PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 10, October 1996

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 $\mathrm{PSp}(2m,q)$ and $\mathrm{Sp}(2m,q)$ 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 $F=F(Y)=Y^n+T^qY^u+XY^v+TY^w+1$ and $F^*=F^*(Y)=Y^{n^*}+XY+1$ in indeterminates T,X,Y over an algebraically closed field k of characteristic p, where $n=1+q+\cdots+q^{2m-1}$, $u=1+q+\cdots+q^m$, $v=1+q+\cdots+q^{m-1}$, $w=1+q+\cdots+q^{m-2}$, $n^*=1+q+\cdots+q^{m-1}$, and consider their respective Galois groups $\mathrm{Gal}(F,k(X,T))$ 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 symplectic group $\mathrm{PSp}(2m,q)$. 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 $\mathrm{PSp}(2m,q)$, I shall show that the Galois group of a more general polynomial f is also $\mathrm{PSp}(2m,q)$. Moreover, by slightly changing f and F, I shall show that we get polynomials ϕ and ϕ_1 whose Galois group is the symplectic group $\mathrm{Sp}(2m,q)$. The polynomials f,ϕ and ϕ_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).

Received by the editors March 21, 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.

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.[1] To abbreviate frequently occurring expressions, for every integer $i \geq -1$ we put

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

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

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

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 $k_p[X, T_1, \ldots, T_{m-1}]$. 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 $\mathrm{Disc}_Y(f) = 1$ where $\mathrm{Disc}_Y(f)$ is the Y-discriminant of f, and hence the Galois group $\mathrm{Gal}(f, k_p(X, T_1, \ldots, T_{m-1}))$ is well-defined as a subgroup of the symmetric group $\mathrm{Sym}_{\langle 2m-1 \rangle}$. 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

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

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

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 $q\langle 2m-3 \rangle$ and q^{2m-1}. In

[1] 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 $1 \le e \le m-1$, and therefore $\mathrm{Gal}(f, k(X, T_1, \ldots, T_{m-1}))$ and $\mathrm{Gal}(f_e, k_p(X, T_1, \ldots, T_e))$ are Rank 3 groups with subdegrees 1, $q\langle 2m-3\rangle$ 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 $\mathrm{Gal}(f, k_p(X, T_1, \ldots, T_{m-1})) = \mathrm{Gal}(f_e, k_p(X, T_1, \ldots, T_e)) = \mathrm{PSp}(2m, q)$ for $1 \le e \le m-1$.

Consider the monic polynomials

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

and

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

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, $\mathrm{Disc}_Y(\phi) = \mathrm{Disc}_Y(\phi_e) = 1$. In Section 6, as a consequence of the above result about the Galois groups of f and f_e, we show that if $m > 2$ and k_p is algebraically closed then $\mathrm{Gal}(\phi, k_p(X, T_1, \ldots, T_{m-1})) = \mathrm{Gal}(\phi_e, k_p(X, T_1, \ldots, T_e)) = \mathrm{Sp}(2m, q)$ for $1 \le e \le m-1$.

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

3. Twisted derivative and its factorization

Solving the equation $f = 0$ we get

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

and hence

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

and therefore

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

To simplify g we observe that

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

and hence

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

and also

$$\begin{aligned}
\frac{Z^{\langle m-1\rangle(q^m+1)}-1}{Z^{\langle m-1\rangle}-1} - 1 &= Z^{\langle m-1\rangle} + Z^{2\langle m-1\rangle} + \cdots + Z^{q^m\langle m-1\rangle} \\
&= Z^{\langle m-1\rangle}\left(Z^{\langle m-1\rangle}-1\right)^{(q^m-1)} \\
&= Z^{\langle m-1\rangle}\left(Z^{\langle m-1\rangle}-1\right)^{(q-1)\langle m-1\rangle} \\
&= \left[Z\left(Z^{\langle m-1\rangle}-1\right)^{(q-1)}\right]^{\langle m-1\rangle}
\end{aligned}$$

and therefore

$$\begin{aligned}
&\frac{Z^{\langle 2m-1\rangle}-1}{Z-1} - \frac{Z^{\langle m-1\rangle}-1}{Z-1}\left(1+Y^{\langle 2m-1\rangle}\right) \\
&= \frac{Z^{\langle m-1\rangle}-1}{Z-1}\left\{\left[Z\left(Z^{\langle m-1\rangle}-1\right)^{(q-1)}\right]^{\langle m-1\rangle} - \left[Y^{q^m+1}\right]^{\langle m-1\rangle}\right\}.
\end{aligned}$$

Moreover

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

and

$$Y^{\langle 2m-1\rangle - \langle m-1+i\rangle} = Y^{q^{m+i}\langle m-1-i\rangle}$$

and hence

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

Similarly

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

Thus

$$g = A - B + C \tag{3.0}$$

where

$$A=\sum_{i=1}^{m-1}\frac{Z^{\langle m-1\rangle}\left(Z^{\langle i-1\rangle}-1\right)^{q^m}}{Z-1}Y^{q^{m+i}\langle m-1-i\rangle}T_i^{q^i},$$

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

and

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

To simplify g further, upon letting

$$\widehat{g}=g/L,\quad \widehat{A}=A/L,\quad \widehat{B}=B/L,\quad\text{and}\quad \widehat{C}=C/L,\quad\text{where } L=\frac{Z^{\langle m-1\rangle}-1}{Z-1},$$

we get

$$g = L\widehat{g}\quad\text{and}\quad \widehat{g}=\widehat{A}-\widehat{B}+\widehat{C}$$

with

$$\widehat{A}=\sum_{i=1}^{m-1}\frac{Z^{\langle m-1\rangle}\left(Z^{\langle i-1\rangle}-1\right)^{q^m}}{Z^{\langle m-1\rangle}-1}Y^{q^{m+i}\langle m-1-i\rangle}T_i^{q^i},$$

$$\widehat{B}=\sum_{i=1}^{m-1}\frac{Z^{\langle m-1-i\rangle}\left(Z^{\langle i-1\rangle}-1\right)^{q^{m-i}}}{Z^{\langle m-1\rangle}-1}Y^{q^{m-i}\langle m-1+i\rangle}T_i$$

and

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

and hence upon letting

$$U = Z\left(Z^{\langle m-1\rangle} - 1\right)^{(q-1)}, \qquad J = Y^{q^m+1},$$

and

$$V_i = \frac{Z^{\langle m-1-i\rangle}\left(Z^{\langle i-1\rangle} - 1\right)^{q^{m-i}}}{\left(Z^{\langle m-1\rangle} - 1\right)Y^{\langle m-1-i\rangle}} \quad \text{for } 1 \le i \le m-1$$

we get

$$\widehat{A} = \sum_{i=1}^{m-1} U^{\langle i-1\rangle}(V_iT_i)^{q^i}J^{\langle m-1\rangle-\langle i-1\rangle}, \qquad \widehat{B} = \sum_{i=1}^{m-1}(V_iT_i)J^{\langle m-1\rangle},$$

and

$$\widehat{C} = U^{\langle m-1\rangle} - J^{\langle m-1\rangle} \quad \text{with} \quad J^{\langle m-1\rangle} = Y^{\langle 2m-1\rangle},$$

and therefore upon letting

$$\widetilde{g} = \widehat{g}/Y^{\langle 2m-1\rangle}, \quad \widetilde{A} = \widehat{A}/Y^{\langle 2m-1\rangle}, \quad \widetilde{B} = \widehat{B}/Y^{\langle 2m-1\rangle}, \quad \widetilde{C} = \widehat{C}/Y^{\langle 2m-1\rangle},$$

and

$$W = U/J, \qquad \widetilde{T}_i = V_iT_i$$

we get

$$g = Y^{\langle 2m-1\rangle}L\widetilde{g} \quad \text{and} \quad \widetilde{g} = \widetilde{A} - \widetilde{B} + \widetilde{C}$$

with

$$\widetilde{A} = \sum_{i=1}^{m-1} W^{\langle i-1\rangle}\widetilde{T}_i^{q^i}, \quad \widetilde{B} = \sum_{i=1}^{m-1}\widetilde{T}_i, \quad \text{and} \quad \widetilde{C} = W^{\langle m-1\rangle} - 1,$$

where

$$W = \frac{Z\left(Z^{\langle m-1\rangle} - 1\right)^{(q-1)}}{Y^{q^m+1}} \quad \text{and} \quad \widetilde{T}_i = \frac{Z^{\langle m-1-i\rangle}\left(Z^{\langle i-1\rangle} - 1\right)^{q^{m-i}}}{\left(Z^{\langle m-1\rangle} - 1\right)Y^{\langle m-1-i\rangle}}T_i.$$

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

$$W\widetilde{T}_1^q - \widetilde{T}_1 + W^{\langle m-1\rangle} - 1.$$

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 $(W, \widetilde{T}_1)$ to (V, R), we try to factor

$$VR^q - R + V^{\langle m-1\rangle} - 1$$

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

$$M = -\sum_{\mu=0}^{m-1} V^{\langle m-2-\mu\rangle}$$

we have

$$VM^q = -\sum_{\mu=0}^{m-1} V^{\langle m-1-\mu\rangle}$$

and hence

$$VM^q - M + V^{\langle m-1\rangle} - 1 = 0$$

and therefore

$$\begin{aligned}(R-M)\left[V\left(R^{q-1}+MR^{q-2}+\cdots+M^{q-1}\right)-1\right] =& V(R^q-M^q)-R+M\\ =& VR^q - R - (VM^q - M)\\ =& VR^q - R + V^{\langle m-1\rangle} - 1.\end{aligned}$$

Now upon taking an indeterminate S and letting

$$P = \sum_{j=0}^{i-1} V^{\langle j-1\rangle} S^{q^j}$$

we have

$$\begin{aligned}VP^q - P =& \left(\sum_{j=1}^{i} V^{\langle j-1\rangle} S^{q^j}\right) - \left(\sum_{j=0}^{i-1} V^{\langle j-1\rangle} S^{q^j}\right)\\ =& V^{\langle i-1\rangle} S^{q^i} - S\end{aligned}$$

and hence upon taking indeterminates $S_1, \dots, S_{m-1}$ and letting

$$D = \sum_{i=1}^{m-1}\sum_{j=0}^{i-1} V^{\langle j-1\rangle} S_i^{q^j}$$

we have

$$VD^q - D = \sum_{i=1}^{m-1}\left(V^{\langle i-1\rangle} S_i^{q^i} - S_i\right)$$

and therefore by substituting D for R in the factorization

$$VR^q - R + V^{\langle m-1\rangle} - 1 = (R-M)\left[V\left(R^{q-1}+MR^{q-2}+\cdots+M^{q-1}\right)-1\right]$$

we get the factorization

$$\begin{aligned}&\left(\sum_{i=1}^{m-1} V^{\langle i-1\rangle} S_i^{q^i}\right) - \left(\sum_{i=1}^{m-1} S_i\right) + V^{\langle m-1\rangle} - 1\\ &= (D-M)\left[V\left(D^{q-1}+MD^{q-2}+\cdots+M^{q-1}\right)-1\right].\end{aligned}$$

Substituting $(W, \widetilde{T}_i)$ for (V, S_i) in the above equation we get

$$\widetilde{g} = (E-N)\left[W\left(E^{q-1}+NE^{q-2}+\cdots+N^{q-1}\right)-1\right]$$

where

$$E = \sum_{i=1}^{m-1}\sum_{j=0}^{i-1} W^{\langle j-1\rangle}\widetilde{T}_i^{q^j} \quad \text{and} \quad N = -\sum_{\mu=0}^{m-1} W^{\langle m-2-\mu\rangle}$$

and hence upon remembering that $g = Y^{\langle 2m-1\rangle} L\widetilde{g}$ we get

$$g = Y^{\langle 2m-1\rangle} L(E-N)\left[W\left(E^{q-1} + NE^{q-2} + \cdots + N^{q-1}\right) - 1\right]$$

and we recall that

$$L = \frac{Z^{\langle m-1\rangle} - 1}{Z-1}$$

and

$$W = \frac{Z\left(Z^{\langle m-1\rangle} - 1\right)^{(q-1)}}{Y^{q^m+1}}, \qquad \widetilde{T}_i = \frac{Z^{\langle m-1-i\rangle}\left(Z^{\langle i-1\rangle} - 1\right)^{q^{m-i}}}{\left(Z^{\langle m-1\rangle} - 1\right) Y^{\langle m-1-i\rangle}} T_i.$$

Substituting the above values of W and $\widetilde{T}_i$ in E we get

$$E = \sum_{i=1}^{m-1}\sum_{j=0}^{i-1} \frac{Z^{\langle m-1-i+j\rangle}\left(Z^{\langle i-1\rangle} - 1\right)^{q^{m-i+j}}}{\left(Z^{\langle m-1\rangle} - 1\right) Y^{q^j\langle m-1-i\rangle + (q^m+1)\langle j-1\rangle}} T_i^{q^j}.$$

Now upon letting

$$G_i = Z\left(Z^{\langle i-1\rangle} - 1\right)^{q-1} \qquad \text{and} \qquad H_i = 1 + Z + Z^2 + \cdots + Z^{\langle i-1\rangle - 1}$$

we get

$$L = H_m, \quad W = \frac{Z\left(Z^{\langle m-1\rangle} - 1\right)^{(q-1)}}{Y^{q^m+1}} = \frac{G_m}{Y^{q^m+1}}, \quad N = -\sum_{\mu=0}^{m-1} \frac{G_m^{\langle m-2-\mu\rangle}}{Y^{(q^m+1)\langle m-2-\mu\rangle}},$$

and

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

and hence

$$LE = \sum_{i=1}^{m-1}\sum_{j=0}^{i-1} \frac{G_i^{\langle m-1-i+j\rangle} H_i}{Y^{q^j\langle m-1-i\rangle + (q^m+1)\langle j-1\rangle}} T_i^{q^j}$$

and

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

By factoring the maximal negative power of Y from N, E, LE and LN, we get

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

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

$$LE = \sum_{i=1}^{m-1}\sum_{j=0}^{i-1} \frac{G_i^{\langle m-1-i+j\rangle} H_i Y^{q^{m+j}\langle m-2-j\rangle + q^{m-i+j}\langle i-j-2\rangle}}{Y^{(q^m+1)\langle m-2\rangle}} T_i^{q^j},$$

and

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

Therefore upon letting

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

we get

$$g = g'g'' \tag{3.1}$$

with

$$\begin{aligned} g' &= \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} G_i^{\langle m-1-i+j\rangle} H_i Y^{q^{m+j}\langle m-2-j\rangle + q^{m-i+j}\langle i-j-2\rangle} T_i^{q^j} \\ &+ \sum_{\mu=0}^{m-1} G_m^{\langle m-2-\mu\rangle} H_m Y^{(q^m+1)q^{m-1-\mu}\langle \mu-1\rangle} \end{aligned} \tag{3.2}$$

and

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

where

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

and

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

and where we recall that

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

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

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

and hence

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

$$\deg_Z G_m^{\langle m-2\rangle} H_m > \deg_Z G_m^{\langle m-2-\mu\rangle} H_m \quad \text{for } 1 \le \mu \le m-1,$$

and

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

therefore, noting that $Y^{(q^m+1)q^{m-1-\mu}\langle \mu-1\rangle} = 1$ for $\mu = 0$, in view of (3.2) we conclude that g' is a monic polynomial of degree $q\langle 2m-3\rangle$ in Z with coefficients in

$\mathrm{GF}(p)[Y,T_1,\dots,T_{m-1}]$. Obviously g is a monic polynomial in Z with coefficients in $\mathrm{GF}(p)[Y,T_1,\dots,T_{m-1}]$ and

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

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 $\mathrm{GF}(p)[Y,T_1,\dots,T_{m-1}]$. Thus

$$(3.7)\qquad \begin{cases} g' \text{ and } g'' \text{ are monic polynomials of degrees } q\langle 2m-3\rangle \text{ and } q^{2m-1} \\ \text{in } Z \text{ with coefficients in } \mathrm{GF}(p)[Y,T_1,\dots,T_{m-1}] \text{ respectively.}\end{cases}$$

4. Irreducibility

For $1 \le e \le m-1$, let f'_e, g_e, g'_e, g''_e be the members of $\mathrm{GF}(p)[Y,Z,T_1,\dots,T_e]$ obtained by putting $T_i = 0$ for all $i > e$ in f', g, g', g'' respectively. Then f'_e is the twisted derivative of 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 $\langle 2m-1\rangle - 1$ in Z with coefficients in $\mathrm{GF}(p)[Y,T_1,\dots,T_e]$. Also

$$(4.1)\qquad \begin{cases} \text{for } 1 \le e \le m-1 \text{ we have } g_e = g'_e g''_e \text{ where } g'_e \text{ and } g''_e \text{ are} \\ \text{monic polynomials of degrees } q\langle 2m-3\rangle \text{ and } q^{2m-1} \text{ in } Z \\ \text{with coefficients in } \mathrm{GF}(p)[Y,T_1,\dots,T_e] \text{ respectively.}\end{cases}$$

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 $\mathrm{GF}(p)[Y,Z]$ given by

$$A_1 = Z^{\langle m-1\rangle}(Z-1)^{(q-1)\langle m-1\rangle} Y^{q^{m+1}\langle m-2\rangle},$$

$$B_1 = Z^{\langle m-2\rangle}(Z-1)^{(q-1)\langle m-2\rangle} Y^{q^{m-1}\langle m\rangle},$$

and

$$C_1 = \left(1 + Z + Z^2 + \dots + Z^{\langle m-1\rangle - 1}\right) \times \left\{ \left[Z\left(Z^{\langle m-1\rangle} - 1\right)^{(q-1)}\right]^{\langle m-1\rangle} - \left[Y^{q^m+1}\right]^{\langle m-1\rangle}\right\}.$$

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 $\mathrm{GF}(p)[Y,Z]$ given by

$$A'_1 = Z^{\langle m-2\rangle}(Z-1)^{(q-1)\langle m-2\rangle} Y^{q^m\langle m-2\rangle}$$

and

$$B'_1 = \sum_{\mu=0}^{m-1} \left[Z\left(Z^{\langle m-1\rangle} - 1\right)^{q-1}\right]^{\langle m-2-\mu\rangle} \times \left(1 + Z + Z^2 + \dots + Z^{\langle m-1\rangle - 1}\right) Y^{(q^m+1)q^{m-1-\mu}\langle \mu-1\rangle}.$$

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 $g_0 = g_0'g_0''$ 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 $\mathrm{GCD}(q-1, I(B_0/A_0)) = 1$. Then g_0'' is irreducible in $Q[T]$.*

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

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

where Λ is an element in an algebraic closure Q^* of Q with $\Lambda^{q-1} = B_0/A_0$. It follows that for any root Δ of g'' in Q^* we must have $\Delta = j\Lambda - (B_0'/A_0')$ for some $0 \neq j \in \mathrm{GF}(q)$. 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

$$\begin{aligned} I^*(\Delta + (B_0'/A_0')) &= I^*(j\Lambda) \\ &= I^*(j^{q-1}\Lambda^{q-1})/(q-1) \\ &= I^*(B_0/A_0)/(q-1) = rI(B_0/A_0)/(q-1). \end{aligned}$$

Therefore, since $I^*(\Delta + (B_0'/A_0'))$ is obviously an integer, so is $rI(B_0/A_0)/(q-1)$. Since $\mathrm{GCD}(q-1, I(B_0/A_0)) = 1$, it follows that r is divisible by $q-1$. Since the field degree $[Q(\Delta) : Q]$ is at least r, we conclude that $[Q(\Delta) : Q] \geq q-1$. Since Δ 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 κ be a field, and let $g_0 = g_0'g_0''$ 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 $\kappa(X_1, \ldots, X_d, Z)[T]$. 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' 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 $\mathrm{GCD}(q-1, I(B_1/A_1)) = 1$. 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) the polynomials g_1' and g_1'' are irreducible in $k_p(Y, T_1)[Z]$.

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

$$(4.5)\quad \begin{cases} \text{the polynomials } g' \text{ and } g'' \text{ are irreducible in } k_p(Y, T_1, \ldots, T_{m-1})[Z] \\ \text{and, for } 1 \leq e \leq m-1, \\ \text{the polynomials } g_e' \text{ and } g_e'' \text{ are irreducible in } k_p(Y, T_1, \ldots, T_e)[Z]. \end{cases}$$

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 $1 \le e \le m-1$, we have that* $\mathrm{Gal}(f_e, k_p(X, T_1, \dots, T_e))$ *is a transitive permutation group of Rank 3 with subdegrees 1,* $q\langle 2m-3\rangle$ *and* q^{2m-1}*. Hence in particular,* $\mathrm{Gal}(f, k_p(X, T_1, \dots, T_{m-1}))$ *is a transitive permutation group of Rank 3 with subdegrees 1,* $q\langle 2m-3\rangle$ *and* q^{2m-1}*.*

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] we get the following:

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

$$\mathrm{Gal}(\phi_e, k_p(X, T_1, \dots, T_e)) < \mathrm{GL}(2m, q)$$

and

$$\mathrm{Gal}(f_e, k_p(X, T_1, \dots, T_e)) < \mathrm{PGL}(2m, q)$$

and then we have

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

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

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

and

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

and then we have

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

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

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

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

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

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* $\mathrm{Sp}(2m, q)$ as the group of all $e = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2m, q)$, where a, b, c, d are m by m matrices over $\mathrm{GF}(q)$, 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., $\psi(xe, ye) = \psi(x, y)$, or equivalently for which: $ad - bc =$ the m by m identity matrix, and $ab' - ba' = 0 = cd' - dc'$ where $'$ = transpose; note that $\mathrm{Sp}(2m, q) < \mathrm{SL}(2m, q)$, and define the *projective symplectic group* $\mathrm{PSp}(2m, q) = \Theta_{2m}(\mathrm{Sp}(2m, q))$.[2] Let the *general symplectic group* $\mathrm{GSp}(2m, q)$ 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 $\psi(\xi e, \eta e) = \lambda(e)\psi(\xi, \eta)$ for all ξ, η in $\mathrm{GF}(q)^{2m}$. Let the *semilinear symplectic group* $\Gamma\mathrm{Sp}(2m, q)$ 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 $\psi(\xi^\tau e, \eta^\tau e) = \lambda(\tau, e)\psi(\xi, \eta)^\tau$ for all ξ, η in $\mathrm{GF}(q)^{2m}$. Also define: the *projective general symplectic group* $\mathrm{PGSp}(2m, q) = \Theta_{2m}(\mathrm{GSp}(2m, q))$, and the *projective semilinear symplectic group* $\mathrm{P}\Gamma\mathrm{Sp}(2m, q) = \Theta_{2m}(\Gamma\mathrm{Sp}(2m, q))$. For the definition of the orthogonal groups $\Omega(2m+1, q) < \mathrm{O}(2m+1, q) < \mathrm{GO}(2m+1, q) < \Gamma\mathrm{O}(2m+1, q)$ and $\mathrm{P}\Omega(2m+1, q) < \mathrm{PO}(2m+1, q) < \mathrm{PGO}(2m+1, q) < \mathrm{P}\Gamma\mathrm{O}(2m+1, q)$ see [Tay].[3]

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

$$\mathrm{Sp}(2m, q) < H \Leftrightarrow \mathrm{PSp}(2m, q) < \Theta_{2m}(H). \tag{5.1}$$

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

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

$$\mathrm{Sp}(2m, q) \lhd H \Leftrightarrow \mathrm{Sp}(2m, q) < H < \mathrm{GSp}(2m, q) \tag{5.2}$$

and by 2.1.C of [LiK] we have

$$[\mathrm{GSp}(2m, q) : \mathrm{Sp}(2m, q)] \not\equiv 0 \pmod{p}. \tag{5.3}$$

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

---

[2] Dickson (pages 89–100 of [Dic]) writes $\mathrm{SA}(2m, q)$ for $\mathrm{Sp}(2m, q)$ and calls it the *special Abelian linear group*; he writes $\mathrm{A}(2m, q)$ for $\mathrm{PSp}(2m, q)$ 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 $\Phi < \mathrm{PGL}(2m, q)$ is such that Φ is isomorphic to $\mathrm{PSp}(2m, q)$ then $\mathrm{PSp}(2m, q) = \delta^{-1}\Phi\delta$ for some $\delta \in \mathrm{PGL}(2m, q)$ (see the fifth line of Table 5.4.C on page 200 of [LiK] which starts with $C_l(q)$).

[3] In [Tay] these are defined for each quadratic form. We take the specific quadratic form $x_1x_{m+1} + \cdots + x_m x_{2m} + x_{2m+1}^2$ which gives us specific orthogonal groups; for $p \neq 2$ we could take it to be $x_1^2 + \cdots + x_{2m+1}^2$. By the *singular points* of $\mathrm{P}\Omega(2m+1, q)$ we mean the images in $\mathcal{P}(\mathrm{GF}(q)^{2m+1})$ of the nonzero $\xi \in \mathrm{GF}(q)^{2m+1}$ at which the quadratic form vanishes. Note that $\mathrm{P}\Omega(2m+1, q)$ 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 $\mathrm{P}\Omega(2m+1, q)$ and $\mathrm{PSp}(2m, q)$ are non-isomorphic groups of the same order (see 11.54 of [Tay]), and there does not exist any homomorphism of $\mathrm{P}\Omega(2m+1, q)$ into $\mathrm{PGL}(2m, q)$ 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 $\mathrm{P}\Omega(2m+1, q)$ and $\mathrm{PSp}(2m, q)$ 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

$$\text{PSp}(2m,q) \lhd G \Leftrightarrow \text{PSp}(2m,q) < G < \text{PGSp}(2m,q) \tag{5.4}$$

and by (5.3) we get

$$[\text{PGSp}(2m,q) : \text{PSp}(2m,q)] \not\equiv 0 \pmod{p}. \tag{5.5}$$

Finally, since GF$(q)^* <$ GSp$(2m,q)$, for any $H <$ GL$(2m,q)$ we have

$$H < \text{GSp}(2m,q) \Leftrightarrow \Theta_{2m}(H) < \text{PGSp}(2m,q). \tag{5.6}$$

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, $q\langle 2m-3\rangle$ and q^{2m-1}. Then either the permuted set can be identified with $\mathcal{P}(\text{GF}(q)^{2m})$ so that $\text{Psp}(2m,q) \lhd G < \text{P}\Gamma\text{Sp}(2m,q)$, or the permuted set can be identified with the singular points of $\text{P}\Omega(2m+1,q)$ so that $\text{P}\Omega(2m+1,q)_1 \lhd G < \text{P}\Gamma\text{O}(2m+1,q)_1$ where $\text{P}\Omega(2m+1,q)_1$ and $\text{P}\Gamma\text{O}(2m+1,q)_1$ denote the permutation groups on the said singular points induced by $\text{P}\Omega(2m+1,q)$ and $\text{P}\Gamma\text{O}(2m+1,q)$ respectively.*

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

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

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 $\text{GF}(q) \subset k_p$ then, for $1 \le e \le m-1$, in a natural manner we have*

$$\text{Sp}(2m,q) < \text{Gal}(\phi_e, k_p(X,T_1,\dots,T_e)) < \text{GSp}(2m,q)$$

and

$$\text{Psp}(2m,q) < \text{Gal}(f_e, k_p(X,T_1,\dots,T_e)) < \text{PGSp}(2m,q).$$

Hence in particular, if $m > 2$ and $\text{GF}(q) \subset k_p$ then, in a natural manner we have

$$\text{Sp}(2m,q) < \text{Gal}(\phi, k_p(X,T_1,\dots,T_e)) < \text{GSp}(2m,q)$$

and

$$\text{Psp}(2m,q) < \text{Gal}(f, k_p(X,T_1,\dots,T_e)) < \text{PGSp}(2m,q).$$

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 $1 \le e \le m-1$, in a natural manner we have*

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

and

$$\text{Gal}(f, k_p(X,T_1,\dots,T_{m-1})) = \text{Gal}(f_e, k_p(X,T_1,\dots,T_e)) = \text{Psp}(2m,q).$$

Remark (6.3). We shall discuss the $m = 2$ 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. CMP 95:04

[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`