TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 348, Number 4, April 1996

FURTHER NICE EQUATIONS FOR NICE GROUPS

SHREERAM S. ABHYANKAR

ABSTRACT. Nice sextinomial equations are given for unramified coverings of the affine line in nonzero characteristic p with $\mathrm{P}\Omega^-(2m,q)$ and $\Omega^-(2m,q)$ as Galois groups where $m>3$ is any integer and $q>1$ is any power of $p>2$.

1. INTRODUCTION

Let $m>3$ be any integer, let $q>1$ be any power of a prime $p>2$, consider the polynomials $F^- = F^-(Y) = Y^n + T^{q^2}Y^{u'} + X^qY^u - XY^w - TY^{w'} - 1$ and $F^* = F^*(Y) = Y^{n^*} + XY + 1$ in indeterminates T, X, Y over an algebraically closed field k of characteristic p, where $n = 1+q+\cdots+q^{2m-1}$, $u' = 1+q+\cdots+q^{m+1}$, $u = 1+q+\cdots+q^m$, $w = 1+q+\cdots+q^{m-2}$, $w' = 1+q+\cdots+q^{m-3}$, $n^* = 1+q+\cdots+q^{m-1}$, and consider their respective Galois groups $\mathrm{Gal}(F^-, k(X,T))$ and $\mathrm{Gal}(F^*, k(X))$. Both these are special cases of the families of polynomials giving unramified coverings of the affine line in nonzero characteristic which were written down in my 1957 paper [A01]. In my "Nice Equations" paper [A04], as a consequence of Cameron-Kantor Theorem I [CaK] on antiflag transitive collineation groups, I proved that $\mathrm{Gal}(F^*, k(X)) =$ the projective special linear group $\mathrm{PSL}(m,q)$. In the present paper, as a consequence of Kantor's characterization of Rank 3 groups in terms of their subdegrees [Kan], supplemented by Cameron-Kantor Theorem IV [CaK], I shall show that $\mathrm{Gal}(F^-, k(X,T)) =$ the projective negative orthogonal group $\mathrm{P}\Omega^-(2m,q)$.[1] Note that Kantor's Rank 3 characterization depends on the Buekenhout-Shult characterization of polar spaces [BuS] which itself depends on Tits' classification of spherical buildings [Tit]. Recall that the Rank of a transitive permutation group is the number of orbits of its 1-point stabilizer, and the sizes of these orbits are called subdegrees.

As a corollary of the above theorem that the Galois group of F^- is $\mathrm{P}\Omega^-(2m,q)$, I shall show that the Galois group of a more general polynomial f^- is also $\mathrm{P}\Omega^-(2m,q)$. Moreover, by slightly changing f^- and F^-, I shall show that we get polynomials ϕ^- and ϕ_2^- whose Galois group is the negative orthogonal group $\Omega^-(2m,q)$. The polynomials f^-, ϕ^- and ϕ_2^- are also special cases of the families of polynomials giving unramified coverings of the affine line in nonzero characteristic written down in [A01].

Received by the editors March 23, 1995.
1991 *Mathematics Subject Classification*. Primary 12F10, 14H30, 20D06, 20E22.
This work was partly supported by NSF grant DMS 91–01424 and NSA grant MDA 904–92–H–3035.

[1] The projective negative (resp: positive) orthogonal group $\mathrm{P}\Omega^-(2m,q)$ (resp: $\mathrm{P}\Omega^+(2m,q)$) is also called the projective elliptic (resp: hyperbolic) orthogonal group.

As in [A03] and [A04], here the basic techniques will be MTR (the Method of Throwing away Roots) and FTP (Factorization of Polynomials).

It is a pleasure to thank Bill Kantor and Ulrich Meierfrankenfeld for inspiring conversations about this paper.

2. Notation and Outline

Let k_p be a field of characteristic $p > 0$, let $q > 1$ be any power of p, and let $m > 1$ be any integer.[2] To abbreviate frequently occurring expressions, for every integer $i \geq -1$ we put

$$\langle i \rangle = 1 + q + q^2 + \cdots + q^i \quad \text{(convention: } \langle 0 \rangle = 1 \text{ and } \langle -1 \rangle = 0).$$

We shall frequently use the geometric series identity

$$1 + Z + Z^2 + \cdots + Z^i = \frac{Z^{i+1} - 1}{Z - 1}$$

and its corollary

$$\langle i \rangle = 1 + q + q^2 + \cdots + q^i = \frac{q^{i+1} - 1}{q - 1}.$$

Let

$$f^- = f^-(Y) = Y^{\langle 2m-1 \rangle} - 1 + \sum_{i=1}^{m-1} \left(T_i^{q^i} Y^{\langle m-1+i \rangle} - T_i Y^{\langle m-1-i \rangle} \right)$$

and note that then f^- is a monic polynomial of degree $\langle 2m-1 \rangle = 1 + q + q^2 + \cdots + q^{2m-1}$ in Y with coefficients in the polynomial ring $k_p[T_1, \ldots, T_{m-1}]$. Now the constant term of f^- is -1 and the Y-exponent of every other term in f^- is 1 modulo p, and hence $f^- - Y f^-_Y = -1$ where f^-_Y is the Y-derivative of f^-. Therefore $\mathrm{Disc}_Y(f^-) = -1$ where $\mathrm{Disc}_Y(f^-)$ is the Y-discriminant of f^-, and hence the Galois group $\mathrm{Gal}(f^-, k_p(T_1, \ldots, T_{m-1}))$ is well-defined as a subgroup of the symmetric group $\mathrm{Sym}_{\langle 2m-1 \rangle}$.

For $1 \leq e \leq m-1$, let f^-_e be obtained by substituting $T_i = 0$ for all $i > e$ in f^-, i.e., let

$$f^-_e = f^-_e(Y) = Y^{\langle 2m-1 \rangle} - 1 + \sum_{i=1}^{e} \left(T_i^{q^i} Y^{\langle m-1+i \rangle} - T_i Y^{\langle m-1-i \rangle} \right)$$

and note that then f^-_e is a monic polynomial of degree $\langle 2m-1 \rangle = 1 + q + q^2 + \cdots + q^{2m-1}$ in Y with coefficients in the polynomial ring $k_p[T_1, \ldots, T_e]$ and, as above, $\mathrm{Disc}_Y(f^-_e) = -1$ and the Galois group $\mathrm{Gal}(f^-_e, k_p(T_1, \ldots, T_e))$ is a subgroup of $\mathrm{Sym}_{\langle 2m-1 \rangle}$. Note that if $m > 2$ and $k = k_p =$ an algebraically closed field (of characteristic $p > 0$), then F^- is obtained by substituting X, T for T_1, T_2 in f^-_2 and hence $\mathrm{Gal}(F^-, k(X, T)) = \mathrm{Gal}(f^-_2, k_p(T_1, T_2))$.

[2] In the Abstract and the Introduction we assumed $p > 2$ and $m > 3$. But in the rest of the paper, unless stated otherwise, we only assume $p > 0$ and $m > 1$.

In Section 3, we factor f^- as $f^- = \overline{f} f^*$ where $\overline{f} = \overline{f}(Y)$ and $f^* = f^*(Y)$ are monic polynomials of degrees $(q^m+1)\langle m-2\rangle$ and $q^{m-1}(q^m+1)$ in Y with coefficients in $k_p[T_1, \dots, T_{m-1}]$, respectively, and in case of $p \neq 2$ we factor f^* further as $f^* = f^{**} f^{***}$ where $f^{**} = f^{**}(Y)$ and $f^{***} = f^{***}(Y)$ are both monic polynomials of degree $q^{m-1}(q^m+1)/2$ in Y with coefficients in $k_p[T_1, \dots, T_{m-1}]$. In Section 3, we show that if $p = 2$ then $\overline{f}$ and f^* are irreducible in $k_p(T_1, \dots, T_{m-1})[Y]$, and if $p \neq 2$ then $\overline{f}$, f^{**} and f^{***} are irreducible in $k_p(T_1, \dots, T_{m-1})[Y]$. Given any e with $1 \le e \le m-1$, by putting $T_i = 0$ for all $i > e$ in $\overline{f}$ and f^* we get $f_e^- = \overline{f}_e f_e^*$ where $\overline{f}_e$ and f_e^* are monic polynomials of degrees $(q^m+1)\langle m-2\rangle$ and $q^{m-1}(q^m+1)$ in Y with coefficients in $k_p[T_1, \dots, T_e]$ respectively. Likewise, if $p \neq 2$ then by putting $T_i = 0$ for all $i > e$ in f^{**} and f^{***} we get $f_e^* = f_e^{**} f_e^{***}$ where f_e^{**} and f_e^{***} are both monic polynomials of degree $q^{m-1}(q^m+1)/2$ in Y with coefficients in $k_p[T_1, \dots, T_{m-1}]$. In Section 3, we also show that if $p = 2$ then $\overline{f}_e$ and f_e^* are irreducible in $k_p(T_1, \dots, T_e)[Y]$, and if $p \neq 2$ then $\overline{f}_e$, f_e^{**} and f_e^{***} are irreducible in $k_p(T_1, \dots, T_e)[Y]$.

In Section 4, we throw away a root of $\overline{f}$ to get its twisted derivative $f'(Y, Z)$, and we let $g(Y, Z)$ be the polynomial obtained by first dividing the Z-roots of $f'(Y, Z)$ by Y and then changing Y to $1/Y$. Assuming $m > 2$, in Section 4, we factor $g(Y, Z)$ into two factors; to motivate the calculations, we first do this for $m = 3$. The Z-degrees of these factors turn out to be $q(q^{m-1}+1)\langle m-3\rangle$ and q^{2m-2}. In Section 4, assuming $m > 2$, we show that these factors are irreducible in case of $\overline{f}_2$ and hence also in case of $\overline{f}$ and $\overline{f}_e$ for $2 \le e \le m-1$, and therefore $\mathrm{Gal}(\overline{f}, k_p(T_1, \dots, T_{m-1}))$ and $\mathrm{Gal}(\overline{f}_e, k_p(T_1, \dots, T_e))$ for $2 \le e \le m-1$ are Rank 3 groups with subdegrees 1, $q(q^{m-1}+1)\langle m-3\rangle$ and q^{2m-2}. In Section 6, from this Rank 3 description, we deduce the result that if $m > 3 \le p$ and k_p is algebraically closed then $\mathrm{Gal}(f^-, k_p(T_1, \dots, T_{m-1})) = \mathrm{Gal}(f_e^-, k_p(T_1, \dots, T_e)) = \mathrm{P}\Omega^-(2m, q)$ for $2 \le e \le m-1$.

Consider the monic polynomials

$$\phi^- = \phi^-(Y) = Y^{q^{2m}-1} - 1 + \sum_{i=1}^{m-1} \left(T_i^{q^i} Y^{q^{m+i}-1} - T_i Y^{q^{m-i}-1} \right)$$

and

$$\phi_e^- = \phi_e^-(Y) = Y^{q^{2m}-1} - 1 + \sum_{i=1}^{e} \left(T_i^{q^i} Y^{q^{m+i}-1} - T_i Y^{q^{m-i}-1} \right) \quad \text{for } 1 \le e \le m-1$$

of degree $q^{2m} - 1$ in Y with coefficients in $k_p[T_1, \dots, T_{m-1}]$ and $k_p[T_1, \dots, T_e]$, respectively, and note that, as before, $\mathrm{Disc}_Y(\phi^-) = \mathrm{Disc}_Y(\phi_e^-) = -1$. In Section 6, as a consequence of the above result about the Galois groups of f^- and f_e^-, we show that if $m > 3 \le p$ and k_p is algebraically closed then $\mathrm{Gal}(\phi^-, k_p(T_1, \dots, T_{m-1})) = \mathrm{Gal}(\phi_e^-, k_p(T_1, \dots, T_e)) = \Omega^-(2m, q)$ for $2 \le e \le m-1$.

In Section 5, we give a review of linear algebra including definitions of $\mathrm{P}\Omega^-(2m, q)$ and $\Omega^-(2m, q)$.

3. Factorization of the Basic Equation

We find a root $h_m(Y) \in \mathrm{GF}(p)[Y]$ of the polynomial

$$Y^{q^m+1} R^q - R - \left(Y^{\langle 2m-1\rangle} - 1 \right)$$

by telescopically putting

$$h_m(Y) = \sum_{\mu=0}^{m-1} Y^{(q^m+1)\langle m-2-\mu\rangle}$$

and checking that then

$$Y^{q^m+1}h_m(Y)^q - h_m(Y) - \left(Y^{\langle 2m-1\rangle} - 1\right) = 0$$

and, for any integer $0 < i < m$, we find a root $h_i(Y, T_i) \in \mathrm{GF}(p)[Y, T_i]$ of the polynomial

$$Y^{q^m+1}R^q - R - \left(T_i^{q^i}Y^{\langle m-1+i\rangle} - T_iY^{\langle m-1-i\rangle}\right)$$

by telescopically putting

$$h_i(Y, T_i) = \sum_{\mu=0}^{i-1} T_i^{q^{i-1-\mu}} Y^{q^m\langle i-2-\mu\rangle + \langle m-2-\mu\rangle}$$

and checking that then

$$Y^{q^m+1}h_i(Y, T_i)^q - h_i(Y, T_i) - \left(T_i^{q^i}Y^{\langle m-1+i\rangle} - T_iY^{\langle m-1-i\rangle}\right) = 0.$$

By summing the above equations, upon letting

$$\overline{f} = \overline{f}(Y) = \sum_{\mu=0}^{m-1} Y^{(q^m+1)\langle m-2-\mu\rangle} + \sum_{i=1}^{m-1}\sum_{\mu=0}^{i-1} T_i^{q^{i-1-\mu}} Y^{q^m\langle i-2-\mu\rangle + \langle m-2-\mu\rangle},$$

we get

$$Y^{q^m+1}\overline{f}(Y)^q - \overline{f}(Y) - f^-(Y) = 0.$$

From the above equation it follows that

$$f^- = \overline{f}f^* \quad \text{where} \quad f^* = f^*(Y) = Y^{q^m+1}\overline{f}(Y)^{q-1} - 1$$

and

$$\text{if } p \neq 2 \text{ then } f^* = f^{**}f^{***}$$

where

$$f^{**} = f^{**}(Y) = Y^{(q^m+1)/2}\overline{f}(Y)^{(q-1)/2} - 1$$

and

$$f^{***} = f^{***}(Y) = Y^{(q^m+1)/2}\overline{f}(Y)^{(q-1)/2} + 1.$$

Note that the $(\mu = 0)$ term in the above first summation is $Y^{(q^m+1)\langle m-2\rangle}$ and its exponent $(q^m+1)\langle m-2\rangle$ is strictly greater than the Y-exponent of every other term in the above two summations. Hence $\overline{f}$ is a monic polynomial of degree $(q^m+1)\langle m-2\rangle$ in Y with coefficients in $k_p[T_1, \ldots, T_{m-1}]$. Therefore f^* is a monic polynomial of degree $(q^m+1)[1 + (q-1)\langle m-2\rangle] = q^{m-1}(q^m+1)$ in Y with coefficients in $k_p[T_1, \ldots, T_{m-1}]$, and if $p \neq 2$ then f^{**} and f^{***} are both monic polynomials of degree $q^{m-1}(q^m+1)/2$ in Y with coefficients in $k_p[T_1,\dots,T_{m-1}]$. Thus

(3.0)

$$\begin{cases} f^- = \overline{f} f^* \text{ where } \overline{f} \text{ and } f^* \text{ are monic polynomials of degrees } (q^m+1)\langle m-2\rangle \\ \text{and } q^{m-1}(q^m+1) \text{ in } Y \text{ with coefficients in } k_p[T_1,\dots,T_{m-1}] \text{ respectively,} \\ \text{and if } p\neq 2 \text{ then } f^* = f^{**}f^{***} \text{ where } f^{**} \text{ and } f^{***} \text{ are both monic polynomials} \\ \text{of degree } q^{m-1}(q^m+1)/2 \text{ in } Y \text{ with coefficients in } k_p[T_1,\dots,T_{m-1}]. \end{cases}$$

For $1 \le e \le m-1$, let $\overline{f}_e = \overline{f}_e(Y)$ and $f_e^* = f_e^*(Y)$ be obtained by putting $T_i = 0$ for all $i > e$ in $\overline{f}$ and f^*, respectively, and if $p \neq 2$ then let $f_e^{**} = f_e^{**}(Y)$ and $f_e^{***} = f_e^{***}(Y)$ be obtained by putting $T_i = 0$ for all $i > e$ in f^{**} and f^{***}, respectively. Then by (3.0),

(3.1)

$$\begin{cases} \text{for } 1 \le e \le m-1 \text{ we have:} \\ f_e^- = \overline{f}_e f_e^* \text{ where } \overline{f}_e \text{ and } f_e^* \text{ are monic polynomials of degrees } (q^m+1)\langle m-2\rangle \\ \text{and } q^{m-1}(q^m+1) \text{ in } Y \text{ with coefficients in } k_p[T_1,\dots,T_e] \text{, respectively,} \\ \text{and if } p\neq 2 \text{ then } f_e^* = f_e^{**}f_e^{***} \text{ where } f_e^{**} \text{ and } f_e^{***} \text{ are both monic polynomials} \\ \text{of degree } q^{m-1}(q^m+1)/2 \text{ in } Y \text{ with coefficients in } k_p[T_1,\dots,T_e]. \end{cases}$$

Now

$$f_e^- = A_e T_1^q - B_e T_1 + C_e$$

where

$$0 \neq A_e = Y^{\langle m\rangle} \in k_p[Y] \text{ and } 0 \neq B_e = Y^{\langle m-2\rangle} \in k_p[Y]$$

and

$$C_e = Y^{\langle 2m-1\rangle} - 1 + \sum_{i=2}^{e} \left(T_i^{q^i} Y^{\langle m-1+i\rangle} - T_i Y^{\langle m-1-i\rangle} \right) \in k_p[Y, T_1, \dots, T_e]$$

and hence in particular $\deg_{T_1} f_e^- = q$. Also clearly $\deg_{T_1} \overline{f}_e = 1$ and hence $\deg_{T_1} f_e^* = q-1$ and if $p \neq 2$ then $\deg_{T_1} f_e^{**} = (q-1)/2 = \deg_{T_1} f_e^{***}$.

In case of $p = 2$, the irreducibility of $\overline{f}_e$ and f_e^* will follow from Lemmas (4.2) and (4.3) of [A05]. In case of $p \neq 2$, for establishing the irreducibility of $\overline{f}_e$, f_e^{**} and f_e^{***} we now prove the following lemma.

Lemma (3.2). *Let Q be a field of characteristic p and consider a univariate polynomial $g_0 = A_0 T^q - B_0 T + C_0$ with A_0, B_0, C_0 in Q such that $A_0 \neq 0 \neq B_0$. Assume that $g_0 = g_0' g_0'' g_0'''$ in $Q[T]$ with $\deg_T g_0' = 1$ and $\deg_T g_0'' > 0 < \deg_T g_0'''$. Also assume that for some real discrete valuation I of Q (whose value group is the group of all integers) we have $GCD(q-1, I(B_0/A_0)) = 2$. Then g_0'' and g_0''' are irreducible in $Q[T]$.*

To see this, we note that by assumption $g_0' = A_0' T + B_0'$ with $0 \neq A_0' \in Q$ and $B_0' \in Q$. Now $-B_0'/A_0'$ is a root of $g_0/A_0 = T^q - (B_0/A_0)T + (C_0/A_0)$ and hence

$$[T - (B_0'/A_0')]^q - (B_0/A_0)[T - (B_0'/A_0')] + (C_0/A_0) = T[T^{q-1} - (B_0/A_0)].$$

Therefore, in view of the Q-automorphism $T \to T - (B_0'/A_0')$ of $Q[T]$, we see that g_0/A_0 factors into exactly one more nonconstant monic irreducible factor in $Q[T]$ as $T^{q-1} - (B_0/A_0)$, i.e., upon writing $g_0/A_0 = \theta_1\theta_2\ldots\theta_\rho$ and $T^{q-1} - (B_0/A_0) = \theta_1'\theta_2'\ldots\theta_{\rho'}'$ where $\theta_1,\theta_2,\ldots,\theta_\rho,\theta_1',\theta_2',\ldots,\theta_{\rho'}'$ are nonconstant monic irreducible polynomials in $Q[t]$, we have $\rho = 1+\rho'$. By assumption 2 divides $q-1$ and hence we must have $p \neq 2$. Also 2 divides $I(B_0/A_0)$ and hence $I(B_0/A_0) = 2s$ where s is an integer. We can take an element Λ in Q with $I(\Lambda) = 1$, and then we can take an element Δ in an algebraic closure Q^* of Q with $B_0/A_0 = (\Delta\Lambda^s)^2$. Now $I((B_0/A_0)/\Lambda^{2s}) = 0$ and hence by the Discriminant Criterion we see that I is unramified in $Q(\Delta)$. Therefore upon taking an extension I^* of I to $Q(\Delta)$ we have $I^*(\Delta\Lambda^s) = s$ and hence $\mathrm{GCD}((q-1)/2, I^*(\Delta\Lambda^s)) = 1 = \mathrm{GCD}((q-1)/2, I^*(-\Delta\Lambda^s))$. In $Q(\Delta)[T]$ we have $T^{q-1} - (B_0/A_0) = [T^{(q-1)/2} - \Delta\Lambda^s][T^{(q-1)/2} + \Delta\Lambda^s]$. By taking $\Delta' \in Q^*$ with $\Delta'^{(q-1)/2} = \Delta\Lambda^s$ and then taking an extension I' of I^* to $Q(\Delta,\Delta')$ and letting r be the reduced ramification exponent of I' over I^*, we have $I'(\Delta\Lambda^s)/[(q-1)/2] = rI^*(\Delta\Lambda^s)/[(q-1)/2] = rs/[(q-1)/2]$. Consequently $rs/[(q-1)/2]$ must be an integer and hence, because $\mathrm{GCD}((q-1)/2, I^*(\Delta\Lambda^s)) = 1$, it follows that r divides $(q-1)/2$. Since the field degree $[Q(\Delta,\Delta') : Q(\Delta)]$ is at least r, we conclude that $[Q(\Delta,\Delta') : Q(\Delta)] \geq (q-1)/2$. Since Δ' is a root of the polynomial $T^{(q-1)/2} - \Delta\Lambda^s$, this polynomial must be irreducible in $Q(\Delta)[T]$. Similarly the polynomial $T^{(q-1)/2} + \Delta\Lambda^s$ is also irreducible in $Q(\Delta)[T]$. Consequently $\rho' \leq 2$ and hence $\rho \leq 3$. Therefore the polynomials g_0'' and g_0''' must be irreducible in $Q[T]$.

The following lemma is an easy consequence of the Gauss Lemma.

Lemma (3.3). *Let κ be a field, and let $g_0 = g_0'g_0''g_0'''$ where g_0, g_0', g_0'', g_0''' are monic polynomials of positive degrees in Z with coefficients in the $(d+1)$-variable polynomial ring $\kappa[X_1,\ldots,X_d,T]$. Assume that the polynomials g_0', g_0'', and g_0''' have positive T-degrees and are irreducible in the ring $\kappa(X_1,\ldots,X_d,Z)[T]$. Also assume that the coefficients of g_0 as a polynomial in T have no nonconstant common factor in $\kappa[X_1,\ldots,X_d,Z]$. Then the polynomials g_0', g_0'' and g_0''' are irreducible in the ring $\kappa(X_1,\ldots,X_d,T)[Z]$.*

By letting I to be the Y-adic valuation of $Q = k_p(Y,T_2,\ldots,T_e)$, i.e., the real discrete valuation whose valuation ring is the localization of $k_p[Y,T_2,\ldots,T_e]$ at the principal prime ideal generated by Y, we see that $I(A_e) = \langle m\rangle$ and $I(B_e) = \langle m-2\rangle$ and hence $I(B_e/A_e) = \langle m-2\rangle - \langle m\rangle = -q^{m-1}(1+q)$. Therefore $\mathrm{GCD}(q-1, I(B_e/A_e)) = 1$ or 2 according as $p = 2$ or $p \neq 2$. Also obviously A_e and C_e have no nonconstant common factors in $k_p[Y,T_2,\ldots,T_e]$. Therefore, if $p = 2$ then by Lemmas (4.2) and (4.3) of [A05], and if $p \neq 2$ then by the above Lemmas (3.2) and (3.3), for $1 \leq e \leq m-1$ we have that

$$(3.4)\qquad \begin{cases} \text{if } p = 2 \text{ then } \overline{f}_e \text{ and } f_e^* \text{ are irreducible in } k_p(T_1,\ldots,T_e)[Y], \text{ and} \\ \text{if } p \neq 2 \text{ then } \overline{f}_e,\ f_e^{**} \text{ and } f_e^{***} \text{ are irreducible in } k_p(T_1,\ldots,T_e)[Y]. \end{cases}$$

By taking $e = m-1$ in (3.4) we see that

$$(3.5)\qquad \begin{cases} \text{if } p = 2 \text{ then } \overline{f} \text{ and } f^* \text{ are irreducible in } k_p(T_1,\ldots,T_{m-1})[Y], \text{ and} \\ \text{if } p \neq 2 \text{ then } \overline{f},\ f^{**} \text{ and } f^{***} \text{ are irreducible in } k_p(T_1,\ldots,T_{m-1})[Y]. \end{cases}$$

4. Twisted Derivative and its Factorization

Recall that

$$\overline{f} = \overline{f}(Y) = \sum_{\mu=0}^{m-1} Y^{(q^m+1)\langle m-2-\mu\rangle} + \sum_{i=1}^{m-1}\sum_{\mu=0}^{i-1} T_i^{q^{i-1-\mu}} Y^{q^m\langle i-2-\mu\rangle+\langle m-2-\mu\rangle}.$$

Solving the equation $\overline{f} = 0$, we get

$$T_1 = \frac{\sum_{\mu=0}^{m-1} Y^{(q^m+1)\langle m-2-\mu\rangle} + \sum_{i=2}^{m-1}\sum_{\mu=0}^{i-1} T_i^{q^{i-1-\mu}} Y^{q^m\langle i-2-\mu\rangle+\langle m-2-\mu\rangle}}{-Y^{\langle m-2\rangle}}$$

and hence

$$\begin{aligned}
f'(Y,Z) =& \frac{\overline{f}(Z)-\overline{f}(Y)}{Z-Y} \quad \text{(def of the twisted derivative } f' \text{ of } \overline{f}\text{)}\\
=& \frac{\sum_{\mu=0}^{m-2}\left(Z^{(q^m+1)\langle m-2-\mu\rangle} - Y^{(q^m+1)\langle m-2-\mu\rangle}\right)}{Z-Y}\\
&+ \frac{\sum_{\mu=0}^{m-1} Y^{(q^m+1)\langle m-2-\mu\rangle}}{-Y^{\langle m-2\rangle}} \times \frac{Z^{\langle m-2\rangle}-Y^{\langle m-2\rangle}}{Z-Y}\\
&+ \frac{\sum_{i=2}^{m-1}\sum_{\mu=0}^{i-1} T_i^{q^{i-1-\mu}} Y^{q^m\langle i-2-\mu\rangle+\langle m-2-\mu\rangle}}{-Y^{\langle m-2\rangle}} \times \frac{Z^{\langle m-2\rangle}-Y^{\langle m-2\rangle}}{Z-Y}\\
&+ \sum_{i=2}^{m-1}\sum_{\mu=0}^{i-1} \frac{T_i^{q^{i-1-\mu}}\left(Z^{q^m\langle i-2-\mu\rangle+\langle m-2-\mu\rangle} - Y^{q^m\langle i-2-\mu\rangle+\langle m-2-\mu\rangle}\right)}{Z-Y}.
\end{aligned}$$

Therefore

$$\begin{aligned}
g =& g(Y,Z)\\
=& Y^{(q^m+1)\langle m-2\rangle-1} f'(1/Y, Z/Y) \quad \text{(def of polynomial } g \text{ obtained by dividing}\\
& \qquad\qquad \text{roots of } f' \text{ by } Y \text{ and then changing } Y \text{ to } 1/Y\text{)}\\
=& \frac{\sum_{\mu=0}^{m-2}\left(Z^{(q^m+1)\langle m-2-\mu\rangle}-1\right) Y^{(q^m+1)q^{m-1-\mu}\langle \mu-1\rangle}}{Z-1}\\
&+ \frac{\sum_{\mu=0}^{m-1} Y^{(q^m+1)q^{m-1-\mu}\langle \mu-1\rangle}}{-1} \times \frac{Z^{\langle m-2\rangle}-1}{Z-1}\\
&+ \frac{\sum_{i=2}^{m-1}\sum_{\mu=0}^{i-1} T_i^{q^{i-1-\mu}} Y^{q^{m-1-\mu+i}\langle m-1+\mu-i\rangle + q^{m-1-\mu}\langle \mu-1\rangle}}{-1} \times \frac{Z^{\langle m-2\rangle}-1}{Z-1}\\
&+ \sum_{i=2}^{m-1}\sum_{\mu=0}^{i-1} \frac{T_i^{q^{i-1-\mu}}\left(Z^{q^m\langle i-2-\mu\rangle+\langle m-2-\mu\rangle}-1\right) Y^{q^{m-1-\mu+i}\langle m-1+\mu-i\rangle+q^{m-1-\mu}\langle \mu-1\rangle}}{Z-1}.
\end{aligned}$$

For $i = m$, the powers of Z in the last summation coincide with the corresponding powers of Z in the first summation; moreover, for $\mu = m-1$, by convention $\left(Z^{(q^m+1)\langle m-2-\mu\rangle}-1\right) = 0$, and hence the first summation can be extended to $m-1$. Consequently, upon letting

$$D_{i\mu} = \frac{Z^{q^m\langle i-2-\mu\rangle+\langle m-2-\mu\rangle}-1}{Z-1} - \frac{Z^{\langle m-2\rangle}-1}{Z-1} \quad \text{for } 2 \le i \le m \text{ and } 0 \le \mu \le i-1$$

we get

$$g = \sum_{\mu=0}^{m-1} D_{m\mu} Y^{(q^m+1)q^{m-1-\mu}\langle\mu-1\rangle} + \sum_{i=2}^{m-1}\sum_{\mu=0}^{i-1} D_{i\mu} Y^{q^{m-1-\mu+i}\langle m-1+\mu-i\rangle + q^{m-1-\mu}\langle\mu-1\rangle} T_i^{q^{i-1-\mu}}.$$

It follows that if $m = 2$ then

$$g = \frac{Z\left(Z^{q^2}-1\right)}{Z-1} - Y^{q^2+1} \quad \text{with} \quad \frac{Z\left(Z^{q^2}-1\right)}{Z-1} \in (Zk_p[Z]) \setminus \left(Z^2 k_p[Z]\right)$$

and hence g is irreducible in $k_p(Z)[Y]$ and therefore by the Gauss Lemma g is irreducible in $k_p(Y)[Z]$. Thus

(4.0) $$\begin{cases} \text{if } m=2, \text{ then } g \text{ is a monic polynomial of degree } q^2 \text{ in } Z \\ \text{with coefficients in } k_p[Y], \text{ and } g \text{ is irreducible in } k_p(Y)[Z]. \end{cases}$$

Henceforth assuming $m > 2$, and displaying dependence on T_2, we get

$$\begin{aligned} g =& D_{20} Y^{q^{m+1}\langle m-3\rangle} T_2^q + D_{21} Y^{q^m\langle m-2\rangle + q^{m-2}} T_2 \\ &+ \sum_{\mu=0}^{m-1} D_{m\mu} Y^{(q^m+1)q^{m-1-\mu}\langle\mu-1\rangle} \\ &+ \sum_{i=3}^{m-1}\sum_{\mu=0}^{i-1} D_{i\mu} Y^{q^{m-1-\mu+i}\langle m-1+\mu-i\rangle + q^{m-1-\mu}\langle\mu-1\rangle} T_i^{q^{i-1-\mu}}. \end{aligned}$$

Now upon letting

$$\widetilde{T}_i = Y^{q^m\langle m-1-i\rangle} T_i \quad \text{for } 2 \le i \le m-1$$

we get

$$\begin{aligned} g =& D_{20} \widetilde{T}_2^q + D_{21} Y^{(q^m+1)q^{m-2}} \widetilde{T}_2 \\ &+ \sum_{\mu=0}^{m-1} D_{m\mu} Y^{(q^m+1)q^{m-1-\mu}\langle\mu-1\rangle} \\ &+ \sum_{i=3}^{m-1}\sum_{\mu=0}^{i-1} D_{i\mu} Y^{(q^m+1)q^{m-1-\mu}\langle\mu-1\rangle} \widetilde{T}_i^{q^{i-1-\mu}}. \end{aligned}$$

Hence upon letting

$$\widehat{Y} = Y^{q^m+1}$$

and

$$\widehat{T}_i = \begin{cases} \widetilde{T}_i & \text{for } 2 \le i \le m-1, \\ 1 & \text{for } i = m, \end{cases}$$

we get

$$g = D_{20}\widehat{T}_2^q + D_{21}\widehat{Y}^{q^{m-2}}\widehat{T}_2 + \sum_{i=3}^{m}\sum_{\mu=0}^{i-1} D_{i\mu}\widehat{Y}^{q^{m-1-\mu}\langle\mu-1\rangle}\widehat{T}_i^{q^{i-1-\mu}}.$$

Expanding the exponents of $\widehat{Y}$ we get

$$g = D_{20}\widehat{T}_2^q + D_{21}\widehat{Y}^{q^{m-2}}\widehat{T}_2 + \sum_{i=3}^{m}\sum_{\mu=0}^{i-1} D_{i\mu}\widehat{Y}^{q^{m-1-\mu}+\cdots+q^{m-2}}\widehat{T}_i^{q^{i-1-\mu}}$$

where the dots indicate geometric series with ratio q. Upon letting

$$\widehat{D}_{i\mu} = D_{i,i-1-\mu} \quad \text{for } 2 \le i \le m \text{ and } 0 \le \mu \le i-1$$

we get

$$\widehat{D}_{i\mu} = \frac{Z^{q^m\langle\mu-1\rangle+\langle m-1-i+\mu\rangle} - Z^{\langle m-2\rangle}}{Z-1} \quad \text{for } 2 \le i \le m \text{ and } 0 \le \mu \le i-1$$

and arranging the terms according to descending powers of $\widehat{Y}$ we get

$$g = \widehat{D}_{20}\widehat{Y}^{q^{m-2}}\widehat{T}_2 + \widehat{D}_{21}\widehat{T}_2^q + \sum_{i=3}^{m}\sum_{\mu=0}^{i-1} \widehat{D}_{i\mu}\widehat{Y}^{q^{m-i+\mu}+\cdots+q^{m-2}}\widehat{T}_i^{q^{\mu}}$$

and simplifying the expression of $\widehat{D}_{20}$ and $\widehat{D}_{21}$ we have

$$\widehat{D}_{20} = -\frac{Z^{\langle m-3\rangle}\left(Z^{q^{m-2}}-1\right)}{Z-1} \quad \text{and} \quad \widehat{D}_{21} = \frac{Z^{\langle m-2\rangle}\left(Z^{q^m}-1\right)}{Z-1}.$$

For a moment, assuming $m = 3$, we note that

$$g = \widehat{D}_{20}\widehat{Y}^q\widehat{T}_2 + \widehat{D}_{21}\widehat{T}_2^q + \widehat{D}_{30}\widehat{Y}^{1+q} + \widehat{D}_{31}\widehat{Y}^q + \widehat{D}_{32}$$

where

$$\widehat{D}_{20} = -\frac{Z\left(Z^q-1\right)}{Z-1} \quad \text{and} \quad \widehat{D}_{21} = \frac{Z^{1+q}\left(Z^{q^3}-1\right)}{Z-1} \quad \text{and} \quad \widehat{D}_{30} = -\frac{\left(Z^{1+q}-1\right)}{Z-1}$$

and

$$\widehat{D}_{31} = \frac{Z^{1+q}\left(Z^{q^3-q}-1\right)}{Z-1} \quad \text{and} \quad \widehat{D}_{32} = \frac{Z^{1+q}\left(Z^{q^3+q^4}-1\right)}{Z-1}$$

and to factor g we try to find a $\widehat{T}_2$-root $E_{30}\widehat{Y} + E_{31}$ of g. To do this we first put

$$E_{30} = \frac{\widehat{D}_{30}}{-\widehat{D}_{20}} = \frac{\frac{\left(Z^{1+q}-1\right)}{Z-1}}{\frac{-Z\left(Z^q-1\right)}{Z-1}} = \frac{\left(Z^{1+q}-1\right)}{-Z\left(Z^q-1\right)},$$

then we put

$$
\begin{aligned}
E_{31} &= \frac{\widehat{D}_{31} + \widehat{D}_{21} E_{30}^q}{-\widehat{D}_{20}} \\
&= \frac{\frac{Z^{1+q}\left(Z^{q^3-q}-1\right)}{Z-1} + \frac{Z^{1+q}\left(Z^{q^3}-1\right)}{Z-1}\left(\frac{\left(Z^{1+q}-1\right)}{-Z(Z^q-1)}\right)^q}{\frac{Z(Z^q-1)}{Z-1}} \\
&= \frac{Z^q\left(Z^{q^3-q}-1\right)\left(Z^{q^2}-1\right) - \left(Z^{q^3}-1\right)\left(Z^{q^2+q}-1\right)}{\left(Z^q-1\right)\left(Z^{q^2}-1\right)} \\
&= \frac{\left(Z^{q^3+q^2} - Z^{q^3} - Z^{q^2+q} + Z^q\right) - \left(Z^{q^3+q^2+q} - Z^{q^3} - Z^{q^2+q} + 1\right)}{\left(Z^q-1\right)\left(Z^{q^2}-1\right)} \\
&= \frac{Z^{q^3+q^2} - Z^{q^3q^2+q} + Z^q - 1}{\left(Z^q-1\right)\left(Z^{q^2}-1\right)} \\
&= \frac{\left(Z^q-1\right)\left(-Z^{q^3+q^2}+1\right)}{\left(Z^q-1\right)\left(Z^{q^2}-1\right)} \\
&= \frac{\left(-Z^{q^3+q^2}+1\right)}{\left(Z^{q^2}-1\right)},
\end{aligned}
$$

and finally we calculate the term free of $\widehat{Y}$ to be

$$
\begin{aligned}
\widehat{D}_{32} + \widehat{D}_{21} E_{31}^q &= \frac{Z^{1+q}\left(Z^{q^3+q^4}-1\right)}{Z-1} + \left(\frac{Z^{1+q}\left(Z^{q^3}-1\right)}{Z-1}\right)\left(\frac{\left(-Z^{q^3+q^2}+1\right)}{\left(Z^{q^2}-1\right)}\right)^q \\
&= \frac{Z^{1+q}\left(Z^{q^3+q^4}-1\right)}{Z-1} + \frac{Z^{1+q}\left(-Z^{q^3+q^4}+1\right)}{Z-1} \\
&= 0.
\end{aligned}
$$

Alternatively, for "the fictitious term" E_{32}, we have

$$
\begin{aligned}
E_{32} = \frac{\widehat{D}_{32} + \widehat{D}_{21} E_{31}^q}{-\widehat{D}_{20}} &= \frac{\widehat{D}_{32}}{-\widehat{D}_{20}} + \left(\frac{\widehat{D}_{21}}{-\widehat{D}_{20}}\right)\left(\frac{\widehat{D}_{31} + \widehat{D}_{21} E_{30}^q}{-\widehat{D}_{20}}\right)^q \\
&= -\frac{\widehat{D}_{32}}{\widehat{D}_{20}} + \frac{\widehat{D}_{21}\widehat{D}_{31}^q}{\widehat{D}_{20}^{1+q}} + \frac{\widehat{D}_{21}^{1+q} E_{30}^{q^2}}{\widehat{D}_{20}^{1+q}} \\
&= -\frac{\widehat{D}_{32}}{\widehat{D}_{20}} + \frac{\widehat{D}_{21}\widehat{D}_{31}^q}{\widehat{D}_{20}^{1+q}} - \frac{\widehat{D}_{21}^{1+q}\widehat{D}_{30}^{q^2}}{\widehat{D}_{20}^{1+q+q^2}}
\end{aligned}
$$

and by substituting the values of $\widehat{D}_{20}$, $\widehat{D}_{21}$, $\widehat{D}_{30}$, $\widehat{D}_{31}$, $\widehat{D}_{32}$, we see this to be 0.

Now, without assuming $m = 3$, but henceforth again assuming $m > 2$, to factor g, for any $3 \le i \le m$, we try to find a $\widehat{T}_2$-root

$$
\sum_{\mu=0}^{i-2} E_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\cdots+q^{m-3}} \widehat{T}_i^{q^\mu}
$$

of

$$\widehat{D}_{20}\widehat{Y}^{q^{m-2}}\widehat{T}_2+\widehat{D}_{21}\widehat{T}_2^{q}+\sum_{\mu=0}^{i-1}\widehat{D}_{i\mu}\widehat{Y}^{q^{m-i+\mu}+\cdots+q^{m-2}}\widehat{T}_i^{q^{\mu}},$$

i.e., we try to find $E_{i\mu}$ in $\mathrm{GF}(p)(Z)$ such that

$$\begin{aligned}\sum_{\mu=0}^{i-1}\widehat{D}_{i\mu}\widehat{Y}^{q^{m-i+\mu}+\cdots+q^{m-2}}\widehat{T}_i^{q^{\mu}} =& -\widehat{D}_{20}\widehat{Y}^{q^{m-2}}\left(\sum_{\mu=0}^{i-2}E_{i\mu}\widehat{Y}^{q^{m-i+\mu}+\cdots+q^{m-3}}\widehat{T}_i^{q^{\mu}}\right)\\ &-\widehat{D}_{21}\left(\sum_{\mu=0}^{i-2}E_{i\mu}\widehat{Y}^{q^{m-i+\mu}+\cdots+q^{m-3}}\widehat{T}_i^{q^{\mu}}\right)^{q}.\end{aligned}$$

Equating coefficients of

$$\widehat{Y}^{q^{m-i+\mu}+\cdots+q^{m-2}}\widehat{T}_i^{q^{\mu}}$$

to zero, we try to find $E_{i\mu}$ in $\mathrm{GF}(p)(Z)$ such that

$$\widehat{D}_{i\mu}=\begin{cases}-\widehat{D}_{20}E_{i\mu} & \text{for } \mu=0,\\ -\widehat{D}_{20}E_{i\mu}-\widehat{D}_{21}E_{i,\mu-1}^{q} & \text{for } 1\le\mu\le i-2,\\ -\widehat{D}_{21}E_{i,\mu-1}^{q} & \text{for } \mu=i-1.\end{cases}$$

Since $\widehat{D}_{20}\neq 0$, we can successively find the values of $E_{i\mu}$ for $0\le\mu\le i-2$ by solving all except the last equation, and then get a condition by substituting these in the last equation. Upon letting

$$J_{i\mu}=\sum_{j=0}^{\mu}(-1)^{\langle\mu-j\rangle}\frac{\widehat{D}_{21}^{\langle\mu-j-1\rangle}\widehat{D}_{ij}^{q^{\mu-j}}}{\widehat{D}_{20}^{\langle\mu-j\rangle}}\qquad\text{for } 0\le\mu\le i-1$$

these values are

$$E_{i\mu}=J_{i\mu}\qquad\text{for } 0\le\mu\le i-2$$

and the condition is

$$J_{i,i-1}=0.$$

Substituting the simplified expressions of $\widehat{D}_{20}$ and $\widehat{D}_{21}$, for $0\le\mu\le i-1$ and $0\le j\le\mu$ we get

$$\begin{aligned}\frac{\widehat{D}_{21}^{\langle\mu-j-1\rangle}}{\widehat{D}_{20}^{\langle\mu-j\rangle}} &= \left[\frac{Z^{\langle m-2\rangle}\left(Z^{q^m}-1\right)}{Z-1}\right]^{\langle\mu-j-1\rangle}\left[\frac{Z-1}{-Z^{\langle m-3\rangle}\left(Z^{q^{m-2}}-1\right)}\right]^{\langle\mu-j\rangle}\\ &= \frac{Z^{\langle m-2\rangle\langle\mu-j-1\rangle-\langle m-3\rangle\langle\mu-j\rangle}\prod_{l=0}^{\mu-j-1}\left(Z^{q^m}-1\right)^{q^l}}{(-1)^{\langle\mu-j\rangle}(Z-1)^{-q^{\mu-j}}\prod_{l=0}^{\mu-j}\left(Z^{q^{m-2}}-1\right)^{q^l}}\\ &= \frac{Z^{\langle m-2\rangle\langle\mu-j-1\rangle-\langle m-3\rangle\langle\mu-j\rangle}\prod_{l=0}^{\mu-j-1}\left(Z^{q^{m+l}}-1\right)}{(-1)^{\langle\mu-j\rangle}(Z-1)^{-q^{\mu-j}}\prod_{l=0}^{\mu-j}\left(Z^{q^{m-2+l}}-1\right)}\\ &= \frac{Z^{\langle m-2\rangle\langle\mu-j-1\rangle-\langle m-3\rangle\langle\mu-j\rangle}\prod_{l=m}^{m+\mu-j-1}\left(Z^{q^l}-1\right)}{(-1)^{\langle\mu-j\rangle}(Z-1)^{-q^{\mu-j}}\prod_{l=m-2}^{m+\mu-j-2}\left(Z^{q^l}-1\right)}\\ &= \frac{Z^{\langle m-2\rangle\langle\mu-j-1\rangle-\langle m-3\rangle\langle\mu-j\rangle}\left(Z^{q^{m+\mu-j-1}}-1\right)}{(-1)^{\langle\mu-j\rangle}(Z-1)^{-q^{\mu-j}}\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)}\end{aligned}$$

where, for the last equation, a separate but trivial argument may be made in the case of $j = \mu$ by noting that then the extra (purposefully inserted) term $\left(Z^{q^{m+\mu-j-1}} - 1\right)$ in the numerator equals the extra term $\left(Z^{q^{m-1}} - 1\right)$ in the denominator. Therefore by substituting the values of $\widehat{D}_{ij}$, for $0 \le \mu \le i-1$ we get

$$
\begin{aligned}
J_{i\mu} = \sum_{j=0}^{\mu} (-1)^{\langle \mu-j\rangle} & \left[\frac{Z^{\langle m-2\rangle\langle \mu-j-1\rangle - \langle m-3\rangle\langle \mu-j\rangle}\left(Z^{q^{m+\mu-j-1}} - 1\right)}{(-1)^{\langle \mu-j\rangle}(Z-1)^{-q^{\mu-j}}\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \right] \times \\
& \times \left[\frac{Z^{q^m\langle j-1\rangle + \langle m-1-i+j\rangle} - Z^{\langle m-2\rangle}}{Z-1} \right]^{q^{\mu-j}} \\
= & \sum_{j=0}^{\mu} \frac{Z^{\langle m-2\rangle\langle \mu-j-1\rangle - \langle m-3\rangle\langle \mu-j\rangle + q^{m+\mu-j}\langle j-1\rangle + q^{\mu-j}\langle m-1-i+j\rangle}\left(Z^{q^{m+\mu-j-1}} - 1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
& - \sum_{j=0}^{\mu} \frac{Z^{\langle m-2\rangle\langle \mu-j-1\rangle - \langle m-3\rangle\langle \mu-j\rangle + q^{\mu-j}\langle m-2\rangle}\left(Z^{q^{m+\mu-j-1}} - 1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)}
\end{aligned}
$$

where

$$
\begin{aligned}
& \text{the first exponent of } Z \text{ in the last summation} \\
& = \langle m-2\rangle\langle \mu-j-1\rangle - \langle m-3\rangle\langle \mu-j\rangle + q^{\mu-j}\langle m-2\rangle \\
& = [\langle m-2\rangle(\langle \mu-j\rangle - q^{\mu-j}) - (\langle m-2\rangle - q^{m-2})\langle \mu-j\rangle] + q^{\mu-j}\langle m-2\rangle \\
& = q^{m-2}\langle \mu-j\rangle
\end{aligned}
$$

and

$$
\begin{aligned}
& \text{the first exponent of } Z \text{ in the last but one summation} \\
& = \langle m-2\rangle\langle \mu-j-1\rangle - \langle m-3\rangle\langle \mu-j\rangle + q^{m+\mu-j}\langle j-1\rangle + q^{\mu-j}\langle m-1-i+j\rangle \\
& = [\langle m-2\rangle(\langle \mu-j\rangle - q^{\mu-j}) - (\langle m-2\rangle - q^{m-2})\langle \mu-j\rangle] \\
& \qquad + q^{m+\mu-j}\langle j-1\rangle + q^{\mu-j}\langle m-1-i+j\rangle \\
& = [q^{m-2}\langle \mu-j\rangle - q^{\mu-j}\langle m-2\rangle] + q^{m+\mu-j}\langle j-1\rangle + q^{\mu-j}\langle m-1-i+j\rangle \\
& = [q^{m-2}\langle \mu-j\rangle + q^{m+\mu-j-1} + q^{m+\mu-j}\langle j-1\rangle] - q^{\mu-j}[\langle m-2\rangle - \langle m-1-i+j\rangle] \\
& \qquad - q^{m+\mu-j-1} \\
& = q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-2-j\rangle - q^{m+\mu-j-1}.
\end{aligned}
$$

Hence

$$\begin{aligned}
J_{i\mu} &= \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-2-j\rangle - q^{m+\mu-j-1}}\left(Z^{q^{m+\mu-j-1}}-1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&\quad - \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu-j\rangle}\left(Z^{q^{m+\mu-j-1}}-1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&= \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-2-j\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} - \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-1-j\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&\quad - \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu-j+1\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} + \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu-j\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&= \sum_{j=1}^{\mu+1} \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-1-j\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} - \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-1-j\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&\quad - \sum_{j=0}^{\mu} \frac{Z^{q^{m-2}\langle \mu-j+1\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} + \sum_{j=1}^{\mu+1} \frac{Z^{q^{m-2}\langle \mu-j+1\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&= \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-2-\mu\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} - \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-1\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&\quad - \frac{Z^{q^{m-2}\langle \mu+1\rangle}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} + \frac{Z^{q^{m-2}}}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&= \frac{Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-1\rangle}\left(Z^{q^{m+\mu-i}(\langle i-1\rangle - \langle i-2-\mu\rangle)}-1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&\quad - \frac{Z^{q^{m-2}}\left(Z^{q^{m-2}(\langle \mu+1\rangle - 1)}-1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&= \frac{\left(Z^{q^{m-2}\langle \mu+1\rangle - q^{m+\mu-i}\langle i-1\rangle} - Z^{q^{m-2}}\right)\left(Z^{q^{m-1}\langle \mu\rangle}-1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)}.
\end{aligned}$$

Therefore

$$\begin{aligned}
J_{i\mu} &= \frac{\left(Z^{-q^{m+\mu-i}\langle i-3-\mu\rangle} - Z^{q^{m-2}}\right)\left(Z^{q^{m-1}\langle \mu\rangle}-1\right)}{\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \\
&= \frac{-\left(Z^{q^{m+\mu-i}\langle i-2-\mu\rangle}-1\right)\left(Z^{q^{m-1}\langle \mu\rangle}-1\right)}{Z^{q^{m+\mu-i}\langle i-3-\mu\rangle}\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)}.
\end{aligned}$$

Now by putting $\mu = i-1$ we see that

$$J_{i,i-1} = 0.$$

It follows that, upon letting

$$E_{i\mu} = \frac{-\left(Z^{q^{m+\mu-i}\langle i-2-\mu\rangle}-1\right)\left(Z^{q^{m-1}\langle \mu\rangle}-1\right)}{Z^{q^{m+\mu-i}\langle i-3-\mu\rangle}\left(Z^{q^{m-2}}-1\right)\left(Z^{q^{m-1}}-1\right)} \quad \text{for } 3 \le i \le m \text{ and } 0 \le \mu \le i-1$$

we have

$$\begin{aligned}
&\sum_{\mu=0}^{i-1} \widehat{D}_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-2}} \widehat{T}_i^{q^\mu} \\
&\qquad = -\widehat{D}_{20} \widehat{Y}^{q^{m-2}} \left(\sum_{\mu=0}^{i-2} E_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-3}} \widehat{T}_i^{q^\mu} \right) \\
&\qquad\quad - \widehat{D}_{21} \left(\sum_{\mu=0}^{i-2} E_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-3}} \widehat{T}_i^{q^\mu} \right)^q \quad \text{for } 3 \le i \le m.
\end{aligned}$$

By q-linearity, summing the above equations we get

$$\begin{aligned}
&\sum_{i=3}^{m} \sum_{\mu=0}^{i-1} \widehat{D}_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-2}} \widehat{T}_i^{q^\mu} \\
&\qquad = -\widehat{D}_{20} \widehat{Y}^{q^{m-2}} \left(\sum_{i=3}^{m} \sum_{\mu=0}^{i-2} E_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-3}} \widehat{T}_i^{q^\mu} \right) \\
&\qquad\quad - \widehat{D}_{21} \left(\sum_{i=3}^{m} \sum_{\mu=0}^{i-2} E_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-3}} \widehat{T}_i^{q^\mu} \right)^q.
\end{aligned}$$

Therefore recalling that

$$\widehat{D}_{20} = -\frac{Z^{\langle m-3\rangle}\left(Z^{q^{m-2}}-1\right)}{Z-1} \quad \text{and} \quad \widehat{D}_{21} = \frac{Z^{\langle m-2\rangle}\left(Z^{q^m}-1\right)}{Z-1}$$

and letting

$$D = -\widehat{D}_{21}/\widehat{D}_{20}^q \quad \text{and} \quad E = \widehat{D}_{20} \sum_{i=3}^{m} \sum_{\mu=0}^{i-2} E_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-3}} \widehat{T}_i^{q^\mu}$$

we get

$$D = Z(Z-1)^{(q^{m-1}+1)(q-1)}$$

and

$$E = \sum_{i=3}^{m} \sum_{\mu=0}^{i-2} \left(\frac{Z^{q^{m+\mu-i}\langle i-2-\mu\rangle}-1}{Z-1} \right) \left(\frac{Z^{\langle \mu\rangle}-1}{Z-1} \right)^{q^{m-1}} Z^{\langle m+\mu-i-1\rangle} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-3}} \widehat{T}_i^{q^\mu}$$

and

$$-DE^q + \widehat{Y}^{q^{m-2}} E + \sum_{i=3}^{m} \sum_{\mu=0}^{i-1} \widehat{D}_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-2}} \widehat{T}_i^{q^\mu} = 0.$$

The above equation says that $E/\widehat{D}_{20}$ is a $\widehat{T}_2$-root of

$$g = \widehat{D}_{21} \widehat{T}_2^q + \widehat{D}_{20} \widehat{Y}^{q^{m-2}} \widehat{T}_2 + \sum_{i=3}^{m} \sum_{\mu=0}^{i-1} \widehat{D}_{i\mu} \widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-2}} \widehat{T}_i^{q^\mu}.$$

Hence upon letting

$$g' = E - \widehat{D}_{20}\widehat{T}_2 \qquad \text{and} \qquad g'' = DE^{q-1} - \widehat{Y}^{q^{m-2}} + \sum_{l=1}^{q-1} D\widehat{D}_{20}^{l}E^{q-1-l}\widehat{T}_2^{l}$$

we obtain

$$\begin{aligned} g'g'' &= \left(DE^{q} - \widehat{Y}^{q^{m-2}}E\right) + \sum_{l=1}^{q-1} D\widehat{D}_{20}^{l}E^{q-l}\widehat{T}_2^{l} \\ &\quad - \left(D\widehat{D}_{20}E^{q-1} - \widehat{D}_{20}\widehat{Y}^{q^{m-2}}\right)\widehat{T}_2 - \sum_{l=2}^{q} D\widehat{D}_{20}^{l}E^{q-l}\widehat{T}_2^{l} \\ &= \left(DE^{q} - \widehat{Y}^{q^{m-2}}E\right) + \left(D\widehat{D}_{20}E^{q-1}\right)\widehat{T}_2 + \sum_{l=2}^{q-1} D\widehat{D}_{20}^{l}E^{q-l}\widehat{T}_2^{l} \\ &\quad - \left(D\widehat{D}_{20}E^{q-1} - \widehat{D}_{20}\widehat{Y}^{q^{m-2}}\right)\widehat{T}_2 - \left(\sum_{l=2}^{q-1} D\widehat{D}_{20}^{l}E^{q-l}\widehat{T}_2^{l}\right) - D\widehat{D}_{20}^{q}\widehat{T}_2^{q} \\ &= \widehat{D}_{21}\widehat{T}_2^{q} + \widehat{D}_{20}\widehat{Y}^{q^{m-2}}\widehat{T}_2 + \left(DE^{q} - \widehat{Y}^{q^{m-2}}E\right) \\ &= \widehat{D}_{21}\widehat{T}_2^{q} + \widehat{D}_{20}\widehat{Y}^{q^{m-2}}\widehat{T}_2 + \sum_{i=3}^{m}\sum_{\mu=0}^{i-1} \widehat{D}_{i\mu}\widehat{Y}^{q^{m-i+\mu}+\dots+q^{m-2}}\widehat{T}_i^{q^{\mu}} \\ &= g. \end{aligned}$$

Thus we get the factorization

$$g = g'g'' \tag{4.1}$$

where by substituting the values of $\widehat{Y}$ and $\widehat{T}_i$ we have

(4.2)

$$\begin{aligned} g =& \widehat{D}_{21}Y^{q^{m+1}\langle m-3\rangle}T_2^{q} + \widehat{D}_{20}\widehat{Y}^{q^{m-2}+q^{m}\langle m-2\rangle}T_2 + \sum_{\mu=0}^{m-1}\widehat{D}_{m\mu}Y^{(q^m+1)q^{\mu}\langle m-2-\mu\rangle} \\ &+ \sum_{i=3}^{m-1}\sum_{\mu=0}^{i-1}\widehat{D}_{i\mu}Y^{(q^m+1)q^{m-i+\mu}\langle i-2-\mu\rangle+q^{m+\mu}\langle m-1-i\rangle}T_i^{q^{\mu}} \end{aligned}$$

and

$$g' = E - \widehat{D}_{20}Y^{q^{m}\langle m-3\rangle}T_2 \tag{4.3}$$

and

$$g'' = DE^{q-1} - Y^{(q^m+1)q^{m-2}} + \sum_{l=1}^{q-1} D\widehat{D}_{20}^{l}E^{q-1-l}Y^{q^{m}\langle m-3\rangle l}T_2^{l} \tag{4.4}$$

and

(4.5)

$$E = \sum_{\mu=0}^{m-2}\widehat{E}_{m\mu}Y^{(q^m+1)q^{\mu}\langle m-3-\mu\rangle} + \sum_{i=3}^{m-1}\sum_{\mu=0}^{i-2}\widehat{E}_{i\mu}Y^{(q^m+1)q^{m-i+\mu}\langle i-3-\mu\rangle+q^{m+\mu}\langle m-1-i\rangle}T_i^{q^{\mu}}$$

with

$$\widehat{E}_{i\mu} = \left(\frac{Z^{q^{m+\mu-i}\langle i-2-\mu\rangle}-1}{Z-1}\right)\left(\frac{Z^{\langle\mu\rangle}-1}{Z-1}\right)^{q^{m-1}} Z^{\langle m+\mu-i-1\rangle} \tag{4.6}$$
$$\text{for } 3 \le i \le m \text{ and } 0 \le \mu \le i-2,$$

and where we recall that

$$\widehat{D}_{i\mu} = \frac{Z^{q^m\langle\mu-1\rangle+\langle m-1-i+\mu\rangle} - Z^{\langle m-2\rangle}}{Z-1} \qquad \text{for } 3 \le i \le m \text{ and } 0 \le \mu \le i-1 \tag{4.7}$$

and

$$\widehat{D}_{20} = -\frac{Z^{\langle m-3\rangle}\left(Z^{q^{m-2}}-1\right)}{Z-1} \quad \text{and} \quad \widehat{D}_{21} = \frac{Z^{\langle m-2\rangle}\left(Z^{q^m}-1\right)}{Z-1} \tag{4.8}$$

and

$$D = -\widehat{D}_{21}/\widehat{D}_{20}^{q} = Z(Z-1)^{(q^{m-1}+1)(q-1)}. \tag{4.9}$$

By (4.6) we see that, for $3 \le i \le m$ and $0 \le \mu \le i-2$, $\widehat{E}_{i\mu}$ is a monic polynomial of degree

$$q^{m+\mu-i}\langle i-2-\mu\rangle - 1 + q^{m-1}(\langle\mu\rangle - 1) + \langle m+\mu-i-1\rangle = q\langle m-3\rangle + q^m\langle\mu-1\rangle$$

in Z with coefficients on $\mathrm{GF}(p)$. Therefore, since $Y^{(q^m+1)q^\mu\langle m-3-\mu\rangle} = 1$ for $\mu = m-2$, by (4.5) we see that E is a monic polynomial of degree

$$q\langle m-3\rangle + q^m\langle (m-2)-1\rangle = q(q^{m-1}+1)\langle m-3\rangle$$

in Z with coefficients in $\mathrm{GF}(p)[Y, T_2, \dots, T_{m-1}]$. Consequently, in view of (4.3) and (4.8) we conclude that g' is a monic polynomial of degree $q(q^{m-1}+1)\langle m-3\rangle$ in Z with coefficients in $\mathrm{GF}(p)[Y, T_2, \dots, T_{m-1}]$. Obviously g is a monic polynomial of degree

$$(\deg_Y \overline{f}) - 1 = (q^m+1)\langle m-2\rangle - 1 = q^m\langle m-2\rangle + q\langle m-3\rangle$$

in Z with coefficients in $\mathrm{GF}(p)[Y, T_2, \dots, T_{m-1}]$. Hence in view of (4.1), (4.4), (4.8) and (4.9) we see that g'' is a monic polynomial of degree

$$q^m\langle m-2\rangle + q\langle m-3\rangle - q(q^{m-1}+1)\langle m-3\rangle = q^{2m-2}$$

in Z with coefficients in $\mathrm{GF}(p)[Y, T_2, \dots, T_{m-1}]$. Thus

(4.10)
$$\begin{cases} g' \text{ and } g'' \text{ are monic polynomials of degrees } q(q^{m-1}+1)\langle m-3\rangle \text{ and } q^{2m-2} \\ \text{in } Z \text{ with coefficients in } \mathrm{GF}(p)[Y, T_2, \dots, T_{m-1}] \text{ respectively.} \end{cases}$$

Without assuming $m > 2$, for $1 \le e \le m-1$, let f'_e and g_e denote the members of $\mathrm{GF}(p)[Y, Z, T_2, \dots, T_e]$ obtained by putting $T_i = 0$ for all $i > e$ in f' and g

respectively. Then f'_e is the twisted derivative of $\overline{f}_e$, and dividing the Z-roots of f'_e by Y and afterwards changing Y to $1/Y$ we get g_e which is a monic polynomial of degree $q^m\langle m-2\rangle + q\langle m-3\rangle$ in Z with coefficients in $\mathrm{GF}(p)[Y, T_2, \ldots, T_e]$.

Again henceforth assuming $m > 2$, for $1 \le e \le m-1$, let g'_e and g''_e denote the members of $\mathrm{GF}(p)[Y, Z, T_2, \ldots, T_e]$ obtained by putting $T_i = 0$ for all $i > e$ in g' and g'' respectively. Then in view of (4.1) and (4.10),

$$(4.11)\quad \begin{cases} \text{for } 1 \le e \le m-1 \text{ we have } g_e = g'_e g''_e \text{ where } g'_e \text{ and } g''_e \text{ are} \\ \text{monic polynomials of degrees } q(q^{m-1}+1)\langle m-3\rangle \text{ and } q^{2m-2} \text{ in } Z \\ \text{with coefficients in } \mathrm{GF}(p)[Y, T_2, \ldots, T_e] \text{ respectively.} \end{cases}$$

By (4.2), (4.3), (4.5), (4.6), (4.7) and (4.8) we have

$$g_2 = A_2 T_2^q - B_2 T_2 + C_2 \quad \text{and} \quad g'_2 = A'_2 T_2 + B'_2$$

where $A_2, B_2, C_2, A'_2, B'_2$ are the nonzero elements in $\mathrm{GF}(p)[Y, Z]$ given by

$$A_2 = \widehat{D}_{21} Y^{q^{m+1}\langle m-3\rangle} \quad \text{and} \quad B_2 = -\widehat{D}_{20} \widehat{Y}^{q^{m-2}+q^m\langle m-2\rangle}$$

and

$$C_2 = \sum_{\mu=0}^{m-1} \widehat{D}_{m\mu} Y^{(q^m+1)q^\mu\langle m-2-\mu\rangle}$$

and

$$A'_2 = -\widehat{D}_{20} Y^{q^m\langle m-3\rangle} \quad \text{and} \quad B'_2 = \sum_{\mu=0}^{m-2} \widehat{E}_{m\mu} Y^{(q^m+1)q^\mu\langle m-3-\mu\rangle}.$$

By letting I to be the Z-adic valuation of $Q = k_p(Y, Z)$, i.e., the real discrete valuation whose valuation ring is the localization of $k_p[Y, Z]$ at the principal prime ideal generated by Z, we see that $I(A_2) = \langle m-2\rangle$ and $I(B_2) = \langle m-3\rangle$ and hence $I(B_2/A_2) = \langle m-3\rangle - \langle m-2\rangle = -q^{m-2}$ and therefore $\mathrm{GCD}(q-1, I(B_2/A_2)) = 1$. In view of (4.7) and (4.8) we also see that A_2 and C_2 have no nonconstant common factor in $k_p[Y, Z]$, because $\mu = m-1$ gives the nonzero term $\widehat{D}_{m,m-1}$ of C_2 which is independent of Y, and $\mu = 0$ gives the highest Y-degree term of C_2 and its coefficient is

$$\widehat{D}_{m0} = \frac{1 - Z^{\langle m-2\rangle}}{Z-1}.$$

Therefore by Lemmas (4.2) and (4.3) of [A05] we conclude that

(4.12) the polynomials g'_2 and g''_2 are irreducible in $k_p(Y, T_2)[Z]$.

As an immediate consequence of (4.12) we see that

$$(4.13)\quad \begin{cases} \text{the polynomials } g' \text{ and } g'' \text{ are irreducible in } k_p(Y, T_2, \ldots, T_{m-1})[Z] \\ \text{and, for } 2 \le e \le m-1, \\ \text{the polynomials } g'_e \text{ and } g''_e \text{ are irreducible in } k_p(Y, T_2, \ldots, T_e)[Z]. \end{cases}$$

Note that

(4.14) in (4.1) to (4.13) we assumed $m > 2$.

Recall that $\overline{f}_e$ is irreducible in $k_p(T_1, T_2, \ldots, T_e)[Y]$, its twisted derivative is $f'_e(Y, Z)$, and g_e is obtained by dividing the Z-roots of $f'_e(Y, Z)$ by Y and then changing Y to $1/Y$; therefore by (4.0), (4.1), (4.10), (4.11), (4.13) and (4.14) we get the following

Theorem (4.15). *If $m = 2$ then $Gal(\overline{f}, k_p(T_1)) = Gal(\overline{f}_1, k_p(T_1))$ is a 2-transitive permutation group of degree $q^m + 1$. If $m > 2$ and $2 \le e \le m-1$ then $Gal(\overline{f}_e, k_p(T_1, \dots, T_e))$ is a transitive permutation group of Rank 3 with subdegrees 1, $q(q^{m-1}+1)\langle m-3\rangle$ and q^{2m-2}. Hence in particular, if $m > 2$ then $Gal(\overline{f}, k_p(T_1, \dots, T_{m-1}))$ is a transitive permutation group of Rank 3 with subdegrees 1, $q(q^{m-1}+1)\langle m-3\rangle$ and q^{2m-2}.*

Notation. Recall that $<$ denotes a subgroup, and $\triangleleft$ denotes a normal subgroup. Let the groups $\mathrm{SL}(m,q) \triangleleft \mathrm{GL}(m,q) \triangleleft \Gamma\mathrm{L}(m,q)$ and $\mathrm{PSL}(m,q) \triangleleft \mathrm{PGL}(m,q) \triangleleft \mathrm{P}\Gamma\mathrm{L}(m,q)$ and their actions on $\mathrm{GF}(q)^m$ and $\mathcal{P}(\mathrm{GF}(q)^m)$ be as on pages 78-80 of [A03]. Let

$$\Theta_m : \Gamma\mathrm{L}(m,q) \to \mathrm{P}\Gamma\mathrm{L}(m,q) = \Gamma\mathrm{L}(m,q)/\mathrm{GF}(q)^*$$

be the canonical epimorphism where we identify the multiplicative group $\mathrm{GF}(q)^*$ with scalar matrices, which constitute the center of $\mathrm{GL}(m,q)$.

Now in view of Proposition 3.1 of [A04], by (3.0), (3.1), (3.4) and (3.5) we get the following

Theorem (4.16). *Assuming $GF(q) \subset k_p$, for $1 \le e \le m-1$, in a natural manner we may regard*

$$Gal(\phi_e^-, k_p(T_1, \dots, T_e)) < GL(2m,q) \text{ and } Gal(f_e^-, k_p(T_1, \dots, T_e)) < PGL(2m,q)$$

and then

$$\Theta_{2m}(Gal(\phi_e^-, k_p(T_1, \dots, T_e))) = Gal(f_e^-, k_p(T_1, \dots, T_e))$$

and $Gal(f_e^-, k_p(T_1, \dots, T_e))$ has two or three orbits on $\mathcal{P}(GF(q)^{2m})$ of sizes $(q^m+1)\langle m-2\rangle$, $q^{m-1}(q^m+1)$ or $(q^m+1)\langle m-2\rangle$, $q^{m-1}(q^m+1)/2$, $q^{m-1}(q^m+1)/2$ according as $p = 2$ or $p \ne 2$. In particular, again assuming $GF(q) \subset k_p$, in a natural manner we may regard

$$Gal(\phi^-, k_p(T_1, \dots, T_{m-1})) < GL(2m,q)$$

and

$$Gal(f^-, k_p(T_1, \dots, T_{m-1})) < PGL(2m,q)$$

and then

$$\Theta_{2m}(Gal(\phi^-, k_p(T_1, \dots, T_{m-1}))) = Gal(f^-, k_p(T_1, \dots, T_{m-1}))$$

and $Gal(f^-, k_p(T_1, \dots, T_e))$ has two or three orbits on $\mathcal{P}(GF(q)^{2m})$ of sizes $(q^m+1)\langle m-2\rangle$, $q^{m-1}(q^m+1)$ or $(q^m+1)\langle m-2\rangle$, $q^{m-1}(q^m+1)/2$, $q^{m-1}(q^m+1)/2$ according as $p = 2$ or $p \ne 2$.

Recall that a *quasi-p group* is a finite group which is generated by its p-Sylow subgroups. Since $\mathrm{Disc}_Y f_e^- = -1 = \mathrm{Disc}_Y \phi_e^-$ for $1 \le e \le m-1$, by the techniques of the proofs of Proposition 6 of [A01] and Lemma 34 of [A02] we get the following

Theorem (4.17). *If k_p is algebraically closed then, $Gal(f_e^-, k_p(T_1, \dots, T_e))$ and $Gal(\phi_e^-, k_p(T_1, \dots, T_e))$ for $1 \le e \le m-1$, are quasi-p groups. In particular, if k_p is algebraically closed then, $Gal(f^-, k_p(T_1, \dots, T_{m-1}))$ and $Gal(\phi^-, k_p(T_1, \dots, T_{m-1}))$ are quasi-p groups.*

5. Review of Linear Algebra

Recall that we are assuming $m > 1$. Let $\epsilon \in \{+,-\}$. Let $\epsilon' = (1-\epsilon 1)/2$ and note that then $\epsilon' = 0$ or 1 according as $\epsilon = +$ or $-$ respectively.

Fix $\nu \in \mathrm{GF}(q)$ such that $T^2 + T + \nu$ is irreducible in $\mathrm{GF}(q)[T]$. Consider the quadratic forms $\psi^+(x) = x_1x_{m+1} + \cdots + x_mx_{2m}$ and $\psi^-(x) = x_1x_{m+1} + \cdots + x_{m-1}x_{2m-1} + x_m^2 + x_mx_{2m} + \nu x_{2m}^2$. Define the *orthogonal group* $\mathrm{O}^\epsilon(2m,q)$ as the group of all $e \in \mathrm{GL}(2m,q)$ which leave the quadratic form ψ^ϵ unchanged, i.e., $\psi^\epsilon(xe) = \psi^\epsilon(x)$. Let the *general orthogonal group* $\mathrm{GO}^\epsilon(2m,q)$ be defined as the group of all $e \in \mathrm{GL}(2m,q)$ such that for some $\lambda(e) \in \mathrm{GF}(q)$ we have $\psi^\epsilon(\xi e) = \lambda(e)\psi^\epsilon(\xi)$ for all $\xi \in \mathrm{GF}(q)^{2m}$. Let the *semilinear orthogonal group* $\Gamma\mathrm{O}^\epsilon(2m,q)$ be defined as the group of all $(\tau,e) \in \Gamma\mathrm{L}(2m,q)$, with $\tau \in \mathrm{Aut}(\mathrm{GF}(q))$ and $e \in \mathrm{GL}(2m,q)$, such that for some $\lambda(\tau,e) \in \mathrm{GF}(q)$ we have $\psi^\epsilon(\xi^\tau e) = \lambda(\tau,e)\psi^\epsilon(\xi)^\tau$ for all $\xi \in \mathrm{GF}(q)^{2m}$. Define the *special orthogonal group* $\mathrm{SO}^\epsilon(2m,q) = \mathrm{SL}(2m,q) \cap \mathrm{O}^\epsilon(2m,q)$. Let $\mathrm{O}'^\epsilon(2m,q)$ be the commutator subgroup of $\mathrm{O}^\epsilon(2m,q)$. Let $\Omega^\epsilon(2m,q) = \mathrm{O}'^\epsilon(2m,q)$ if $(m,q,\epsilon) \neq (2,2,+)$, and let $\Omega^+(4,2)$ be the subgroup of $\mathrm{SO}^+(4,2)$ containing $\mathrm{O}'^+(4,2)$, as defined in Definition 4 on page 30 of [LiK], such that $[\mathrm{SO}^+(4,2) : \Omega^+(4,2)] = 2 = [\Omega^+(4,2) : \mathrm{O}'^+(4,2)]$. Thus we get the sequence $\mathrm{O}'^\epsilon(2m,q) < \Omega^\epsilon(2m,q) < \mathrm{SO}^\epsilon(2m,q) < \mathrm{O}^\epsilon(2m,q) < \mathrm{GO}^\epsilon(2m,q) < \Gamma\mathrm{O}^\epsilon(2m,q)$ of orthogonal groups and by applying Θ_{2m} to them we get the corresponding sequence $\mathrm{PO}'^\epsilon(2m,q) < \mathrm{P}\Omega^\epsilon(2m,q) < \mathrm{PSO}^\epsilon(2m,q) < \mathrm{PO}^\epsilon(2m,q) < \mathrm{PGO}^\epsilon(2m,q) < \mathrm{P}\Gamma\mathrm{O}^\epsilon(2m,q)$ of projective orthogonal groups.[3]

Note that for any $H < \mathrm{GL}(2m,q)$ we have

$$\Omega^\epsilon(2m,q) < H \Leftrightarrow \mathrm{P}\Omega^\epsilon(2m,q) < \Theta_{2m}(H). \tag{5.1}$$

In case $(m,q,\epsilon) \neq (2,2,+)$, this follows exactly as in the proof of Lemma 2.3 of [A04] because then by Theorem 11.46 of [Tay] $\Omega^\epsilon(2m,q)$ is generated by Siegel transformations. By the definition of a Siegel transformation (11.17 of [Tay]) we see that its order is p or 1, and the said proof is based on the fact that the group is generated by elements of p-power order, i.e., equivalently the fact that it is a quasi-p group. So (5.1) holds also for $(m,q,\epsilon) = (2,2,+)$ because by Proposition 2.9.1(iv) of [LiK] $\Omega^+(4,2)$ is a quasi-2 group.

[3]Instead of taking the specific quadratic form ψ^ϵ, in [LiK] these groups are defined for each quadratic form of "Witt defect ϵ'". Dickson [Dic] defines these groups for $p \neq 2$ by taking a different set of specific quadratic forms thus: if either $\epsilon = +$ and $q \equiv 1 \pmod 4$ or $\epsilon = +$ and $q \equiv 3 \pmod 4$ with m even or $\epsilon = -$ and $q \equiv 3 \pmod 4$ with m odd then take the quadratic form to be $x_1^2 + \cdots + x_{2m}^2$; if either $\epsilon = +$ and $q \equiv 3 \pmod 4$ with m odd or $\epsilon = -$ and $q \equiv 3 \pmod 4$ with m even then take the quadratic form to be $x_1^2 + \cdots + x_{2m-1}^2 - x_{2m}^2$; and finally if $\epsilon = -$ and $q \equiv 1 \pmod 4$ then take the quadratic form to be $x_1^2 + \cdots + x_{2m-1}^2 - \mu x_{2m}^2$ with $\mu \in \mathrm{GF}(q) \setminus \mathrm{GF}(q)^2$. By the *singular points* of $\mathrm{P}\Omega^\epsilon(2m,q)$ we mean the images in $\mathcal{P}(\mathrm{GF}(q)^{2m})$ of the nonzero $\xi \in \mathrm{GF}(q)^{2m}$ at which the quadratic form vanishes. By Exercise 11.3 on page 174 of [Tay] we see that the cardinality of the singular points of $\mathrm{P}\Omega^\epsilon(2m,q)$ is $(q^{m-1+\epsilon'}+1)\langle m-1-\epsilon'\rangle$, and hence the cardinality of the *nonsingular points* of $\mathrm{P}\Omega^\epsilon(2m,q)$ is $q^{m-1}(q^m - 1 + 2\epsilon')$. By 11.24 and 11.27 on pages 150-151 of [Tay] we see that $\mathrm{P}\Omega^\epsilon(2m,q)$ acts transitively on its singular points, and by using Witt's Lemma (page 81 of [Asc]) we see that if $p = 2$, then $\mathrm{P}\Omega^\epsilon(2m,q)$ acts transitively on its nonsingular points, whereas if $p \neq 2$, then $\mathrm{P}\Omega^\epsilon(2m,q)$ has two equal size orbits of nonsingular points. Finally, by the sixth line of Table 5.4.C on page 200 of [LiK] which starts with $D_l^{\pm}(q)$), we see that if $m > 3$ and $\Phi < \mathrm{PGL}(2m,q)$ is isomorphic to $\mathrm{P}\Omega^\epsilon(2m,q)$, then $\mathrm{P}\Omega^\epsilon(2m,q) = \delta^{-1}\Phi\delta$ for some $\delta \in \mathrm{PGL}(2m,q)$.

By 2.1.B, 2.10.4(ii) and 2.10.6(i) of [LiK], for any $H < \mathrm{GL}(2m,q)$ we have

$$\Omega^\epsilon(2m,q) \triangleleft H \Leftrightarrow \Omega^\epsilon(2m,q) < H < \mathrm{GO}^\epsilon(2m,q) \tag{5.2}$$

and by 2.1.C of [LiK] we have

$$[\mathrm{GO}^\epsilon(2m,q) : \Omega^\epsilon(2m,q)] \begin{cases} \not\equiv 0 \pmod p & \text{if } p > 2, \\ = 2 & \text{if } p = 2. \end{cases} \tag{5.3}$$

Since $\Omega^\epsilon(2m,q)$ is quasi-p, it is generated by the p-power elements of $\Omega^\epsilon(2m,q)\mathrm{GF}(q)^*$, and hence these two subgroups have the same normalizer in $\mathrm{GL}(2m,q)$. Also clearly $\mathrm{GF}(q)^* < \mathrm{GO}^\epsilon(2m,q)$. Therefore by (5.2), for any $G < \mathrm{PGL}(2m,q)$ we have

$$\mathrm{P}\Omega^\epsilon(2m,q) \triangleleft G \Leftrightarrow \mathrm{P}\Omega^\epsilon(2m,q) < G < \mathrm{PGO}^\epsilon(2m,q) \tag{5.4}$$

and by (5.3) we get

$$[\mathrm{PGO}^\epsilon(2m,q) : \mathrm{P}\Omega^\epsilon(2m,q)] \begin{cases} \not\equiv 0 \pmod p & \text{if } p > 2 \\ = 2 & \text{if } p = 2. \end{cases} \tag{5.5}$$

Finally, since $\mathrm{GF}(q)^* < \mathrm{GO}^\epsilon(2m,q)$, for any $H < \mathrm{GL}(2m,q)$ we have

$$H < \mathrm{GO}^\epsilon(2m,q) \Leftrightarrow \Theta_{2m}(H) < \mathrm{PGO}^\epsilon(2m,q). \tag{5.6}$$

In view of Theorem IV of [CaK], by Corollary 1(iii) of Kantor [Kan] we get the following:

Theorem (5.7) [KANTOR]. *Assume that $m > 3$. Let G be a transitive permutation group of Rank 3 with subdegrees 1, $q(q^{m-2+\epsilon'}+1)\langle m-2-\epsilon'\rangle$ and q^{2m-2}. Then the permuted set can be identified with the singular points of $P\Omega^\epsilon(2m,q)$ so that $P\Omega^\epsilon(2m,q)_1 \triangleleft G < P\Gamma O^\epsilon(2m,q)_1$ where $P\Omega^\epsilon(2m,q)_1$ and $P\Gamma O^\epsilon(2m,q)_1$ denote the permutation groups on the said singular points induced by $P\Omega^\epsilon(2m,q)$ and $P\Gamma O^\epsilon(2m,q)$ respectively.*

For applying (5.7), we first prove the following

Lemma (5.8). *Let $G < PGL(m,q)$ have orbits $\Delta_1 \dots, \Delta_e$ of sizes $d_1, \dots, d_e$ on $\mathcal{P}(GF(q)^m)$, and note that then $\sum_{i=1}^n d_i = \langle m-1\rangle$. Assume that there is no positive integer $r < m$ together with a proper subset ρ of $\{1,\dots,e\}$ such that $\sum_{i\in\rho} d_i = \langle r-1\rangle$. Also assume that there is no integral divisor $s > 1$ of m together with a disjoint partition $\sigma(1)\cup\cdots\cup\sigma(s) = \{1,\dots,e\}$ of $\{1,\dots,e\}$ into pairwise disjoint nonempty subsets $\sigma(1),\dots,\sigma(s)$ such that for $1 \le j \le s$ we have $\sum_{i\in\sigma(j)} d_i = \binom{s}{j}(q-1)^{j-1}\langle (m/s)-1\rangle^j$. Then G acts faithfully on each of its orbits.*

Namely, the first assumption implies that $\Theta_m^{-1}(G)$ does not map any proper subspace of $\mathrm{GF}(q)^m$ (of positive dimension $r < m$) onto itself.[4] Therefore, regarding

[4]In view of this observation, by the last line of Table 5.4.A on page 199 of [LiK] which starts with $D_l^{\pm}(q)$, we see that if $m = 3$ and $\Phi < \mathrm{PGL}(2m,q)$ is isomorphic to and has the same size orbits as $\mathrm{P}\Omega^\epsilon(2m,q)$, then $\mathrm{P}\Omega^\epsilon(2m,q) = \delta^{-1}\Phi\delta$ for some $\delta \in \mathrm{PGL}(2m,q)$.

$\mathcal{P}(\mathrm{GF}(q)^m)$ as the set of all 1-dimensional subspaces of $\mathrm{GF}(q)^m$, it follows that Δ_1 spans $\mathrm{GF}(q)^m$. Let $\Psi = \{\gamma \in \Theta_m^{-1}(G) : \gamma(M) = M$ for all $M \in \Delta_1\}$. Then $\Psi \triangleleft \Theta_m^{-1}(G)$. Recall that a maximal eigenspace of Ψ is a maximal subspace L of $\mathrm{GF}(q)^m$ such that for some homomorphism $\alpha_L : \Psi \to \mathrm{GF}(q)^*$ we have $\gamma(z) = \alpha_L(\gamma)z$ for all $\gamma \in \Theta_m(\Psi)$ and $z \in L$. Since Δ_1 spans $\mathrm{GF}(q)^m$, we get a direct sum decomposition $\mathrm{GF}(q)^m = L_1 + \cdots + L_s$ where $L_1, \ldots, L_s$ are maximal eigenspaces of Ψ. Since $\Psi \triangleleft \Theta_m^{-1}(G)$, it follows that $\Theta_m^{-1}(G)$ acts transitively on this decomposition, and hence $\dim L_i = m/s$ for $1 \le i \le s$. For $1 \le j \le s$ let Λ_j be the set of all $M \in \mathcal{P}(\mathrm{GF}(q)^m)$ such that, for every $0 \ne z \in M$, the cardinality of $\{1 \le i \le s : \mathrm{proj}_i(z) \ne 0\}$ is j where $\mathrm{proj}_i : L_1 + \cdots + L_s \to L_i$ is the natural projection. Then the cardinality of Λ_j is $\binom{s}{j}(q-1)^{j-1}\langle (m/s)-1\rangle^j$. Since $\Theta_m^{-1}(G)$ acts transitively on the above decomposition, there is a disjoint partition $\sigma(1) \cup \cdots \cup \sigma(s) = \{1, \ldots, e\}$ of $\{1, \ldots, e\}$ such that for $1 \le j \le s$ we have $\Lambda_j = \cup_{i\in\sigma(j)}\Delta_i$. Therefore for $1 \le j \le s$ we have $\sum_{i\in\sigma(j)} d_i = \binom{s}{j}(q-1)^{j-1}\langle (m/s)-1\rangle^j$. Consequently by the second assumption we must have $s = 1$. Therefore $\Psi = \mathrm{GF}(q)^*$ and hence G acts faithfully on Δ_1. Similarly G acts faithfully on each of its orbits.

In view of (5.8) and the previous two footnotes, we get the following corollary of (5.7):

Corollary (5.9). *Assume that $m > 3$. Let $G < PGL(2m, q)$ have 2 or 3 orbits on $\mathcal{P}(GF(q)^{2m})$ of sizes $(q^m + 1)\langle m-2\rangle$, $q^{m-1}(q^m + 1)$ or $(q^m + 1)\langle m-2\rangle$, $q^{m-1}(q^m + 1)/2$, $q^{m-1}(q^m + 1)/2$ according as $p = 2$ or $p \ne 2$. Assume that G is Rank 3 with subdegrees 1, $q(q^{m-2+\epsilon'} + 1)\langle m-2-\epsilon'\rangle$ and q^{2m-2} on the orbit of size $(q^m + 1)\langle m-2\rangle$. Then $P\Omega^\epsilon(2m, q) \triangleleft \delta^{-1}G\delta$ for some $\delta \in PGL(2m, q)$.*

As in (5.7), let $\mathrm{P}\Omega^\epsilon(2m, q)_1$ denote the permutation group induced by $\mathrm{P}\Omega^\epsilon(2m, q)$ on its singular points (whose cardinality is $(q^m + 1)\langle m-2\rangle$). In case of $p = 2$, let $\mathrm{P}\Omega^\epsilon(2m, q)_2$ denote the permutation group induced by $\mathrm{P}\Omega^\epsilon(2m, q)$ on its nonsingular points (whose cardinality is $q^{m-1}(q^m + 1)$). In case of $p \ne 2$, the permutation groups induced by $\mathrm{P}\Omega^\epsilon(2m, q)$ on its two nonsingular orbits (whose common cardinality is $q^{m-1}(q^m + 1)/2$) are easily seen to be equivalent and we denote them by $\mathrm{P}\Omega^\epsilon(2m, q)_2$. Now by (5.8) we see that

$$\mathrm{P}\Omega^\epsilon(2m, q)_1 \approx \mathrm{P}\Omega^\epsilon(2m, q) \approx \mathrm{P}\Omega^\epsilon(2m, q)_2 \tag{5.10}$$

where $\approx$ denotes isomorphism as abstract groups.

6. Galois Groups

By (4.15), (4.16), (5.1), (5.6) and (5.9) we get the following

Theorem (6.1). *If $m > 3$ and $GF(q) \subset k_p$, then, for $2 \le e \le m-1$, in a natural manner, we have*

$$\Omega^-(2m, q) < Gal(\phi_e^-, k_p(T_1, \ldots, T_e)) < GO^-(2m, q)$$

and

$$P\Omega^-(2m, q) < Gal(f_e^-, k_p(T_1, \ldots, T_e)) < PGO^-(2m, q).$$

Hence in particular, if $m > 3$ and $GF(q) \subset k_p$ then, in a natural manner we have

$$\Omega^-(2m, q) < Gal(\phi^-, k_p(T_1, \ldots, T_{m-1})) < GO^-(2m, q)$$

and

$$P\Omega^-(2m,q) < Gal(f^-, k_p(T_1,\dots,T_{m-1})) < PGO^-(2m,q).$$

By (3.0), (3.1), (3.4), (3.5), (4.17), (5.2), (5.3), (5.4), (5.5), (5.10) and (6.1) we get the following

Theorem (6.2). *If $m > 3 \le p$ and k_p is algebraically closed, then, for $2 \le e \le m-1$, in a natural manner we have*

$$Gal(\phi^-, k_p(T_1,\dots,T_{m-1}) = Gal(\phi_e^-, k_p(T_1,\dots,T_e) = \Omega^-(2m,q)$$

and

$$Gal(f^-, k_p(T_1,\dots,T_{m-1})) = Gal(f_e^-, k_p(T_1,\dots,T_e)) = P\Omega^-(2m,q)$$

and

$$\begin{aligned} Gal(\overline{f}, k_p(T_1,\dots,T_{m-1})) &= Gal(\overline{f}_e, k_p(T_1,\dots,T_e)) \\ &= P\Omega^-(2m,q)_1 \approx P\Omega^-(2m,q) \end{aligned}$$

and

$$\begin{aligned} Gal(f^{**}, k_p(T_1,\dots,T_{m-1})) &= Gal(f_e^{**}, k_p(T_1,\dots,T_e)) \\ &= P\Omega^-(2m,q)_2 \approx P\Omega^-(2m,q) \end{aligned}$$

and

$$\begin{aligned} Gal(f^{***}, k_p(T_1,\dots,T_{m-1})) &= Gal(f_e^{***}, k_p(T_1,\dots,T_e)) \\ &= P\Omega^-(2m,q)_2 \approx P\Omega^-(2m,q). \end{aligned}$$

Remark (6.3). We shall discuss the $m \le 3$ or $p = 2$ case elsewhere.

References

[A01] S. S. Abhyankar, *Coverings of algebraic curves*, American Journal of Mathematics **79** (1957), 825-856. MR **20:**872

[A02] S. S. Abhyankar, *Tame coverings and fundamental groups of algebraic varieties, Part I*, American Journal of Mathematics **81** (1959), 46-94. MR **21:**3428

[A03] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic, Dedicated to "Feit-Serre-Email"*, Bulletin of the American Mathematical Society **27** (1992), 68-133. MR **94a:**12004

[A04] S. S. Abhyankar, *Nice equations for nice groups*, Israel Journal of Mathematics **88** (1994), 1-24. MR **95:**04

[A05] S. S. Abhyankar, *More nice equations for nice groups*, Proceedings of the American Mathematical Society (to appear).

[Asc] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1986. MR **89b:**20001

[BuS] F. Buekenhout and E. E. Shult, *On the foundations of polar geometry*, Geometriae Dedicata **3** (1974), 155-170. MR **50:**3091

[CaK] P. J. Cameron and W. M. Kantor, *2-Transitive and antiflag transitive collineation groups of finite projective spaces*, Journal of Algebra **60** (1979), 384-422. MR **81c:**20032

[Dic] L. E. Dickson, *Linear Groups*, Teubner, 1901.

[Kan] W. M. Kantor, *Rank 3 characterizations of classical geometries*, Journal of Algebra **36** (1975), 309-313. MR **52:**8229

[LiK] M. W. Liebeck and P. Kleidman, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, 1990. MR **91g:**20001

[Tay] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992. MR **94d:**20028

[Tit] J. Tits, *Buildings of Spherical Type and Finite BN-Pairs*, Springer Lecture Notes In Mathematics Number 386, 1974. MR **57:**9866

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