then H_0 is a symmetric polynomial in the y_i (Mestre actually considers it as a polynomial in the coefficients of $\mathscr{P}(X)$).

THEOREM 2 (Mestre). *Let $y_1, ..., y_n \in K$ be such that $H_0(y_1, ..., y_n) \neq 0$, and let $P(X) = \prod_i (X - y_i)$. Let $Q(X)$ be as above, let $\mathscr{F}_t(X) = P(X) - tQ(X)$, and let $x_1, ..., x_n$ be the roots of $\mathscr{F}_t(X)$ in some algebraic closure of $K(t)$. Let $E = K(t)(x_1)$ and $L = K(t)(x_1, ..., x_n)$. Then* $\mathrm{Gal}(L/K(t)) = A_n$ *and $Tr_{E/K(t)}(x^2)$ is K-isomorphic to $X_1^2 + \cdots + X_n^2$.*

It is an immediate consequence of this theorem that $\tilde{A}_n$ is realizable as a Galois group over $K(t)$.

The main theorem of this article is the following:

THEOREM 3. *Let $P(X)$, $Q(X)$, $R(X)$, $\mathscr{F}_t(X)$, $y_1, ..., y_n$, $x_1, ..., x_n$, and the fields E and L be as in Theorem 2. For $i = 1, ..., n$, let*

$$u_i(X) = \frac{R(y_i)}{P'(y_i)} \prod_{\substack{k=1 \\ k \neq i}}^{n} (X - y_k).$$

Let $\mathscr{M}$ be the matrix $(u_i(x_j))$, and let $\mathscr{R} = \mathrm{diag}(R(x_1), -R(x_2), -R(x_3), ..., -R(x_n))$. Let $\gamma = \det(\mathscr{M} + \mathscr{R})$. Then

(i) $E(A_n, \tilde{A}_n, K(t), L) = \{L(\sqrt{r\gamma}) \mid r \in K(t)^*\}$ *and*

(ii) $E^{\mathrm{unr}}(A_n, \tilde{A}_n, K(t), L) = \{L(\sqrt{r\gamma}) \mid r \in K^*\}$.

Remark. Serre has already shown using group theoretic arguments that such a γ must exist (cf. [52]).

Proof. In order to prove (i), we use a result of T. Crespo (cf. [C]). Let F be any field of characteristic different from 2. Let $\mathscr{F}(X)$ be a polynomial defined over F having Galois group A_n, $x_1, ..., x_n$ the roots of $\mathscr{F}(X)$, and $E = F(x_1)$. Then whenever the Witt invariant $W(Tr_{E/F}(x^2))$ splits, Crespo has given a method to obtain an element $\gamma \in L =^{\mathrm{def}} F(x_1, ..., x_n)$ such that $E(A_n, \tilde{A}_n, F, L) = \{L(\sqrt{r\gamma}) \mid r \in F^*\}$. In the particular case where $Tr_{E/F}(x^2) \simeq X_1^2 + \cdots + X_n^2$ over F her method simplifies as follows. Let $\mathscr{B} = (v_1(x_1), ..., v_n(x_1))$ be a basis of $E = F(x_1)$ over F, where the $v_i(x_1)$ are rational functions of x_1. The existence of an isomorphism $Tr_{E/F}(x^2) \simeq X_1^2 + \cdots + X_n^2$ implies that there is an $n \times n$ matrix $\mathscr{P}$ with coefficients in F such that ${}^t\mathscr{P}\mathscr{A}_{\mathscr{F},\mathscr{B}}\mathscr{P} = I$, where $A_{\mathscr{F},\mathscr{B}}$ is the matrix whose (i, j)th component is given by $Tr_{E/F}(v_i(x_1)\, v_j(x_1))$, i.e. $\mathscr{A}_{\mathscr{F},\mathscr{B}}$ is the matrix associated to the quadratic form $Tr_{E/F}(x^2)$ in the basis $\mathscr{B}$. Let $\mathscr{M}$ be the $n \times n$ matrix whose (i, j)th component is given by $v_i(x_j)$, so that ${}^t\mathscr{M} \cdot \mathscr{M} = \mathscr{A}_{\mathscr{F},\mathscr{B}}$.

PROPOSITION 1 (Crespo). *Let $\gamma = \det(\mathscr{M}\mathscr{P} + I)$. Then if $\gamma \neq 0$,*

$$E(A_n, \tilde{A}_n, F, L) = \{L(\sqrt{r\gamma}) \mid r \in F^*\}.$$

In order to apply this proposition, we set $F = K(t)$ and $v_i(X) = u_i(X)/R(X)$, where the $u_i(X)$ are as in the statement of the theorem. Then the $v_i(x_1)$ form a basis of $E/K(t)$ and the $v_i(X)$ satisfy the relations $v_i(y_j) = \delta_j^i$ and $\sum_{i=1}^n v_i(X) = 1$; for the latter, note that $\sum_i u_i(y_j) = u_j(y_j) = R(y_j)$ for $j = 1, ..., n$ and thus $\sum_i u_i(X) = R(X)$. Moreover, the quadratic form $Tr_{E/K(t)}(x^2)$ in this basis is independent of t by the following argument (due to Serre). The coefficients of $Tr_{E/K(t)}(x^2)$ are traces of expressions whose numerators are polynomials in x_1 of degree less than or equal to $2n-2$, and whose denominators are $R(x_1)^2$. Now, E is ramified over $K(t)$ precisely at the roots of $R(X)$, and the different $\mathscr{D}$ of E over $K(t)$ is the ideal generated by $R(x_1)^2$. Therefore the coefficients of $Tr_{E/K(t)}(X^2)$ in the above basis are in fact polynomials in t. But these polynomials have no poles at infinity because the degree of the denominator in each term is greater than that of the numerator. Therefore they are constants and independent of t, and it suffices to calculate them at $t = 0$. This argument together with the relations satisfied by the $v_i(x_1)$ shows that $Tr_{E/K(t)}(x^2) = X_1^2 + \cdots + X_n^2$. Let $\mathscr{M}'$ be the matrix $(v_i(x_j))$. Then by Proposition 1, if we set $\gamma_1 = \det(\mathscr{M}' + I)$, then $L(\sqrt{\gamma_1}) \in E(A_n, \tilde{A}_n, K(t), L)$, and the same is true if we replace γ_1 by $\gamma_2 = \det(\mathscr{M}'\mathscr{J} + I)$, where $\mathscr{J} = \operatorname{diag}(1, -1, -1, ..., -1)$ (this formulation is nicer for reasons which appear later on). Set $\gamma = R(x_1)\, R(x_2) \cdots R(x_n) \gamma_2$. Then since $R(x_1) \cdots R(x_n)$ is a symmetric polynomial in $x_1, ..., x_n$, it is an element of $K(t)$ and thus we have $L(\sqrt{\gamma}) \in E(A_n, \tilde{A}_n, K(t), L)$, so $E(A_n, \tilde{A}_n, K(t), L) = \{L(\sqrt{r\gamma}) \mid r \in K(t)^*\}$. It is easily seen that $\gamma = \det(\mathscr{M} + \mathscr{R})$. This suffices to prove (i) (it will be shown in the proof of (ii) that $\gamma \neq 0$).

We shall obtain (ii) as a consequence of a more general result. We begin by considering the whole situation generically (and geometrically). Let $y_1, ..., y_n$ be indeterminates and let $\mathscr{P}(X) = \prod_{i=1}^{n} (X - y_i)$. As before, we associate to $\mathscr{P}(X)$ polynomials $\mathscr{Q}(X)$ and $\mathscr{R}(X)$ satisfying $\mathscr{P}'\mathscr{Q} - \mathscr{P}\mathscr{Q}' = \mathscr{R}^2$. We also define $\mathscr{F}(X) = \mathscr{P}(X) - t\mathscr{Q}(X)$, and exactly as before we associate to it a generic element which we now call Γ. Let U be the Zariski open subset of $\mathbf{P}^1 \times \mathbf{A}^n$ defined by: the point $(t, y_1, ..., y_n)$ is in U if and only if $H_0(y_1, ..., y_n) \neq 0$. Let V be the subset of $\mathbf{P}^1 \times \mathbf{A}^n \times \mathbf{P}^n$ given by: the point $(t, y_1, ..., y_n, x_1, ..., x_n)$ is in V if and only if

(i) $H_0(y_1, ..., y_n) \neq 0$,

(ii) $x_1, ..., x_n$ are the roots of $\mathscr{F}(X)$, and

(iii) $\prod_{i<j} (x_i - x_j) = \prod_{i<j} (y_i - y_j)\, \mathscr{S}(t)$.

V is a Galois covering of U of Galois group A_n, ramified at the hypersurface of equation $\mathscr{S}(t) = 0$, with ramification index 3. If we fix values of $y_1, ..., y_n$ such that $H_0(y_1, ..., y_n) \neq 0$, and set $P(X) = \prod_{i=1}^{n} (X - y_i)$, the fibre of V which we obtain is exactly the curve C_P whose function field is $K(t)(x_1, ..., x_n)$ where $x_1, ..., x_n$ are the roots of $P(X) - tQ(X)$. Then C_P is a Galois covering of $\mathbf{P}^1$ of Galois group A_n, and it is stable under the action of A_n on V.

Let $\tilde{V}$ be the degree 2 covering of V which is the open subset of $\mathbf{P}^1 \times V$ such that for $v \in V$, $(x, v) \in \tilde{V}$ if and only if $x^2 = \Gamma$.

PROPOSITION 2. *$\tilde{V}$ is unramified over V.*

Remark. Part (ii) of Theorem 3 is a consequence of this proposition when $y_1, ..., y_n$ are specialized to elements of K satisfying $H_0(y_1, ..., y_n) \neq 0$.

Proof. We must show that all the poles and zeros of Γ have even order, i.e., that $\operatorname{Div}(\Gamma)$ is divisible by 2. We have:

$$\Gamma = \det \begin{pmatrix} u_1(x_1) + R(x_1) & u_1(x_2) & \cdots & u_1(x_n) \\ u_2(x_1) & u_2(x_2) - R(x_2) & \cdots & u_2(x_n) \\ \vdots & \vdots & \ddots & \vdots \\ u_n(x_1) & u_n(x_2) & \cdots & u_n(x_n) - R(x_n) \end{pmatrix}.$$

Since Γ is a polynomial in the x_i, the only poles occur at $t=\infty$, and since the highest degree of Γ in the x_i is $n-1$, they have degree at most $n-1$. For each of the $n-1$ roots v of $\mathcal{R}(X)$, when t takes the value $\mathcal{P}(v)/\mathcal{Q}(v)$, exactly three of the x_i are equal to v. Since $\mathcal{R}(v)=0$, this makes three columns of the matrix identical, so there is a zero of order at least 2 at each such point.

Let $\mathcal{H}_\infty$ be the hypersurface of equation $t=\infty$, and let $\mathcal{H}_{\mathrm{Ram}}$ be the hypersurface of equation $\mathcal{S}(t)=0$. Let D_0 be the divisor $-(n-1)(\mathcal{H}_\infty)+2(\mathcal{H}_{\mathrm{Ram}})$. Let $D=\mathrm{Div}(\Gamma)-D_0$. We will show that D is divisible by 2. Note first that if D had a zero of odd order, then since $\Gamma\Gamma^\sigma$ is a square for all $\sigma\in A_n$ by Proposition 1, $D+D^\sigma$ is even, so we must have a whole orbit of zeros of odd order under A_n.

Now, if $H_0(y_1, ..., y_n)\neq 0$, then $\mathcal{S}(t)$ has $n-1$ distinct roots and so the intersection of D_0 with the curve C_P is a divisor of degree $-(n-1)n!/6$. As $D+D_0$ is the divisor of a function, if we write D_P for the intersection of D with C_P, then D_P must have degree $(n-1)n!/6$, and each hypersurface appearing in D intersects C_P in a number of points independent of $P(X)$. In particular, if D has an orbit under the action of A_n, the intersection of this orbit with each of the C_P will be a sum of divisors stable by A_n. Now, since D is an effective divisor, this means that D_P will be the sum of an effective non-zero divisor stable by A_n and another effective divisor. Thus, in order to prove that D is divisible by 2, and that $\tilde{V}$ is unramified over V, it is sufficient to give one explicit polynomial $P(X)$ with roots y_i in $\bar{K}$ such that $H_0(y_1, ..., y_n)\neq 0$, and such that D_P does not contain any divisor stable by A_n. We will take $P(X)=X^n-X$, $Q(X)=n^2X^{n-1}-(n-2)^2$, and $R(X)=nX^{n-1}+(n-2)$. Let C_P be the curve whose function field is $K(t)(x_1, ..., x_n)$ where the x_i are the roots of $P(X)-tQ(X)$. Let H_∞ be the intersection of $\mathcal{H}_\infty$ with C_P, and H_{Ram} the intersection of $\mathcal{H}_{\mathrm{Ram}}$ with C_P. Recall that $D_P=\mathrm{Div}(\gamma)-2(H_{\mathrm{Ram}})+(n-1)(H_\infty)$.

LEMMA. *Let $\bar{P}(X)=X^n-X$. Then D_P does not possess an orbit of zeros under A_n.*

Proof. We treat separately the cases $t=0$, $t=\infty$, $t=P(v)/Q(v)$ for v a root of $R(X)$, and other values of t.

Case 1. $t=0$. It suffices to remark that when $t=0$, the roots of $\mathcal{F}(X)$ are just the $y_1, ..., y_n$. The point $y_1, ..., y_n$ is on C_P, and therefore so is the point $P_\sigma=(y_{\sigma(1)}, ..., y_{\sigma(n)})$ for $\sigma=(1, 2, ..., n)$. But it is easy to check that γ evaluated at P_σ is equal to $2R(y_1)\cdots R(y_n)$, which is non-zero because $R(X)$ is prime to $P(X)$. This also shows that $\gamma\neq 0$ for any polynomial $P(X)$.

Case 2. $t=\infty$. In this case, it suffices to prove that γ has at least one pole of order exactly $n-1$. Let $a=2(n-1)(n-2)/n$, $b=4(2-n)(1-n)/n^2$, and $c=8(1-n)/n^2$. Let z_0 be the $(n-1)$th root of $(n-2)^2/n^2$ in $\mathbf{R}^+$, and let $\zeta=\exp(2i\pi/(n-1))$. Let $z=z_0\zeta$. We choose to number the roots of $P(X)$ in the following order: $y_1=0$, $y_i=\zeta^{i-1}$ for $i=2, \dots, n$. We will consider the pole occurring at the point $(x_1, \dots, x_n)$ where $x_1=\infty$ and $x_i=z\zeta^{i-1}$ for $i=2, \dots, n$ (we may check that this point is on the curve by verifying that the signs are the same on both sides of the equation $\prod_{i<j}(x_i-x_j)=\mathscr{S}(t)\prod_{i<j}(y_i-y_j)$). We find that

$$\gamma=\det\begin{pmatrix} 2x_1^{n-1}+\cdots & b & b & \cdots & b \\ 2x_1^{n-1}+\cdots & \frac{cz}{z-1}-a & \frac{cz}{z-\zeta^{n-2}} & \cdots & \frac{cz}{z-\zeta} \\ 2x_1^{n-1}+\cdots & \frac{cz}{z-\zeta} & \frac{cz}{z-1}-a & \cdots & \frac{cz}{z-\zeta^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2x_1^{n-1}+\cdots & \frac{cz}{z-\zeta^{n-2}} & \frac{cz}{z-\zeta^{n-1}} & \cdots & \frac{cz}{z-1}-a \end{pmatrix}.$$

We want to prove that the order of the pole is $n-1$, so it suffices to show that the coefficient of x_1^{n-1} in γ is non-zero. If we subtract the first row from all the others, we see immediately that this coefficient is 2 times the determinant of a cyclic matrix, and is equal to

$$-\frac{8(n-1)(n-2)}{n}\prod_{k=1}^{n-2}\left(\frac{-2(n-1)(n-2)}{n}+2(n-1)z^k\right).$$

The only factor which might be zero is for $k=(n-1)/2$. But since we chose $z_0\in\mathbf{R}^+$, this factor is non-zero.

Case 3. $t\neq 0$, $t\neq\infty$, $t\neq P(v)/Q(v)$ for v a root of $R(X)$, say $t=t_0$. If D_P possessed an orbit of zeros for $t=t_0$, it would then also have orbits of zeros for the values $t=\zeta^k t_0$ where ζ is a primitive $(n-1)$th root of unity and $k=1, \dots, n-2$. We see this as follows. Let $x_1, \dots, x_n$ be the roots of $P(X)-t_0Q(X)$. Then the roots of $P(X)-\zeta^k t_0 Q(X)$ are $\zeta^k x_1, \dots, \zeta^k x_n$. Now, we check easily using the sign of the product of the differences that the point $P_k=(\zeta^k x_1, \zeta^k x_{n+1-k}, \dots, \zeta^k x_{n-k})$ is on C_P for $k=1, \dots, n-2$. We also see that $u_1(X)=(2-n)(X^{n-1}-1)$ and $u_i(X)=2(X^n-X)/(X-\zeta^{i-1})$ for $i=2, \dots, n$, so that $u_1(\zeta^k X)=u_1(X)$, $u_i(\zeta^k X)=u_{n+i-k-1}(X)$ for $i=2, \dots, k+1$, and $u_i(\zeta^k X)=u_{i-k}(X)$ for $i=k+2, \dots, n$. Moreover it is evident that $R(\zeta^k X)=R(X)$ for all k. We may now confirm that each zero over $t=t_0$ implies one over $t=\zeta^k t_0$. For if we suppose that $\det(\mathscr{M}+\mathscr{R})=0$, then replacing the point $(x_1, \dots, x_n)$ by P_k gives the same matrix up to permutation of the rows and columns.

Now, if D_P really had complete orbits of zeros for all the values of

$t=\zeta^k t_0$, $k=1, ..., n-1$, we would have at least $(n-1)n!/2$ zeros, which is far more than $\deg D_P$.

Case 4. $t=P(v)/Q(v)$ for v a root of $R(X)$. Recall that $\deg D_P = (n-1)n!/6$. It is easy to see that there are exactly $n!/6$ points on C_P over $t=P(v)/Q(v)$, and moreover that if a zero occurred for one root v one would occur for all v as remarked in Case 3. This would give a total of $(n-1)n!/6$ zeros, which would mean that D_P had no other zeros. But that is false; for instance, when $t=0$ the roots of $F(X)$ are equal to those of $P(X)$ and since $u_i(y_j)=R(y_j)$ for $i=1, ..., n$ and $u_i(y_j)=0$ whenever $i \neq j$, $n-1$ columns of the matrix become identically zero, so there is a zero of order at least $n-1$.

This concludes the proof of the lemma. The lemma suffices to prove Proposition 2, and therefore the proof of Theorem 3 is complete.

A Remark on the zeros of γ. In general, we were unable to determine all the zeros of γ. However, a good many of them occur at the value $t=0$. In fact, permuting the columns of the matrix when the x_i's are equal to the y_i's gives the following minimization of the number of zeros at $t=0$. For each $\sigma \in A_n$, let $\omega(\sigma)$ be the number of disjoint cycles in σ. Then for each σ, there is a zero of order at least $\omega(\sigma)-1$. This order can be larger than $\omega(\sigma)-1$ if there is sufficient symmetry in the roots of $P(X)$.

Set $\mathscr{R}' = \operatorname{diag}(R(x_1), ..., R(x_n))$. If we defined $\gamma = \det(\mathscr{M}+\mathscr{R}')$ instead of $\det(\mathscr{M}+\mathscr{R})$, then γ would generate the right extension but it would have many less zeros at $t=0$; this is why we introduced the matrix $\mathscr{J}$ in the proof of part (i) of Theorem 3.

EXAMPLE. $n=5$. Let us consider the polynomial $P(X)=X(X^2-1)(X^2-4)$. Counting poles of γ via a computer calculation, we find that all but two of them have order 4; two poles have order 2, those associated to the permutations (12)(35) and (13524) when we number the roots in the order $y_1=-2$, $y_2=-1$, $y_3=0$, $y_4=1$, $y_5=2$. So there are 236 poles. We know that there are 160 zeros at the ramification points. We calculate the orders of the zeros at $t=0$ and we find that they all have order exactly $\omega(\sigma)-1$ except the zero at (15)(24) which for reasons of symmetry in the roots has order 4. So we have a total of $160+76=236$ zeros, and in this case we know $\operatorname{Div}(\gamma)$ completely.

REFERENCES

[C] T. CRESPO, Explicit construction of $\tilde{A}_n$ type fields, *J. Algebra* **127** (1989), 452–461.

[M] J.-F. MESTRE, Extensions régulières de $\mathbb{Q}(t)$ de groupe de Galois $\tilde{A}_n$, *J. Algebra* **131** (1990), 483–495.

[S] J.-P. SERRE, L'invariant de Witt de la forme $\operatorname{Tr}(x^2)$, *Comment. Math. Helv.* **59** (1984), 651–676.

[S2] J.-P. SERRE, Relèvements dans $\tilde{A}_n$, Note C.R.A.S. Tome 311, Série I, (1990), 477–482.