PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 5, May 1995

SMALL MATHIEU GROUP COVERINGS IN CHARACTERISTIC TWO

SHREERAM S. ABHYANKAR AND IKKWON YIE

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. Explicit equations are given for unramified coverings of the affine line in characteristic two whose Galois groups are the Mathieu groups of degrees 11 and 12 and the automorphism group of the Mathieu group of degree 12.

1. INTRODUCTION

In Proposition 2 of the 1957 paper [Ab1], for any elements $c_0, c_1, \ldots, c_{(n/p)-1}$ in a field k of characteristic $p \neq 0$ with $c_0 \neq 0$, where n is any positive integer divisible by p, the polynomial

$$f(Y) = Y^n + c_{(n/p)-1}Y^{n-p} + \cdots + c_1 Y^p + c_0 Y$$

was considered, and it was noted that the equation $f(Y) + X = 0$ gives an unramified covering of the affine line L_k over k. In [Ab1] it was also suggested that the Galois group $\mathrm{Gal}(f(Y) + X, k(X))$ of this covering be computed. Recently (cf. [Ab5], [Ab6], [Ab7], [Ab8], [AOS], [AY1], [AY2]) this has been done for some values of the parameters $p, n, c_0, c_1, \ldots, c_{(n/p)-1}$. In this paper we shall do it for a few more cases.

Henceforth *we take k to be any field of characteristic $p = 2$ (for instance k = GF(2))* and, as a case of f with $n = 12$, we consider the polynomial

$$f_{12}(Y) = Y^{12} + Y^6 + Y^4 + Y^2 + Y \in k[Y].$$

Concerning this polynomial, in Section 6 we shall prove that:

First Mathieu Group Theorem (1.1). *The equation $f_{12}(Y) + X = 0$ gives an unramified covering of the affine line L_k with $\mathrm{Gal}(f_{12}(Y) + X, k(X)) = M_{12}$.*

Now the "twisted derivative" (cf. Section 18 of [Ab5]) of $f_{12}(Y)+X$ is given by

$$f'_{11}(X, Y) = Y^{-1}[f_{12}(Y + X) - f_{12}(X)]$$

and upon simplifying we get

$$f'_{11}(X, Y) = Y^{11} + X^4Y^7 + Y^5 + (X^8 + X^2 + 1)Y^3 + (X^4 + 1)Y + 1 \in k[X, Y].$$

As a consequence of (1.1), in Section 6 we shall show that:

Received by the editors August 4, 1993.
1991 *Mathematics Subject Classification.* Primary 12F10, 14H30, 20D06, 20E22.
Abhyankar's work was partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-92-H-3035. Yie's work was partly supported by PRF grant 690-1395-1920.

0002-9939/95 $1.00 + $.25 per page

Second Mathieu Group Theorem (1.2). *The equation* $f'_{11}(X, Y) = 0$ *gives an unramified covering of the affine line* L_k *with* $\mathrm{Gal}(f'_{11}(X, Y), k(X)) = M_{11}$.

As a biproduct of the proof of (1.1), in Section 6 we shall show that:

Third Mathieu Group Theorem (1.3). *The equation* $f_{12}(Y) + f_{12}(X) + 1 = 0$ *gives an unramified covering of the affine line* L_k *with*

$$\mathrm{Gal}(f_{12}(Y) + f_{12}(X) + 1, k(X)) = M_{11}(12).$$

Upon letting

$$f_{24}(Y) = [f_{12}(Y)]^2 + f_{12}(Y)$$

we clearly have

$$f_{24}(Y) = Y^{24} + Y^8 + Y^6 + Y$$

which is a case of f with $n = 24$. As a companion to (1.1), in Section 6 we shall prove that:

Fourth Mathieu Group Theorem (1.4). *The equation* $f_{24}(Y)+X = 0$ *gives an unramified covering of the affine line* L_k *with* $\mathrm{Gal}(f_{24}(Y)+X, k(X)) = \mathrm{Aut}(M_{12})$.

Note that M_{12} and its one-point stabilizer M_{11} are respectively the unique sharply 5-transitive and the unique sharply 4-transitive permutation groups of degree 12 and 11 discovered by Mathieu [Mat] in 1861. Also note that $M_{11}(12)$ is the 3-transitive but not 4-transitive representation of M_{11} acting on 12 letters. Finally note that M_{12} is an index 2 subgroup of its automorphism group $\mathrm{Aut}(M_{12})$ which is transitive but not doubly transitive permutation group of degree 24. For information about Mathieu groups see Chapter XII of [HuB].

The fact that Theorems (1.2) and (1.3) both give M_{11} can be explained by observing that the polynomials involved in them are closely related by the equation $Yf'_{11}(X, Y) + 1 = f_{12}(Y + X) + f_{12}(X) + 1$. At any rate, in Sections 2 and 3, by resolution of singularities of plane curves (cf. [Ab2], [Ab3], [Ab4]), we shall prove Irreducibility Lemmas (2.1) and (3.1) which respectively say that the polynomials $f'_{11}(X, Y)$ and $f_{12}(Y)+f_{12}(X)+1$ are irreducible, and which yield some estimates for the sizes of the above four Galois groups.

In (1.5) of [Ab6] it was shown that the polynomial $Y^{23} + XY^3 + 1$ divides an additive polynomial of degree 2^{11}, i.e., a polynomial of the form $Y^{2^{11}} + \sum_{i=0}^{10} a_i Y^{2^i}$ with $a_0 \neq 0$. By slightly modifying the proof of this, in Section 4 we shall prove Linearization Lemma (4.1) which says that the polynomial $f_{24}(Y) + X$ divides an additive polynomial of degree 2^{12}, and which yields some more estimates for the sizes of the said Galois groups.

In Section 6 we shall put together these estimates to prove Theorems (1.1) to (1.4). Some other auxiliary lemmas needed in these theorems will be proved in Section 5.

2. Resolution of singularities

By resolving singularities of a plane curve, let us prove the following:

First Irreducibility Lemma (2.1). *The polynomial* $f'_{11}(X, Y)$ *is irreducible in* $(\mathrm{GF}(2)(X))[Y]$ *and the order* $|\mathrm{Gal}(f'_{11}(X, Y), \mathrm{GF}(2)(X))|$ *is divisible by* 8.

Upon letting

$$\phi(X, Y) = X^{11} f'_{11}(1/X, Y/X)$$

we have

$$\begin{aligned}\phi(X, Y) &= Y^{-1}[(Y+1)^{12}-1] + X^6Y^{-1}[(Y+1)^6-1] + X^8Y^{-1}[(Y+1)^4-1] \\ &\quad + X^{10}Y^{-1}[(Y+1)^2-1] + X^{11} \\ &= Y^{11} + Y^7 + X^6Y^5 + (X^8+X^6+1)Y^3 + (X^4+1)X^6Y + X^{11}\end{aligned}$$

and clearly (2.1) is equivalent to saying that: (*) $\phi(X, Y)$ is irreducible in $(\mathrm{GF}(2)(X))[Y]$ and $|\mathrm{Gal}(\phi(X, Y), \mathrm{GF}(2)(X))|$ is divisible by 8.

Let C be the curve in the (X, Y)-plane over GF(2) given by the equation $\phi(X, Y) = 0$. Considering the quadratic irreducible polynomial $\Theta = Y^2 + Y + 1 \in \mathrm{GF}(2)[Y]$ we have

$$(\dagger) \qquad \phi = \phi(X, Y) = \Theta^4 Y^3 + X^6\Theta^2 Y + X^8 Y^3 + X^{10}Y + X^{11}.$$

In particular

$$(\ddagger) \qquad \phi = \Theta^4 Y^3 + Xh(X, Y) \quad \text{where} \quad h(X, Y) \in \mathrm{GF}(2)[X, Y]$$

and hence the intersection of the line $X = 0$ and the curve C consists of the two points P and Q given by the maximal ideals $(X, Y)\mathrm{GF}(2)[X, Y]$ and $(X, \Theta)\mathrm{GF}(2)[X, Y]$ in $\mathrm{GF}(2)[X, Y]$ respectively, and the said intersection has no point on the line at infinity.

We shall show that: (I) C is analytically irreducible at Q. From (‡) and (I) it follows that $\phi(X, Y)$ has an irreducible factor of Y-degree = (4 times the degree of Θ) = 8 with coefficients in the formal power series ring $\mathrm{GF}(2)[[X]]$, and hence $|\mathrm{Gal}(\phi(X, Y), \mathrm{GF}(2)(X))|$ is divisible by 8. We shall also show that: (II) C has exactly two (analytically irreducible) branches at P, they are rational over GF(2), and their mutual intersection multiplicity at P is 6. Finally we shall show that: (III) C has no singularities on the line at infinity, and P and Q are the only singularities of C at finite distance. If C had two components, then their degrees would be d and $11-d$ with $0 < d < 11$ and, by Bezout's Theorem, their intersection multiplicity (in the projective plane) would be $d(11-d)$ which is at least 10. Thus (I) to (III) imply (*). Therefore it suffices to prove (I), (II) and (III).

To prove (I) we shall resolve the singularity of C at the point Q by applying a succession of QDTs, i.e., quadratic transformations. The initial form of ϕ at Q is $\Theta^4 Y^3$ and by applying the QDT: $X = X_1$, $\Theta = X_1\Theta_1$, centered at Q, we get

$$\phi = X_1^4\phi_1 \quad \text{where} \quad \phi_1 = (\Theta_1 + X_1)^4 Y^3 + X_1^4\Theta_1^2 Y + X_1^6 Y + X_1^7.$$

Here the factor X_1^4 is the contribution of the exceptional line, and the proper transform of C is given by $C_1 : \phi_1 = 0$. There is a unique point Q_1 on C_1 corresponding to Q, and (X_1, Θ_1) is a basis of the maximal ideal in the local ring of Q_1.

Now the initial form of ϕ_1 at Q_1 is $(\Theta_1 + X_1)^4 Y^3$ and by applying the QDT: $X_1 = X_2$, $\Theta_1 = X_2(\Theta_2 + 1)$, centered at Q_1, we get

$$\phi_1 = X_2^4\phi_2 \quad \text{where} \quad \phi_2 = \Theta_2^4 Y^3 + X_2^2\Theta_2^2 Y + X_2^3.$$

Again the factor X_2^4 is the contribution of the exceptional line, and the proper transform of C_1 is given by $C_2 : \phi_2 = 0$. There is a unique point Q_2 on C_2 corresponding to Q_1, and (X_2, Θ_2) is a basis of the maximal ideal in the local ring of Q_2.

The initial form of ϕ_2 at Q_2 is X_2^3 and by applying the QDT: $\Theta_2 = \Theta_3$, $X_2 = \Theta_3 X_3$, centered at Q_2, we get

$$\phi_2 = \Theta_3^3 \phi_3 \quad \text{where} \quad \phi_3 = \Theta_3 Y^3 + X_3^2 \Theta_3 Y + X_3^3.$$

The factor Θ_3^3 is the contribution of the exceptional line, and the proper transform of C_2 is given by $C_3 : \phi_3 = 0$. There is a unique point Q_3 on C_3 corresponding to Q_2, and (X_3, Θ_3) is a basis of the maximal ideal in the local ring of Q_3. The initial form of ϕ_3 at Q_3 is $\Theta_3 Y^3$. Thus C is analytically irreducible at Q.

To prove (II) we shall resolve the singularity of C at the point P again by applying a succession of QDTs. The initial form of ϕ at P is Y^3 and by applying the QDT: $X = X_1$, $Y = X_1 Y_1$, centered at P, we get

$$\phi = X_1^3 \phi_1 \quad \text{where} \quad \phi_1 = Y_1^3 + X_1^4 Y_1 + X_1^8 + X_1^8 Y_1 + X_1^6 Y_1^3 + X_1^8 Y_1^3 + X_1^4 Y_1^7 + X_1^8 Y_1^5 + X_1^8 Y_1^{11}.$$

The factor X_1^3 is the contribution of the exceptional line, and the proper transform of C is given by $C_1 : \phi_1 = 0$. There is a unique point P_1 on C_1 corresponding to P, and (X_1, Y_1) is a basis of the maximal ideal in the local ring of P_1.

The initial form of ϕ_1 at P_1 is Y_1^3 and by applying the QDT: $X_1 = X_2$, $Y_1 = X_2 Y_2$, centered at P_1, we get

$$\phi_1 = X_2^3 \phi_2 \quad \text{where} \quad \phi_2 = Y_2(Y_2 + X_2)^2 + X_2^5 + X_2^6 h_2(X_2, Y_2)$$

with $h_2(X_2, Y_2) \in \mathrm{GF}(2)[X_2, Y_2]$. Here the factor X_2^3 is the contribution of the exceptional line, and the proper transform of C_1 is given by $C_2 : \phi_2 = 0$. There is a unique point P_2 on C_2 corresponding to P_1, and (X_2, Y_2) is a basis of the maximal ideal in the local ring of P_2.

The initial form of ϕ_2 at P_2 is $Y_2(Y_2 + X_2)^2$ and by applying the QDT: $X_2 = X_3$, $Y_2 = X_3(Y_3 + 1)$, centered at P_2, we get

$$\phi_2 = X_3^3 \phi_3 \quad \text{where} \quad \phi_3 = Y_3^2 + X_3^2 + Y_3^3 + X_3^4 h_3(X_3, Y_3)$$

with $h_3(X_3, Y_3) \in \mathrm{GF}(2)[X_3, Y_3]$. The factor X_3^3 is the contribution of the exceptional line, and the proper transform of C_2 is given by $C_3 : \phi_3 = 0$. There are exactly two points P_3 and P_3' on C_3 corresponding to P_2, and (X_3, Y_3) and $(X_3, Y_3 + 1)$ are bases of the maximal ideals in the respective local rings of P_3 and P_3'.

Now $\phi_3 = (Y_3 + 1) + (Y_3 + 1)^3 + X_3^2 + X_3^4 h_3(X_3, Y_3)$ and hence P_3' is a simple point of C_3. The initial form of ϕ_3 at P_3 is $(Y_3 + X_3)^2$ and hence P_3 is a double point of C_3, and by applying the QDT: $X_3 = X_4$, $Y_3 = X_4(Y_4 + 1)$, centered at P_3, we get

$$\phi_3 = X_4^2 \phi_4 \quad \text{where} \quad \phi_4 = X_4 + X_4 Y_4 + Y_4^2 + X_4 Y_4^2 + X_4 Y_4^3 + X_4^2 h_3(X_4, X_4 Y_4).$$

The factor X_4^2 is the contribution of the exceptional line, and the proper transform of C_3 is given by $C_4 : \phi_4 = 0$. There is a unique point P_4 on C_4 corresponding to P_3, and (X_4, Y_4) is a basis of the maximal ideal in the local ring of P_4. The initial form of ϕ_4 at P_4 is X_4, and hence C_4 has a simple point at P_4.

Thus C has two analytically irreducible branches at P. Since the multiplicity of P on C is 3, one of the branches should have a simple point and the

other a double point at P. Those two branches split after three QDTs, and hence their intersection multiplicity is $2+2+2=6$.

To prove (III), we homogenize $\phi(X, Y)$ to get

$$\Phi = Y^{11} + Z^4Y^7 + X^6Y^5 + (X^8 + X^6Z^2 + Z^8)Y^3 + (X^4 + Z^4)X^6Y + X^{11}.$$

The partial derivatives of Φ are

$$\Phi_X = X^{10},$$
$$\Phi_Y = Y^2(Y^2 + ZY + Z^2)^4 + X^6(Y^4 + X^2Y^2 + Z^2Y^2 + X^4 + Z^4),$$
$$\Phi_Z = 0.$$

Solving the equations $\Phi = \Phi_X = \Phi_Y = \Phi_Z = 0$, we see that C has no singularity at infinity and P and Q are its only singularities at finite distance.

3. More resolution of singularities

Again by resolution of singularities of plane curves, we shall now prove the following:

Second Irreducibility Lemma (3.1). *The polynomial* $f_{12}(Y) + f_{12}(X) + 1$ *is irreducible in* $(\mathrm{GF}(2)(X))[Y]$.

Upon letting

$$\psi(X, Y) = X^{12}[f_{12}(Y/X + 1/X) + f_{12}(1/X) + 1]$$

we have

$$\begin{aligned}\psi(X, Y) &= [(Y+1)^{12} - 1] + X^6[(Y+1)^6 - 1] + X^8[(Y+1)^4 - 1] \\ &\quad + X^{10}[(Y+1)^2 - 1] + X^{11}Y + X^{12} \\ &= Y^{12} + Y^8 + X^6Y^6 + (X^8 + X^6 + 1)Y^4 + (X^4 + 1)X^6Y^2 \\ &\quad + X^{11}Y + X^{12}\end{aligned}$$

and clearly (3.1) is equivalent to saying that: ($'$) $\psi(X, Y)$ is irreducible in $(\mathrm{GF}(2)(X))[Y]$.

Let D be the curve in the (X, Y)-plane over GF(2) given by the equation $\psi(X, Y) = 0$. Clearly the intersection of the line $Y = 0$ and the curve D consists of the point P given by the maximal ideal $(X, Y)\mathrm{GF}(2)[X, Y]$, and the said intersection has no points on the line at infinity. Since, by Bezout's Theorem, the line $Y = 0$ has a nonempty intersection with each component of D, it follows that P must lie on each (global) component of D. Therefore to prove ($'$) it suffices to show that: ($''$) D is analytically irreducible at P.

To prove ($''$) we shall again resolve the singularity of D at the point P by applying a succession of QDTs. The initial form of ψ at P is Y^4 and by applying the QDT: $X = X_1$, $Y = X_1Y_1$, centered at P, we get

$$\psi = X_1^4\psi_1 \quad \text{where} \quad \psi_1 = Y_1^4 + X_1^4Y_1^2 + X_1^8 + X_1^8Y_1 + X_1^8Y_1^2 + X_1^4Y_1^4g(X_1, Y_1)$$

with $g(X_1, Y_1) \in \mathrm{GF}(2)[X_1, Y_1]$. Here the factor X_1^4 is the contribution of the exceptional line, and the proper transform of D is given by $D_1 : \psi_1 = 0$. There is a unique point P_1 on D_1 corresponding to P, and (X_1, Y_1) is a basis of the maximal ideal in the local ring of P_1.

The initial form of ψ_1 at P_1 is Y_1^4 and by applying the QDT: $X_1 = X_2$, $Y_1 = X_2Y_2$, centered at P_1, we get

$$\psi_1 = X_2^4\psi_2 \quad \text{where} \quad \psi_2 = (Y_2^2 + X_2Y_2 + X_2^2)^2 + X_2^5Y_2 + X_2^6Y_2^2 + X_2^4Y_2^4 g(X_2, X_2Y_2).$$

Again the factor X_2^4 is the contribution of the exceptional line, and the proper transform of D_1 is given by $D_2 : \psi_2 = 0$. There is a unique point P_2 on D_2 corresponding to P_1, and (X_2, Y_2) is a basis of the maximal ideal in the local ring of P_2.

The initial form of ψ_2 at P_2 is $(Y_2^2 + X_2Y_2 + X_2^2)^2$ and by applying the QDT: $X_2 = X_3$, $Y_2 = X_3Y_3$, centered at P_2, and considering the quadratic irreducible polynomial $\Delta_3 = Y_3^2 + Y_3 + 1 \in \mathrm{GF}(2)[Y_3]$, we get

$$\psi_2 = X_3^4\psi_3 \quad \text{where} \quad \psi_3 = \Delta_3^2 + X_3^2\Delta_3 + X_3^2(Y_3+1)^2 + X_3^4Y_3^2 + X_3^4Y_3^4 g(X_3, X_3^2Y_3).$$

The factor X_3^4 is the contribution of the exceptional line, and the proper transform of D_2 is given by $D_3 : \psi_3 = 0$. There is a unique point P_3 (which is not rational over GF(2)) on D_3 corresponding to P_2, and (X_3, Δ_3) is a basis of the maximal ideal in the local ring of P_3. Let $\Lambda_3 = \Delta_3 + X_3(Y_3 + 1)$. Then (X_3, Λ_3) is another basis of the said maximal ideal, and we have

$$\psi_3 = \Lambda_3^2 + X_3^2\Lambda_3 + X_3^3(Y_3 + 1) + X_3^4Y_3^2 + X_3^4Y_3^4 g(X_3, X_3^2Y_3).$$

The initial form of ψ_3 with respect to the basis (X_3, Λ_3) is Λ_3^2 and by applying the QDT: $X_3 = X_4$, $\Lambda_3 = X_4\Lambda_4$, centered at P_3, we get

$$\psi_3 = X_4^2\psi_4 \quad \text{where} \quad \psi_4 = \Lambda_4^2 + X_4\Lambda_4 + X_4(Y_3+1) + X_4^2Y_3^2 + X_4^2Y_3^4 g(X_4, X_4^2Y_3).$$

The factor X_4^2 is the contribution of the exceptional line, and the proper transform of D_3 is given by $D_4 : \psi_4 = 0$. There is a unique point P_4 (which is not rational over GF(2)) on D_4 corresponding to P_3, and (X_4, Λ_4) is a basis of the maximal ideal in the local ring of P_4. Since $Y_3 + 1$ does not belong to the said maximal ideal, we see that ψ_4 belongs to it but not to its square. Therefore D_4 has a simple point at P_4, and hence D is analytically irreducible at P.

4. Linearization

By slightly modifying the proof of (1.5) of [Ab6], let us prove the following:

Linearization Lemma (4.1). *Let $F = f_{24}(Y) + X$. Then there exist elements $A_0, A_1, \ldots, A_{12}$ in $k[X]$ with $A_0 \neq 0$ and $A_{12} = 1$ such that $\sum_{i=0}^{12} A_i Y^{2^i} = HF$ for some $H \in k[X, Y]$.*

Now

$$F = Y^{24} + Y^8 + Y^6 + Y + X$$

and by adding $F + Y^{24}$ to both sides of this we get

$$(J'_{24}) \qquad Y^{24} = Y^8 + Y^6 + Y + X + F.$$

Let $P \equiv Q$ mean $P - Q = HF$ for some $H \in k[X][Y]$. Then multiplying (J'_{24}) by Y^{i-24} for $i = 24, 26, 28, 32, 36$ we get:

$$(J_{24}) \qquad Y^{24} \equiv Y^8 + Y^6 + Y + X,$$

$$(J_{26}) \qquad Y^{26} \equiv Y^{10} + Y^8 + Y^3 + XY^2,$$

$$(J_{28}) \qquad Y^{28} \equiv Y^{12} + Y^{10} + Y^5 + XY^4,$$

$$(J'_{32}) \qquad Y^{32} \equiv Y^{16} + Y^{14} + Y^9 + XY^8,$$

$$(J_{36}) \qquad Y^{36} \equiv Y^{20} + Y^{18} + Y^{13} + XY^{12}.$$

From (J'_{32}) we get

$$(J_{32}) \qquad Y^{32} + Y^{16} + XY^8 \equiv Y^{14} + Y^9.$$

Squaring (J_{32}) we get

$$Y^{64} + Y^{32} + X^2Y^{16} \equiv Y^{28} + Y^{18},$$

and using (J_{28}) we obtain

$$(J_{64}) \qquad Y^{64} + Y^{32} + X^2Y^{16} + XY^4 \equiv Y^{18} + Y^{12} + Y^{10} + Y^5.$$

Likewise, by squaring (J_{64}) and then using (J_{24}) and (J_{36}) we obtain

$$(J_{128}) \qquad Y^{128} + Y^{64} + X^4Y^{32} + (X+1)^2Y^8 + Y \equiv Y^{18} + Y^{13} + XY^{12} + Y^{10} + Y^6 + X.$$

Again, by squaring (J_{128}) and then using (J_{24}), (J_{26}), and (J_{36}), we obtain

$$\begin{aligned}(J'_{256}) \qquad & Y^{256} + Y^{128} + X^8Y^{64} + (X+1)^4Y^{16} \\ & + (X+1)^2Y^8 + (X+1)Y^2 + X^2Y \\ & \equiv Y^{18} + Y^{13} + (X+1)Y^{12} + Y^{10} + X^2Y^6 + Y^3 + X^3 + X^2.\end{aligned}$$

Now adding (J_{128}) to (J'_{256}) we obtain

$$\begin{aligned}(J_{256}) \qquad & Y^{256} + (X+1)^8Y^{64} + X^4Y^{32} + (X+1)^4Y^{16} + (X+1)Y^2 + (X+1)^2Y \\ & \equiv Y^{12} + (X+1)^2Y^6 + Y^3 + X^3 + X^2 + X.\end{aligned}$$

Again, by squaring (J_{256}) and then using (J_{24}) we obtain

$$\begin{aligned}(J_{512}) \qquad & Y^{512} + (X+1)^{16}Y^{128} + X^8Y^{64} + (X+1)^8Y^{32} \\ & + Y^8 + (X+1)^2Y^4 + (X+1)^4Y^2 + Y \\ & \equiv (X+1)^4Y^{12} + X^6 + X^4 + X^2 + X.\end{aligned}$$

Likewise, by squaring (J_{512}) and then using (J_{24}) we obtain

$$\begin{aligned}(J_{1024}) \qquad & Y^{1024} + (X+1)^{32}Y^{256} + X^{16}Y^{128} + (X+1)^{16}Y^{64} \\ & + Y^{16} + X^4(X+1)^4Y^8 + (X+1)^8Y^4 + Y^2 + (X+1)^8Y \\ & \equiv (X+1)^8Y^6 + X^{12} + X^9 + X^8 + X^4 + X^2 + X.\end{aligned}$$

By squaring (J_{1024}) we obtain

$$\begin{aligned}(J'_{2048}) \qquad & Y^{2048} + (X+1)^{64}Y^{512} + X^{32}Y^{256} + (X+1)^{32}Y^{128} \\ & + Y^{32} + X^8(X+1)^8Y^{16} + (X+1)^{16}Y^8 + Y^4 + (X+1)^{16}Y^2 \\ & \equiv (X+1)^{16}Y^{12} + X^{24} + X^{18} + X^{16} + X^8 + X^4 + X^2.\end{aligned}$$

By adding $(X+1)^{12}$ times (J_{512}) to (J'_{2048}) we obtain

$$\begin{aligned}(J_{2048}) \qquad & Y^{2048} + [(X+1)^{64} + (X+1)^{12}]Y^{512} + X^{32}Y^{256} \\ & + [(X+1)^{32} + (X+1)^{28}]Y^{128} + X^8(X+1)^{12}Y^{64} \\ & + [(X+1)^{20} + 1]Y^{32} + X^8(X+1)^8Y^{16} \\ & + [(X+1)^{16} + (X+1)^{12}]Y^8 + [(X+1)^{14} + 1]Y^4 + (X+1)^{12}Y \\ & \equiv X^{24} + X^{13} + X^{12} + X^9 + X^5 + X.\end{aligned}$$

Finally, by multiplying the above equation by its right hand side $X^{24}+X^{13}+X^{12}+X^9+X^5+X$ and then adding the resulting equation to the square of the above equation we get

$$\begin{aligned}
&Y^{4096}+(X^{24}+X^{13}+X^{12}+X^9+X^5+X)Y^{2048}\\
&\quad+(X^{128}+X^{24}+X^{16}+X^8)Y^{1024}\\
&\quad+(X^{88}+X^{77}+X^{76}+X^{73}+X^{69}+X^{65}+X^{64}+X^{36}+X^{32}+X^{28}\\
&\qquad+X^{25}+X^{24}+X^{20}+X^{17}+X^{16}+X^{13}+X^5)Y^{512}\\
&\quad+(X^{64}+X^{48}+X^{45}+X^{44}+X^{41}+X^{40}+X^{37}\\
&\qquad+X^{33}+X^{32}+X^{24}+X^{16}+X^8)Y^{256}\\
&\quad+(X^{56}+X^{52}+X^{48}+X^{45}+X^{40}+X^{37}+X^{32}+X^{20}+X^{13}+X^5)Y^{128}\\
&\quad+(X^{44}+X^{36}+X^{33}+X^{32}+X^{28}+X^{25}+X^{24}+X^{20}+X^{17}+X^9+X^8)Y^{64}\\
&\quad+X^{44}+X^{40}+X^{33}+X^{13}+X^9+X^5)Y^{32}\\
&\quad+(X^{40}+X^{29}+X^{28}+X^{25}+X^{24}+X^{20}+X^{16}+X^{13}+X^9+X^8)Y^{16}\\
&\quad+(X^{40}+X^{36}+X^{32}+X^{29}+X^{28}+X^{21}+X^{13}+X^{12}+X^8+X^5+X^4)Y^8\\
&\quad+(X^{38}+X^{36}+X^{34}+X^{32}+X^{30}+X^{28}+X^{27}+X^{25}+X^{24}+X^{22}+X^{20}\\
&\qquad+X^{19}+X^{18}+X^{17}+X^{16}+X^{14}+X^{13}+X^{11}+X^5+X^3)Y^4\\
&\quad+X^{24}+X^{16}+X^8+1)Y^2\\
&\quad+(X^{36}+X^{32}+X^{28}+X^{25}+X^{20}+X^{17}+X^{16}+X^{12}+X^9+X)Y\\
&\quad\equiv 0,
\end{aligned}$$

and this proves (4.1).

5. Auxiliary lemmas

We shall now prove two auxiliary lemmas needed in the proof of Theorems (1.1) to (1.4).

Lemma (5.1). *There is no field* Γ *with* $k(f_{24}(Y))\subset\Gamma\subset k(Y)$ *such that* $[k(Y):\Gamma]=2$.

Suppose, if possible, that there is such a field Γ. Then by Lüroth's theorem (see (2.6) of [AEH]) we have $\Gamma=k(T)$ for some $T=Y^2+aY+b$ with $a,b\in k$, and we can write $f_{24}(Y)=T^{12}+\alpha T^{11}+\beta T^{10}+\gamma T^9+\cdots$ with $\alpha,\beta,\gamma,\cdots\in k$. By substituting the first equation into the second we get:

$$\begin{aligned}
&Y^{24}+Y^8+Y^6+Y\\
&\quad=[Y^{24}+a^4Y^{20}+(a^8+b^4)Y^{16}+\cdots]+\alpha[Y^{22}+aY^{21}+\cdots]\\
&\qquad+\beta[Y^{20}+a^2Y^{18}+b^2Y^{16}+\cdots]+\gamma[Y^{18}+aY^{17}+bY^{16}+\cdots].
\end{aligned}$$

Since αY^{22} is the only term of Y-degree 22, we must have $\alpha=0$, and now by simplifying the above equation we get:

$$Y^{24}+Y^8+Y^6+Y=Y^{24}+(a^4+\beta)Y^{20}+(a^2\beta+\gamma)Y^{18}+a\gamma Y^{17}+\cdots.$$

Comparing coefficients we get $\beta=a^4$, $\gamma=a^2\beta=a^6$, $a\gamma=a^7=0$, and hence we must have $a=0$. Therefore $T\in k[Y^2]$ and hence $f_{24}(Y)\in k[Y^2]$ which is a contradiction.

Lemma (5.2). *Let H and $\overline{H}$ be normal subgroups of a finite group G such that $H \cap \overline{H} = 1$, and G/H is isomorphic to $G/\overline{H}$. Assume that for some prime number π, the order of G is nondivisible by π^2 and the order of every nonidentity normal subgroup of G/H is divisible by π. Then $H = \overline{H} = 1$.*

Namely, the subgroup $H\overline{H}$ of G is isomorphic to the direct product $[(H\overline{H})/H]\times[(H\overline{H})/\overline{H}]$. Therefore either the order of $(H\overline{H})/H$ is nondivisible by π or the order of $(H\overline{H})/\overline{H}$ is nondivisible by π. By symmetry we may assume that the order of $(H\overline{H})/H$ is nondivisible by π. Now $(H\overline{H})/H$ is isomorphic to a normal subgroup of G/H and hence we must have $(H\overline{H})/H = 1$. Consequently $\overline{H} \subset H$ and hence $\overline{H} = 1$. Since G/H is isomorphic to $G/\overline{H}$, we get $H = 1$.

6. Mathieu groups

To prove Theorems (1.1) to (1.4), let K_{12}, $\overline{K}_{12}$, K'_{11}, J_{12}, and K_{24} be the respective splitting fields of $f_{12}(Y) + X$, $f_{12}(Y) + X + 1$, $f'_{11}(X, Y)$, $f_{12}(Y)+f_{12}(X)+1$, and $f_{24}(Y)+X$ over $l(X)$ in a fixed algebraic closure Ω of $k(X)$ where we have put $l = \mathrm{GF}(2)$. Note that then $K_{12}(k)$, $\overline{K}_{12}(k)$, $K'_{11}(k)$, $J_{12}(k)$, and $K_{24}(k)$ are the respective splitting fields of $f_{12}(Y)+X$, $f_{12}(Y)+X+1$, $f'_{11}(X, Y)$, $f_{12}(Y)+f_{12}(X)+1$, and $f_{24}(Y)+X$ over $k(X)$ in Ω, and obviously $G(\overline{K}_{12}(k), k(X)) \approx G(K_{12}(k), k(X))$ where $\approx$ stands for isomorphism, and the Galois group of any Galois extension K/K_0 is denoted by $G(K, K_0)$. What we want to prove is that $G(K_{12}(k), k(X)) = M_{12}$, $G(K'_{11}(k), k(X)) = M_{11}$, $G(J_{12}(k), k(X)) = M_{11}(12)$, and $G(K_{24}(k), k(X)) = \mathrm{Aut}(M_{12})$ where we regard the Galois groups as permutation groups on the roots of the corresponding polynomials.

In view of the relation between "twisted derivatives" and one-point stabilizers discussed in [Ab5], by (2.1) we see that $G(K_{12}, l(X))$ is a doubly transitive permutation group of degree 12, $G(K'_{11}, l(X))$ is the one-point stabilizer of $G(K_{12}, l(X))$, and the order of the said one-point stabilizer is divisible by 8. Therefore by CTT and Special CDT on pages 86 to 89 of [Ab5] (or alternatively by [Mil]), we have $G(K_{12}, l(X)) = M_{12}$ or A_{12} or S_{12}. It also follows that: $G(K'_{11}, l(X)) = M_{11} \Leftrightarrow G(K_{12}, l(X)) = M_{12}$.

We can take a root y of $f_{24}(Y)+X$ in Ω, and then upon letting $X^* = f_{12}(y)$ we have $X^{*2} + X^* + X = f_{24}(y) + X = 0$. It follows that $l(X) \subset l(X^*) \subset K_{24}$, and $l(X^*)/l(X)$ is a Galois extension with Galois group $\mathbb{Z}_2$ (= the cyclic group of order 2). Also $X \mapsto X^*$ gives an isomorphism of $l(X)$ onto $l(X^*)$, and upon letting K^*_{12} and $\overline{K}^*_{12}$ to be the respective splitting fields of $f_{12}(Y) + X^*$ and $f_{12}(Y) + X^* + 1$ over $l(X^*)$ in Ω we have $G(K^*_{12}, l(X^*)) \approx G(K_{12}, l(X)) \approx G(\overline{K}_{12}, l(X)) \approx G(\overline{K}^*_{12}, l(X^*))$. Since $X^{*2} + X^* + X = 0$, we get $f_{24}(Y) + X = (f_{12}(Y) + X^*)(f_{12}(Y) + X^* + 1)$. Therefore K_{24} is the compositum of K^*_{12} and $\overline{K}^*_{12}$, and $G(K_{24}, K^*_{12})$ and $G(K_{24}, \overline{K}^*_{12})$ are normal subgroups of $G(K_{24}, l(X^*))$ with $G(K_{24}, K^*_{12}) \cap G(K_{24}, \overline{K}^*_{12}) = 1$ and

$$G(K_{24}, l(X^*))/G(K_{24}, K^*_{12}) \approx G(K^*_{12}, l(X^*)) \approx G(\overline{K}^*_{12}, l(X^*)) \approx G(K_{24}, l(X^*))/G(K_{24}, \overline{K}^*_{12}).$$

Clearly $|G(K_{24}, l(X^*))|$ divides $|G(K_{24}, l(X))|$ and, in view of the Basic Projection Principle on page 94 of [Ab5] and (5.1) of [AY1], by (4.1), $G(K_{24}, l(X))$

is a homomorphic image of a subgroup of GL(12, 2) and hence $|G(K_{24}, l(X^*))|$ divides $|\mathrm{GL}(12, 2)|$. As a factorization of $|\mathrm{GL}(12, 2)|$ into powers of prime numbers we have

$$|\mathrm{GL}(12, 2)| = \prod_{i=0}^{11}(2^{12}-2^i) = 2^{66}\times 3^8\times 5^3\times 7^4\times 11\times 13\times 17\times 23\times 31^2\times 73\times 89\times 127$$

and hence $|G(K_{24}, l(X^*))| \not\equiv 0 \pmod{11^2}$. Now the groups M_{12}, A_{12}, S_{12} have the property that the order of any nonidentity normal subgroup is divisible by 11 (the nonidentity normal subgroups are: M_{12} in the first case, A_{12} in the second case, and A_{12} and S_{12} in the third case). Consequently by taking $G(K_{24}, K_{12}^*)$, $G(K_{24}, \overline{K}_{12}^*)$, $G(K_{24}, l(X^*))$, and 11 for $H, \overline{H}, G$, and π in (5.2) we see that $G(K_{24}, K_{12}^*) = G(K_{24}, \overline{K}_{12}^*) = 1$, and hence $K_{24} = K_{12}^* = \overline{K}_{12}^*$.

Thus K_{24} is the common splitting field of $f_{12}(Y) + X^*$ as well as $f_{12}(Y) + X^* + 1$ over $l(X^*)$ in Ω, and as a permutation group on the roots of either polynomial we have $G(K_{24}, l(X^*)) = M_{12}$ or A_{12} or S_{12}. We can take $x \in K_{24}$ with $f_{12}(x)+X^* = 0$ and then $l(X^*, x) = l(x)$ and $f_{12}(Y)+X^*+1 = f_{12}(Y)+f_{12}(x)+1$. Therefore by (3.1) we see that $f_{12}(Y)+X^*+1$ remains irreducible in $l(x)[Y]$, and hence $G(K_{24}, l(x))$ is a transitive subgroup of $G(K_{24}, l(X^*))$ when we view the latter as a permutation group on the roots of $f_{12}(Y)+X^*+1$. Since $l(x)$ is a root field of $f_{12}(Y) + X^*$ over $l(X^*)$ in K_{24}, the index of $G(K_{24}, l(x))$ in $G(K_{24}, l(X^*))$ is 12. Neither A_{12} nor S_{12} has a transitive subgroup of index 12 (see (2.19) on page 300 and Exercise 8 on page 308 of [Suz]), and hence we must have $G(K_{24}, l(X^*)) = M_{12}$ and $G(K_{24}, l(x)) = M_{11}(12)$. It follows that $G(K_{12}, l(X)) = M_{12}$, $G(K'_{11}, l(X)) = M_{11}$, and $G(J_{12}, l(X)) = M_{11}(12)$.

Let k_0 and k_1 be the algebraic closures of l and k in Ω respectively. Since M_{11} and M_{12} are nonabelian finite simple groups, by Corollary (1.8) of the Refined Extension Principle on page 97 of [Ab5] we see that the groups $G(K_{24}, l(X^*))$, $G(K_{12}, l(X))$, $G(K'_{11}, l(X))$, $G(J_{12}, l(X))$ coincide with the groups $G(K_{24}(k_0), k_0(X^*))$, $G(K_{12}(k_0), k_0(X))$, $G(K'_{11}(k_0), k_0(X))$, $G(J_{12}(k_0), k_0(X))$ respectively, and by (2.10) of [AY1] we see that these groups relative to k_0 coincide with their respective versions relative to k_1, and by the Basic Extension Principle on page 93 of [Ab5] we see that the said versions relative to k_1 are subgroups of the respective versions relative to k which themselves are subgroups of the respective original versions over l. Thus we get $G(K_{24}(k), k(X^*)) = M_{12}$, $G(K_{12}(k), k(X)) = M_{12}$, $G(K'_{11}(k), k(X)) = M_{11}$, $G(J_{12}(k), k(X)) = M_{11}(12)$.

Now $k(X^*)/k(X)$ and $K_{24}(k)/k(X^*)$ are Galois extensions with Galois groups $\mathbb{Z}_2$ and M_{12} respectively, and $K_{24}(k)/k(X)$ is a Galois extension whose Galois group is a group extension of $G(K_{24}(k), k(X^*))$ by $G(k(X^*), k(X))$. Since M_{12} is centerless and $\mathrm{Out}(M_{12}) = \mathrm{Aut}(M_{12})/M_{12} = \mathbb{Z}_2$, by the Extension Lemma (as stated and proved in [Ab9]) it follows that there are exactly two nonisomorphic extensions of M_{12} by $\mathbb{Z}_2$. Obviously $M_{12}\times\mathbb{Z}_2$ and $\mathrm{Aut}(M_{12})$ are two such extensions. Therefore, $G(K_{24}(k), k(X)) = M_{12}\times\mathbb{Z}_2$ or $\mathrm{Aut}(M_{12})$.

Suppose, if possible, that $G(K_{24}(k), k(X)) = M_{12}\times\mathbb{Z}_2$ and let $\mu : G(K_{24}(k), k(X)) \to M_{12}$ and $\nu : G(K_{24}(k), k(X)) \to \mathbb{Z}_2$ be the corresponding projections. Since $G(K_{24}(k), k(X^*))$ is a nonabelian simple subgroup of

$G(K_{24}(k), k(X))$, we must have

$$\nu(G(K_{24}(k), k(X^*))) = 1.$$

Since $G(K_{24}(k), k(y))$ is a subgroup of $G(K_{24}(k), k(X^*))$, we get

$$\nu(G(K_{24}(k), k(y))) = 1.$$

Therefore $G(K_{24}(k), k(y))$ is an index 2 subgroup of $\mu^{-1}(\mu(G(K_{24}(k), k(y))))$. Hence for the fixed field Γ of $\mu^{-1}(\mu(G(K_{24}(k), k(y))))$ we have $k(f_{24}(y)) = k(X) \subset \Gamma \subset k(y)$ with $[k(y) : \Gamma] = 2$ which contradicts (5.1). Consequently we must have $G(K_{24}(k), k(X)) = \mathrm{Aut}(M_{12})$.

References

[Ab1] S. S. Abhyankar, *Coverings of algebraic curves*, Amer. J. Math. **79** (1957), 825–856.

[Ab2] ———, *Resolution of singularities of embedded algebraic surfaces*, Academic Press, New York, 1966.

[Ab3] ———, *Desingularization of plane curves*, Proc. Sympos. Pure Math., vol. 40, Amer. Math. Soc., Providence, RI, 1983, 267–271.

[Ab4] ———, *Algebraic geometry for scientists and engineers*, Amer. Math. Soc., Providence, RI, 1990.

[Ab5] ———, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. (N.S.) **27** (1992), 68–133.

[Ab6] ———, *Mathieu group coverings in characteristic two*, C. R. Acad. Sci. Paris Sér. I Math. **316** (1993), 267–271.

[Ab7] ———, *Alternating group coverings of the affine line in characteristic greater than two*, Math. Ann. **296** (1993), 63–68.

[Ab8] ———, *Fundamental group of the affine line in positive characteristic*, Proceedings of the 1992 Bombay International Colloquium on Geometry and Analysis held at the Tata Institute of Fundamental Research (to appear).

[Ab9] ———, *Wreath product and enlargements of groups*, Discrete Math. **120** (1993), 1–12.

[AEH] S. S. Abhyankar, P. Eakin, and W. Heinzer, *On the uniqueness of the coefficient ring in a polynomial ring*, J. Algebra **23** (1972), 310–342.

[AOS] S. S. Abhyankar, J. Ou, and A. Sathaye, *Alternating group coverings of the affine line in characteristic two*, Discrete Math. (to appear).

[AY1] S. S. Abhyankar and I. Yie, *Small degree coverings of the affine line in characteristic two*, Discrete Math. (to appear).

[AY2] ———, *Some more Mathieu group coverings of the affine line in characteristic two*, Proc. Amer. Math. Soc. **122** (1994), 1007–1014.

[HuB] B. Huppert and N. Blackburn, *Finite groups* III, Springer-Verlag, New York, 1983.

[Mat] E. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former, et sur les substitutions qui les laissent invariables*, J. Math Pures Appl. **18** (1861), 241–323.

[Mil] G. A. Miller, *List of transitive substitution groups of degree twelve*, Quart. J. Pure Appl. Math. **28** (1896), 193–231.

[Suz] M. Suzuki, *Group theory.* I, Springer-Verlag, New York, 1982.

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907
E-mail address: ram@cs.purdue.edu
E-mail address: yie@math.purdue.edu