Small degree coverings of the affine line in characteristic two

Shreeram S. Abhyankar*, Ikkwon Yie

Mathematics Department, Purdue University, West Lafayette, IN 47907, USA

Received 15 December 1992

Abstract

Unramified coverings of the affine line in characteristic two are constructed having alternating groups of degree six and seven as Galois groups. Some other small degree unramified coverings of the affine line in characteristic two are also considered.

1. Introduction

Let $L_k$ be the affine line over an algebraically closed field $k$ of characteristic $p > 0$, and let $\pi_A(L_k)$ be the algebraic fundamental group of $L_k$, i.e., $\pi_A(L_k)$ is the set of finite Galois groups of unramified coverings of $L_k$. In [2] it was observed that every member of $\pi_A(L_k)$ is a quasi $p$-group, i.e., a finite group which is generated by all its $p$-Sylow subgroups, and it was conjectured that conversely $\pi_A(L_k)$ contains all quasi $p$-groups, and hence in particular $\pi_A(L_k)$ contains the alternating group $A_n$ for all $n \geq p$ in case of $p > 2$, and for all $n \not\equiv 3, 4$ in case of $p = 2$. In [3] this was proved to be so for $n \geq p > 2$, and the case of $n \not\equiv 3, 4, 6, 7$ and $p = 2$ was taken care of in [4] and [5]. In this paper we finish off the matter by writing down explicit equations giving unramified coverings of the affine line over a field of characteristic 2 having $A_6$ and $A_7$ as Galois groups. In other words we shall prove the following result.

Main Result. For $p = 2$, the alternating groups $A_6$ and $A_7$ belong to $\pi_A(L_k)$. (See Theorem (2.11) and (2.12).)

As in [3–5], here also it turns out that some of the equations found in [2] suffice. However, as in [5], to show that the said equations do the job we need to use

* Corresponding author.

1 Partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-92-H-3035.
Jacobson's Criterion. Unlike the more classical criterion which does not work for characteristic 2, Jacobson's Criterion [7, Section 4.8, Exercise 33] for deciding when the Galois group of an equation is contained in the alternating group, works for every characteristic; for various versions of Jacobson’s Criterion see [5].

Namely, by taking \( p = 2 = h = t - 1 \) and \( c_1 = c_2 = 1 \) in Proposition 1 of [2] we get the unramified covering \( F^o = 0 \) of \( L_k \) for \( p = 2 \) where the circle polynomial is given by

\[
F^o = Y^7 + XY^4 + Y^2 + 1
\]

and by using Jacobson's Criterion we shall show that

\[
\text{Gal}(F^o, k(X)) = A_7. \tag{1.1}
\]

By throwing away a root of \( F^o \) and modifying things suitably we get the primed circle polynomial

\[
F'^o = Y^6 + X^{27}Y^5 + X^{54}Y^4 + (X^{18} + X^{36})Y^3 + X^{108}Y^2 + (X^{90} + X^{135})Y + X^{162}
\]

and by invoking Abhyankar's lemma we shall show that, for \( p = 2 \), the equation \( F'^o = 0 \) gives an unramified covering of \( L_k \) with

\[
\text{Gal}(F'^o, k(X)) = A_6. \tag{1.2}
\]

In Section 2, as a direct consequence of Jacobson's Criterion, we shall prove Proposition 2.8 claiming that, for \( p = 2 \) but without assuming \( k \) to be algebraically closed, we have: \( \text{Gal}(F^o, k(X)) \subseteq A_7 \Leftrightarrow GF(4) \subseteq \text{GF}(2^p) \), where as usual, for any prime power \( q \), by \( \text{GF}(q) \) we denote the finite field of cardinality \( q \). From Proposition 2.8 we shall swiftly, deduce Theorem 2.11 about the Galois group of \( F^o \), which in turn will yield Theorem 2.11 about the Galois group of \( F'^o \). In Section 3 we shall give an alternative proof of Proposition 2.8 which still uses Jacobson's Criterion, but replaces some numerical lemmas and discriminant calculations by factorizations of certain polynomials over \( \text{GF}(2^j) \) for various values of \( j \). In Section 4 we shall give another alternative proof of Proposition 2.8 by using the resultant criterion of [5] which was itself deduced from Jacobson's Criterion.

Two of the equations used in [3–5] giving unramified coverings of \( L_k \) are \( \bar{F}_{n, q, s, a} = 0 \) and \( \bar{F}_{n, t, s, a} = 0 \) where

\[
\bar{F}_{n, q, s, a} = Y^n - aX^sY^t + 1 \quad \text{with } q = n - t = a \text{ positive power of } p
\]

and

\[
\bar{F}_{n, t, s, a} = Y^n - aY^t + X^s \quad \text{with } n = 0(p) \text{ and } s = 0(t)
\]

and where, for both the equations, \( a \) is a nonzero element in the algebraically closed field \( k \) of characteristic \( p \) and \( n, t, s \) are positive integers with \( t < n \) and \( \text{GCD}(n, t) = 1 \). In the said papers, for various values of \( n \) and \( t \) it was shown that the corresponding Galois group (over \( k(X) \)) is \( A_n \). This suggests that for \( p = 2 \) we check if the Galois
group of $\tilde{F}_{7,2,s,a}$ or $\tilde{F}_{7,4,s,a}$ is $A_7$, and if the Galois group of $\tilde{F}_{6,1,s,a}$ or $\tilde{F}_{6,5,s,a}$ is $A_6$; actually, in [3] it was shown that

$$\text{Gal}(\tilde{F}_{7,2,s,a}, k(X)) = S_7$$

(1.3)

and Serre has sent us a proof (e-mail of October 1991), which we shall reproduce in Section 5, showing that

$$\text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) = PSL(3, 2)$$

(1.4)

and, finally, in Section 6 we shall show that

$$\text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = \text{Gal}(\tilde{F}_{6,5,s,a}, k(X)) = PSL(2, 5).$$

(1.5)

By throwing away a root of $\tilde{F}_{n,1,s,a}$ and deforming things suitably we get the monic polynomial $\tilde{F}_{n,1,s,a}$ of degree $n-1$ in $Y$ with coefficients in $k(X)$ given by

$$\tilde{F}_{n,1,s,a} = Y^{n-1}[(Y+1)^n-1] - aX^{-s}Y^{n-1}[(Y+1)^f-1].$$

In Section 6, we shall show for $p = 2$ we have

$$\text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = ASL(1, 5)$$

(1.6)

where we observe that

$$\tilde{F}_{6,1,s,a} = Y^5 + Y^3 + Y - aX^{-s} \text{ with } s \equiv 0(5).$$

Notation. Note that as usual $S_n$ is the symmetric group of degree $n$. Also note that $PGL(m, q) = GL(m, q)/(\text{scalar matrices})$ and $PSL(m, q) = SL(m, q)/(\text{scalar matrices})$, where $GL(m, q)$ is the group of all nonsingular $m$ by $m$ matrices with entries in $GF(q)$ and $SL(m, q)$ is the group of those members of $GL(m, q)$ whose determinant is 1. Moreover note that $PSL(2, 5)$ and $A_5$ are isomorphic as abstract groups but not as permutation groups, and likewise $PGL(2, 5)$ and $S_5$ are isomorphic as abstract groups but not as permutation groups. Finally note that $AGL(1, q)$ is the group of all transformations $x \mapsto \lambda x + \mu$ with $0 \neq \lambda \in GF(q)$ and $\mu \in GF(q)$ and $ASL(1, q)$ is a certain subgroup of $AGL(1, q)$ of index 1 or 2 depending on whether $q$ is even or odd; the easiest way to describe $ASL(1, q)$ is to realize that $AGL(1, q)$ is the one-point stabilizer of $PGL(2, q)$ and then define $ASL(1, q)$ to be the one-point stabilizer of $PSL(2, q)$; observe that $ASL(1, 5)$ is also called the dihedral group of degree 5.

2. The circle polynomial

To turn to Jacobson's Criterion, let

$$f = f(Y) = Y^n + \sum_{i=1}^{n} b_i Y^{n-i}$$
be a monic polynomial of degree \( n > 1 \) in \( Y \) with coefficients \( b = (b_1, b_2, \ldots, b_n) \) in a field \( K \), and let \( r = (r_1, r_2, \ldots, r_n) \) be the roots of \( f \) in some overfield of \( K \).

Consider the polynomials \( D(R), D^*(R), \Delta(R) \) in indeterminates \( R = (R_1, R_2, \ldots, R_n) \) with coefficients in \( \mathbb{Z} \) given by

\[
D(R) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} R_{\sigma(i)}^{-1}
\]

and

\[
D^*(R) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} R_{\sigma(i)}^{1}
\]

and

\[
\Delta(R) = \prod_{1 \leq i < j \leq n} (R_j - R_i).
\]

Let \( B = (B_1, B_2, \ldots, B_n) \) be indeterminates and, for \( 1 \leq i \leq n \), let us assign weight \( i \) to \( B_i \). Let \( C(R) = (C_1(R), C_2(R), \ldots, C_n(R)) \) where for \( 1 \leq i \leq n \), we have put \( C_i(R) = (-1)^i \) times the \( i \)th elementary symmetric function of \( R \), i.e.,

\[
Y^n + \sum_{i=1}^{n} C_i(R) Y^{n-i} = \prod_{i=1}^{n} (Y - R_i).
\]

Now \( D(R) + D^*(R), D(R)D^*(R), \Delta^2(R) \) are symmetric homogeneous polynomials of degrees \( n(n-1)/2, n(n-1), n(n-1) \) in \( R \) with coefficients in \( \mathbb{Z} \) and hence there exist unique isobaric polynomials \( U(B), V(B), W(B) \), of weights \( n(n-1)/2, n(n-1), n(n-1) \) in \( B \) with coefficients in \( \mathbb{Z} \) such that

\[
U(C(R)) = D(R) + D^*(R) \quad \text{and} \quad V(C(R)) = D(R)D^*(R) \quad \text{and} \quad W(C(R)) = \Delta^2(R).
\]

Now by (2.7) of [5] we have

\[
U^2(B) = 4V(B) + W(B).
\]

By (2.9)–(2.11) of [5] we also have

\[
U(b) = D(r) + D^*(r) \quad \text{and} \quad V(b) = D(r)D^*(r) \quad \text{and} \quad W(b) = (-1)^{n(n-1)/2} \text{Disc}_Y(f)
\]

where \( \text{Disc}_Y(f) \) is the \( Y \)-discriminant of \( f \). We put

\[
J(f) = Z^2 - U(b)Z + V(b)
\]

and we call this Jacobson's quadratic of \( f \). By (2.12) of [5] we have the following.

**Jacobson's Criterion 2.1.** If \( f \) has no multiple roots then: \( \text{Gal}(f, K) \subset A_n \) iff \( J(f) \) has a root in \( K \).

We shall now prove some lemmas about the polynomials \( U(B), V(B), W(B) \).

**Lemma 2.2.** None of the polynomials \( U(B), V(B), W(B) \), has a term independent of \( B_{n-1} \) and \( B_n \), i.e., they are all reduced to zero by putting \( B_{n-1} = B_n = 0 \).

**Proof.** Take \( b_i = B_i \) or \( b_i = 0 \) according as \( i < n-1 \) or \( i \geq n - 1 \). Then 0 is a multiple root of \( f \) and hence \( D(r) = 0 = D^*(r) \) and therefore \( U(b) = V(b) = W(b) = 0. \)
Lemma 2.3. Given any positive integer $d < n$ with $\text{GCD}(n, d) = 1$, let $e = n - d$ and let $\widetilde{W}(B_d, B_n)$ be the polynomial in $B_d$ and $B_n$ with coefficients in $\mathbb{Z}$ obtained by putting zero for the remaining variables in $W(B)$. Then

$$\widetilde{W}(B_d, B_n) = (-1)^n (n-1)^2 n^e B_n + (-1)^{(n+2)(n-1)/2} d^e B_n^{-1} B_d^e.$$  

Proof. Apply the discriminant calculation of Section 19 of [3] to $Y^n + B_d Y + B_n$. \qed

Lemma 2.4. Given any positive integer $d < n$ with $d \geq (n-1)/2$ and $\text{GCD}(n, d) = 1$, let $e = n - d$ and let $\widetilde{U}(B_d, B_n)$, and $\widetilde{V}(B_d, B_n)$, be the polynomials in $B_d$ and $B_n$ with coefficients in $\mathbb{Z}$ obtained by putting zero for the remaining variables in $U(B)$ and $V(B)$ respectively. Then

$$\widetilde{U}(B_d, B_n) = \begin{cases} u B_n^{(n-1)/2} & \text{with } u \in \mathbb{Z} \backslash 2\mathbb{Z} \text{ if } n \neq 0(2), \\ u' B_n^{(n-1)/2} B_d & \text{with } u' \in \mathbb{Z} \backslash 2\mathbb{Z} \text{ if } n \equiv 0(2) \end{cases}$$

and

$$\widetilde{V}(B_d, B_n) = v B_n^{e-1} + v' B_n^{-1} B_d^e \text{ with } v, v' \in \mathbb{Z}$$

where

$$v = \begin{cases} (1/4) \left[ u^2 - (-1)^n (n-1)/2 n^e \right] \in 2\mathbb{Z} & \text{if } n \equiv 1(8), \\ (1/4) \left[ u^2 - (-1)^n (n-1)/2 n^e \right] \in 2\mathbb{Z} & \text{if } n \equiv 7(8), \\ (1/4) \left[ u^2 - (-1)^n (n-1)/2 n^e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 3(8), \\ (1/4) \left[ u^2 - (-1)^n (n-1)/2 n^e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 5(8), \\ (1/4) \left[ u^2 - (-1)^n (n-1)/2 n^e \right] \in 2\mathbb{Z} & \text{if } 2 < n \equiv 0(2), \\ (1/4) \left[ u^2 - (-1)^n (n-1)/2 n^e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 2. \end{cases}$$

and

$$v' = \begin{cases} (1/4) \left[ (-1)^{(n+2)(n-1)/2} d^e e \right] \in 2\mathbb{Z} & \text{if } n \equiv 0(2) \text{ and } 2 < d \equiv 0(2), \\ (1/4) \left[ (-1)^{(n+2)(n-1)/2} d^e e \right] \in 2\mathbb{Z} & \text{if } n \equiv 0(2) \text{ and } 2 < e \equiv 0(2), \\ (1/4) \left[ (-1)^{(n+2)(n-1)/2} d^e e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 0(2) \text{ and } d \equiv 2, \\ (1/4) \left[ (-1)^{(n+2)(n-1)/2} d^e e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 0(2) \text{ and } e \equiv 2 \end{cases}$$

and

$$v'' = \begin{cases} (1/4) \left[ u'^2 - (-1)^{(n+2)(n-1)/2} d^e e \right] \in 2\mathbb{Z} & \text{if } n \equiv 0(8), \\ (1/4) \left[ u'^2 - (-1)^{(n+2)(n-1)/2} d^e e \right] \in 2\mathbb{Z} & \text{if } n \equiv 2(8) \text{ and } e = d(8), \\ (1/4) \left[ u'^2 - (-1)^{(n+2)(n-1)/2} d^e e \right] \in 2\mathbb{Z} & \text{if } n \equiv 6(8) \text{ and } e \equiv d(8), \\ (1/4) \left[ u'^2 - (-1)^{(n+2)(n-1)/2} d^e e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 2(8) \text{ and } e \neq d(8), \\ (1/4) \left[ u'^2 - (-1)^{(n+2)(n-1)/2} d^e e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 6(8) \text{ and } e \neq d(8), \\ (1/4) \left[ u'^2 - (-1)^{(n+2)(n-1)/2} d^e e \right] \in \mathbb{Z} \backslash 2\mathbb{Z} & \text{if } n \equiv 4(8). \end{cases}$$
Proof. Clearly $B_n^{-1}$, $B_n^{-2} B_d$, $B_n^{-2} B_d^2$ are the only monomials of weight $n(n-1)$ in $B_n$ and $B_d$ (where the last monomial $B_n^{-d} B_d^2$ is included iff $n-1-2d=0$), and hence $B_n^{(n-1)/2}$, $B_n^{(e-1)/2} B_d^2$, $B_n^{(e-1)-2d}/2$ are the only possible monomials of weight $n(n-1)/2$ in $B_n$ and $B_d$. Therefore, since $U(B)$ and $V(B)$ are isobaric of weight $n(n-1)/2$ and $n(n-1)$ respectively, by Lemma 2.2 we conclude that

$$\bar{U}(B_d, B_n) = \begin{cases} u B_n^{(e-1)/2} & \text{with } u \in \mathbb{Z} \quad \text{if } n \not\equiv 0(2), \\ u' B_n^{(e-1)/2} B_d^{n/2} & \text{with } u' \in \mathbb{Z} \quad \text{if } n \equiv 0(2) \end{cases}$$

and

$$\bar{V}(B_d, B_n) = \nu B_n^{(e-1)/2} B_d^{n/2} \nu' \quad \text{with } \nu, \nu' \in \mathbb{Z}$$

and hence in view of (2.1) and Lemma 2.3 we get

$$n = \begin{cases} (1/4)[u^2-(-1)^{(n-1)/2} n^2] \in \mathbb{Z} & \text{if } n \not\equiv 0(2), \\ (1/4)[(-1)^{(n-1)/2} n^2] \in \mathbb{Z} & \text{if } 2 < n \equiv 0(2), \\ (1/4)[(-1)^{(n-1)/2} n^2] \in \mathbb{Z} \setminus 2\mathbb{Z} & \text{if } n = 2 \end{cases}$$

and we get the first displayed portion of the description of $\nu'$ together with the fact that

$$\nu' = (1/4)[u'^2-(-1)^{(n+2(n-1)/2} d^2 e^*] \in \mathbb{Z} \quad \text{if } n \equiv 0(2).$$

Now an integer is odd iff its square is odd, and hence by what we have said so far we get the asserted description of $\bar{U}(B_d, B_n)$. For any odd integer $w$ we have $w = 1 + 2w^*$ for some integer $w^*$ and this gives $w^2 = 1 + 4w^*(w^* + 1)$ and hence $w^2 \equiv 1(8)$ because $w^*(w^* + 1)$ is always even; therefore by what we have said so far we get the asserted description of $v$ and the second portion of the asserted description of $v'$. $\square$

Lemma 2.5. For $Y^7 + B_3 Y^4 + B_5 Y^2 + B_7 \in \mathbb{Z}[B_3, B_5, B_7][Y]$ we have

$$\text{Disc}_Y(Y^7 + B_3 Y^4 + B_5 Y^2 + B_7) = 2^8 3^3 B_7^2 B_7^3 - 2^7 3^3 B_5 B_5^2 B_7^2 + 2^4 3^3 B_5^2 B_7^2$$

$$- 2^4 3^2 7^2 B_3 B_5 B_7 + 2^2 5^2 7^2 (11) B_3 B_5 B_7^2$$

$$- 2^2 5^4 7^2 B_3 B_5 B_7^2 + 2^2 5^5 B_3 B_7 + 7^2 B_7^5.$$

Proof. Now

$$\text{Disc}_Y(Y^7 + B_3 Y^4 + B_5 Y^2 + B_7)$$

$$= \text{Res}_Y(Y^7 + B_3 Y^4 + B_5 Y^2 + B_7, 7 Y^6 + 4 B_3 Y^3 + 2 B_5 Y)$$

$$= 7^{-6} \text{Res}_Y(7 Y^7 + 7 B_3 Y^4 + 7 B_5 Y^2 + 7 B_7, 7 Y^6 + 4 B_3 Y^3 + 2 B_5 Y)$$

$$= 7^{-3} \text{Res}_Y(3 B_3 Y^4 + 5 B_5 Y^2 + 7 B_7, 7 Y^6 + 4 B_3 Y^3 + 2 B_5 Y)$$

$$= 7^{-2} B_7 \text{Res}_Y(3 B_3 Y^4 + 5 B_5 Y^2 + 7 B_7, 7 Y^5 + 4 B_3 Y^2 + 2 B_5)$$

$$= 7^{-2} 3^{-4} B_7^2 \text{Res}_Y(3 B_3 Y^4 + 5 B_5 Y^2 + 7 B_7, 21 B_3 Y^5 + 12 B_3^2 Y^2 + 6 B_3 B_5)$$

$$= 7^{-2} 3^{-2} B_3 B_7 \text{Res}_Y(M, N)$$
where
\[ M = 3B_3 Y^4 + 5B_5 Y^2 + 7B_7 \]
and
\[ N = -35B_3 Y^3 + 12B_5 Y^2 - 49B_7 Y + 6B_3 B_5 \]
and clearly
\[ (35B_5)^2 M + (105B_3 B_5 Y + 36B_3) N = P Y^2 + P' Y + P^* \]
with
\[ P = 5^{372} B_3 - 315^{173} B_3 B_5 B_7 + 2^{433} B_3 \]
and
\[ P' = 2^{135} 71 B_3 B_5 B_7 - 2^{372} 71 B_3 B_7 \]
and
\[ P^* = 5^{272} B_5 B_7 + 2^{333} B_5 B_7 \]
and obviously
\[ P^2 N + (35B_3 P Y - 12B_5 P - 35B_3 P')(PY^2 + P' Y + P^*) = Q Y + Q' \]
with
\[ Q = -49B_7 P^2 - 12B_5 P P' + 35B_3 P P^* - 35B_5 P^2 \]
and
\[ Q' = 6B_3 B_5 P^2 - 12B_5 P P^* - 35B_5 P' P^* \]
and clearly
\[ Q^2 (PY^2 + P' Y + P^*) + (-PQ Y + PQ' - P'Q)(Q Y + Q') = R \]
where
\[ R = PQ^2 - P' QQ' + P^* Q^2. \]
It follows that \( \text{Res}_v(M, N) = (35B_5)^{-4} P^{-2} R \) and by substituting the values of \( Q \) and \( Q' \) in the above expression of \( R \) we get
\[ R = P [P^2 (6B_3 B_5 P - 12B_5 P*)^2 - 70P (6B_3 B_5^2 PP^* P - 12B_5^2 B_5 P P^* P^*)]
+ (35B_3 P P^* P^*)^2] + Q [P^* Q - P' Q'] \]
\[ = P^2 (36B_3^2 D_3^2) + P^4 (-144B_5^3 B_5 P*) + P^3 (144B_5^3 P^* P - 420B_3 B_5^2 P P^*)
+ P^2 (840B_3^2 B_5 P P^* P^*) + P (35B_5 P P^*)^2
+ Q [P^2 (-49B_7 P^* - 6B_3 B_5 P') + P (35B_5 P^* P)] \]
\[ P^5(36B_3^2B_2^3) + P^4(-144B_3^3B_4P^*) + P^3(144B_3^2P^*2 - 420B_3B_5P'P^*) + P^2(840B_3^2B_5P^*2) + P(35B_5P^*P^2) \]

\[ + P^4\left[(-49B_7)(-49B_7P^* - 6B_3B_5P')\right] + P^3\left[(-49B_7)(35B_5P^*2) + (-12B_3P^* + 35B_5P^*)(-49B_7P^* - 6B_3B_5P')\right] + P^2\left[(-12B_3P^* + 35B_5P^*)(35B_5P^*2) + (-35B_5P^*2)(-49B_7P^* - 6B_3B_5P')\right] + P\left[(-35B_5P^*2)(35B_5P^*2)\right]. \]

Consequently \( R_3(M, N) = (35B_5)^{-4}(R_3 + R_2 + R_1 + R_0) \) where 

\[ R_3 = P^3(2^33^2B_2^3B_2^3) \]

and 

\[ R_2 = P^2(-2^43^3B_3^3B_3P^* + 7^4B_4B_4P^* + 2^13^17^2B_4B_4B_7P') \]

and 

\[ R_1 = P(2^43^2B_3^2P^*2 - 2^15^17^2B_3B_3P^*2 - 2^23^15^17^1B_3B_3P'P^* + 2^33^2B_3B_3B_3P^2) \]

and 

\[ R_0 = 3^27^2B_4^2P^*3 + 2^23^15^17^1B_3B_2^2P^*2 + 5^17^3B_3B_2^2P^* + 2^13^15^17^1B_3B_2^2P^* \]

and now by substituting the values of \( P, P', P^* \) in the above expressions of \( R_3, R_2, R_1, R_0 \) we get 

\[ R_3 = [2^13^9B_3^15 - 2^83^85^17^3B_3^1B_3B_3 + 2^83^75^17^7B_3^1B_3^2 + 2^43^65^77^6B_3^1B_3^3] \]

\[ - 2^53^55^57^5B_3^3B_3^4 + 2^43^45^67^4B_3^2B_3^4 - 3^35^37^3B_3^2B_3^4 \]

\[ + 3^35^37^3B_3^2B_3^4 \]

\[ = 2^13^43^11B_3^3B_3^2B_3^3 - 2^103^105^17^3B_3^3B_3^4B_3^4 + 2^103^95^97^3B_3^2B_3^3 + 2^63^65^27^6B_3^3B_3^4 \]

\[ - 2^73^75^77^7B_3^2B_3^4 + 2^63^65^67^6B_3^3B_3^4 - 2^23^55^57^7B_3^3B_3^4B_3^4 + 2^23^35^57^8B_3^4B_3^3 \]

\[ - 2^23^45^77^7B_3^3B_3^2B_3^4 + 2^23^35^37^9B_3^4B_3^3B_3^4 \]

and 

\[ R_2 = [2^83^6B_3^10 - 2^53^45^17^3B_3^3B_3B_7 + 2^53^35^37^2B_3^3B_3^3 + 3^25^27^6B_3^3B_3^3B_3^3] \]

\[ - 2^13^15^57^5B_3^3B_3^4 + 2^53^45^74B_3^3B_3^3B_3^3 \]

\[ + 2^33^37^3B_3^2B_3^3B_3^3B_3^3 + 2^53^27^6B_3^3B_3^3B_3^3B_3^3 \]

\[ + 2^13^15^47^5B_3^3B_3^4B_3^3 + 5^67^4B_3^3B_3^3B_3^3 \]

\[ - 2^73^75^7B_3^3B_3^4B_3^3B_3^3 + 2^23^55^57^7B_3^3B_3^4B_3^3B_3^3 + 3^25^27^6B_3^3B_3^3B_3^3B_3^3 \]

\[ - 2^13^15^47^5B_3^3B_3^4B_3^3B_3^3 + 5^67^4B_3^3B_3^3B_3^3 \]
\[
-215311B_1^7 B_2^3 - 210385273B_3^3 B_4^3 B_7 - 212385372B_3^3 B_2^3
+ 28365277 B_2^3 B_3^3 + 28365277 B_3^3 B_4^3 B_7 - 27335475(11)B_3^3 B_6^3 B_7
- 2733574 B_3^3 B_5^3 - 253453710B_5^3 B_2^4
+ 2333579(149) B_3^3 B_4^3 B_7 + 2333578(17) B_3^3 B_2^3 B_4^3
+ 2333579(149) B_3^3 B_4^3 B_7 + 3254713 B_3^3 B_2^3 - 213356712B_3 B_6^3 B_7^3 + 58711B_3 B_7^3.
\]

and
\[
R_1 = [433 B_3^3 - 315173 B_3 B_7 + 5^3 B_3^3][(21038 B_2^3 B_3^3 + 28365273 B_3^3 B_2^3 B_7
+ 28365273 B_2^3 B_3^3 B_7) + (-27335475 B_3^3 B_4^3 B_7 - 253453710 B_5^3 B_2^4)
- 2133574 B_3^3 B_5^3 B_7 + 2333578(17) B_3^3 B_4^3 B_7 + 2333579(149) B_3^3 B_4^3 B_7]
\]

\[
R_0 = [29395272 B_2^3 B_5^3 - 26375479 B_5^3 B_2^3 B_7 + 23345677 B_4^3 B_2^3 B_7 + 58711 B_3 B_7^3]
+ (-210395173 B_3 B_4^3 B_7 + 29395272 B_5^3 B_2^3 B_7 + 28365376 B_2^3 B_4^3 B_7
+ 27375177 B_1^0 B_3 B_5^3 + 27375276 B_5^3 B_2^3 B_7 + 25375375 B_2^3 B_5^3 B_2^3 + 23345579 B_3 B_2^3 B_7
+ 2333578(17) B_3 B_4^3 B_7 - 213356712 B_3 B_6^3 B_7^3 + 214511 B_3 B_7^3]
\]

\[
-215311B_1^7 B_2^3 - 210385273B_3^3 B_4^3 B_7 - 212385372B_3^3 B_2^3
+ 28365277 B_2^3 B_3^3 + 28365277 B_3^3 B_4^3 B_7 - 27335475(11)B_3^3 B_6^3 B_7
- 2733574 B_3^3 B_5^3 - 253453710B_5^3 B_2^4
+ 2333579(149) B_3^3 B_4^3 B_7 + 2333578(17) B_3^3 B_2^3 B_4^3
+ 2333579(149) B_3^3 B_4^3 B_7 + 3254713 B_3^3 B_2^3 - 213356712B_3 B_6^3 B_7^3 + 58711B_3 B_7^3.
\]
By adding the above four displays we get
\[ R_3 + R_2 + R_1 + R_0 = 28355476 B_3 B_5 B_7 - 27355476 B_2 B_5 B_7 + 24355476 B_2 B_5 B_7 - 243454710 B_2 B_5 B_7 + 22325878(11) B_2 B_5 B_7 + 22325976 B_2 B_5 B_7 + 3254713 B_2 B_5 B_7. \]
and now the desired formula for the discriminant follows by dividing the above RHS by \( 3^2 5^7 6 B_3 B_5 B_7 \). □

**Lemma 2.6.** Assume that \( n = 7 \) and let \( \hat{W}(B_3, B_5, B_7) \) be the polynomial in \( B_3, B_5, B_7 \) with coefficients in \( \mathbb{Z} \) obtained by putting \( B_1 = B_2 = B_4 = B_6 = 0 \) in \( W(B) \). Then
\[ \hat{W}(B_3, B_5, B_7) = -2833 B_3 B_5 B_7 + 2733 B_3 B_5 B_7 - 2433 B_3 B_5 B_7 + 243274 B_3 B_5 B_7 - 225273(11) B_3 B_5 B_7 + 225472 B_3 B_5 B_7 - 2255 B_3 B_5 B_7 - 77 B_3 B_5 B_7. \]

**Proof.** Follows by multiplying the formula of Lemma 2.5 by \((-1)^{7(7-1)/2} = -1\). □

**Lemma 2.7.** Assume that \( n = 7 \) and let \( \hat{U}(B_3, B_5, B_7) \) and \( \hat{V}(B_3, B_5, B_7) \) be the polynomials in \( B_3, B_5, B_7 \) with coefficients in \( \mathbb{Z} \) obtained by putting \( B_1 = B_2 = B_4 = B_6 = 0 \) in \( U(B) \) and \( V(B) \) respectively. Then
\[ \hat{U}(B_3, B_5, B_7) = (1 + 2u_{001}) B_3^3 + 2u'_{311} B_3 B_5 B_7 \]
and
\[ \hat{V}(B_3, B_5, B_7) = [(1 + 2v_{001}) B_3^3 B_5 B_7 + (1 + 2v_{0152}) B_3 B_5^4 B_7 + (1 + 2v_{233}) B_3^3 B_5^3 B_7] + [2v_{006} B_3^2 B_7 + 2v_{0541} B_3 B_5^3 B_7 + 2v_{0703} B_3^3 B_5 B_7] + [v'_{314} B_3 B_5^2 B_7 + v_{622} B_3^2 B_5 B_7] \]
where \( u_{003}, u_{311}, v_{071}, v_{152}, v_{233}, v_{006}, v_{0541}, v_{0703}, v'_{314}, v_{622} \) are elements of \( \mathbb{Z} \) such that
\[ u'_{311} = 0(2) \iff v'_{314} = 0(2) \iff v_{622} = 0(2). \]

**Proof.** Now \( \hat{V}(B_3, B_5, B_7) \) and \( \hat{U}(B_3, B_5, B_7) \) are isobaric of weights \((7(7-1))/2\) in \( B_3, B_5, B_7 \) and in the notation of Lemma 2.4 we have \( \hat{V}(0, B_3, B_7) = \hat{V}(B_3, B_7), \hat{V}(B_3, 0, B_7) = \hat{V}(B_3, B_7), \hat{U}(0, B_3, B_7) = \hat{U}(B_3, B_7), \hat{U}(B_3, 0, B_7) = \hat{U}(B_3, B_7), \) and clearly
\[ B_3 B_2 B_5^2, B_3 B_2 B_7, B_3 B_2 B_5 B_7, B_3 B_5^2 B_7, B_3 B_5 B_7, B_3 B_5 B_7, B_3 B_2 B_7. \]
are exactly all the monomials of weight \(7(7-1)=42\) in \(B_3, B_4, B_7\) in which all the three variables occur with positive exponents, and hence \(B_3^2 B_4 B_7\) is the only such monomial of weight \(7(7-1)/2=21\). Therefore our assertions follow from (2.1), Lemmas 2.4 and 2.6.

**Proposition 2.8.** Consider the polynomial \(F_1^* = Y^7 + XY^4 + Y^2 + 1\) in \(k(X)[Y]\) where \(k\) is a field of characteristic 2 which need not be algebraically closed. Then: \(\text{Gal}(F_1^*, k(X)) \subset A_7 \Leftrightarrow GF(4) \subset k\).

**Proof.** By Lemma 2.7 for Jacobson's quadratic \(J(F_1^*)\) of \(F_1^*\) we have \(J(F_1^*) = Z^2 + Z + 1 + X + X^2\) or \(Z^2 + Z + 1 + X + X^2 + X^3 + X^6\), and hence our assertion immediately follows from the Jacobson's Criterion 2.1. 

**Lemma 2.9.** Let \(k_1\) be an overfield of an algebraically closed field \(k_0\), and let \(F\) be a monic polynomial of positive degree in \(Y\) with coefficients in \(k_0(X)\) having no multiple roots. Then \(\text{Gal}(F, k_1(X)) = \text{Gal}(F, k_0(X))\).

**Proof.** Clearly \(\text{Gal}(F, k_1(X)) \subset \text{Gal}(F, k_0(X))\) and hence it suffices to show that \(|\text{Gal}(F, k_1(X))| = |\text{Gal}(F, k_0(X))|\). Upon letting \(m = |\text{Gal}(F, k_0(X))|\), we can find a monic irreducible polynomial \(H\) of degree \(m\) in \(Y\) with coefficient in \(k_0[X]\) such that the splitting field of \(F\) over \(k_0(X)\) is obtained by adjoining a root of \(H\). It follows that the splitting field of \(F\) over \(k_1(X)\) is obtained by adjoining a root of \(H\) to \(k_1(X)\). Therefore it suffices to show that \(H\) is irreducible in \(k_1[X, Y]\). This however follows from the obvious fact that the irreducibility of \(H\) in \(k_1[X, Y]\) (resp: in \(k_0[X, Y]\)) is equivalent to its irreducibility in \(k_1[X, Y]\) (resp: in \(k_0[X, Y]\)), and the fact (see [9, Theorem 39, page 230]) that: if \(\Phi\) is a nonconstant irreducible polynomial in a finite number of indeterminates \(Z_1, Z_2, \ldots, Z_N\) with coefficients in \(k_0\) such that the quotient field of \(k_0[Z_1, Z_2, \ldots, Z_N]/\Phi\) is separably generated over \(k_0\) then \(\Phi\) remains irreducible in \(k_1[Z_1, Z_2, \ldots, Z_N]\). 

**Theorem 2.10.** Let \(k\) be a field of characteristic 2 which need not be algebraically closed and consider the polynomial

\[F_1^* = Y^7 + XY^4 + Y^2 + 1 \in k(X)[Y].\]

Then \(F_1^* = 0\) gives an unramified covering of \(L_k\). Moreover: \(\text{Gal}(F_1^*, k(X)) = A_7 \Leftrightarrow GF(4) \subset k\), and \(\text{Gal}(F_1^*, k_1(X)) = S_7 \Leftrightarrow GF(4) \not\subset k\).

**Proof.** Clearly \(\text{Discr}(F_1^*) = 1\) and hence \(F_1^* = 0\) gives an unramified covering of \(L_k\). After putting \(X = 0\) in \(F_1^*\) we get the factorization \(Y^7 + Y^2 + 1 = (Y^2 + Y + 1)(Y^5 + Y^4 + Y^2 + Y + 1)\) into irreducible factors in \(GF(2)[Y]\). Therefore by the Residue Cycle Lemma of [4] we see that \(\text{Gal}(F_1^*, GF(2)(X))\) contains a transposition. Since \(F_1^*\) is irreducible of prime degree, by (8.3) of [8] we also see that \(\text{Gal}(F_1^*, GF(2)(X))\) is primitive. Consequently by (13.3) of [8] we conclude that
$\text{Gal}(F^\circ, GF(2)(X)) = S_7$. Therefore, in view of Proposition 2.8, by Corollary (1.1) of the Refined Extension Principle of Section 19 of [3] we have $\text{Gal}(F^\circ, k'_1(X)) = A_7$ for every finite algebraic field extension $k'$ of GF(4). From this it follows that $\text{Gal}(F^\circ, k^*(X)) = A_7$ for the algebraic closure $k^*$ of GF(2). Hence by Lemma 2.9 we get $\text{Gal}(F^\circ, \bar{k}(X)) = A_7$ for the algebraic closure $\bar{k}$ of $k$. Since $\text{Gal}(F^\circ, \bar{k}(X)) \subset \text{Gal}(F^\circ, k(X)) \subset S_6$, we must have $\text{Gal}(F^\circ, k(X)) = A_6$ or $S_6$. From this our assertions follow by Proposition 2.8. 

**Theorem 2.11.** Let $k$ be a field of characteristic 2 which need not be algebraically closed and consider the polynomial

$$F^\circ = Y^6 + X^{27}Y^5 + X^{54}Y^4 + (X^{18} + X^{36})Y^3 + X^{108}Y^2 + (X^{90} + X^{135})Y + X^{162}$$

in $k(X)[Y]$. Then $F^\circ = 0$ gives an unramified covering of $L_3$, and: $\text{Gal}(F^\circ, k(X)) = A_6$ or $S_6$. Moreover: if $GF(4) \subset k$ then $\text{Gal}(F^\circ, k(X)) = A_6$.

**Proof.** With $F^\circ$ as in Theorem 2.10, by solving the equation $F^\circ = 0$ we get $X \equiv [Y^7 + Y^2 + 1]/Y^4$ and hence $k(X, Y) = k(Y)$, i.e., $k(Y)$ is a root field of $F^\circ$ over $k(X)$. By throwing away the root $Y$ of $F^\circ$ we get

$$(1/Z)[(Z + Y)^7 + X(Z + Y)^4 + (Z + Y)^2 + 1 - (Y^7 + XY^4 + Y^2 + 1)]$$

$$= Z^6 + YZ^5 + Y^2Z^4 + (X + Y^3)Z^3 + Y^4Z^2 + (1 + Y^3)Z + Y^6$$

and by substituting $X \equiv [Y^7 + Y^2 + 1]/Y^4$ in the RHS we get

$$Z^6 + YZ^5 + Y^2Z^4 + [(1 + Y^2)/Y^4]Z^3 + Y^4Z^2 + (1 + Y^3)Z + Y^6$$

and writing $Z = Z'/Y^2$ and multiplying throughout by $Y^{12}$ we obtain

$$Z'^6 + Y^3Z'^5 + Y^6Z'^4 + (Y^2 + Y^4)Z'^3 + Y^{12}Z'^2 + (Y^{10} + Y^{15})Z' + Y^{18}$$

and finally by writing $(X, Y)$ for $(Y, Z')$ we get $F^*$ where

$$F^* = Y^6 + X^3Y^3 + X^6Y^3 + (X^2 + X^4)Y^3 + X^{12}Y^2 + (X^{10} + X^{15})Y + X^{18}.$$
where Ω is the meromorphic series field in \( X^{-1} \) with coefficients in \( k^* \). Since \( \text{Gal}(F^\circ, \Omega) \subset \text{Gal}(F^\circ, k^*(X)) \subset A_4 \), and \( \text{Gal}(F_3, \Omega) = \text{a cyclic group of order 3} \), we must have \( \text{Gal}(F_4, \Omega) \subset A_4 \). Consequently, again by Section 2 of [1], we see that the reduced ramification of any extension of the valuation \( X = \infty \) to the splitting field of \( F^\circ \) over \( k^*(X) \) is 12 or 36. Therefore by Abhyankar’s Lemma, \( X = \infty \) is the only valuation of \( k^*(X)/k \) which is ramified in a root field of \( F^\circ \) over \( k^*(X) \). Since \( k^* \) is separable algebraic over \( \text{GF}(2) \), it follows that \( X = \infty \) is the only valuation of \( \text{GF}(2)(X)/\text{GF}(2) \) which is ramified in a root field of \( F^\circ \) over \( \text{GF}(2)(X) \). Therefore \( X = \infty \) is the only valuation of \( k(X)/k \) which is ramified in a root field of \( F^\circ \) over \( k(X) \). Thus \( F^\circ = 0 \) gives an unramified extension of \( L_4 \).

**Remark 2.12.** The above Theorems 2.10 and 2.11 complete the proof of our Main Result.

**Problem 2.13.** Let the situation be as in Theorem 2.11. By the above proof it is conceivable that \( F^\circ_1 = 0 \) gives an unramified covering of \( L_4 \) where \( F^\circ_1 \) is obtained by substituting \( X^{1/3} \) for \( X \) in \( F^\circ \); decide if this is so or not. By the above proof it follows that: \( \text{Gal}(F^\circ_1, k(X)) = A_6 \) or \( S_6 \), and: if \( \text{GF}(4) \not\subset k \) then \( \text{Gal}(F^\circ_1, k(X)) = A_6 \). Apply Jacobson’s Criterion to decide for which fields \( k \) with \( \text{GF}(4) \not\subset k \) we have \( \text{Gal}(F^\circ_1, k(X)) = A_6 \), and for which fields \( k \) with \( \text{GF}(4) \subset k \) we have \( \text{Gal}(F^\circ_1, k(X)) = A_6 \).

3. Alternative proof of Proposition 2.8 by factorization

In Section 2 we proved Proposition 2.8 by using Lemma 2.4 together with discriminant calculation. In this section we shall give an alternative proof of 2.8 by factoring polynomials over Galois fields. Note that Corollaries 3.2, 3.4, 3.5, Lemmas 3.1, and 3.3 constitute a characteristic 2 weaker version of Lemma 2.4, whereas Lemma 3.6 is a characteristic 2 weaker version of Lemma 2.7. We shall use the notation of the beginning part of Section 2 ending at Lemma 2.2. Moreover, by \( U'(B), V'(B) \) we shall denote the members of \( \text{GF}(2)[B] \) obtained by reducing the coefficients of \( U(B), V(B) \) mod 2, and by \( \tilde{U}'(B_n), \tilde{V}'(B_n) \), we shall denote the members of \( \text{GF}(2)[B_n] \) obtained by putting zero for the remaining variables in \( U'(B), V'(B) \), and, for any positive integer \( d < n \), by \( \tilde{U}'(B_d, B_n), \tilde{V}'(B_d, B_n) \) we shall denote the members of \( \text{GF}(2)[B_d, B_n] \) obtained by putting zero for the remaining variables in \( U'(B), V'(B) \), and finally, for any positive integers \( d < d < n \), by \( \tilde{U}'(B_d, B_d, B_n), \tilde{V}'(B_d, B_d, B_n) \), we shall denote the members of \( \text{GF}(2)[B_d, B_d, B_n] \) obtained by putting zero for the remaining variables in \( U'(B), V'(B) \). Note that then for any monic polynomial \( f = Y^n + b_1 Y^{n-1} + \cdots + b_n \) with coefficients \( b = (b_1, \ldots, b_n) \) in a field of characteristic 2, by (2.1) and the displayed line immediately following it, we have \( \text{Disc}_r(f) = U'^2(b) \).
Lemma 3.1. Let \( f_n = Y^n + 1 \in \text{GF}(2)[Y] \) and \( g_n = \text{Gal}(f_n, \text{GF}(2)) \). Then

\[
\tilde{V}(B_n) = \begin{cases} 
0 & \text{if } n \text{ is odd and } g_n \subset A_n, \\
B_n^{-1} & \text{if } n \text{ is odd and } g_n \notin A_n.
\end{cases}
\]

Proof. Assume that \( n \) is odd. Then \( \tilde{U}^2(1) = \text{Disc}_Y(f_n) = 1 \) and hence \( J(f_n) = Z^2 + Z + \tilde{V}(1) \) and therefore by Jacobson Criterion 2.1 we see that: \( \tilde{V}(1) = 0 \) or 1 according as \( g_n \subset A_n \) or not. By weight consideration, the only possible term of \( \tilde{V}(B_n) \) is \( B_n^{-1} \). Therefore \( \tilde{V}(B_n) = 0 \) or \( B_n^{-1} \) according as \( g_n \subset A_n \) or not.

Corollary 3.2. If \( n = 7 \) then \( \tilde{V}(B_7) = 0 \).

Proof. Clearly \( f_7 = Y^7 + 1 = (Y+1)(Y^3 + Y + 1)(Y^3 + Y^2 + 1) \) where the factors are irreducible over \( \text{GF}(2) \) and hence \( g_7 \subset A_7 \). Therefore our assertion follows from Lemma 3.1.

Lemma 3.3. Given any positive integer \( d < n \) with \( d \geq (n-1)/2 \) and \( \text{GCD}(n, d) = 1 \), let \( f_{n,d} = Y^n + Y^{n-d} + 1 \in \text{GF}(2)[Y] \) and \( g_{n,d} = \text{Gal}(f_{n,d}, \text{GF}(2)) \). Then

\[
\tilde{V}(B_d, B_n) = \begin{cases} 
0 & \text{if } \tilde{V}(B_n) = 0 \text{ and } g_{n,d} \subset A_n, \\
B_d^n B_n^{-d-1} & \text{if } \tilde{V}(B_n) = 0 \text{ and } g_{n,d} \notin A_n, \\
B_d^n B_n^{-d-1} + B_n^{-1} & \text{if } \tilde{V}(B_n) \neq 0 \text{ and } g_{n,d} \subset A_n, \\
B_n^{-1} & \text{if } \tilde{V}(B_n) \neq 0 \text{ and } g_{n,d} \notin A_n.
\end{cases}
\]

Proof. Now \( \tilde{U}^2(1, 1) = \text{Disc}_Y(f_{n,d}) = 1 \) and hence \( J(f_{n,d}) = Z^2 + Z + \tilde{V}(1, 1) \) and therefore by Jacobson’s Criterion 2.1 we see that: \( \tilde{V}(1, 1) = 0 \) or 1 according as \( g_{n,d} \subset A_n \) or not. By weight consideration, \( B_d^n B_n^{-d-1} \) and \( B_n^{-1} \) are the only possible terms of \( \tilde{V}(B_d, B_n) \), and hence \( \tilde{V}(B_d, B_n) = \tilde{V}(B_n) + wB_d^n B_n^{-d-1} \) with \( w \in \text{GF}(2) \). This yields our assertion.

Corollary 3.4. If \( n = 7 \) and \( d = 3 \) then \( \tilde{V}(B_3, B_7) = 0 \).

Proof. Clearly \( f_{n,d} \) is irreducible over \( \text{GF}(2) \) and hence \( g_{n,d} \subset A_7 \). Therefore our assertion follows from Lemma 3.3.

Corollary 3.5. If \( n = 7 \) and \( d = 5 \) then \( \tilde{V}(B_5, B_7) = B_7^5 \).

Proof. Clearly \( f_{n,d} = (Y^2 + Y + 1)(Y^4 + Y^4 + Y^2 + Y + 1) \) where the factors are irreducible over \( \text{GF}(2) \) and hence \( g_{n,d} \notin A_7 \). Therefore our assertion follows from Lemma 3.3.

Lemma 3.6. Assume \( n = 7 \). Then

\[
\tilde{U}^2(B_3, B_5, B_7) = B_7^5.
\]
Table 1

<table>
<thead>
<tr>
<th>(k' )</th>
<th>( \text{GF}(2) )</th>
<th>( \text{GF}(4) )</th>
<th>( \text{GF}(4) )</th>
<th>( \text{GF}(4) )</th>
<th>( \text{GF}(8) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{Gal}(F,k') )</td>
<td>( \not\in A_7 )</td>
<td>( \in A_7 )</td>
<td>( \not\in A_7 )</td>
<td>( \in A_7 )</td>
<td>( \not\in A_7 )</td>
</tr>
<tr>
<td>( \tilde{U}'(B_3,B_5,B_7) )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>( b+1 )</td>
</tr>
<tr>
<td>( \tilde{V}'(B_3,B_5,B_7) )</td>
<td>1</td>
<td>0 or 1</td>
<td>( a ) or ( a+1 )</td>
<td>0 or 1</td>
<td>( b+\gamma )</td>
</tr>
<tr>
<td>( B_3^2 B_5 )</td>
<td>1</td>
<td>( x )</td>
<td>( x+1 )</td>
<td>( x )</td>
<td>( \beta )</td>
</tr>
<tr>
<td>( B_3^3 B_5^2 B_7 )</td>
<td>1</td>
<td>( x+1 )</td>
<td>( x+1 )</td>
<td>1</td>
<td>( \beta^2 )</td>
</tr>
<tr>
<td>( B_3^2 B_5^2 B_7 )</td>
<td>1</td>
<td>( x )</td>
<td>( x )</td>
<td>1</td>
<td>( \beta )</td>
</tr>
<tr>
<td>( B_3^2 B_5^3 B_7 )</td>
<td>1</td>
<td>( x+1 )</td>
<td>( x )</td>
<td>( x+1 )</td>
<td>( \beta^2 )</td>
</tr>
<tr>
<td>( B_3^2 B_5 B_7 )</td>
<td>1</td>
<td>( x )</td>
<td>( x+1 )</td>
<td>( x )</td>
<td>( \beta^3+\beta )</td>
</tr>
<tr>
<td>( B_3^3 B_5 B_7 )</td>
<td>1</td>
<td>( x )</td>
<td>1</td>
<td>( \beta )</td>
<td></td>
</tr>
</tbody>
</table>

Table 2

<table>
<thead>
<tr>
<th>( \text{GF}(2) )</th>
<th>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</th>
<th>( \text{GF}(4) )</th>
<th>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</th>
<th>( \text{GF}(4) )</th>
<th>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{GF}(4) )</td>
<td>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</td>
<td>( \text{GF}(4) )</td>
<td>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</td>
<td>( \text{GF}(4) )</td>
<td>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</td>
</tr>
<tr>
<td>( \text{GF}(8) )</td>
<td>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</td>
<td>( \text{GF}(8) )</td>
<td>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</td>
<td>( \text{GF}(8) )</td>
<td>( Y^7+Y^4+Y^2+1=(Y+1)(Y^6+Y^5+Y^4+Y+1) )</td>
</tr>
</tbody>
</table>

and

\[ \tilde{V}'(B_3,B_5,B_7) = B_3^2 B_5 + B_3 B_5^2 B_7 + v(B_3^3 B_5 + B_3 B_5^3 B_7) \]

with \( v \in \text{GF}(2) \).

**Proof.** Let \( F = Y^7+B_3 Y^4+B_5 Y^2+B_7 \). Then \( \tilde{U}'(B_3,B_5,B_7) = \text{Disc}_F(F) \) and hence the first assertion follows by noting that clearly \( \text{Disc}_F(F) = B_3^7 \). In view of Lemma 2.2, Corollaries 3.2 and 3.4, by weight consideration, \( B_3^2 B_5 \), \( B_3^0 B_5 B_7 \), \( B_3^2 B_5^2 B_7 \), \( B_3^3 B_5 B_7 \), \( B_3^3 B_5^2 B_7 \) and \( B_3^2 B_5^3 B_7 \) are the only possible terms of \( \tilde{V}'(B_3,B_5,B_7) \), and by Corollary 3.5 we know that \( B_3^2 B_7 \) is a term of \( \tilde{V}'(B_3,B_5,B_7) \). Now we shall refer to the Tables 1 and 2 where \( \text{GF}(4) = \text{GF}(2)(a) \) and \( \text{GF}(8) = \text{GF}(2)(\beta) \) with \( a^2+1=0 \) and \( b^3+b+1=0 \), and where in the fifth row of Table 1 we have \( \gamma \in \{0,1,\beta,\beta+1\} \).

To explain the tables, first we substitute the values from the first row of Table 1 in \( F \) and factor it over the field \( k' \) given in the second row of Table 1, and we record the result in Table 2, where vertical columns have become horizontal rows for the sake of printing. Also we record the values of the relevant terms after this substitution in the last 5 rows of Table 1. Now we can tell whether \( \text{Gal}(F,k') \subseteq A_7 \) or not by looking at the degrees of the factors and we record this in the third row of Table 1. In the fourth row of Table 1, we record the values of \( \tilde{U}'(B_3,B_5,B_7) = B_3^2 \). Now consider \( J(F) = Z_5 + \tilde{U}'(B_3,B_5,B_7)Z + \tilde{V}'(B_3,B_5,B_7) \). In view of Jacobson's Criterion 2.1,
by looking at the third and the fourth rows of Table 1, we can decide what are
the possible values for \( \hat{W}(B_3, B_5, B_7) \) and we record them in the fifth row of
Table 1.

From now on we shall only refer to the last 8 rows of Table 1. Note that
\( \hat{W}(B_3, B_5, B_7) \) is a sum of monomials including \( B_3 B_5 B_7 \), which are among the monomials listed under it. We shall examine columns 2 to 6, one by one, where the results obtained from earlier columns will affect the result of the next column. Looking at the
2nd column, we see that \( \hat{W}(B_3, B_5, B_7) \) is the sum of an odd number of monomials. Now looking at the 3rd column, we see that \( B_3 B_5 B_7 \) occurs. Looking at the 4th column, we see that \( B_3 B_5 B_7 \) is not a term of \( \hat{W}(B_3, B_5, B_7) \). Now, looking at the 5th column, we see that precisely one of \( B_3 B_5 B_7 \) or \( B_3 B_5 B_7 \) occurs and that both or none of \( B_3 B_5 B_7 \) and \( B_3 B_5 B_7 \) occur. Finally, looking at the 6th column, we conclude that
\( B_3 B_5 B_7 \) does not occur.

Remark 3.7. In Lemma 3.1 we did not consider the case when \( n \) is even which
was included in Lemma 2.4. Here is a combinatorial proof of that case which says that: for
\( n \) even, but different from 2, we have \( \hat{W}(B_n) = 0 \). To see this write \( n = 2^m l \) with \( l \) odd.
Then \( Y^n + 1 \) has \( l \) distinct roots of the same multiplicity \( 2^m \). We may label these roots as \( \rho = (\rho_1, \rho_2, \ldots, \rho_n) \) with \( \rho_n = \rho_{n+m} \) for \( m = 1, 2^m + 1, \ldots, [2^m \times (l-1)] + 1 \) and
\( \nu = 1, 2, \ldots, 2^m - 1 \), and \( \rho_{\mu} \neq \rho_{\mu'} \) whenever \( \mu = [2^m \times (\lambda - 1)] + 1 \) and
\( \mu' = [2^m \times (\lambda' - 1)] + 1 \) where \( \lambda \) and \( \lambda' \) are distinct members of the set \{1, 2, \ldots, l-1\}. Thus we may regard that the \( n \) roots of \( Y^n + 1 \) are divided into \( l \) blocks of size \( 2^m \). Now consider the group of all permutations fixing all these blocks, and also the subgroup consisting of even permutations amongst them. This group contains a transposition and has order \((2^m)!^l\) and hence the subgroup has order \((2^m)!^l/2\) which is even because either \( m > 1 \) or \( l > 2 \). Moreover, for any \( \tau \in S_n \), the sets \( \{\sigma \in A_n : \|\sigma\|_{\rho_{\mu}} = 1 \} = \{\|\tau\|_{\rho_{\mu}} = 1 \} \)
and \( \{\sigma \in S_n \setminus A_n : \|\sigma\|_{\rho_{\mu}} = 1 \} = \{\|\tau\|_{\rho_{\mu}} = 1 \} \) are unions of cosets of the said subgroup in \( S_n \).
Therefore \( D(p) = 0 = D^*(p) \) and hence \( \hat{W}(B_n) = \hat{W}(B_n) = 0 \).

First alternative proof of Proposition 2.8. We are considering the polynomial
\( F^o = Y^7 + X Y^4 + Y^2 + 1 \) in \( k(X)[Y] \) where \( k \) is a field of characteristic 2 which need not be algebraically closed, and we want to show that: \( \text{Gal}(F^o, k(X)) \subseteq A_7 \Rightarrow \text{GF}(4) \subseteq k \). Now clearly \( \text{Disc}(F^o) = 1 \) and hence in view of Lemma 3.6, by substituting
\( (X, 1, 1) \) for \( (B_3, B_5, B_7) \), we get \( J(F^o) = Z^2 + Z + 1 + X + X^2 \) or \( Z^2 + Z + 1 + X + X^2 + X^3 + X^6 \). In either case \( J(F^o) \) has a root in \( k(X) \) if \( \text{GF}(4) \subseteq k \). Therefore by Jacobson's Criterion 2.1 we conclude that: \( \text{Gal}(F^o, k(X)) \subseteq A_7 \Rightarrow \text{GF}(4) \subseteq k \).

4. Alternative proof of Proposition 2.8 by resultant criterion

In this Section, we shall deduce our Proposition 2.8 as a consequence of (3.17) and
(3.32) of [5]. In proving Lemma 4.2 we shall tacitly use the following obvious
Sublemma 4.1 which was implicitly used in the proof of Lemma 2.5.
Sublemma 4.1. Let $f = a Y^n + \cdots$ and $\phi = a Y^v + \cdots$ be polynomials of degrees $n \leq v$ with coefficients $a, \ldots, a, \ldots$, in any field where we assume that $a \neq 0 \neq a$. Let $r = v - n$, let $u$ and $\theta$ be constants with $u$ nonzero and let $\psi = u \phi + \theta Y^r \psi = \beta Y^m + \cdots$ where $\beta$ is a nonzero constant and $\mu$ is a nonnegative integer (obviously $\mu \leq v$). Let $s = v - \mu$. Then

$$\text{Res}_y(f, \psi) = [(a^r)/(u^n)] \text{Res}_y(f, \psi)$$

and

$$\text{Res}_y(\phi, f) = [(-1)^{\mu}] [(a^r)/(u^n)] \text{Res}_y(\psi, f).$$

Lemma 4.2. Consider the polynomial $f(Y) = Y^n + b_3 Y^4 + b_5 Y^2 + b_7$ where $b_3, b_5, b_7$ are nonzero elements in a field $K$ of characteristic 2. Following the notation of Section 3 of [5] let $f^0(Y) = Y^2$ and $f^2(Y) = b_3 Y^2 + b_5 Y + b_7$ so that $f(Y) = Y^2 f^0(Y^2) + 2 f^2(Y^2)$. Let $f^*(Y) = Y^2 f^0(Y^2) + Y f^2(Y^2)$ where subscript $Y$ indicates $Y$-derivative. Then

$$\text{Res}_y(f(Y), T f(Y) + f^*(Y)) = b_7 T^7 + b_5 T^6$$

$$+ [b_3^2 b_3^2 b_5^2 + b_3 b_3 b_5 b_5 + b_3 b_5^3 + b_3^2] T^5 + b_3 T^4$$

$$+ [b_3^2 b_3 b_5 + b_3^2 b_3 b_5 + b_3 b_5^2] T^3 + [b_3 b_3^2 b_5 + b_3^2] T^2$$

$$+ [b_3 b_3^2 b_5 + b_3 b_3 b_5 + b_3 b_5^2] T + [b_3^2 b_3 b_5 + b_3^2].$$

Proof. Clearly $f^2(Y) = Y^2$ and $f^0(Y) = b_3$ and hence $f^*(Y) = Y^6 + b_3 Y$. Also $f(Y) = Y^6$ and hence $T f(Y) + f^*(Y) = Y f(Y)$ where $f(Y) = (T + 1) Y^5 + b_3 Y$. Therefore

$$\text{Res}_y(f(Y), T f(Y) + f^*(Y))$$

$$= f(0) \text{Res}_y(f, f) = \frac{b_7}{(T + 1)^2} \text{Res}_y(G, f) = \frac{b_7}{b_3} \text{Res}_y(G, g)$$

where

$$G = (T + 1) f + Y^2 f = b_3 (T + 1) Y^4 + b_5 T Y^2 + b_7 (T + 1)$$

and

$$g = b_3 f + Y G = b_3 T Y^3 + b_7 (T + 1) Y + b_3 b_5$$

and clearly

$$\frac{b_7}{b_3} \text{Res}_y(G, g) = \frac{b_7}{b_3 b_5 T} \text{Res}_y(E, g) = \frac{b_7}{b_3 b_5 T H} \text{Res}_y(E, e)$$

where

$$E = b_5 T G + b_3 (T + 1) Y g = H Y^2 + I Y + J.$$
with
\[ H = (b_3 b_7 + b_5^2) T^2 + b_3 b_7 \quad \text{and} \quad I = b_3^2 b_7 (T + 1) \quad \text{and} \quad J = b_3 b_7 T (T + 1) \]
and
\[ e = H g + b_5 T Y E = h Y^2 + i Y + j \]
with
\[ h = b_3^3 b_5^2 T (T + 1) \quad \text{and} \quad i = b_3 b_5^2 (T + 1)^3 \quad \text{and} \quad j = b_3 b_5 H. \]

Expanding the 4 by 4 matrix by the first two rows \( H, I, J, 0 \) and \( 0, H, I, J \) (the last two rows being \( h, i, j, 0 \) and \( 0, h, i, j \)) we get
\[ \text{Res}_y (E, e) = H^2 j^2 + H I j + I J i + (I^2 + H J) h j + I J h i + J^2 h^2 \]
and now substituting \( j = b_3 b_5 H \) we get
\[ H^{-1} \text{Res}_y (E, e) = b_3^3 b_5 H^3 + b_3 b_5 I I H + J I j + b_3 b_5 I^2 h + J h H^{-1} [I i + J h] \]
and clearly
\[ I i + J h = [b_3 b_5 b_7 (T + 1)^2] [b_3 b_7 (T + 1)^4] = [b_3 b_5 b_7 (T + 1)^4] H \]
and hence
\[ H^{-1} \text{Res}_y (E, e) = b_3^3 b_5 H^3 + b_3 b_5 I I H + J I j + b_3 b_5 I^2 h + b_3^3 b_5 b_7 J h (T + 1)^2 \]
and therefore substituting
\[ h = b_3^3 b_5^2 (T + 1) \quad \text{and} \quad i = b_3 b_5^2 (T + 1)^3 \quad \text{and} \quad J = b_3 b_7 T (T + 1) \]
we get
\[ [b_3^2 b_5 H]^{-1} \text{Res}_y (E, e) = b_3 H^3 + [b_3^2 (T + 1)^2] I H + b_3^2 T (T + 1)^7 \]
\[ + [b_3 b_5^2 T (T + 1)] I^2 + b_3 b_5^2 b_5^2 T^2 (T + 1)^4 \]
and now substituting \( I = b_3^2 b_5 (T + 1) \) we have
\[ [b_3^2 b_5 H]^{-1} \text{Res}_y (E, e) = b_3 H^3 + [b_3^2 b_5 b_5^2 (T + 1)^4] H + b_3^2 T (T + 1)^7 \]
\[ + b_3^2 b_5^2 T (T + 1)^3 + b_3^2 b_5^2 b_5^2 T^2 (T + 1)^4 \]
and now using the fact that \( H = (b_3 b_7 + b_5^2) T^2 + b_3 b_7 \) we get
\[ b_3 H^3 + [b_3^2 b_5 b_5^2 (T + 1)^4] H = b_3 H [H^2 + b_3^2 b_5^2 (T^4 + 1)] \]
and
\[ H^2 = b_3^2 b_5^2 T^4 + b_5^2 T^4 + b_3 b_5^2 \]
and hence
\[ b_5 H^3 + [b_3 b_5 (T + 1)^4] H = b_5 H [b_3 b_5 T^4] = [b_3 b_5 b_7 + b_3 T^6 + b_3 b_5 b_7 T^4] \]
and therefore
\[ [b_3 b_5 TH]^{-1} \text{Res}_Y(E, e) = [b_3 b_5 b_7 + b_3 T^6 + b_3 b_5 b_7 T^4] \]
and clearly
\[ (T + 1)^7 = T^7 + T^6 + T^5 + T^4 + T^3 + T^2 + T + 1 \]
and
\[ (T + 1)^3 = T^3 + T^2 + T + 1 \quad \text{and} \quad (T + 1)^4 = T^5 + T \]
and hence
\[ [b_3 b_5 TH]^{-1} \text{Res}_Y(E, e) = b_3 T^7 + b_5 T^7 + b_3 T^6 + [b_3 b_5 b_7 + b_3 T^6 + b_3 b_5 b_7 T^4] \]

Now our assertion follows from the last equation and the first two displays involving Res_Y. \( \square \)

**Second alternative proof of Proposition 2.8.** We are considering the polynomial 
\( F^0 = Y^7 + X Y^4 + Y^2 + 1 \) in \( k(X)[Y] \) where \( k \) is a field of characteristic 2 which need not be algebraically closed, and we want to show that: \( \text{Gal}(F^0, k(X)) \triangleleft A_7 \Rightarrow \text{GF}(4) \subset k \). Now clearly \( \text{Discr}(F^0) = 1 \), and by substituting \( (X, 1, 1) \) for \( (b_3, b_5, b_7) \) the coefficient of \( T^5 \) in the RHS of the asserted equation of (4.2) we get \( X^2 + X \). Hence by (3.16) and (3.32.3) of [5] we have \( \text{Rat}(F^0) = X^2 + X + 1 \) where \( \text{Rat} \) is as defined in the cited item (3.16). Obviously: \( X^2 + X + 1 = z^2 + z \) for some \( z \in k(X) \) iff \( \text{GF}(4) \subset k \). Therefore by (3.17) of [5] we conclude that: \( \text{Gal}(F^0, k(X)) \triangleleft A_7 \Rightarrow \text{GF}(4) \subset k \). \( \square \)

### 5. The bar polynomial

**Lemma 5.1.** Let \( K \) be a field of characteristic \( p > 0 \), let \( m \) be a positive integer, and let \( \Theta = \Theta(Y) = Y^{p^m} + \sum_{i=0}^{p-1} \lambda_i Y^p \) with \( \lambda_i \in K \). Assume that \( \lambda_0 \neq 0 \), i.e., equivalently assume that \( \Theta \) has no multiple roots. Then \( \text{Gal}(\Theta, K) \) is a subgroup of \( \text{GL}(m, p) \).

**Proof.** The roots of \( \Theta \) form an additive subgroup of the splitting field \( K^* \) of \( \Theta \) over \( K \). In other words the said splitting field is a vector space over \( \text{GF}(p) \) and the roots form
a subspace. By cardinality, the dimension of this subspace is \( m \). Now \( \text{Gal}(\Theta, K) \) is a subgroup of the group of all \( GF(p) \)-automorphisms of \( K^* \) which itself is a subgroup of the group of all vector space automorphisms of \( K^* \). Therefore \( \text{Gal}(\Theta, K) \) is a subgroup of \( GL(m, p) \). \( \square \)

**Lemma 5.2.** Let \( K \) be a field of characteristic \( p > 0 \), let \( m \) be a positive integer, and let 
\[
\Lambda = \Lambda(Y) = Y^{p^m-1} + \sum_{i=0}^{m} \lambda_i Y^{p^i-1} \quad \text{with} \quad \lambda_i \in K.
\]
Assume that \( \lambda_0 \neq 0 \), i.e., equivalently assume that \( \Lambda \) has no multiple roots. Then \( \text{Gal}(\Lambda, K) \) is a subgroup of \( GL(m, p) \) when we regard \( GL(m, p) \) as acting on nonzero vectors.

**Proof.** In Lemma 5.1 take \( \Theta(Y) = Y\Lambda(Y) \). \( \square \)

**Theorem 5.3.** Let \( a \) be a nonzero element of a field \( k \) of characteristic 2 which need not be algebraically closed, let \( s \) be a positive integer, and consider the polynomial
\[
\tilde{F}_{7,4,s,a} = Y^7 - aX^3 Y^3 + 1 \in k(X)[Y].
\]
Then \( \tilde{F}_{7,4,s,a} = 0 \) gives an unramified covering of \( L_k \), and \( \text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) = PSL(3, 2) \).

**Proof.** Clearly \( \text{Disc}_Y(\tilde{F}_{7,4,s,a}) = 1 \) and hence \( \tilde{F}_{7,4,s,a} = 0 \) gives an unramified covering of \( L_k \). Now \( \tilde{F}_{7,4,s,a} = 0 \) is irreducible because it is linear in \( X \). Therefore \( \text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) \) is transitive and hence its order is divisible by 7. By solving the equation \( \tilde{F}_{7,4,s,a} = 0 \) we get \( X = (Y^7 + 1)/aY^3 \) and hence the valuation \( X = \infty \) of \( k(X)/k \) splits into the valuations \( Y = \infty \) and \( Y = 0 \) of \( k(X, Y) = k(Y) \) with reduced ramification exponents 4 and 3 respectively. Therefore the order of \( \text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) \) is divisible by 4 as well as 3. Consequently the order of \( \text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) \) is divisible by \( 7 \times 4 \times 3 = 84 = 168/2 \). By Lemma 5.2 we know that \( \text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) \) is a subgroup of \( PSL(3, 2) \). Since \( PSL(3, 2) \) is a simple group of order 168, we must have \( \text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) = PSL(3, 2) \). Therefore, since \( PSL(3, 2) \) is a nonabelian simple group, by Corollary 2.8 of the Substitutional Principle of Section 19 of [3] we conclude that \( \text{Gal}(\tilde{F}_{7,4,s,a}, k(X)) = PSL(3, 2) \). \( \square \)

6. The Tilde polynomial

**Theorem 6.1.** Let \( a \) be a nonzero element of a field \( k \) of characteristic 2 which need not be algebraically closed, let \( s \) be a positive integer, and consider the polynomials
\[
\tilde{F}_{6,1,s,a} = Y^6 - aY + X^s \in k(X)[Y] \quad \text{and} \quad \tilde{F}_{6,1,s,a} = Y^5 + Y^3 + Y - aX^{-s} \in k(X)[Y].
\]
Then \( \tilde{F}_{6,1,s,a} = 0 \) gives an unramified covering of \( L_k \), and for its Galois group we have: \( \text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = PSL(2, 5) \Leftrightarrow GF(4) \subset k \), and: \( \text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = PGL(2, 5) \Leftrightarrow GF(4) \not\subset k \). Moreover, if \( s = 0 \) then \( \tilde{F}_{6,1,s,a} = 0 \) gives an unramified covering of \( L_k \) and
for its Galois group we have: \( \text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = \text{ASL}(1,5) \) or \( \text{AGL}(1,5) \). Furthermore, if \( s = 0(5) \) and \( \text{GF}(4) = k \) then: \( \text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = \text{ASL}(1,5) \). Finally, if \( s = 5 \) and \( \text{GF}(4) \neq k \) then: \( \text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = \text{AGL}(1,5) \). [Note that \( \text{PSL}(2,5) \) and \( A_5 \) are isomorphic as abstract groups but not as permutation groups, and likewise \( \text{PGL}(2,5) \) and \( S_5 \) are isomorphic as abstract groups but not as permutation groups. Observe that \( \text{ASL}(1,5) \) is also called the dihedral group of degree 5].

**Proof.** Obviously \( \text{Disc}_Y(\tilde{F}_{6,1,s,a}) = a^6 \) and hence \( \tilde{F}_{6,1,s,a} = 0 \) gives an unramified covering of \( L \). In the notation of Lemma 2.4 we have \( \widetilde{U}(B_5, B_6) = u'B_2^3 \) with \( u' \in \mathbb{Z} \setminus 2\mathbb{Z} \), and \( \tilde{V}(B_5, B_6) = vB_5^3 + v'B_6^3 \) with \( v \in 2\mathbb{Z} \) and \( v' \in \mathbb{Z} \setminus 2\mathbb{Z} \). Therefore Jacobson’s polynomial of \( \tilde{F}_{6,1,s,a} \) is \( Z^2 + a^3 Z + a^6 \), and clearly: this has a root in \( k(X) \) iff \( \text{GF}(4) \subseteq k \). Hence by Jacobson’s Criterion 2.1 we see that: \( \text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) \subseteq A_5 \Rightarrow \text{GF}(4) \subseteq k \).

Now \( \tilde{F}_{6,1,1,a} \) is irreducible because it is linear in \( X \). By solving \( \tilde{F}_{6,1,1,a} = 0 \) we get \( X = aY - Y^6 \) and hence \( k(X, Y) = k(Y) \), i.e., \( k(Y) \) is a root field of \( \tilde{F}_{6,1,1,a} = 0 \) over \( k(X) \). By throwing the root \( Y \) of \( \tilde{F}_{6,1,1,a} \) we get

\[
\frac{1}{Z}[(Z + Y)^6 - a(Z + Y) + X - (Y^6 - aY + X)] = Z^5 + Y^2 Z^3 + Y^4 Z - a
\]

and by substituting \( Y = 1/Y' \) and \( Z = Z'/Y' \) in the right hand side (RHS) and then multiplying throughout by \( Y'^2 \) we get the polynomial

\[
\Psi(Y', Z') = Z'^5 + Z'^3 + Z' - aY'^5
\]

which is irreducible because \( Z'^5 + Z'^3 + Z' \) is divisible by \( Z' \) but not \( Z'^2 \). Clearly the valuation \( X = \infty \) of \( k(X)/k \) has the valuation \( Y = \infty \) as the only extension to \( k(Y) \), and by changing \( (Y, Z') \) to \( (X, Y) \) in \( \Psi(Y'^{-1}, Z') \) we get \( \tilde{F}_{6,1,5,a} \). Therefore \( \tilde{F}_{6,1,5,a} = 0 \) gives an unramified covering of \( L \). The group \( \text{Gal}(\tilde{F}_{6,1,5,a}, k(X)) \) is the one-point stabilizer of the group \( \text{Gal}(\tilde{F}_{6,1,1,a}, k(X)) \), and the group \( \text{Gal}(\tilde{F}_{6,1,1,a}, k(X)) \) is doubly transitive.

By throwing away the root \( Z' \) of \( \Psi(Y', Z') \) we get

\[
\frac{1}{T}[(T + Z)^5 + (T + Z)^3 + (T + Z)^3 + aY^5 - (Z^5 + Z^3 + Z' - aY^5)]
\]

\[
- T^4 + Z'T^3 + T^2 + Z'T + Z'^4 + Z'^2 + 1
\]

and by substituting \( Z' = 1/Z^* \) and \( T = T^*/Z^* \) in the RHS and then multiplying throughout by \( Z'^* \) we get the polynomial

\[
\Omega(Z^*, T^*) - T'^*4 + T'^*3 + Z'^*2 T'^*2 + Z'^*2 T^* + 1 + Z'^*2 + Z'^*4.
\]

In \( \text{GF}(4)[Z^*, T^*] \) we have the factorization

\[
\Omega(Z^*, T^*) = \Omega_1(Z^*, T^*) \Omega_2(Z^*, T^*)
\]

with

\[
\Omega_l(Z^*, T^*) = T'^*2 + a'T'^* + a^2Z'^*2 + a^4 \quad \text{for } 1 \leq l \leq 2
\]
where \( \text{GF}(4) = \text{GF}(2)(a) \), i.e.,
\[ x^2 + x + 1 = 0 \] or equivalently \( x^3 = 1 \neq x \).

By changing \( Z^* \) to \( Z^{-1} \) we get
\[ \Omega(Z^{-1}, T^*) = \Omega_1(Z^{-1}, T^*) \Omega_2(Z^{-1}, T^*). \]

For a moment assume that \( \text{GF}(4) \subseteq k \). For \( 1 \leq i \leq 2 \), by degree considerations we see that \( \Omega_i(Z^*, T^*) \) has no root in \( k[Z^*] \) and hence \( \Omega_i(Z^*, T^*) \) is irreducible in \( k(Z^*)[T^*] \). For the root field \( k(Y', Z') \) of \( \Psi(Y', Z') \) over \( k(Z') \) we clearly have \( [k(Y', Z') : k(Z')] = 5 \neq 0(2) \) and hence, for \( 1 \leq i \leq 2 \), the irreducibility of the quadratic \( \Omega_i(Z^{-1}, T^*) \) in \( k(Z^*)[T^*] \) implies its irreducibility in \( k(Y', Z')[T^*] \). Also we have
\[ x^2 \Omega_1(Z^{-1}, x^2 T^* + 1) = \Omega_2(Z^{-1}, T^*). \]

Therefore \( |\text{Gal}(\tilde{F}_{6,1,1,a}(k(X)))| = 6 \times 5 \times 2 = 60 \), and the group \( \text{Gal}(\tilde{F}_{6,1,1,a}(k(X))) \) is doubly transitive but not triply transitive. Since \( \text{Gal}(\tilde{F}_{6,1,1,a}(k(X))) \) is a subgroup of \( A_6 \) of index 6, considering the permutation representation of \( A_6 \) by cosets according to \( \text{Gal}(\tilde{F}_{6,1,1,a}(k(X))) \) we see that \( \text{Gal}(\tilde{F}_{6,1,1,a}(k(X))) \approx A_6 \). Since \( \text{Gal}(\tilde{F}_{6,1,1,a}(k(X))) \) is doubly transitive but not triply transitive, we get \( \text{Gal}(\tilde{F}_{6,1,1,a}(k(X))) = \text{PSL}(2, 5) \) (see [6], Chapter II 4.7, 6.14). Therefore, since \( \text{PSL}(2, 5) \) is nonabelian simple, by Corollary 2.8 of the Substitutional Principle of Section 19 of [3] we have \( \text{Gal}(\tilde{F}_{6,1,1,a}(k(X))) = \text{PSL}(2, 5) \). Since \( \text{ASL}(1, 5) \) is the one-point stabilizer of \( \text{PSL}(2, 5) \), we also get \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) = \text{ASL}(1, 5) \). Since \( k \) was any field containing \( \text{GF}(4) \), we get \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) = \text{ASL}(1, 5) \) provided \( s \equiv 0(5) \). Therefore we must have \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) = \text{ASL}(1, 5) \) provided \( s \equiv 0(5) \).

Now assume that \( \text{GF}(4) \notin k \). Then it is clear that \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(z(X))) \) is a subgroup of \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) \) of index 1 or 2, and by what we have provided above we get \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(z(X))) \notin A_6 \) and \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) = \text{PSL}(2, 5) \approx S_5 \) (see [6], Chapter II 4.7, 6.14). Since \( \text{AGL}(1, 5) \) is the one-point stabilizer of \( \text{PSL}(2, 5) \), we get \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) = \text{AGL}(1, 5) \). Now \( |\text{AGL}(1, 5) : \text{ASL}(1, 5) = 2 \), and if \( s \equiv 0(5) \) then \( \text{ASL}(1, 5) = \text{Gal}(\tilde{F}_{6,1,5,a}(k(z(X))) \subseteq \text{Gal}(\tilde{F}'_{6,1,5,a}(k(x))) \subseteq \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) \). Therefore if \( s \equiv 0(5) \) then \( \text{Gal}(\tilde{F}_{6,1,5,a}(k(X))) = \text{ASL}(1, 5) \) or \( \text{AGL}(1, 5) \).

\[ \text{Theorem 6.2.} \text{ Let } k \text{ be a field of characteristic 2 which need not be algebraically closed and consider the polynomial} \]
\[ \tilde{F}_{6,5,a} = Y^6 - aY^5 + X^4 \in k[X][Y] \text{ with } 0 \neq a \in k \text{ and positive integers } s \equiv 0(5). \]

Then \( \tilde{F}_{6,5,a} = 0 \) gives an unramified covering of \( L_k \). Moreover: \( \text{Gal}(\tilde{F}_{6,5,a}(k(X))) = \text{PSL}(2, 5) \Leftrightarrow \text{GF}(4) \subset k \) and: \( \text{Gal}(\tilde{F}_{6,5,a}(k(X))) = \text{PGL}(2, 5) \Leftrightarrow \text{GF}(4) \notin k \). [Again note
that $\text{PSL}(2,5)$ and $A_5$ are isomorphic as abstract groups but not as permutation groups, and likewise $\text{PGL}(2,5)$ and $S_5$ are isomorphic as abstract groups but not as permutation groups.

**Proof.** By Section 20 of [3] we see that $\tilde{F}_{6,5,s,a} = 0$ gives an unramified covering of $L_k$. By reciprocating the roots of $\tilde{F}_{6,5,s,a}$ we get the polynomial $Y^6 - aX^{-5}Y + X^{-s}$. By multiplying the roots of this last polynomial by $X^{-4/5}$ and then substituting $X^{-1}$ for $X$ we get $\tilde{F}_{6,1,s,a}$. Therefore $\text{Gal}(\tilde{F}_{6,5,s,a}, k(X)) = \text{Gal}(\tilde{F}_{6,1,s,a}, k(X))$, and hence our assertions follow from Theorem 6.1. □

**Problem 6.3.** In the remaining cases of Theorem 6.1, decide whether $\text{Gal}(\tilde{F}_{6,5,s,a}, k(X))$ is $\text{ASL}(1,5)$ or $\text{AGL}(1,5)$. This can be done by using Jacobson's Criterion because we know that if $s = 0(5)$ then $\text{Gal}(\tilde{F}_{6,1,s,a}, k(X)) = \text{ASL}(1,5)$ or $\text{AGL}(1,5)$, and clearly $\text{ASL}(1,5) \subset A_5$ and $\text{AGL}(1,5) \not\subset A_5$.

**References**