PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 138, Number 4, April 2010, Pages 1205–1212
S 0002-9939(09)10130-2
Article electronically published on November 20, 2009

GALOIS GROUPS OVER FUNCTION FIELDS OF POSITIVE CHARACTERISTIC

JOHN CONWAY, JOHN McKAY, AND ALLAN TROJAN

(Communicated by Jonathan I. Hall)

Abstract. We prove examples motivated by work of Serre and Abhyankar.

1. The main result

Let K be a field of characteristic p with algebraic closure $\overline{K}$, $K(t)$ the field of functions in the variable t, and q a power of p; Galois fields of order q will be denoted by F_q. A survey of computational Galois theory is found in [6]; here we describe techniques for computing Galois groups over $K(t)$.

Questions and conjectures concerning Galois theory over $\overline{K}(t)$ were raised by Abhyankar [1] in 1957. Apparently the first result was obtained in 1988 by Serre (in Abhyankar, [2], appendix), who proved that $\mathrm{PSL}_2(q)$ occurs for the polynomial $x^{q+1} - tx + 1$.

Abhyankar continued in [1], obtaining results for unramified coverings of the form:

$$x^n - at^u x^v + 1, \quad (v, p) = 1, \quad n = p + v,$$

and

$$x^n - ax^v + t^u, \quad (v, p) = 1, \quad n \equiv 0 \pmod{p}, \quad u \equiv 0 \pmod{v}.$$

The groups obtained have the form S_n, A_n, $\mathrm{PSL}_2(p)$ or $\mathrm{PSL}_2(2^3)$.

They used algebraic geometry to construct a Galois covering. Abhyankar used a method that relied on a characterization of the Galois groups as permutation groups while Serre used a method based on Lüroth's theorem and the invariant theory of Dickson. Later, in [3], Abhyankar obtained the Mathieu group, M_{23}, as the Galois group of $x^{23} + tx^3 + 1$ over $F_2(t)$. His proof was based on an idea used by Serre (in Abhyankar and Yie, [5]), who showed that $\mathrm{PSL}(3, 2)$ is the Galois group of $x^7 + tx^3 + 1$ over $F_2(t)$.

They express the irreducible polynomial as a factor of an additive polynomial, that is, a polynomial of the form: $g(x) = \sum_{i=0}^{n} a_i x^{p^i}$.

Such a polynomial has the property that its zeros form a vector space over F_p. Thus the Galois group of any polynomial dividing g is bounded above by $\mathrm{GL}(n, p)$. The action of the Frobenius element, and further knowledge on transitivity, may provide lower bounds, sometimes determining the group. Abhyankar obtained these transitivity conditions by the technique of throwing away a root [2, section 2] and

Received by the editors November 25, 2008, and, in revised form, July 27, 2009.
2000 *Mathematics Subject Classification.* Primary 11F22, 11F03; Secondary 30F35, 20C34.
Key words and phrases. Galois groups, Mathieu groups, function fields.

he continued in a long series of papers. In [4] he has written an expository summary with many references.

Using simpler arguments, avoiding algebraic geometry, and, furthermore, not requiring algebraic closure, we [9] found the Galois groups of several polynomials over $F_p(t)$ for $p = 2, 3$.

If t is algebraic over F_p, and if the polynomial $f(x,t)$ over $F_p(t)$ has distinct roots and irreducible factors of degrees d_1, d_2, ..., then the Galois group of $f(x,t)$ contains a permutation of shape d_1, d_2, ... (van der Waerden, [11]).

The following Galois groups were obtained over $F_2(t)$ and $F_3(t)$ respectively:

$x^{24}+x+t$	M_{24}
$x^{23}+x^3+t$	M_{23}
$x^{13}+x+t$	$\mathrm{PSL}_3(3)$
x^8+x^7+t	$\mathrm{PSL}_2(7)$
x^7+x+t	$\mathrm{PSL}_3(2)$
x^4+x+t	D_4

$x^{12}+x+t$	M_{11}
$x^{11}+tx^2-1$	M_{11}

Here is the proof for the polynomial $f = x^{24}+x+t$:

1. Specialize t to be a root of one of the following equations:

$$t = 0, \quad t = 1, \quad t^3+t^2+1 = 0.$$

2. Over the algebraic closure of F_2 we find irreducible factors of respective degree shapes:

$$[11^2 1^2], \quad [21,3], \quad [23,1].$$

3. It follows that the Galois group G (over $F_2(t)$) is at least 3-transitive and has order a multiple of $7{\cdot}11{\cdot}23$; thus, as a permutation group, it is one of S_{24}, A_{24}, or M_{24}.

4. We obtain an additive polynomial as a multiple of f as follows:

$$\begin{aligned}
0 &\equiv x^{32}+x^9+tx^8 \pmod f \\
&\equiv x^{256}+x^{72}+t^8x^{64} && \text{(raising to the } 8^{\text{th}} \text{ power)} \\
&\equiv x^{256}+t^8x^{64}+x^3+tx^2+t^2x+t^3 && \text{(substituting } x^{72} \equiv (x+t)^3\text{)} \\
&\equiv x^{2048}+t^{64}x^{512}+x^{24}+t^8x^{16}+t^{16}x^8+t^{24} && \text{(raising to the } 8^{\text{th}} \text{ power);}
\end{aligned}$$

thus, since $x^{24} = x+t$, we get the semi-linear relationship

$$t+t^{24} = L = x^{2048}+t^{64}\,x^{512}+t^8\,x^{16}+t^{16}\,x^8+x,$$

so $L^2 = (t+t^{24})L$ is an equation of degree 2^{12} in x whose terms involve only the powers of

$$x^{2^n} : 0 \le n \le 12.$$

5. The zeros of f satisfy an additive polynomial and so lie in a vector space of dimension 12 over F_2. But neither A_{24} nor S_{24} can act on such a space ($G \subseteq \mathrm{GL}_{12}(2)$), so $G = M_{24}$.

Except for the M_{11} degree 11 case, similar methods are used to determine the other Galois groups, and a computer is used only for the factorization of the polynomial over finite fields. In the last case: $f(x) = x^{11}+tx^2-1$ over F_3. We seek an additive polynomial of degree 3^5 but find only an additive polynomial of degree 3^{10}

with 326 terms. It was unclear to us whether one can derive a degree 3^5 additive polynomial using this method but modifying the initial $f(x)$.[1]

The zeros of f satisfy an additive polynomial whose zeros form a vector space of dimension 10 over F_3. As before, by factoring f over various finite extensions of $F_3(t)$, $G = \mathrm{Gal}(f)$ is shown to contain permutations of shapes: $[5^2, 1]$, $[6, 3, 2]$, $[8, 2, 1]$, and $[11]$, which are shapes occurring in M_{11}. So the group is at least 3-transitive, which means it is one of S_{11}, A_{11}, M_{11}, but S_{11} is excluded since the discriminant of $f(x,t)$ with respect to x is a square.

To exclude A_{11} requires more. The 5-set resolvent polynomial $f^{\times 5}$ (see [8]) is computed over its coefficient ring. (The zeros of this polynomial, of degree $\binom{11}{5} = 462$, are the products formed from the 5-element subsets of the zeros of f.) This resolvent polynomial has a factor of x-degree 66:

$$\begin{aligned} f_{66} = {} & x^{66} + tx^{62} + 2\,t^5x^{57} + t^3x^{54} + t^6x^{53} + tx^{51} + 2\,t^7x^{49} \\ & + t^{10}x^{48} + 2\,t^2x^{47} + t^5x^{46} + 2\,t^8x^{45} + t^3x^{43} + 2\,t^6x^{42} + tx^{40} \\ & + 2\,t^7x^{38} + t^2x^{36} + t^8x^{34} + x^{33} + 2\,t^6x^{31} + t^9x^{30} + 2\,tx^{29} \\ & + 2\,t^7x^{27} + 2\,t^5x^{24} + 2\,t^3x^{21} + 2\,t^6x^{20} + 2\,tx^{18} + 2\,t^7x^{16} \\ & + t^2x^{14} + t^5x^{13} + t^8x^{12} + 2\,t^3x^{10} + 2\,t^6x^9 + 2\,tx^7 + 2\,t^2x^3 + 1, \end{aligned}$$

so finally the Galois group is M_{11}, not A_{11}.

2. Series solutions to the equations

The methods so far are non-constructive. To construct the group and to study the Galois correspondence, it is useful to work with exact zeros of the polynomial, either as formal Taylor series or as formal Puiseux series in the variable t over the field F_q.

We write Fano(x) for the polynomial $x^7 + tx + 1$ over $F_2(t)$, which we shall see is related closely to Serre's $x^7 + tx^3 + 1$.

Proposition 2.1. Fano(x) *has seven formal Taylor series solutions, of the form:*

$$f_\varepsilon = \sum_{i \in \Omega} \varepsilon^{2^{N(i)}} t^i,$$

where Ω is the set of non-negative integers, n, such that $n = 0$ or the lengths of the blocks of zeros in the binary expansion of n are all multiples of 3; $N(i)$ is the number of 1's in the binary expansion of i; and ε is a primitive 7^{th} root of unity in F_{2^3}.

We show that the series f_ε are solutions to the additive polynomial $x^8 + tx^2 + x$ and we identify them with the set of pairs

$$\Lambda = \{\, (i, N(i) \bmod 3) : i \in \Omega \,\}.$$

The map Ψ_0 that sends the series f to f^8 sends $(i, N(i))$ to $(j, N(i))$, where the binary expansion of j is obtained from that of i by appending the block 000; however, $N(i) = N(j)$, so $(i, N(i))$ is sent to $(j, N(j))$ and so Ψ_0 sends Λ onto the subset

$$\Lambda_0 = \{\, (i, N(i)) : i \in \Omega \text{ and } i \equiv 0 \bmod 8 \,\}.$$

[1]Florian Möller and Peter Müller of Würzberg have pointed out that orbit considerations preclude our needs, but we may replace $f(x,t)$ by $f(x^2,t)$ and attain our goal with the additive polynomial $x^{243} + t^9x^{81} - tx^{27} + t^2x^9 - x$.

The map Ψ_1 that sends the series f to tf^2 sends $(i, N(i))$ to $(j, N(i)+1)$, where j is obtained from i by appending the digit 1 to the binary representation of i, but in this case also, $(i, N(i))$ is again sent to $(j, N(j))$ since $N(i)+1 = N(j)$, so Ψ_1 sends Λ onto the subset

$$\Lambda_1 = \{\, (i, N(i)) : i \in \Omega \text{ and } i \equiv 1 \bmod 2 \,\}.$$

Hence the map $f^8 + tf^2 = \Psi_0 + \Psi_1$ is a bijection of Λ with Λ.

The preceding proof indicates how to obtain series solutions to an additive polynomial. However, not every additive polynomial has a complete set of solutions in the form of a Taylor series or even a Puiseux series.

The polynomial $x^4 + x^2 + tx$, for example, has only one series solution $(t + t^3 + t^5 + t^9 + \cdots)$, but if we substitute $t = \frac{1}{s}$ the polynomial equation becomes: $sx^4 + sx^2 + x$, which has 3 solutions:

$$x = As^{-\frac{1}{3}} + B \cdot s^{\frac{1}{3}} + A \cdot s^{\frac{5}{3}} + B \cdot s^{\frac{7}{3}} + \cdots,$$

where A is any of the three cube roots of unity and $B = A^2$. These solutions may be thought of as Puiseux series "about the point at infinity".

When the polynomial is not additive, one can get series solutions by working with an additive polynomial multiple.

Proposition 2.2. *The polynomial* $\text{Mathieu}(x) = x^{24}+x+t$ *has twenty-three formal Taylor series solutions of the form*

$$f_\alpha = \sum_{i \in \Omega} \alpha^{1-i} t^i,$$

where α *is any non-zero solution to the equation* $x^{24} = x$ *in an extension of* F_2 *and* Ω *is the set of non-negative integers,* n*, such that the binary representation of* n *has the form* 0 *or* 11 *or* 101000 *or* 100000000 *followed by any combination of* 010*,* 0001*,* 000001000*,* 00000000000 *followed by* 000*.*

First, suppose

$$f = \sum_{i \in \Lambda} \alpha^{K(i)} t^i$$

is a Taylor series solution to $\text{Mathieu}(x) = 0$; then for every i, we have $K(i) + i \equiv 1 \pmod{23}$.

This follows by induction from the fact that the terms of f^{24} are of the form $\alpha^{24K(i)} t^{24i}$ or $\alpha^{16K(i)+8K(i')} t^{16i+8i'}$, so such a Taylor series solution is determined by α, which satisfies $\alpha^{23} = 1$, and the exponents of t, which are independent of α. To determine $f(x)$ it is sufficient to determine the exponents of t occurring, so we may assume $\alpha = 1$.

We make the substitutions $g = f + t, u = t^8$ in the semi-linear equation (1) satisfied by f to get

$$g^{2048} + u^8 g^{512} + u g^{16} + u^2 g^8 + g + u^{256} + u^{72} + u^3 = 0.$$

We define the following binary sequences:

$$Z = 0, \quad A = 100000000, \quad B = 1001000, \quad C = 11,$$
$$K = 000000000000, \quad L = 000001000, \quad M = 0001, \quad N = 010.$$

For g a Taylor series in u over F_2 with constant term equal to 1, let Ω_g be the set of binary strings which occur as exponents of u in g. Since the constant term of g

is 1 and the terms $u^{256} + u^{72} + u^3$ occur in the semi-linear polynomial, Z, A, B, $C \in \Omega_g$.

As in the proof of Proposition 2.1 we can consider g^{2048}, $u^8 \cdot g^{512}$, etc., as operators on the set of binary strings. g^{2048}, $u^8 \cdot g^{512}$, ... append the strings K, L, ..., respectively. Since the images of these four operators are disjoint, if the string $S \in \Omega_g$, then $S \circ K$, $S \circ L$, $S \circ M$, $S \circ N \in \Omega_g$, where $\circ$ represents string concatenation.

Remark. The remaining series solution, with constant term 0, can be found using the same conditions omitting the initial term Z.

We return now to the polynomial Fano(x) of Proposition 2.1 and its complementary polynomial Serre(x).

It is instructive to see how the Galois group can be determined just from the series solutions determined by Proposition 2.1 using the fields given by the Galois correspondence.

In the notation of Proposition 2.1, let ε satisfy $\varepsilon^3 + \varepsilon + 1 = 0$ and

$$\begin{aligned} &P_i = f_{\varepsilon^i}, \\ &L_0 = P_1 \cdot P_2 \cdot P_4,\ L_1 = P_2 \cdot P_3 \cdot P_5,\ \ldots,\ L_6 = P_0 \cdot P_1 \cdot P_3 \\ &\qquad \text{(corresponding to the lines in the Fano projective plane)}, \\ &K = F_2(t, P_0, P_1, \ldots, P_6), \end{aligned}$$

and let R be the subfield of K containing all Taylor series in t whose coefficients are in F_2.

Proposition 2.3.

(1) $P_0, P_1, \ldots, P_6$ *are the zeros of* Fano$(x) = x^7 + t \cdot x + 1$.
$L_0, L_1, \ldots, L_6$ *are the zeros of* Serre$(x) = x^7 + s \cdot x^3 + 1$, *where* $s = t^2$.

(2) *The Galois groups* $G = G(\text{Fano}) = \text{PSL}_3(2) = G(\text{Serre})$.

(3) $\forall i, j\ F_2(P_i) \cap F_2(L_j) = F_2$.

(4) *The seven fields* $F_2(P_i)$ *correspond to seven subgroups of* G, *conjugate and isomorphic to* S_4.

(5) *The seven fields* $F_2(L_i)$ *correspond to the other seven subgroups of* G, *isomorphic to the previous seven subgroups under an outer automorphism of* G.

(6) *For the tower of fields* $F_2(t) \subset F_2(P_0) \subset F_2(L_0, P_0) \subset R$:

$$\begin{aligned} [K : R] &= 3 \quad \textit{(Frobenius automorphism)}, \\ [R : F_2(L_0, P_0, t)] &= 2, \\ [F_2(L_0, P_0, t) : F_2(P_0, t)] &= 4, \\ [F_2(P_0, t) : F_2(t)] &= 7. \end{aligned}$$

(7) $R = F_2(L_0, P_0, t, y)$, *where* y *is a zero of the polynomial* $x^2 + L_0 \cdot x + t$.

Proof. Since Fano(x) is irreducible and G contains the Frobenius automorphism obtained by applying the map $C \to C^2$ to the coefficients of the series P_i (or equivalently any series $S(t) \to S(t)^2$), 7 and 3 divide $|G|$, so by consideration of maximal subgroups, $G \cong \text{PSL}_3(2)$ or $|G|$=21.

To prove the first isomorphism, we show $2 \mid |G|$. Let

$$h(x) = (x - P_1) \cdot (x - P_2) \cdot (x - P_4) = x^3 + u \cdot x + L_0. \tag{1}$$

By the definition of P_i and Proposition 2.1, $P_1 + P_2 + P_4 = 0$; and u, $L_0 \in F_2[[t]] =$ the set of power series in t with coefficients in F_2 (since the coefficients of these series are fixed by the Frobenius automorphism). Dividing $h(x)$ into Fano(x) we get a remainder

$$r(x) = (t + L_0^2 + u^3) \cdot x + (1 + u^2 \cdot L_0) = 0. \tag{2}$$

Equating the coefficients to zero, we derive the equation

$$L_0^7 + t^2 \cdot L_0^3 + 1 = 0, \tag{3}$$

which shows that L_0 is a zero of Serre(x). We also have

$$u = t \cdot L_0 + L_0^3 \in F_2(L_0, t). \tag{4}$$

Dividing Fano(x) by its factor, $(x - P_0) \cdot (x^3 + u \cdot x + L_0)$, we get the full factorization

$$\text{Fano}(x) = (x - P_0) \cdot (x^3 + u \cdot x + L_0) \cdot (x^3 + P_0 \cdot x^2 + (u + P_0^2) \cdot x + (L_0 + u \cdot P_0 + P_0^3), \tag{5}$$

valid over $F_2(P_0, L_0, t)$ by (4). Again consider $h(x) = x^3 + u \cdot x + L_0 = (x - P_1) \cdot (x - P_2) \cdot (x - P_4)$.

Since $h(P_i) = 0, i = 1, 2, 4$ for these values of i,

$$P_i^3 = u \cdot P_i + L_0.$$

Let $y = P_1^2 \cdot P_2 + P_2^2 \cdot P_4 + P_4^2 \cdot P_1$ and $y' = P_2^2 \cdot P_1 + P_4^2 \cdot P_2 + P_1^2 \cdot P_4$; then

$$y + y' = L_0, \text{ and} \tag{6}$$

$$y \cdot y' = t. \tag{7}$$

Let $S(i, j, k)$ be the symmetric polynomial obtained by applying the cyclic permutation $(1, 2, 4)$ to the subscripts of $P_1^i \cdot P_2^j \cdot P_4^k$ and adding the products obtained:

$$\begin{aligned} 0 &= S(1, 0, 0) = P_1 + P_2 + P_4, \\ u &= S(1, 1, 0) = P_1 \cdot P_2 + P_2 \cdot P_4 + P_4 \cdot P_1, \\ L_0 &= S(1, 1, 1) = P_1 \cdot P_2 \cdot P_4, \end{aligned}$$

so

$$0 = S(1, 0, 0) \cdot S(1, 1, 0) = y + y' + L_0,$$

establishing equation (6), also

$$y \cdot y' = S(3, 3, 0) + S(2, 2, 2) + S(4, 1, 1).$$

Using (5):

$$\begin{aligned} S(3, 3, 0) &= u^2 \cdot S(1, 1, 0) + L_0^2 = u^3 + L_0^2, \\ S(2, 2, 2) &= L_0^2, \\ S(4, 1, 1) &= S(1, 1, 1) \cdot S(3, 0, 0) = L_0 \cdot (u \cdot S(1, 0, 0) + L_0), \end{aligned}$$

so

$$y \cdot y' = u^3 + L_0^2 = t$$

by equation (1), establishing equation (7). Since the coefficients of y and y' are fixed by the Frobenius automorphism, the coefficients are in F_2 and y, $y' \in R$.

By (6) and (7), $L_0 = y + \frac{t}{y}$, so using (3), there is an equation of degree 16 in y, which decomposes into irreducible factors over $F_2(t)$:

$$(y^{14} + t \cdot y^{12} + y^7 + t^6 \cdot y^2 + t^7) \cdot (y^2 + t) = 0,$$

so $|G|$ is even, implying $G \cong \mathrm{PSL}_3(2)$ and establishing statement (2). By the factorization (5) : $8 \nmid [K : F_2(L_0, P_0, t)]$ but $[K : F_2(L_0, t)] = 24$. So $P_0 \notin F_2(L_0, t)$ and so by (5) : $(x^4 + u \cdot x^2 + L_0 \cdot x + u^2) \cdot (x^3 + u \cdot x + L_0)$ are the irreducible factors of Fano(x) over $F_2(L_0, t)$. We find $[F_2(L_0, P_0, t) : F_2(P_0, t)] = 4$ and statement (6) follows since the Frobenius automorphism has order 3.

Now the Fano geometry can be defined by taking points as elements of $F_{2^3}^{\times}$ and lines as 3-element sets α, β, γ such that $\alpha + \beta + \gamma = 0$. All such sets are of the form $\{\alpha = \varepsilon^k, \beta = \varepsilon^{k+1}, \gamma = \varepsilon^{k+3}\}$, with exponents mod 7. We have $P_i + P_j + P_k = 0$ if and only if $\{\varepsilon^i, \varepsilon^j, \varepsilon^k\}$ is a line, which establishes statement (1).

The permutation $(1\,2)(3\,6) \in G$ fixes L_0 and P_0 but interchanges y and y', which establishes statement (7). Applying G to $F_2(P_0) \cap F_2(L_i) = F_2$, $i = 1, \ldots, 6$, establishes statement (3), and statement (4) follows from Galois theory and the subgroup structure of $\mathrm{PSL}_3(2)$.

For each i,j there is an outer automorphism taking the point stabilizer of P_i onto the line stabilizer of L_j (see [7]). This establishes statement (5).

Finally, there is a natural correspondence between the series solutions to $s_{11}(x) = x^{11} + tx^2 - 1$ over $F_3(t)$ and the 11 points of the Steiner system $\Sigma(4, 5, 11)$, [10], which is sketched in:

Proposition 2.4. *The polynomial $s_{11}(x) = x^{11} + tx^2 - 1$ has eleven Taylor series solutions $\theta_0(t)$, $\theta_1(t)$, ..., $\theta_{10}(t)$, where*

(1) *The constant term, $\theta_i(0)$, is ε^i, where ε is a primitive 11^{th} root of 1, for which $\varepsilon^5 + 2\,\varepsilon^3 + \varepsilon^2 + 2\,\varepsilon + 2 = 0$.*
(2) *$\theta_i = \sum_k c_k \varepsilon^{(2k+1)i} t^k$, where the $c_k \in F_3$ satisfy the recursion relations:*
   i. *$c_{3j+2} = 0$,*
   ii. *$c_{3j+1} = c_j$, and*
   iii. *$c_{3j} = \sum_{3m+n=j} c_m c_n$ mod 3.*
(3) *The Galois group, M_{11}, of $s_{11}(x)$, is generated by $\sigma = (0123456789\mathrm{X})$ and $\tau = (36)(40)(5\mathrm{X})(89)$ (where X represents the number 10), acting on the subscripts of the θ_i.*
(4) *The 66 Steiner 5-ads are the orbit of the 5-ad $\{\mathrm{X}8267\}$ under the actions of σ and τ, and to every 5-ad, $\{ijklm\}$, the corresponding product, $\theta_i\theta_j\theta_k\theta_l\theta_m$, is a zero of the polynomial f_{66}.*

Let $\theta_{i,0} = \varepsilon^i$. The Taylor series solution, θ_i, is generated by the recursion, $\theta_{i,j+1} = \theta_{i,j}^{12} + t\,\theta_{i,j}^3$, establishing (1). Let this series be $\sum_k c_k \varepsilon^{\rho(k)} t^k$. It follows from the recursion that $c_k = 0$ if $k \equiv 2 \bmod 3$.

If $k \equiv 1 \bmod 3$ and $k = 3j+1$, then $c_k \varepsilon^{\rho(k)} t^k = c_j^3 \varepsilon^{3\rho(j)i} t^{3j+1} \equiv c_j \varepsilon^{2k+1} t^k \bmod 3$ if $\rho(j) = 2j + 1$, which establishes (2:i, ii) by induction.

If $k \equiv 0 \bmod 3$, $k = 3j$, since $(a+b)^{12} \equiv a^{12} + a^9\,b^3 + a^3\,b^9 + b^{12} \bmod 3$,

$$\begin{aligned} c_k \varepsilon^{\rho(k)} t^k &= \sum\nolimits_{9m+3n=k} c_m^9 c_n^3 \varepsilon^{(9\rho(m)+3\rho(n))i}\, t^k \\ &\equiv \sum\nolimits_{9m+3n=k} c_m\, c_n\, \varepsilon^{(9\cdot 2m+3\cdot 2n+12)i}\, t^k \bmod 3 \\ &= \sum\nolimits_{3m+n=j} c_m\, c_n\, \varepsilon^{(2k+1)i}\, t^k, \end{aligned}$$

assuming $\rho(m) = 2m + 1$ and $\rho(n) = 2n + 1$. So (2:iii) also follows by induction.

For (3) and (4), a calculation shows that the permutations σ and τ generate a group of order $11 \cdot 10 \cdot 9 \cdot 8$ and that the orbit of $\{\mathrm{X}8267\}$ under this group

is the standard set of Steiner 5-ads, $\Sigma(4,5,11)$, obtained by the construction in [10]. Another computation shows that the corresponding products, $\theta_i\theta_j\theta_k\theta_l\theta_m$, for $\{ijklm\}$ a Steiner 5-ad, are zeros of the polynomial f_{66} mod t^{100}. The remaining 396 5-element products have a non-zero term of t-degree 4 when substituted into this polynomial. Since M_{11}, the Galois group of $s_{11}(x)$, permutes the zeros of f_{66}, it is the automorphism group of the set of 5-ads determined by (3) and so is generated by σ and τ. □

References

[1] Abhyankar, S. "Coverings of algebraic curves", Amer. J. Math., 79, 825–856, 1957. MR0094354 (20:872)

[2] Abhyankar, S. "Galois theory on the line in nonzero characteristic", Bull. Amer. Math. Soc. (N.S.), 27, no. 1, pp. 68–133, 1992. MR1118002 (94a:12004)

[3] Abhyankar, S. "Mathieu group coverings in characteristic two", Comptes Rendus Sci. Paris Sér. I. Math., 316, no. 3, pp. 267–271, 1993. MR1205196 (94g:14013)

[4] Abhyankar, S. "Resolution of singularities and modular Galois theory", Bull. Amer. Math. Soc. (N.S.) 38, no. 2, pp. 131–169 (electronic), 2001. MR1816069 (2002a:14013)

[5] Abhyankar, S., Yie, I. "Small degree coverings of the affine line in characteristic two", Discrete Math., 133, pp. 1–23, 1994. MR1298961 (95h:14017)

[6] "Algorithmic Methods in Galois Theory", J. Symb. Comp., 30, Elsevier, pp. 635–872, 2000. MR1800030 (2001f:12001)

[7] "Atlas of Finite Group Representations", `brauer.maths.qmul.ac.uk/Atlas/v3`.

[8] Casperson, D., McKay, J., "Symmetric functions, m-sets and Galois groups", Math. Comp., 63, pp. 749–757, 1994. MR1234424 (95a:12001)

[9] Conway, J., McKay, J., "M_{24} is the Galois group over $F_2(t)$ of $x^{24}+x+t$", Mathematical Abstracts, Amer. Math. Soc., 93T-12-69, p. 391, 1993.

[10] MacWilliams, F.J., Sloane, N.J.A., "The Theory of Error-Correcting Codes. I", North Holland, p. 70, 1977. MR0465509 (57:5408a)

[11] van der Waerden, B.L., "Algebra, Vol. 1", Frederick Ungar Publishing Co., 8.10, 1970. MR263582 (41:8187a)

Department of Mathematics, Fine Hall, Princeton University, Washington Road, Princeton, New Jersey 08544-1000

E-mail address: `conway@math.princeton.edu`

Department of Mathematics and CICMA, Concordia University, 1455 de Maisonneuve Boulevard, West, Montreal, Quebec H3G 1M8, Canada

E-mail address: `mac@mathstat.concordia.ca`

Department of Mathematics, York University, 4700 Keele Street, Toronto, Ontario M3J 1P3, Canada

E-mail address: `atrojan@yorku.ca`