MORE NICE EQUATIONS FOR NICE GROUPS

SHREERAM S. ABHYANKAR

(Communicated by Ronald M. Solomon)

Abstract. Nice quintinomial equations are given for unramified coverings of the affine line in nonzero characteristic $p$ with $\text{PSp}(2m,q)$ and $\text{Sp}(2m,q)$ as Galois groups where $m > 2$ is any integer and $q > 1$ is any power of $p$.

1. Introduction

Let $m > 2$ be any integer, let $q > 1$ be any power of a prime $p$, consider the polynomials $F = F(Y) = Y^n + T^q Y^m + T Y^m + Y + 1$ and $F^* = F^*(Y) = Y^{n^*} + XY + 1$ in indeterminates $T, X, Y$ over an algebraically closed field $k$ of characteristic $p$, where $n = 1 + q + \cdots + q^{2m-1}$, $u = 1 + q + \cdots + q^m$, $v = 1 + q + \cdots + q^{m-1}$, $w = 1 + q + \cdots + q^{m-2}$, $n^* = 1 + q + \cdots + q^{m-1}$, and consider their respective Galois groups $\text{Gal}(F,k(X,T))$ and $\text{Gal}(F^*,k(X))$. 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 $\text{Gal}(F^*,k(X)) = \text{PSL}(m,q)$. 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 $\text{Gal}(F,k(X,T)) = \text{PSp}(2m,q)$. 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 $\text{PSp}(2m,q)$, I shall show that the Galois group of a more general polynomial $f$ is also $\text{PSp}(2m,q)$. Moreover, by slightly changing $f$ and $F$, I shall show that we get polynomials $\phi$ and $\phi_1$ whose Galois group is the symplectic group $\text{Sp}(2m,q)$. The polynomials $f, \phi$ and $\phi_1$ are also special cases of the families of polynomials giving unramified coverings of the affine line in nonzero characteristic written down in [A01].

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 Dinesh Thakur for stimulating conversations concerning the material of 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. To abbreviate frequently occurring expressions, for every integer $i \geq -1$ we put

$$\langle i \rangle = 1 + q + q^2 + \cdots + q^i$$

(convention: $\langle 0 \rangle = 1$ 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

$$f = f(Y) = Y^{(2m-1)} + 1 + XY^{(m-1)} + \sum_{i=1}^{m-1} \left( T_i Y^{(m-1+i)} + T_1 Y^{(m-1-i)} \right)$$

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 $k_p[X, T_1, \ldots, T_{m-1}]$. Now the constant term of $f$ is 1 and the $Y$-exponent of every other term in $f$ is 1 modulo $p$, and hence $f - Yf_Y = 1$ where $f_Y$ is the $Y$-derivative of $f$. Therefore $\text{Disc}_Y(f) = 1$ where $\text{Disc}_Y(f)$ is the $Y$-discriminant of $f$, and hence the Galois group $\text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1}))$ is well-defined as a subgroup of the symmetric group $\text{Sym}_{2m-1}$. Since $f$ is linear in $X$, by the Gauss Lemma it follows that $f$ is irreducible in $k_p(X, T_1, \ldots, T_{m-1})[Y]$, and hence its Galois group is transitive.

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

$$f_e = f_e(Y) = Y^{(2m-1)} + 1 + XY^{(m-1)} + \sum_{i=1}^{e} \left( T_i Y^{(m-1+i)} + T_1 Y^{(m-1-i)} \right)$$

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 $k_p[X, T_1, \ldots, T_e]$ and, as above, $\text{Disc}_Y(f_e) = 1$ and the Galois group $\text{Gal}(f_e, k_p(X, T_1, \ldots, T_e))$ is a transitive subgroup of $\text{Sym}_{2m-1}$. Note that if $k = k_p$ is an algebraically closed field (of characteristic $p > 0$), then $F$ is obtained by substituting $T$ for $T_1$ in $f_1$ and hence $\text{Gal}(F, k(X, T)) = \text{Gal}(f_1, k_p(X, T_1))$.

In Section 3, we throw away a root of $f$ 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 $1/Y$. Next we factor $g(Y, Z)$ into two factors. The $Z$-degrees of these factors turn out to be $q(2m - 3)$ and $q^{2m-1}$. In

\footnote{In the Abstract and the Introduction we assumed $m > 2$. But in the rest of the paper, unless stated otherwise, we only assume $m > 1$.}
Section 4, we show that these factors are irreducible in case of \( f_1 \) and hence also in case of \( f \) and \( f_e \) for \( 1 \leq e \leq m - 1 \), and therefore \( \text{Gal}(f, k(X, T_1, \ldots, T_{m-1})) \) and \( \text{Gal}(f_e, k_p(X, T_1, \ldots, T_e)) \) are Rank 3 groups with subdegrees 1, \( q(2m - 3) \) and \( q^{2m-1} \). In Section 6, from this Rank 3 description, we deduce the result that if \( m > 2 \) and \( k_p \) is algebraically closed then \( \text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1})) = \text{Gal}(f_e, k_p(X, T_1, \ldots, T_e)) = \text{PSp}(2m, q) \) for \( 1 \leq e \leq m - 1 \).

Consider the monic polynomials

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

and

\[
\phi_e = \phi_e(Y) = Y^{q^{2m-1}} + 1 + XY^{q^m-1} + \sum_{i=1}^{m} \left( T_i X^{q^{m+i-1}} + T_i Y^{q^{m+i-1}} \right) \text{ for } 1 \leq e \leq m - 1
\]

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

In Section 5, we give a review of linear algebra including definitions of \( \text{PSp}(2m, q) \) and \( \text{Sp}(2m, q) \).

### 3. Twisted derivative and its factorization

Solving the equation \( f = 0 \) we get

\[
X = \frac{Y^{(2m-1)} + 1 + \sum_{i=1}^{m-1} \left( T_i X^{q^{m-1+i}} + T_i Y^{q^{m-1+i}} \right)}{-Y^{(m-1)}}
\]

and hence

\[
f'(Y, Z) = \frac{f(Z) - f(Y)}{Z - Y} \quad \text{(def of the twisted derivative } f' \text{ of } f)
\]

\[
= \frac{Z^{(2m-1)} - Y^{(2m-1)}}{Z - Y} + \frac{Y^{(2m-1)} + 1 + \sum_{i=1}^{m-1} \left( T_i X^{q^{m-1+i}} + T_i Y^{q^{m-1+i}} \right)}{-Y^{(m-1)}} \times \frac{Z^{(m-1)} - Y^{(m-1)}}{Z - Y} + \sum_{i=1}^{m-1} \left( T_i \frac{Z^{(m-1+i)} - Y^{(m-1+i)}}{Z - Y} + T_i \frac{Z^{(m-1-i)} - Y^{(m-1-i)}}{Z - Y} \right)
\]
and therefore
\[ g = g(Y, Z) = Y^{(2m-1) - 1} f'(1/Y, Z/Y) \]

(degree of polynomial \( g \) obtained by dividing
roots of \( f' \) by \( Y \) and then changing \( Y \) to \( 1/Y \))
\[
\begin{align*}
&= \frac{Z^{(2m-1)} - 1}{Z - 1} - \frac{Z^{(m-1)} - 1}{Z - 1} \left( 1 + Y^{(2m-1)} \right) \\
&- \sum_{i=1}^{m-1} T_i \left( \frac{Z^{(m-1)} - 1}{Z - 1} - \frac{Z^{(m-1-i)} - 1}{Z - 1} \right) Y^{(2m-1)-(m-1-i)} \\
&+ \sum_{i=1}^{m-1} T_i^{q_i} \left( \frac{Z^{(m+1-i)} - 1}{Z - 1} - \frac{Z^{(m-1)} - 1}{Z - 1} \right) Y^{(2m-1)-(m-1+i)}.
\end{align*}
\]

To simplify \( g \) we observe that
\[ 2(m - 1) = (q^m + 1)(m - 1) \]
and hence
\[
\frac{Z^{(2m-1)} - 1}{Z - 1} - \frac{Z^{(m-1)} - 1}{Z - 1} \left( 1 + Y^{(2m-1)} \right) = \frac{Z^{(m-1)} - 1}{Z - 1} \left( \frac{Z^{(m-1)(q^m+1)} - 1}{Z^{(m-1)} - 1} - 1 - Y^{(q^m+1)(m-1)} \right)
\]
and also
\[
\frac{Z^{(m-1)(q^m+1)} - 1}{Z^{(m-1)} - 1} - 1 = Z^{(m-1)} + Z^{2(m-1)} + \ldots + Z^{q^m(m-1)}
\]
\[
= Z^{(m-1)} \left( Z^{(m-1)} - 1 \right)^{(q^m-1)}
\]
\[
= Z^{(m-1)} \left( Z^{(m-1)} - 1 \right)^{(q-1)(m-1)}
\]
\[
= \left[ Z \left( Z^{(m-1)} - 1 \right)^{(q-1)} \right]^{(m-1)}
\]
and therefore
\[
\frac{Z^{(2m-1)} - 1}{Z - 1} - \frac{Z^{(m-1)} - 1}{Z - 1} \left( 1 + Y^{(2m-1)} \right) = \frac{Z^{(m-1)} - 1}{Z - 1} \left\{ \left[ \left( Z^{(m-1)} - 1 \right)^{(q-1)} \right]^{(m-1)} - \left[ Y^{q^m+1} \right]^{(m-1)} \right\}.
\]
Moreover
\[
\frac{Z^{(m-1+i)} - 1}{Z - 1} = \frac{Z^{(m-1)} - 1}{Z - 1} \\
= \left( 1 + Z + Z^2 + \ldots + Z^{q^2 + \ldots + q^{m-1+i}} \right) - \left( 1 + Z + Z^2 + \ldots + Z^{q^2 + \ldots + q^{m-1}} \right)
\]
\[
= Z^{1+q+q^2+\ldots+q^{m-1}} \left( 1 + Z + Z^2 + \ldots + Z^{q^m(i-1)-1} \right)
\]
\[
= Z^{(m-1)} \left( Z^{(i-1)} - 1 \right)^{q^m}
\]
and
\[ Y^{(2m-1)-(m-1+i)} = Y q^{m+i(m-1-i)} \]

and hence
\[
T_i^q \left( \frac{Z^{(m-1+i)} - 1}{Z - 1} - \frac{Z^{(m-1)} - 1}{Z - 1} \right) Y^{(2m-1) - (m-1+i)}
= \frac{Z^{(m-1)} (Z^{(i-1)} - 1)^q_m}{Z - 1} Y q^{m+i(m-1-i)} T_i^q.
\]

Similarly
\[
- T_i \left( \frac{Z^{(m-1)} - 1}{Z - 1} - \frac{Z^{(m-1-i)} - 1}{Z - 1} \right) Y^{(2m-1) - (m-1-i)}
= - \frac{Z^{(m-1-i)} (Z^{(i-1)} - 1)^{q_m-i}}{Z - 1} Y q^{m-i(m-1+i)} T_i.
\]

Thus
\[
(3.0) \quad g = A - B + C
\]

where
\[
A = \sum_{i=1}^{m-1} \frac{Z^{(m-1)} (Z^{(i-1)} - 1)^{q_m}}{Z - 1} Y q^{m+i(m-1-i)} T_i^q,
\]
\[
B = \sum_{i=1}^{m-1} \frac{Z^{(m-1-i)} (Z^{(i-1)} - 1)^{q_m-i}}{Z - 1} Y q^{m-i(m-1+i)} T_i
\]

and
\[
C = \frac{Z^{(m-1)} - 1}{Z - 1} \left\{ \frac{q_m}{Y q^{m+1} - [Y q^{m+1}]^{(m-1)}} \right\}
= \frac{Z^{(m-1)} (Z^{(m-1)} - 1)^{q_m} - (Z^{(m-1)} - 1)^{Y (2m-1)}}{Z - 1}.
\]

To simplify \( g \) further, upon letting
\[
\hat{g} = g/L, \quad \hat{A} = A/L, \quad \hat{B} = B/L, \quad \text{and} \quad \hat{C} = C/L, \quad \text{where} \quad L = \frac{Z^{(m-1)} - 1}{Z - 1},
\]

we get
\[
g = L \hat{g} \quad \text{and} \quad \hat{g} = \hat{A} - \hat{B} + \hat{C}
\]

with
\[
\hat{A} = \sum_{i=1}^{m-1} \frac{Z^{(m-1)} (Z^{(i-1)} - 1)^{q_m}}{Z^{(m-1)} - 1} Y q^{m+i(m-1-i)} T_i^q,
\]
\[
\hat{B} = \sum_{i=1}^{m-1} \frac{Z^{(m-1-i)} (Z^{(i-1)} - 1)^{q_m-i}}{Z^{(m-1)} - 1} Y q^{m-i(m-1+i)} T_i
\]
and

\[ \tilde{C} = \left[ Z \left( Z^{(m-1)} - 1 \right)^{\left(q-1\right)} \right]^{(m-1)} - \left[ Y^{q^{m+1}} \right]^{(m-1)}, \]

and hence upon letting

\[ U = Z \left( Z^{(m-1)} - 1 \right)^{\left(q-1\right)}, \quad J = Y^{q^{m+1}}, \]

and

\[ V_i = \frac{Z^{(m-1-i)} \left( Z^{(i-1)} - 1 \right)^{q^{m-i}}}{(Z^{(m-1)} - 1) Y^{(m-1-i)}} \quad \text{for } 1 \leq i \leq m - 1 \]

we get

\[ \tilde{A} = \sum_{i=1}^{m-1} U^{(i-1)}(V_i T_i)^{q^i} J^{(m-1)-(i-1)}, \quad \tilde{B} = \sum_{i=1}^{m-1} (V_i T_i)J^{(m-1)}, \]

and

\[ \tilde{C} = U^{(m-1)} - J^{(m-1)} \quad \text{with} \quad J^{(m-1)} = Y^{(2m-1)}, \]

and therefore upon letting

\[ \tilde{g} = \tilde{g}/Y^{(2m-1)}, \quad \tilde{A} = \tilde{A}/Y^{(2m-1)}, \quad \tilde{B} = \tilde{B}/Y^{(2m-1)}, \quad \tilde{C} = \tilde{C}/Y^{(2m-1)}, \]

and

\[ W = U/J, \quad \tilde{T}_i = V_i T_i \]

we get

\[ g = Y^{(2m-1)} L\tilde{g} \quad \text{and} \quad \tilde{g} = \tilde{A} - \tilde{B} + \tilde{C} \]

with

\[ \tilde{A} = \sum_{i=1}^{m-1} W^{(i-1)}\tilde{T}_i^{q^i}, \quad \tilde{B} = \sum_{i=1}^{m-1} \tilde{T}_i, \quad \text{and} \quad \tilde{C} = W^{(m-1)} - 1, \]

where

\[ W = \frac{Z \left( Z^{(m-1)} - 1 \right)^{\left(q-1\right)}}{Y^{q^{m+1}}} \quad \text{and} \quad \tilde{T}_i = \frac{Z^{(m-1-i)} \left( Z^{(i-1)} - 1 \right)^{q^{m-i}}}{(Z^{(m-1)} - 1) Y^{(m-1-i)}} T_i. \]

To factor \( g \) we try to factor \( \tilde{g} \). First we try to factor \( \tilde{g} \) after putting \( \tilde{T}_i = 0 \) for all \( i > 1 \), i.e., we try to factor

\[ W\tilde{T}_i^q - \tilde{T}_i + W^{(m-1)} - 1. \]

This corresponds to the case of the special polynomial \( f_1 \); we shall then feed it back into the general case of \( g \). By changing \( (W, \tilde{T}_1) \) to \( (V, R) \), we try to factor

\[ VR^q - R + V^{(m-1)} - 1 \]

as a polynomial in an indeterminate \( R \) with coefficients in the univariate polynomial ring \( GF(p)[V] \). To do this, upon letting

\[ M = - \sum_{\mu=0}^{m-1} V^{(m-2-\mu)} \]
we have
\[ VM^q = - \sum_{\mu=0}^{m-1} V^{(m-1-\mu)} \]
and hence
\[ VM^q - M + V^{(m-1)} - 1 = 0 \]
and therefore
\[(R - M) [V (R^{q-1} + MR^{q-2} + \cdots + M^q - 1)] = V(R^q - M^q) - R + M \]

\[ = VR^q - R - (VM^q - M) \]
\[ = VR^q - R + V^{(m-1)} - 1. \]

Now upon taking an indeterminate \( S \) and letting
\[ P = \sum_{j=0}^{i-1} V^{(j-1)} S^q^j \]
we have
\[ VP^q - P = \left( \sum_{j=1}^{i} V^{(j-1)} S^q^j \right) - \left( \sum_{j=0}^{i-1} V^{(j-1)} S^q^j \right) = V^{(i-1)} S^q - S \]
and hence upon taking indeterminates \( S_1, \ldots, S_{m-1} \) and letting
\[ D = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} V^{(j-1)} S^q^j \]
we have
\[ VD^q - D = \sum_{i=1}^{m-1} \left( V^{(i-1)} S^q^i - S_i \right) \]
and therefore by substituting \( D \) for \( R \) in the factorization
\[ VR^q - R + V^{(m-1)} - 1 = (R - M) [V (R^{q-1} + MR^{q-2} + \cdots + M^q - 1)] - 1 \]
we get the factorization
\[ \left( \sum_{i=1}^{m-1} V^{(i-1)} S^q^i \right) - \left( \sum_{i=1}^{m-1} S_i \right) + V^{(m-1)} - 1 \]
\[ = (D - M) [V (D^{q-1} + MD^{q-2} + \cdots + M^q - 1)] - 1. \]

Substituting \((W, T_i)\) for \((V, S_i)\) in the above equation we get
\[ \tilde{g} = (E - N) [W (E^{q-1} + NE^{q-2} + \cdots + N^q - 1) - 1] \]
where
\[ E = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} W^{(j-1)} T^q^i \quad \text{and} \quad N = - \sum_{\mu=0}^{m-1} W^{(m-2-\mu)} \]
and hence upon remembering that \( g = Y^{(2m-1)} L \tilde{g} \) we get
\[
g = Y^{(2m-1)} L(E - N) \left[ W \left( E^{q-2} + NE^{q-2} + \cdots + N^{q-1} \right) - 1 \right]
\]
and we recall that
\[
L = \frac{Z^{(m-1)} - 1}{Z - 1}
\]
and
\[
W = \frac{Z \left( Z^{(m-1)} - 1 \right)^{(q-1)}}{Y q^{m+1}}, \quad \tilde{T}_i = \frac{Z^{(m-1) - i} (Z^{(i-1)} - 1)^{qm-i}}{(Z^{(m-1)} - 1) Y^{(m-1) - i} T_i}.
\]
Substituting the above values of \( W \) and \( \tilde{T}_i \) in \( E \) we get
\[
E = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} Z^{(m-1) - i + j} \left( Z^{(i-1)} - 1 \right)^{qm-i+j} Y q^i (m-1-i) + (q^{m+1})(j-1) T_i^q.
\]
Now upon letting
\[
G_i = Z \left( Z^{(i-1)} - 1 \right)^{q-1} \quad \text{and} \quad H_i = 1 + Z + Z^2 + \cdots + Z^{(i-1) - 1}
\]
we get
\[
L = H_m, \quad W = \frac{Z \left( Z^{(m-1)} - 1 \right)^{(q-1)}}{Y q^{m+1}} = \frac{G_m}{Y q^{m+1}}, \quad N = -\sum_{\mu=0}^{m-1} \frac{G_m^{(m-2-\mu)}}{Y (q^{m+1})(m-2-\mu)},
\]
and
\[
E = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} \frac{G_i^{(m-1) - i + j} \left( Z^{(i-1)} - 1 \right)^{qm-i+j}}{Y q^i (m-1-i) + (q^{m+1})(j-1)} T_i^q,
\]
and hence
\[
LE = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} \frac{G_i^{(m-1) - i + j} H_i}{Y q^i (m-1-i) + (q^{m+1})(j-1)} T_i^q
\]
and
\[
-LN = \sum_{\mu=0}^{m-1} \frac{G_m^{(m-2-\mu)} H_m}{Y (q^{m+1})(m-2-\mu)}.
\]
By factoring the maximal negative power of \( Y \) from \( N, E, LE \) and \( LN \), we get
\[
N = -\sum_{\mu=0}^{m-1} \frac{G_m^{(m-2-\mu)} Y^{(q+1)} Y^{m-1-\mu} (\mu-1)}{Y (q^{m+1})(m-2)},
\]
\[
E = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} \frac{G_i^{(m-1) - i + j} \left( Z^{(i-1)} - 1 \right)^{Y q^{m+j}(m-2-j) + q^{m-i+j}(i-j-2)}}{(Z^{(m-1)} - 1) Y^{(m+1)}(m-2)} T_i^q,
\]
\[
LE = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} \frac{G_i^{(m-1) - i + j} H_i Y q^{m+j}(m-2-j) + q^{m-i+j}(i-j-2)}{Y (q^{m+1})(m-2)} T_i^q,
\]
and

$$-LN = \sum_{\mu=0}^{m-1} \frac{G_m^{(m-2-\mu)} H_m Y^{(q^{m+1}) q^{m-1-\mu} (\mu-1)}}{Y^{(q^{m+1}) (m-2)}}.$$ 

Therefore upon letting

$$g' = Y^{(q^{m+1}) (m-2)} L(E - N) \quad \text{and} \quad g'' = Y^{(q^{m+1}) q^{m-1}} \left( \left( \sum_{l=1}^{q} WN^{l-1} E^{q-l} \right) - 1 \right)$$

we get

(3.1) $$g = g'g''$$

with

(3.2) $$g' = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} G_i^{(m-1-i+j)} H_i Y^{q^{m+j} (m-2-j) + q^{m-1} (i-j-2)} T_i q^j$$

and

(3.3) $$g'' = \left( \sum_{l=1}^{q} Z \left( Z^{(m-1)} - 1 \right)^{q-1} N^{l-1} E^{q-l} \right) - Y^{(q^{m+1}) (q^{m-1}-1)},$$

where

(3.4) $$N = - \sum_{\mu=0}^{m-1} G_m^{(m-2-\mu)} Y^{(q^{m+1}) q^{m-1-\mu} (\mu-1)}$$

and

(3.5) $$E = \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} G_i^{(m-1-i+j)} \left( Z^{(i-1)} - 1 \right) Y^{q^{m+j} (m-2-j) + q^{m-1} (i-j-2)} T_i q^j$$

and where we recall that

(3.6) $$G_i = Z \left( Z^{(i-1)} - 1 \right)^{q-1} \quad \text{and} \quad H_i = 1 + Z + Z^2 + \cdots + Z^{(i-1)-1}.$$ 

By (3.6) we see that $G_i$ and $H_i$ are monic polynomials in $Z$ and for their $Z$-degrees we have

$$\deg_Z G_i = 1 + (i-1)(q-1) = q^i \quad \text{and} \quad \deg_Z H_i = (i-1) - 1$$

and hence

$$\deg_Z G_m^{(m-2)} H_m = (m-2)q^m + (m-1) - 1 = q(2m-3),$$

$$\deg_Z G_m^{(m-2)} H_m > \deg_Z G_m^{(m-2-\mu)} H_m \quad \text{for} \quad 1 \leq \mu \leq m-1,$$

and

$$\deg_Z G_m^{(m-2)} H_m > \deg_Z G_i^{(m-1-i+j)} H_i \quad \text{for} \quad 1 \leq i \leq m-1 \text{ and } 0 \leq j \leq i-1;$$

therefore, noting that $Y^{(q^{m+1}) q^{m-1-\mu} (\mu-1)} = 1$ for $\mu = 0$, in view of (3.2) we conclude that $g'$ is a monic polynomial of degree $q(2m-3)$ in $Z$ with coefficients in
GF(p)[Y,T_1,\ldots,T_{m-1}]. Obviously g is a monic polynomial in Z with coefficients in GF(p)[Y,T_1,\ldots,T_{m-1}] and
\[ \deg_Z g = (\deg_Y f) - 1 = (2m - 1) - 1 = q(2m - 3) + q^{2m-1} \]
and hence in view of (3.1) we see that g'' is a monic polynomial of degree q^{2m-1} in Z with coefficients in GF(p)[Y,T_1,\ldots,T_{m-1}]. Thus
\[
\begin{align*}
\{ g' \text{ and } g'' \text{ are monic polynomials of degrees } & q(2m - 3) \text{ and } q^{2m-1} \\
\text{in } Z \text{ with coefficients in } & GF(p)[Y,T_1,\ldots,T_{m-1}] \text{ respectively.}
\end{align*}
\]

4. IRREDUCIBILITY

For 1 \leq e \leq m - 1, let f'_<, g'_<, g'_e, g''_e be the members of GF(p)[Y,Z,T_1,\ldots,T_e] obtained by putting T_i = 0 for all i > e in f', g', g'' respectively. Then f'_< is the twisted derivative of f_<, and dividing the Z-roots of f'_< by Y and afterwards changing Y to 1/Y we get g_< which is a monic polynomial of degree (2m - 1) - 1 in Z with coefficients in GF(p)[Y,T_1,\ldots,T_e]. Also
\[
\begin{align*}
\{ & \text{for } 1 \leq e \leq m - 1 \text{ we have } g_e = g'_e g''_e \text{ where } g'_e \text{ and } g''_e \text{ are} \\
& \text{monic polynomials of degrees } q(2m - 3) \text{ and } q^{2m-1} \text{ in } Z \\
& \text{with coefficients in } GF(p)[Y,T_1,\ldots,T_e] \text{ respectively.}
\end{align*}
\]

By (3.0) and the immediately following expressions for A, B, C we see that
\[ g_1 = A_1 T_1^q - B_1 T_1 + C_1 \]
where A_1, B_1, C_1 are nonzero elements of GF(p)[Y,Z] given by
\[
\begin{align*}
A_1 &= Z^{(m-1)}(Z - 1)^{(q-1)(m-1)} Y^{q^{m+1}(m-2)}, \\
B_1 &= Z^{(m-2)}(Z - 1)^{(q-1)(m-2)} Y^{q^{m-1}(m)}, \\
\end{align*}
\]

and
\[
C_1 = \left( 1 + Z + Z^2 + \ldots + Z^{(m-1)-1} \right) \times \left[ Z \left( Z^{(m-1)} - 1 \right)^{(q-1)(m-1)} - [Y^{q^{m+1}}]^{(m-1)} \right].
\]

Likewise, by (3.1) to (3.6) we see that
\[ g'_1 = A'_1 T_1 + B'_1 \]
where A'_1, B'_1 are nonzero elements of GF(p)[Y,Z] given by
\[
A'_1 = Z^{(m-2)}(Z - 1)^{(q-1)(m-2)} Y^{q^{m}(m-2)}
\]
and
\[
B'_1 = \sum_{\mu=0}^{m-1} \left[ Z \left( Z^{(m-1)} - 1 \right)^{q-1} \right]^{(m-2-\mu)} \times \left( 1 + Z + Z^2 + \ldots + Z^{(m-1)-1} \right) Y^{(q^{m+1})q^{m-1}(m-1)}.\]

For establishing the irreducibility of g' and g'' we now prove the following lemma.
Lemma (4.2). Let \( Q \) be a field of characteristic \( p \) and consider a univariate polynomial \( g_0 = A_0T^q - B_0T + C_0 \) with \( A_0, B_0, C_0 \) in \( Q \) such that \( A_0 \neq 0 \neq B_0 \). Assume that \( g_0 = g_0g_0'' \) in \( Q[T] \) with \( \deg_T g_0'' = 1 \) (and hence \( \deg_T g_0' = q - 1 \)). Also assume that for some real discrete valuation \( I \) of \( Q \) (whose value group is the group of all integers) we have \( \gcd(q - 1, I(B_0/A_0)) = 1 \). Then \( g_0'' \) is irreducible in \( Q[T] \).

To see this, we note that by assumption \( g_0' = A_0T + B_0' \) with \( 0 \neq A_0' \in Q \) and \( B_0' \in Q \). Now \( -B_0'/A_0' \) is a root of \( T^q - (B_0/A_0)T + (C_0/A_0) \) and hence

\[
T^q - (B_0/A_0)T + (C_0/A_0) = \prod_{j \in GF(q)} [T + (B_0'/A_0') - j\Lambda]
\]

where \( \Lambda \) is an element in an algebraic closure \( Q^* \) of \( Q \) with \( \Lambda^{q-1} = B_0/A_0 \). It follows that for any root \( \Delta \) of \( g'' \) in \( Q^* \) we must have \( \Delta = j\Lambda - (B_0'/A_0') \) for some \( 0 \neq j \in GF(q) \). By taking an extension \( I^* \) of \( I \) to \( Q(\Delta) \) and upon letting \( r \) be the reduced ramification exponent of \( I^* \) over \( I \) we see that

\[
I^*(\Delta + (B_0'/A_0')) = I^*(j\Lambda)
\]

\[
= I^*(j^{q-1}\Lambda^{q-1})/(q - 1)
\]

\[
= I^*(B_0/A_0)/(q - 1) = rI(B_0/A_0)/(q - 1).
\]

Therefore, since \( I^*(\Delta + (B_0'/A_0')) \) is obviously an integer, so is \( rI(B_0/A_0)/(q - 1) \). Since \( \gcd(q - 1, I(B_0/A_0)) = 1 \), it follows that \( r \) is divisible by \( q - 1 \). Since the field degree \( [Q(\Delta) : Q] \) is at least \( r \), we conclude that \( [Q(\Delta) : Q] \geq 1 \). Since \( \Delta \) is a root of \( g_0'' \) and \( \deg_T g_0'' = q - 1 \), the polynomial \( g_0'' \) must be irreducible in \( Q[T] \).

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

Lemma (4.3). Let \( \kappa \) be a field, and let \( g_0 = g_0g_0'' \) where \( g_0, g_0', g_0'' \) 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 \( g_0' \) and \( g_0'' \) have positive \( T \)-degrees and are irreducible in the ring \( \kappa[X_1, \ldots, X_d, T][T] \). 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 \( g_0' \) and \( g_0'' \) are irreducible in the ring \( \kappa[X_1, \ldots, X_d, T][Z] \).

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 \( I(A_1) = \langle m - 1 \rangle \) and \( I(B_1) = \langle m - 2 \rangle \) and hence \( I(B_1/A_1) = \langle m - 2 \rangle - \langle m - 1 \rangle = -q^{m-1} \) and therefore \( \gcd(q - 1, I(B_1/A_1)) = 1 \). Also obviously \( A_1 \) and \( C_1 \) have no nonconstant common factor in \( k_p[Y, Z] \). Therefore by (4.2) and (4.3) we conclude that:

\[
(4.4) \quad \text{the polynomials } g_1' \text{ and } g_1'' \text{ are irreducible in } k_p(Y, T_1)[Z].
\]

As an immediate consequence of (4.4) we see that:

\[
\left\{ \begin{align*}
\text{the polynomials } g'_e \text{ and } g''_e \text{ are irreducible in } k_p(Y, T_1, \ldots, T_{m-1})[Z] \\
\text{and, for } 1 \leq e \leq m - 1,
\text{the polynomials } g'_e \text{ and } g''_e \text{ are irreducible in } k_p(Y, T_1, \ldots, T_e)[Z].
\end{align*} \right.
\]

Recall that \( f_e \) is irreducible in \( k_p(X, T_1, \ldots, T_e)[Y] \), 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 (4.1) and (4.5) we get the following:
Theorem (4.6). For $1 \leq e \leq m - 1$, we have that $\text{Gal}(f_e, k_p(X, T_1, \ldots, T_e))$ is a transitive permutation group of Rank 3 with subdegrees $1$, $q(2m - 3)$ and $q^{2m - 1}$. Hence in particular, $\text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1}))$ is a transitive permutation group of Rank 3 with subdegrees $1$, $q(2m - 3)$ and $q^{2m - 1}$.

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

$$\Theta_m : \text{ΓL}(m, q) \twoheadrightarrow \text{PΓL}(m, q) = \text{ΓL}(m, q)/\text{GF}(q)^\cdot$$

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

Now in view of Proposition 3.1 of [A04] we get the following:

Theorem (4.7). Assuming $\text{GF}(q) \subset k_p$, for $1 \leq e \leq m - 1$, in a natural manner we may regard

$$\text{Gal}(\phi_e, k_p(X, T_1, \ldots, T_e)) \subset \text{GL}(2m, q)$$

and

$$\text{Gal}(f_e, k_p(X, T_1, \ldots, T_e)) \subset \text{PGL}(2m, q)$$

and then we have

$$\Theta_{2m}(\text{Gal}(\phi_e, k_p(X, T_1, \ldots, T_e))) = \text{Gal}(f_e, k_p(X, T_1, \ldots, T_e)).$$

In particular, again assuming $\text{GF}(q) \subset k_p$, in a natural manner we may regard

$$\text{Gal}(\phi, k_p(X, T_1, \ldots, T_{m-1})) \subset \text{GL}(2m, q)$$

and

$$\text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1})) \subset \text{PGL}(2m, q)$$

and then we have

$$\Theta_{2m}(\text{Gal}(\phi, k_p(X, T_1, \ldots, T_{m-1}))) = \text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1})).$$

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

Theorem (4.8). If $k_p$ is algebraically closed, then, for $1 \leq e \leq m - 1$,

$$\text{Gal}(f_e, k_p(X, T_1, \ldots, T_e)) \text{ and } \text{Gal}(\phi_e, k_p(X, T_1, \ldots, T_e))$$

are quasi-$p$ groups. Hence in particular, if $k_p$ is algebraically closed then,

$$\text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1})) \text{ and } \text{Gal}(\phi, k_p(X, T_1, \ldots, T_{m-1}))$$

are quasi-$p$ groups.
5. Review of linear algebra

Recall that we are assuming $m > 1$.

Following Dickson (page 89 of [Dic]) we define the symplectic group $\text{Sp}(2m, q)$ as the group of all $e = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2m, q)$, where $a, b, c, d$ are $m$ by $m$ matrices over $\text{GF}(q)$, which leave the bilinear form $\psi(x, y) = \sum_{i=1}^{m} (x_i y_m+i - y_i x_{m+i})$ unchanged, i.e., $\psi(x, ye) = \psi(x, y)$, or equivalently for which: $ad - bc = m$ by $m$ identity matrix, and $ab' - ba' = 0 = cd' - dc'$ where $' = \text{transpose}$; note that $\text{Sp}(2m, q) < \text{SL}(2m, q)$, and define the projective symplectic group $\text{PSp}(2m, q)$, and define the projective general symplectic group $\Gamma\text{Sp}(2m, q) = \Theta_2m(\text{Sp}(2m, q)).$ 2 Let the general symplectic group $\text{GSp}(2m, q)$ be defined as the group of all $e \in \text{GL}(2m, q)$ such that for some $\lambda(e) \in \text{GF}(q)$ we have $\psi(\xi e, \eta e) = \lambda(e) \psi(\xi, \eta)$ for all $\xi, \eta$ in $\text{GF}(q)^{2m}$. Let the semilinear symplectic group $\Gamma\text{Sp}(2m, q)$ be defined as the group of all $(\tau, e) \in \Gamma\text{GL}(2m, q)$, with $\tau \in \text{Aut}(\text{GF}(q))$ and $e \in \text{GL}(2m, q)$, such that for some $\lambda(\tau, e) \in \text{GF}(q)$ we have $\psi(\xi^\tau e, \eta^\tau e) = \lambda(\tau, e) \psi(\xi, \eta)^\tau$ for all $\xi, \eta$ in $\text{GF}(q)^{2m}$. Also define: the projective general symplectic group $\text{PGSp}(2m, q) = \Theta_{2m}(\text{GSp}(2m, q))$, and the projective semilinear symplectic group $\Gamma\text{PSp}(2m, q) = \Theta_2m(\Gamma\text{Sp}(2m, q))$. For the definition of the orthogonal groups $\Omega(2m+1, q) < \text{GO}(2m+1, q) < \text{GO}(2m+1, q) = \text{GO}(2m+1, q) < \text{PGO}(2m+1, q) < \text{PGO}(2m+1, q) < \text{PGO}(2m+1, q)$ see [Tay]. 3

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

\begin{equation}
\text{Sp}(2m, q) < H \Leftrightarrow \text{PSp}(2m, q) < \Theta_{2m}(H).
\end{equation}

This follows exactly as in the proof of Lemma 2.3 of [A04] because by (22.4) of [Asc] $\text{Sp}(2m, q)$ is generated by transvections. The order of every transvection is $p$ or $1$, and hence $\text{Sp}(2m, q)$ is a quasi-$p$ group.

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

\begin{equation}
\text{Sp}(2m, q) < H \Leftrightarrow \text{Sp}(2m, q) < H < \text{GSp}(2m, q)
\end{equation}

and by 2.1.C of [LiK] we have

\begin{equation}
[\text{GSp}(2m, q) : \text{Sp}(2m, q)] \not\equiv 0 \pmod{p}.
\end{equation}

Since $\text{Sp}(2m, q)$ is quasi-$p$, it follows that it is generated by the $p$-power elements of $\text{Sp}(2m, q)\text{GF}(q)^*$, and hence these two subgroups have the same normalizer in $\text{GL}(2m, q)$.

---

2Dickson (pages 89–100 of [Dic]) writes $\text{SA}(2m, q)$ for $\text{Sp}(2m, q)$ and calls it the special Abelian linear group; he writes $\Lambda(2m, q)$ for $\text{PSp}(2m, q)$ and shows that it is simple provided $(m, q) \neq (2, 2)$.

Our notation essentially follows [LiK] where these are defined for each symplectic form. In this connection note that if $\Phi < \Gamma\text{GL}(2m, q)$ is such that $\Phi$ is isomorphic to $\text{PSp}(2m, q)$ then $\text{PSp}(2m, q) = \delta^{-1} \Phi \delta$ for some $\delta \in \Gamma\text{GL}(2m, q)$ (see the fifth line of Table 5.4.C on page 200 of [LiK] which starts with $C_l(q)$).

3In [Tay] these are defined for each quadratic form. We take the specific quadratic form $x_1 x_{m+1} + \cdots + x_m x_{2m} + x_{2m+1}^2$ which gives us specific orthogonal groups; for $p \neq 2$ we could take it to be $x_1^2 + \cdots + x_m^2 x_{2m+1}$. By the singular points of $\Pi\Omega(2m+1, q)$ we mean the images in $\mathcal{P}(\text{GF}(q)^{2m+1})$ of the nonzero $\xi \in \text{GF}(q)^{2m+1}$ at which the quadratic form vanishes. Note that $\Pi\Omega(2m+1, q)$ acts faithfully and transitively on its singular points (see 11.24, 11.27 and 11.48 of [Tay]). Also note that if $m > 2$ and $p \neq 2$ then $\Pi\Omega(2m+1, q)$ and $\text{PSp}(2m, q)$ are non-isomorphic groups of the same order (see 11.54 of [Tay]), and there does not exist any homomorphism of $\Pi\Omega(2m+1, q)$ into $\Gamma\text{GL}(2m, q)$ except the trivial homomorphism which sends everything to $1$ (see the third line of Table 5.4.C on page 200 of [LiK] which starts with $B_l(q)$). Finally note that if either $m = 2$ or $p = 2$ then $\Pi\Omega(2m+1, q)$ and $\text{PSp}(2m, q)$ are isomorphic (see 11.9 and 12.32 of [Tay]).
GL(2m, q). Also clearly GF(q)* < GSp(2m, q). Therefore by (5.2), for any G < PGL(2m, q) we have
\[(5.4) \quad PSp(2m, q) \triangleleft G \iff PSp(2m, q) < G < PGSp(2m, q)\]
and by (5.3) we get
\[(5.5) \quad [PGSp(2m, q) : PSp(2m, q)] \neq 0 \pmod{p}.
Finally, since GF(q)* < GSp(2m, q), for any H < GL(2m, q) we have
\[(5.6) \quad H < GSp(2m, q) \iff \Theta_{2m}(H) < PGSp(2m, q).
In view of Theorem IV of [CaK], by Corollary 1(i) of Kantor [Kan] we get the following corrected version of the first part of Sample from CR3 on page 90 of [A03]:

**Theorem (5.7) [Kantor].** *Assume that m > 2. Let G be a transitive permutation group of Rank 3 with subdegrees 1, q(2m − 3) and q2m−1. Then either the permuted set can be identified with \( \mathcal{P}(GF(q)^{2m}) \) so that Psp(2m, q) < PSp(2m, q), or the permuted set can be identified with the singular points of PΩ(2m+1, q) so that PΩ(2m+1, q) \( \triangleleft G < PTO(2m+1, q) \) where PΩ(2m+1, q) and PTO(2m+1, q) denote the permutation groups on the said singular points induced by PΩ(2m+1, q) and PTO(2m+1, q) respectively.

In view of the preceding two footnotes, we get the following corollary of (5.7):

**Corollary (5.8).** *Assume that m > 2. Let G < PGL(2m, q) be transitive Rank 3 on \( \mathcal{P}(GF(q)^{2m}) \) with subdegrees 1, q(2m − 3) and q2m−1. Then PSp(2m, q) \( \triangleleft \delta^{-1}G\delta \) for some \( \delta \in PGL(2m, q) \)

6. Galois Groups

By (4.6), (4.7), (5.1), (5.6) and (5.8) we get the following:

**Theorem (6.1).** *If m > 2 and GF(q) \( \subset k_p \) then, for 1 ≤ e ≤ m − 1, in a natural manner we have*
\[\text{Sp}(2m, q) < \text{Gal}(\phi_e, k_p(X, T_1, \ldots, T_e)) < \text{GSp}(2m, q)\]
*and*
\[\text{Psp}(2m, q) < \text{Gal}(f_e, k_p(X, T_1, \ldots, T_e)) < \text{PGSp}(2m, q).\]
*Hence in particular, if m > 2 and GF(q) \( \subset k_p \) then, in a natural manner we have*
\[\text{Sp}(2m, q) < \text{Gal}(\phi, k_p(X, T_1, \ldots, T_e)) < \text{GSp}(2m, q)\]
*and*
\[\text{Psp}(2m, q) < \text{Gal}(f, k_p(X, T_1, \ldots, T_e)) < \text{PGSp}(2m, q).\]
By (4.8), (5.2), (5.3), (5.4), (5.5) and (6.1) we get the following:

**Theorem (6.2).** *If m > 2 and k_p is algebraically closed, then, for 1 ≤ e ≤ m − 1, in a natural manner we have*
\[\text{Gal}(\phi, k_p(X, T_1, \ldots, T_{m-1})) = \text{Gal}(\phi_e, k_p(X, T_1, \ldots, T_e)) = \text{Sp}(2m, q)\]
*and*
\[\text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1})) = \text{Gal}(f_e, k_p(X, T_1, \ldots, T_e)) = \text{Psp}(2m, q).\]
*Remark (6.3).* We shall discuss the \( m = 2 \) case elsewhere.
MORE NICE EQUATIONS FOR NICE GROUPS

REFERENCES


DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907
E-mail address: ram@cs.purdue.edu

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use