

ONCE MORE NICE EQUATIONS FOR NICE GROUPS

SHREERAM S. ABHYANKAR AND PAUL A. LOOMIS

(Communicated by Ronald M. Solomon)

ABSTRACT. In a previous paper, nice quintinomial equations were given for unramified coverings of the affine line in nonzero characteristic p with the projective symplectic isometry group $\mathrm{PSp}(2m, q)$ and the (vectorial) symplectic isometry group $\mathrm{Sp}(2m, q)$ as Galois groups where $m > 2$ is any integer and $q > 1$ is any power of p . Here we deform these equations to get nice quintinomial equations for unramified coverings of the once punctured affine line in characteristic p with the projective symplectic similitude group $\mathrm{PGSp}(2m, q)$ and the (vectorial) symplectic similitude group $\mathrm{GSp}(2m, q)$ as Galois groups.

1. INTRODUCTION

Let $m > 2$ be any integer, let $q > 1$ be any power of a prime p , and consider the polynomial $F = F(Y) = Y^n + T^q Y^u + XY^v + TY^w + 1$ in indeterminates T, X, Y over a field k of characteristic p , where $n = 1 + q + \cdots + q^{2m-1}$, $u = 1 + q + \cdots + q^m$, $v = 1 + q + \cdots + q^{m-1}$, $w = 1 + q + \cdots + q^{m-2}$, and consider its Galois group $\mathrm{Gal}(F, k(X, T))$ and the Galois group $\mathrm{Gal}(\Phi, k(X, T))$ of its subvectorial associate $\Phi = \Phi(Y) = F(Y^{q-1})$. Also consider the deformation $F^\sharp = F^\sharp(Y) = Y^n + T^q Y^u + XY^v + S^{v-w} TY^w + S^v$ of F together with its subvectorial associate $\Phi^\sharp = \Phi^\sharp(Y) = F^\sharp(Y^{q-1})$, where S is another indeterminate, and their Galois groups $\mathrm{Gal}(F^\sharp, k(X, S, T))$ and $\mathrm{Gal}(\Phi^\sharp, k(X, S, T))$. In the “More Nice Equations” paper [A06] it was shown that if k is algebraically closed, then $\mathrm{Gal}(F, k(X, T)) =$ the projective symplectic isometry group $\mathrm{PSp}(2m, q)$ and $\mathrm{Gal}(\Phi, k(X, T)) =$ the (vectorial) symplectic isometry group $\mathrm{Sp}(2m, q)$.¹ By modifying the proof given in [A06], we shall show that if $\mathrm{GF}(q) \subset k$, then $\mathrm{Gal}(F^\sharp, k(X, S, T)) =$ the projective symplectic similitude group $\mathrm{PGSp}(2m, q)$ and $\mathrm{Gal}(\Phi^\sharp, k(X, S, T)) =$ the (vectorial) symplectic similitude group $\mathrm{GSp}(2m, q)$.² The said proof given in [A06], as well as the proofs of the corresponding unitary and orthogonal group equations given in

Received by the editors December 1, 1996.

1991 *Mathematics Subject Classification*. Primary 12F10, 14H30, 20D06, 20E22.

The first author’s work was partly supported by NSA grant MDA 904-97-1-0010, and the second author’s work was partly supported by a PRF grant at Purdue University.

¹Here we regard $\mathrm{Sp}(2m, q)$ as acting on nonzero vectors. For the vectorial associate $\widehat{\Phi}(Y) = Y\Phi(Y)$ we then have $\mathrm{Gal}(\widehat{\Phi}, k(X, T)) = \mathrm{Sp}(2m, q)$ regarded as acting on the entire vector space $\mathrm{GF}(q)^{2m}$. For generalities about the Galois groups of projective, subvectorial, and vectorial polynomials see [A09].

²Again here we regard $\mathrm{GSp}(2m, q)$ as acting on nonzero vectors. For the vectorial associate $\widehat{\Phi}^\sharp(Y) = Y\Phi^\sharp(Y)$ we then have $\mathrm{Gal}(\widehat{\Phi}^\sharp, k(X, S, T)) = \mathrm{GSp}(2m, q)$ regarded as acting on the entire vector space $\mathrm{GF}(q)^{2m}$.

[A05] and [A07] respectively, involved very intricate factorizations for some multivariate polynomials. At the end of [A08] these factorizations were codified into a Mantra. By invoking this Mantra, we shall give here a very short and transparent derivation for the factorization of [A06] and its generalizations needed for the GSp equations.

As a by-product of the present modified proof, we shall show that the above results about the Galois groups of Φ and F continue to hold when we replace the assumption of k being algebraically closed by the weaker assumption that $\text{GF}(q) \subset k$. As another by-product of the present modified proof, we shall show that if $\text{GF}(q) \subset k$, then, for every divisor d of $q-1$, upon letting $\Phi^{(d)}$ be obtained by substituting S^d for S in Φ^\sharp we have $\text{Gal}(\Phi^{(d)}, k(X, S, T)) = \text{GSp}^{(d)}(2m, q)$ where we define $\text{GSp}^{(d)}(2m, q)$ by the condition that $\text{Sp}(2m, q) \triangleleft \text{GSp}^{(d)}(2m, q) \triangleleft \text{GSp}(2m, q)$ with $\text{GSp}(2m, q)/\text{GSp}^{(d)}(2m, q) = Z_d$,³ and upon letting $F^{(d)}$ be obtained by substituting S^d for S in F^\sharp we have $\text{Gal}(F^{(d)}, k(X, S, T)) = \text{PGSp}^{(d)}(2m, q)$ where we define $\text{PGSp}^{(d)}(2m, q) =$ the image of $\text{GSp}^{(d)}(2m, q)$ under the canonical epimorphism of $\text{GL}(2m, q)$ onto $\text{PGL}(2m, q)$, and we note that then $\text{PGSp}^{(d)}(2m, q) = \text{PSp}(2m, q)$ or $\text{PGSp}(2m, q)$ according as d is even or odd.⁴ As noted in [A06], the polynomials Φ and F are specializations of more general polynomials ϕ_e and f_e whose Galois groups are $\text{Sp}(2m, q)$ and $\text{PSp}(2m, q)$ respectively, and which are special cases of the families of polynomials giving unramified coverings of the affine line in characteristic p written down in [A02]. In Section 2 we shall formulate the corresponding more general deformations $\phi_e^\sharp, \phi_e^{(d)}, f_e^\sharp, f_e^{(d)}$ whose Galois groups, under certain conditions, will turn out to be $\text{GSp}(2m, q)$, $\text{GSp}^{(d)}(2m, q)$, $\text{PGSp}(2m, q)$, $\text{PGSp}^{(d)}(2m, q)$ respectively, and which may be regarded as giving unramified coverings of the once punctured affine line.

In addition to factorization, as in [A03] to [A07], here the basic techniques of calculating Galois groups will be MTR (= the Method of Throwing away Roots) and RTG (= Recognition Theorems for Groups). On the RTG side we shall again use Kantor's characterization of Rank 3 groups in terms of their subdegrees [Kan], supplemented by the Cameron-Kantor Theorem IV [CaK] on antiflag transitive collineation groups. 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. It is a pleasure to thank Nick Inglis and Ganesh Sundaram 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 $m > 0$ be any integer.⁵ To abbreviate frequently occurring expressions, for every

³Since $\text{Sp}(2m, q) \triangleleft \text{GSp}(2m, q)$ with $\text{GSp}(2m, q)/\text{Sp}(2m, q) = Z_{q-1}$ (see 2.1.2, 2.1.B and 2.1.C of [KLi]), this uniquely characterizes the intermediate group $\text{GSp}^{(d)}(2m, q)$. Note that, as usual, $<$ and \triangleleft denote subgroup and normal subgroup respectively, and Z_d denotes a cyclic group of order d .

⁴In view of the previous footnote, this follows from the fact that $\text{PGSp}(2m, q)/\text{PSp}(2m, q) = Z_2$ or Z_1 according as q is odd or even (see 2.1.D of [KLi]). Note that if q is even, then $\text{PSp}(2m, q) = \text{PGSp}(2m, q)$.

⁵In the Abstract and the Introduction we assumed $m > 2$. But in the rest of the paper, unless stated otherwise, we only assume $m > 0$.

integer $i \geq -1$ we put

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

Let

$$f^b = f^b(Y) = S^{r(m)}XY^{(m-1)} + \sum_{i=1}^m \left(S^{r(m+i)}T_i^{q^i}Y^{(m-1+i)} + S^{r(m-i)}T_iY^{(m-1-i)} \right)$$

where $r = (r(0), \dots, r(2m))$ is a sequence of nonnegative integers with

$$(*) \quad r(2m) = 0$$

such that for some nonnegative integer t we have

$$(**) \quad q^i r(m-i) = r(m+i) + tq^m \langle i-1 \rangle \quad \text{for } 0 \leq i \leq m$$

and note that then f^b is a polynomial of degree $\langle 2m-1 \rangle = 1 + q + q^2 + \dots + q^{2m-1}$ in Y with coefficients in the polynomial ring $k_p[X, S, T_1, \dots, T_m]$ and in it the coefficient of the highest Y -degree term is $T_m^{q^m}$. Let ϕ^b and $\widehat{\phi}^b$ be the subvectorial and vectorial associates of f^b respectively, i.e., let

$$\begin{aligned} \phi^b &= \phi^b(Y) = f^b(Y^{q-1}) \\ &= S^{r(m)}XY^{q^m-1} + \sum_{i=1}^m \left(S^{r(m+i)}T_i^{q^i}Y^{q^{m+i}-1} + S^{r(m-i)}T_iY^{q^{m-i}-1} \right) \end{aligned}$$

and

$$\begin{aligned} \widehat{\phi}^b &= \widehat{\phi}^b(Y) = Y\phi^b(Y) \\ &= S^{r(m)}XY^{q^m} + \sum_{i=1}^m \left(S^{r(m+i)}T_i^{q^i}Y^{q^{m+i}} + S^{r(m-i)}T_iY^{q^{m-i}} \right). \end{aligned}$$

For $0 \leq e \leq m-1$, let f_e^\sharp be obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in f^b , i.e., let

$$\begin{aligned} f_e^\sharp &= f_e^\sharp(Y) = Y^{\langle 2m-1 \rangle} + S^{r(0)} + S^{r(m)}XY^{\langle m-1 \rangle} \\ &\quad + \sum_{i=1}^e \left(S^{r(m+i)}T_i^{q^i}Y^{\langle m-1+i \rangle} + S^{r(m-i)}T_iY^{\langle m-1-i \rangle} \right) \end{aligned}$$

and note that then f_e^\sharp is a monic polynomial of degree $\langle 2m-1 \rangle = 1 + q + q^2 + \dots + q^{2m-1}$ in Y with coefficients in the polynomial ring $k_p[X, S, T_1, \dots, T_e]$. Now the constant term of f_e^\sharp is $S^{r(0)}$ and the Y -exponent of every other term in f_e^\sharp is 1 modulo p , and hence $f_e^\sharp - Yf_{eY}^\sharp = S^{r(0)}$ where f_{eY}^\sharp is the Y -derivative of f_e^\sharp . Therefore⁶ $\text{Disc}_Y(f_e^\sharp) = S^{r(0)q(2m-2)}$ where $\text{Disc}_Y(f_e^\sharp)$ is the Y -discriminant of f_e^\sharp , and hence the Galois group $\text{Gal}(f_e^\sharp, k_p(X, S, T_1, \dots, T_e))$ is well-defined as a subgroup of the symmetric group $\text{Sym}_{\langle 2m-1 \rangle}$, and the equation $f_e^\sharp = 0$ gives an unramified covering of the once punctured affine line over $k_p(X, T_1, \dots, T_e)$. Since f_e^\sharp is linear in X , by the Gauss Lemma it follows that f_e^\sharp is irreducible in $k_p(X, S, T_1, \dots, T_e)[Y]$, and

⁶See the formulas on page 104 of [A03]. As a misprint correction, in line 13 of page 2979 of [A06] $\text{Disc}_Y(\phi) = \text{Disc}_Y(\phi_e) = 1$ should be changed to $\text{Disc}_Y(\phi) = \text{Disc}_Y(\phi_e) = (-1)^{q^{2m-1}}$.

hence its Galois group is transitive. Let ϕ_e^\sharp and $\widehat{\phi}_e^\sharp$ be obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in ϕ^b and $\widehat{\phi}^b$ respectively, and note that then

$$\begin{aligned} \phi_e^\sharp &= \phi_e^\sharp(Y) = f_e^\sharp(Y^{q-1}) = Y^{q^{2m}-1} + S^{r(0)} + S^{r(m)}XY^{q^m-1} \\ &\quad + \sum_{i=1}^e \left(S^{r(m+i)}T_i^{q^i}Y^{q^{m+i}-1} + S^{r(m-i)}T_iY^{q^{m-i}-1} \right) \end{aligned}$$

and

$$\begin{aligned} \widehat{\phi}_e^\sharp &= \widehat{\phi}_e^\sharp(Y) = Y\phi_e^\sharp(Y) = Y^{q^{2m}} + S^{r(0)}Y + S^{r(m)}XY^{q^m} \\ &\quad + \sum_{i=1}^e \left(S^{r(m+i)}T_i^{q^i}Y^{q^{m+i}} + S^{r(m-i)}T_iY^{q^{m-i}} \right) \end{aligned}$$

are the subvectorial and vectorial associates of f_e^\sharp respectively. By a similar calculation, $\text{Disc}_Y(\phi_e^\sharp) = (-1)^{q^{2m}-1}S^{r(0)(q^{2m}-2)}$ and $\text{Disc}_Y(\widehat{\phi}_e^\sharp) = S^{r(0)q^{2m}}$, and hence the Galois groups $\text{Gal}(\phi_e^\sharp, k_p(X, S, T_1, \dots, T_e))$ and $\text{Gal}(\widehat{\phi}_e^\sharp, k_p(X, S, T_1, \dots, T_e))$ are well-defined as subgroups of the symmetric groups on $q^{2m} - 1$ and q^{2m} letters respectively, and the equations $\phi_e^\sharp = 0$ and $\widehat{\phi}_e^\sharp = 0$ give unramified coverings of the once punctured affine line over $k_p(X, T_1, \dots, T_e)$. For every divisor d of $q - 1$, let $f_e^{(d)}, \phi_e^{(d)}, \widehat{\phi}_e^{(d)}$ be obtained by substituting S^d for S in $f_e^\sharp, \phi_e^\sharp, \widehat{\phi}_e^\sharp$ respectively and note that then, as above, the Galois group $\text{Gal}(f_e^{(d)}, k_p(X, S, T_1, \dots, T_e))$ is a well-defined transitive subgroup of $\text{Sym}_{(2m-1)}$, the Galois groups

$$\text{Gal}(\phi_e^{(d)}, k_p(X, S, T_1, \dots, T_e)) \quad \text{and} \quad \text{Gal}(\widehat{\phi}_e^{(d)}, k_p(X, S, T_1, \dots, T_e))$$

are well-defined subgroups of the symmetric groups on $q^{2m} - 1$ and q^{2m} letters respectively, and the equations $f_e^{(d)} = 0, \phi_e^{(d)} = 0, \widehat{\phi}_e^{(d)} = 0$ give unramified coverings of the once punctured affine line over $k_p(X, T_1, \dots, T_e)$.

For $0 \leq e \leq m - 1$, let ϕ_e and f_e be obtained by putting $S = 1$ in ϕ_e^\sharp and f_e^\sharp respectively. Note that, for $1 \leq e \leq m - 1$, these ϕ_e and f_e are the same as those considered in [A06], and if $m > 1$, then ϕ_{m-1} and f_{m-1} respectively coincide with ϕ and f of [A06]. For $0 \leq e \leq m - 1$, let $K_e = k_p(X, T_1, \dots, T_e)$, let G_e and PG_e be the Galois groups of ϕ_e and f_e over K_e respectively, and let G_e^\sharp and PG_e^\sharp be the Galois groups of ϕ_e^\sharp and f_e^\sharp over $K_e(S)$ respectively. Likewise, for $0 \leq e \leq m - 1$, and for every divisor d of $q - 1$, let $G_e^{(d)}$ and $PG_e^{(d)}$ be the Galois groups of $\phi_e^{(d)}$ and $f_e^{(d)}$ over $K_e(S)$ respectively.

In Section 3, we apply the Mantra of [A08] to the twisted derivative of f^b and thereby we prove the Symplectic Rank Theorem (3.6) which says that PG_e^\sharp is a Rank 3 group with subdegrees 1, $q(2m - 3)$ and q^{2m-1} . By again applying the Mantra of [A08] in the Root Extraction Theorem (3.12) of Section 3 we show that, for $0 \leq e \leq m - 1$, the splitting field of $\widehat{\phi}_e^\sharp$ over $K_e(S)$ contains a $(q - 1)$ -th root of its modified constant term S^{tq^m} ; this is an analogue of the $(q - 1)$ -th root extraction trick given in (2.5)(iii) of [A04] which was used there to go from an SL (= special linear group) covering to a GL (= general linear group) covering. In Section 4, from Theorems (3.6) and (3.12) we deduce Theorem (4.2), which says that if $m > 2$ and $\text{GF}(q) \subset k_p$ and $\text{GCD}(t, q - 1) = 1$, then, for $1 \leq e \leq m - 1$ and for every divisor d of $q - 1$, in a natural manner we have $\text{Sp}(2m, q) = G_e \triangleleft \text{GSp}^{(d)}(2m, q) = G_e^{(d)} \triangleleft G_e^\sharp = \text{GSp}(2m, q)$

and $\mathrm{PSp}(2m, q) = \mathrm{PG}_e \triangleleft \mathrm{PGSp}^{(d)}(2m, q) = \mathrm{PG}_e^{(d)} \triangleleft \mathrm{PG}_e^\sharp = \mathrm{PGSp}(2m, q)$. Note that

$$(*) \quad \begin{cases} \text{if } r(i) = \langle 2m - 1 \rangle - \langle i - 1 \rangle \text{ for } 0 \leq i \leq 2m, \\ \text{then conditions } (*) \text{ and } (**) \text{ are satisfied with } t = q^m + 1 \end{cases}$$

and

$$(**) \quad \begin{cases} \text{if } r(m + i) = 0 \text{ and } r(m - i) = q^{m-i} \langle i - 1 \rangle \text{ for } 0 \leq i \leq m, \\ \text{then conditions } (*) \text{ and } (**) \text{ are satisfied with } t = 1. \end{cases}$$

Case (') arises when we homogenize f_e , i.e., when we put $f_e^\sharp(Y) = S^{\langle 2m-1 \rangle} f_e(Y/S)$, and so we may call it the *homogeneous case*; we shall deal with this in greater detail elsewhere. By analogy, case (**) may be called the *twisted homogeneous case*. In the twisted homogeneous case (**), if $m > 2$ and $\mathrm{GF}(q) \subset k_p$, then by taking $k = k_p$ and $T_1 = T$ in ϕ_1^\sharp and f_1^\sharp we get Φ^\sharp and F^\sharp respectively, and hence by the above result we have $\mathrm{Gal}(\Phi^\sharp, k(X, S, T)) = \mathrm{GSp}(2m, q)$ and $\mathrm{Gal}(F^\sharp, k(X, S, T)) = \mathrm{PGSp}(2m, q)$, and for every divisor d of $q - 1$ we have $\mathrm{Gal}(\Phi^{(d)}, k(X, S, T)) = \mathrm{GSp}^{(d)}(2m, q)$ and $\mathrm{Gal}(F^{(d)}, k(X, S, T)) = \mathrm{PGSp}^{(d)}(2m, q)$. By applying the above result to case (**) we also see that if $m > 2$ and $\mathrm{GF}(q) \subset k_p$, then for $1 \leq e \leq m - 1$ we have $G_e = \mathrm{Sp}(2m, q)$ and $\mathrm{PG}_e = \mathrm{PSp}(2m, q)$ which shows that the results of [A06] remain valid without assuming k_p algebraically closed.

3. TWISTED DERIVATIVE AND ITS FACTORIZATION

Solving the equation $f^b = 0$ we get

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

and substituting this in $\frac{f^b(Z) - f^b(Y)}{Z - Y}$ we get

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

and therefore

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

By simplifying g^b we get

$$\begin{aligned}
 g^b &= \sum_{i=1}^m S^{r(m+i)} T_i^{q^i} \left(\frac{Z^{\langle m-1+i \rangle} - Z^{\langle m-1 \rangle}}{Z - 1} \right) Y^{(2m-1) - \langle m-1+i \rangle} \\
 &\quad - \sum_{i=1}^m S^{r(m-i)} T_i \left(\frac{Z^{\langle m-1 \rangle} - Z^{\langle m-1-i \rangle}}{Z - 1} \right) Y^{(2m-1) - \langle m-1-i \rangle} \\
 &= \sum_{i=1}^m \frac{Z^{\langle m-1 \rangle} (Z^{q^m \langle i-1 \rangle} - 1) Y^{q^{m+i} \langle m-1-i \rangle} S^{r(m+i)} T_i^{q^i}}{Z - 1} \\
 &\quad - \sum_{i=1}^m \frac{Z^{\langle m-1-i \rangle} (Z^{q^{m-i} \langle i-1 \rangle} - 1) Y^{q^{m-i} \langle m-1+i \rangle} S^{r(m-i)} T_i}{Z - 1} \\
 &= \sum_{i=1}^m \frac{Z^{\langle m-1 \rangle} (Z^{\langle i-1 \rangle} - 1)^{q^m} Y^{q^{m+i} \langle m-1-i \rangle} S^{r(m+i)} T_i^{q^i}}{Z - 1} \\
 &\quad - \sum_{i=1}^m \frac{Z^{\langle m-1-i \rangle} (Z^{\langle i-1 \rangle} - 1)^{q^{m-i}} Y^{q^{m-i} \langle m-1+i \rangle} S^{r(m-i)} T_i}{Z - 1} \\
 &= \sum_{i=1}^m \frac{G_i^{q^i \langle m-1-i \rangle} H_i^{q^i} (Z(Z - 1)^{q-1})^{\langle i-1 \rangle} Y^{q^m \langle m-1+i \rangle} S^{r(m+i)} T_i^{q^i}}{Y^{(1+q^m)q^m \langle i-1 \rangle}} \\
 &\quad - \sum_{i=1}^m G_i^{\langle m-1-i \rangle} H_i Y^{q^{m-i} \langle m-1+i \rangle} S^{r(m-i)} T_i
 \end{aligned}$$

where for $1 \leq i \leq m$ we have

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

Hence in view of (**) we see that

$$g^b = \sum_{i=1}^m \left(A^{*\langle i-1 \rangle} B_i^{*q^i} - B_i^* \right) \quad \text{where} \quad A^* = \frac{Z(Z - 1)^{q-1}}{(Y^{q^m+1} S^t)^{q^m}}$$

and for $1 \leq i \leq m$ we have

$$B_i^* = G_i^{\langle m-1-i \rangle} H_i Y^{q^{m-i} \langle m-1+i \rangle} S^{r(m-i)} T_i$$

and therefore by the Mantra on page 19 of [A08] we get

$$g^b = A^* \Gamma^{*q} - \Gamma^* = \Gamma^* (A^* \Gamma^{*q-1} - 1) \quad \text{where} \quad \Gamma^* = \sum_{i=1}^m \sum_{j=0}^{i-1} A^{*(j-1)} B_i^{*q^j}.$$

Now, for $0 \leq j < i \leq m$, we clearly have

$$G_i^{q^j \langle m-1-i \rangle} H_i^{q^j} (Z(Z-1)^{q-1})^{\langle j-1 \rangle} = G_i^{\langle m-1-i+j \rangle} H_i.$$

Hence upon letting

$$g'^b = \frac{\Gamma^*}{(Y^{q^m+1} S^t)^{q^{m-1}}}$$

we get

$$g'^b = \sum_{i=1}^m \sum_{j=0}^{i-1} G_i^{\langle m-1-i+j \rangle} H_i Y^{a(i,j)} S^{b(i,j)} T_i^{q^j}$$

where, for $0 \leq j < i \leq m$, the integers $a(i, j)$ and $b(i, j)$ are given by

$$(3.1) \quad \begin{cases} a(i, j) = q^{m+j} \langle m-2-j \rangle + q^{m-i+j} \langle i-j-2 \rangle \\ \text{and} \\ b(i, j) = q^j r(m-i) - tq^m \langle j-1 \rangle - tq^{m-1} \end{cases}$$

and out of these $a(i, j)$ is obviously nonnegative and $b(i, j)$ is also nonnegative because by (**) we have

$$b(i, j) = q^{j-i} r(m+i) + tq^{m+j-i} \langle i-j-2 \rangle \geq 0.$$

It follows that

$$g'^b \in \text{GF}(p)[Z, Y, S, T_1, \dots, T_m]$$

and hence upon letting

$$g''^b = Z(Z-1)^{q-1} (g'^b)^{q-1} - Y^{(q^m+1)q^{m-1}} S^{tq^{m-1}}$$

we have

$$g''^b \in \text{GF}(p)[Z, Y, S, T_1, \dots, T_m]$$

and, in view of the defining equations of A and g^b , by the factorization $g^b = \Gamma(A\Gamma^{q-1} - 1)$ we get the factorization

$$g^b = g'^b g''^b.$$

By the definitions of G_i and H_i we see that

$$\text{deg}_Z G_m^{\langle m-2 \rangle} H_m = q \langle 2m-3 \rangle > q \langle m-2+j \rangle = \text{deg}_Z G_i^{\langle m-1-i+j \rangle} H_i$$

for $0 \leq j < i \leq m$ with $(i, j) \neq (m, m-1)$, and also $a(m, m-1) = 0$, and by (*) and (**) we have $b(m, m-1) = 0$, and hence by the double summation expression for g'^b we see that g'^b is a polynomial of degree $q \langle 2m-3 \rangle$ in Z with coefficients in $\text{GF}(p)[Y, S, T_1, \dots, T_m]$ and in it the coefficient of the highest Z -degree term is $T_m^{q^{m-1}}$. By the definition of g''^b it now follows that g''^b is a polynomial of degree $1+(q-1)+(q-1)q \langle 2m-3 \rangle = q^{2m-1}$ in Z with coefficients in $\text{GF}(p)[Y, S, T_1, \dots, T_m]$ and in it the coefficient of the highest Z -degree term is $T_m^{(q-1)q^{m-1}}$. Now, upon

letting g_e^\sharp, g'_e, g''_e be obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in g^b, g'^b, g''^b respectively, we see that

$$(3.2) \quad \begin{cases} \text{for } 0 \leq e \leq m - 1 \text{ we have} \\ g_e^\sharp = g'_e g''_e \text{ where } g'_e \text{ and } g''_e \text{ are monic polynomials} \\ \text{of degrees } q(2m - 3) \text{ and } q^{2m-1} \text{ in } Z \\ \text{with coefficients in } \text{GF}(p)[Y, S, T_1, \dots, T_e]. \end{cases}$$

By uniqueness the above factorizations must match with the factorization obtained in [A06].⁷ To get an explicit match, by splitting the first summation in the expression of g^b into two pieces $1 \leq i \leq m - 1$ and $i = m$, and then putting $T_i = 0$ for $e < i < m$ in the first piece and putting $T_m = 1$ and $j = m - 1 - \mu$ in the negative of the second piece, we see that

$$(3.3) \quad \begin{cases} \text{for } 0 \leq e \leq m - 1 \text{ we have} \\ g''_e = E'_e - N' \\ \text{where } E'_e = \sum_{i=1}^e \sum_{j=0}^{i-1} G_i^{\langle m-1-i+j \rangle} H_i Y^{a(i,j)} S^{b(i,j)} T_i^{q^j} \\ \text{and } N' = - \sum_{\mu=0}^{m-1} G_m^{\langle m-2-\mu \rangle} H_m Y^{(q^m+1)q^{m-1-\mu}(\mu-1)} S^{b(m,m-1-\mu)}. \end{cases}$$

Substituting g''_e and g'_e for g''^b and g'^b in the defining equation of g''^b we see that

$$g''_e = Z ((Z - 1)g'_e)^{q-1} - Y^{(q^m+1)q^{m-1}} S^{tq^{m-1}}.$$

Upon letting $E''_e = (Z - 1)E'_e$ and $N'' = (Z - 1)N' / (Z^{(m-1)} - 1)$, by the first equation in (3.3) we get $(Z - 1)g'_e = E''_e - (Z^{(m-1)} - 1)N''$, and hence by the above equation for g''_e we see that

$$g''_e = Z \left(E''_e - (Z^{(m-1)} - 1)N'' \right)^{q-1} - Y^{(q^m+1)q^{m-1}} S^{tq^{m-1}}.$$

Using the geometric series identity

$$(X - Y)^{q-1} = (X^q - Y^q)/(X - Y) = \sum_{l=1}^q Y^{l-1} X^{q-l}$$

with $X = E''_e$ and $Y = (Z^{(m-1)} - 1)N''$, by the above equation for g''_e and the equations for E'_e and N' given in (3.3) we see that

$$(3.4) \quad \begin{cases} \text{for } 0 \leq e \leq m - 1 \text{ we have} \\ g''_e = \left(\sum_{l=1}^q Z (Z^{(m-1)} - 1)^{l-1} N''^{l-1} E''_e{}^{q-l} \right) - Y^{(q^m+1)q^{m-1}} S^{tq^{m-1}} \\ \text{where } E''_e = \sum_{i=1}^e \sum_{j=0}^{i-1} G_i^{\langle m-1-i+j \rangle} (Z^{(i-1)} - 1) Y^{a(i,j)} S^{b(i,j)} T_i^{q^j} \\ \text{and } N'' = - \sum_{\mu=0}^{m-1} G_m^{\langle m-2-\mu \rangle} Y^{(q^m+1)q^{m-1-\mu}(\mu-1)} S^{b(m,m-1-\mu)}. \end{cases}$$

If $m > 1$, then the values of g' and g'' given in (3.2) to (3.6) of [A06] visibly coincide with the values obtained by putting $e = m - 1$ and $S = 1$ in g'_e and g''_e respectively. Since, for $1 \leq e \leq m - 1$, the polynomials g'_e and g''_e of [A06] were obtained by putting $T_i = 0$ for $e < i < m$ in the polynomials g' and g'' respectively, it follows that g'_e and g''_e can also be obtained by putting $S = 1$ in g'_e and g''_e respectively.

⁷As a misprint correction, in (3.3) on page 2985 of [A06] the exponent of $(Z^{(m-1)} - 1)$ should be changed from $q - 1$ to $l - 1$, and the exponent of Y should be changed from $(q^m + 1)(q^{m-1} - 1)$ to $(q^m + 1)q^{m-1}$.

Therefore by the irreducibility of g'_e and g''_e proved in (4.5) of [A06] we conclude that

$$(3.5) \quad \begin{cases} \text{for } 1 \leq e \leq m - 1, \\ \text{the polynomials } g'_e \text{ and } g''_e \text{ are irreducible in } k_p(Y, S, T_1, \dots, T_e)[Z]. \end{cases}$$

For $1 \leq e \leq m - 1$, as we have noted, f_e^\sharp is irreducible in $K_e(S)[Y]$ where $K_e = k_p(X, T_1, \dots, T_e)$, its twisted derivative is $f'_e^\sharp(Y, Z)$, and g_e^\sharp is obtained by dividing the Z -roots of $f'_e^\sharp(Y, Z)$ by Y and then changing Y to $1/Y$; therefore by (3.2) and (3.5) we get the following:

Symplectic Rank Theorem (3.6). *For $1 \leq e \leq m - 1$, the Galois group PG_e^\sharp of f_e^\sharp over $K_e(S)$ is a transitive permutation group of Rank 3 with subdegrees $1, q(2m - 3)$ and q^{2m-1} .*

In view of Proposition (3.1) of [A04] we get the following:

Theorem (3.7). *If $\text{GF}(q) \subset k_p$, then, for $0 \leq e \leq m - 1$, for the respective Galois groups G_e^\sharp and PG_e^\sharp of ϕ_e^\sharp and f_e^\sharp over $K_e(S)$, in a natural manner we have $G_e^\sharp < \text{GL}(2m, q)$ and $\Theta_{2m}(G_e^\sharp) = PG_e^\sharp < \text{PGL}(2m, q)$ where Θ_{2m} is the canonical epimorphism of $\text{GL}(2m, q)$ onto $\text{PGL}(2m, q)$.*

Recall that

$$\widehat{\phi}^b(Y) = S^{r(m)}XY^{q^m} + \sum_{i=1}^m \left(S^{r(m+i)}T_i^{q^i}Y^{q^{m+i}} + S^{r(m-i)}T_iY^{q^{m-i}} \right)$$

is the vectorial associate of $f^b(Y)$, and let

$$\psi^b(Y, Z) = Y^{q^m}\widehat{\phi}^b(Z) - Z^{q^m}\widehat{\phi}^b(Y).$$

Then in view of (**) we see that

$$\psi^b(Y, Z) = \sum_{i=1}^m \left(A^{b(i-1)}B_i^b(Y, Z)^{q^i} - B_i^b(Y, Z) \right) \quad \text{where} \quad A^b = \frac{1}{Stq^m}$$

and for $1 \leq i \leq m$ we have

$$B_i^b(Y, Z) = \left(Z^{q^m}Y^{q^{m-i}} - Y^{q^m}Z^{q^{m-i}} \right) S^{r(m-i)}T_i.$$

Therefore again by the Mantra on page 19 of [A08] we get

$$\psi^b(Y, Z) = A^b\Gamma^b(Y, Z)^q - \Gamma^b(Y, Z) \quad \text{where} \quad \Gamma^b(Y, Z) = \sum_{i=1}^m \sum_{j=0}^{i-1} A^{b(j-1)}B_i^b(Y, Z)^{q^j}.$$

Substituting the values of A^b and B_i^b in the defining equation for Γ^b we get

$$\Gamma^b(Y, Z) = \sum_{i=1}^m \sum_{j=0}^{i-1} \left(Z^{q^{m+j}}Y^{q^{m-i+j}} - Y^{q^{m+j}}Z^{q^{m-i+j}} \right) S^{b(i,j)+tq^{m-1}}T_i^{q^j}$$

and hence we see that Γ^b is a polynomial of degree q^{2m-1} in Z with coefficients in $\text{GF}(p)[Y, S, T_1, \dots, T_m]$ and in it the coefficient of the highest Z -degree term is $(YS^tT_m)^{q^{m-1}}$.

Recall that, for $0 \leq e \leq m - 1$, the vectorial associate of $f_e^\sharp(Y)$ is $\widehat{\phi}_e^\sharp(Y)$ and let

$$(3.8) \quad \psi_e^\sharp(Y, Z) = Y^{q^m}\widehat{\phi}_e^\sharp(Z) - Z^{q^m}\widehat{\phi}_e^\sharp(Y).$$

Then ψ_e^\sharp can be obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in the defining equation of ψ^\sharp , and hence by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in the above expression of ψ^b in terms of Γ^b we get

$$(3.9) \quad \psi_e^\sharp(Y, Z) = S^{-tq^m} \Gamma_e^\sharp(Y, Z)^q - \Gamma_e^\sharp(Y, Z)$$

where

$$(3.10) \quad \Gamma_e^\sharp(Y, Z) = \sum_{i=1}^e \sum_{j=0}^{i-1} \left(Z^{q^{m+j}} Y^{q^{m-i+j}} - Y^{q^{m+j}} Z^{q^{m-i+j}} \right) S^{b(i,j)+tq^{m-1}} T_i^{q^j} + \sum_{j=0}^{m-1} \left(Z^{q^{m+j}} Y^{q^j} - Y^{q^{m+j}} Z^{q^j} \right) S^{tq^j(m-j-1)}.$$

Again, Γ_e^\sharp is obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in Γ^b , and hence

$$(3.11) \quad \left\{ \begin{array}{l} \text{for } 0 \leq e \leq m-1 \text{ we have that} \\ \Gamma_e^\sharp \text{ is a polynomial of degree } q^{2m-1} \text{ in } Z \\ \text{with coefficients in } \text{GF}(p)[Y, S, T_1, \dots, T_e] \text{ and in it} \\ \text{the coefficient of the highest } Z\text{-degree term is } (YS^t)^{q^{m-1}}. \end{array} \right.$$

For $0 \leq e \leq m-1$, since $\text{deg}_Y \widehat{\phi}_e^\sharp(Y) = q^{2m}$ and $\text{Disc}_Y \widehat{\phi}_e^\sharp(Y) = S^{r(0)q^{2m}}$, in view of (3.8), (3.9) and (3.11), we see that there exists a nonzero root y_e of $\widehat{\phi}_e^\sharp(Y)$ in any splitting field L_e^\sharp of $\widehat{\phi}_e^\sharp(Y)$ over $K_e(S)$ where $K_e = k_p(X, T_1, \dots, T_e)$, and given any such y_e there exists a root z_e of $\widehat{\phi}_e^\sharp(Y)$ in L_e^\sharp such that $\Gamma_e^\sharp(y_e, z_e) \neq 0$, and for every such z_e we have $\Gamma_e^\sharp(y_e, z_e)^{q-1} = S^{tq^m}$. Clearly $\text{GCD}(tq^m, q-1) = \text{GCD}(t, q-1)$, and hence for any divisor d of $(q-1)/\text{GCD}(t, q-1)$, we can find integers σ, τ with $\sigma tq^m + \tau(q-1) = (q-1)/d$, and for any such roots y_e, z_e and any such integers σ, τ , upon letting $\widehat{\Lambda}_e = \Gamma_e^\sharp(y_e, z_e)^\sigma S^\tau$ we see that $\widehat{\Lambda}_e^{q-1} = S^{(q-1)/d}$ with $\widehat{\Lambda}_e \in L_e^\sharp$. If also $\text{GF}(q) \subset k_p$, then we can find $\lambda \in \text{GF}(q) \subset k_p$ such that upon letting $\Lambda_e = \lambda \widehat{\Lambda}_e$ we have $\Lambda_e^d = S$ with $\Lambda_e \in L_e^\sharp$, and now, because L_e^\sharp is also a splitting field of ϕ_e^\sharp over $K_e(S)$, by the Substitution Principle on page 98 of [A03], for the Galois groups $G_e^{(d)}$ and G_e^\sharp of $\phi_e^{(d)}$ and ϕ_e^\sharp over $K_e(S)$ respectively, in a natural manner we have $G_e^{(d)} = \text{Gal}(\phi_e^\sharp, K_e(\Lambda_e)) \triangleleft G_e^\sharp$ with $G_e^\sharp/G_e^{(d)} = \text{Gal}(K_e(\Lambda_e), K_e(S)) = Z_d$.

For $0 \leq e \leq m-1$, let $R = k_e[X, S, T_1, \dots, T_e]$ and $\overline{R} = k_p[X, T_1, \dots, T_e]$, and let $\alpha : R \rightarrow \overline{R}$ be the unique \overline{R} -epimorphism which sends S to 1. Then $K_e(S)$ and K_e are the quotient fields of R and \overline{R} respectively, and for every divisor d of $q-1$ we have that $\phi_e^{(d)}$ is a monic polynomial in Y with coefficients in R , and by applying α to the coefficients of $\phi_e^{(d)}$ we get the polynomial ϕ_e which is such that $\text{Disc}_Y(\phi_e) \neq 0$, and therefore, for the Galois group G_e of ϕ_e over K_e , in a natural manner we have $G_e < G_e^{(d)}$.⁸

⁸Here we are using the Specialization Principle which follows from the material of Section 2 of [A01] and which says that if U is a monic polynomial in Y with coefficients in a normal integral domain R which is a localization of an affine ring over a field or a pseudogeometric Dedekind domain, and if $\alpha : R \rightarrow \overline{R}$ is an epimorphism of R onto an integral domain \overline{R} such that for the polynomial \overline{U} obtained by applying α to the coefficients of U we have $\text{Disc}_Y(\overline{U}) \neq 0$, then, in a natural manner, the Galois group of \overline{U} over the quotient field of \overline{R} is isomorphic (as a permutation group) to a subgroup of the Galois group of U over the quotient field of R . The Specialization Principle is also true when, instead of the above assumptions on R , we assume R to be a UFD; see page 190 of [Wae].

Thus we get the following Theorem which may be considered analogous to part (8) of the Composite Polynomial Lemma (2.4) on pages 13-14 of [A04].

Root Extraction Theorem (3.12). *For $0 \leq e \leq m - 1$, there exists a nonzero root y_e of $\widehat{\phi}_e^\sharp(Y)$ in any splitting field L_e^\sharp of $\widehat{\phi}_e^\sharp(Y)$ over $K_e(S)$ where $K_e = k_p(X, T_1, \dots, T_e)$, and given any such y_e there exists a root z_e of $\widehat{\phi}_e^\sharp(Y)$ in L_e^\sharp such that $\Gamma_e^\sharp(y_e, z_e) \neq 0$, and for every such z_e we have $\Gamma_e^\sharp(y_e, z_e)^{q-1} = S^{tq^m}$ (note that for any $y_e \in L_e^\sharp$ and $z_e \in L_e^\sharp$ we obviously have $\Gamma_e^\sharp(y_e, z_e) \in L_e^\sharp$). Moreover, for every divisor d of $(q - 1)/\text{GCD}(t, q - 1)$, there exist integers σ, τ with $\sigma tq^m + \tau(q - 1) = (q - 1)/d$, and if $\text{GF}(q) \subset k_p$, then, given any such roots y_e, z_e and any such integers σ, τ , there exists $\lambda \in \text{GF}(q) \subset k_p$ such that for $\Lambda_e = \lambda \Gamma_e^\sharp(y_e, z_e)^\sigma S^\tau$ we have $\Lambda_e \in L_e^\sharp$ with $\Lambda_e^d = S$, and for the respective Galois groups $G_e, G_e^{(d)}, G_e^\sharp$ of $\phi_e, \phi_e^{(d)}, \phi_e^\sharp$ over $K_e, K_e(S), K_e(S)$ respectively, in a natural manner we have $G_e < G_e^{(d)} \triangleleft G_e^\sharp$ with $G_e^\sharp/G_e^{(d)} = Z_d$.*

4. GALOIS GROUPS

By 2.1.2, 2.1.B and 2.1.C of [KLi] we have

$$(4.0) \quad \text{Sp}(2m, q) \triangleleft \text{GSp}(2m, q) \quad \text{with} \quad \text{GSp}(2m, q)/\text{Sp}(2m, q) = Z_{q-1}$$

and hence in view of (4.6), (4.7), (5.1), (5.6) and (5.8) of [A06], by our Theorems (3.6), (3.7) and (3.12) we get the following:⁹

Theorem (4.1). *If $m > 2$ and $\text{GF}(q) \subset k_p$, then, for $1 \leq e \leq m - 1$ and for every divisor d of $(q - 1)/\text{GCD}(t, q - 1)$, in a natural manner we have*

$$\text{Sp}(2m, q) \triangleleft G_e \triangleleft G_e^{(d)} \triangleleft G_e^\sharp \triangleleft \text{GSp}(2m, q) \quad \text{with} \quad G_e^\sharp/G_e^{(d)} = Z_d$$

and

$$\text{PSp}(2m, q) \triangleleft PG_e \triangleleft PG_e^{(d)} \triangleleft PG_e^\sharp \triangleleft \text{PGSp}(2m, q)$$

where we recall that $G_e, G_e^{(d)}, G_e^\sharp, PG_e, PG_e^{(d)}, PG_e^\sharp$ are the Galois groups of $\phi_e, \phi_e^{(d)}, \phi_e^\sharp, f_e, f_e^{(d)}, f_e^\sharp$ over $K_e, K_e(S), K_e(S), K_e, K_e(S), K_e(S)$ respectively with $K_e = k_p(X, T_1, \dots, T_e)$.

In view of (3.7) and (4.0), by taking $d = q - 1$ in (4.1) we see that

$$\left\{ \begin{array}{l} \text{if } m > 2 \text{ and } \text{GF}(q) \subset k_p \text{ and } \text{GCD}(t, q - 1) = 1, \text{ then for } 1 \leq e \leq m - 1 \text{ we have} \\ \text{Sp}(2m, q) = G_e \triangleleft G_e^\sharp = \text{GSp}(2m, q) \text{ and } \text{PSp}(2m, q) = PG_e \triangleleft PG_e^\sharp = \text{PGSp}(2m, q) \end{array} \right.$$

and therefore again by (4.1) we get the following:

Theorem (4.2). *If $m > 2$ and $\text{GF}(q) \subset k_p$ and $\text{GCD}(t, q - 1) = 1$, then, for $1 \leq e \leq m - 1$ and for every divisor d of $(q - 1)$, in a natural manner we have*

$$\text{Sp}(2m, q) = G_e \triangleleft \text{GSp}^{(d)}(2m, q) = G_e^{(d)} \triangleleft G_e^\sharp = \text{GSp}(2m, q)$$

and

$$\text{PSp}(2m, q) = PG_e \triangleleft \text{PGSp}^{(d)}(2m, q) = PG_e^{(d)} \triangleleft PG_e^\sharp = \text{PGSp}(2m, q)$$

⁹As a misprint correction, in (5.8) on page 2990 of [A06], $\text{PSp}(2m, q) \triangleleft \delta^{-1}G\delta$ should be changed to $\text{PSp}(2m, q) \triangleleft \delta^{-1}G\delta \triangleleft \text{PGSp}(2m, q)$. As another misprint correction, in (6.1) on page 2990 of [A06], $\text{Gal}(\phi, k_p(X, T_1, \dots, T_e))$ and $\text{Gal}(f, k_p(X, T_1, \dots, T_e))$ should be changed to $\text{Gal}(\phi, k_p(X, T_1, \dots, T_{m-1}))$ and $\text{Gal}(f, k_p(X, T_1, \dots, T_{m-1}))$ respectively.

where we recall that $G_e, G_e^{(d)}, G_e^\#, PG_e, PG_e^{(d)}, PG_e^\#$ are the Galois groups of $\phi_e, \phi_e^{(d)}, \phi_e^\#, f_e, f_e^{(d)}, f_e^\#$ over $K_e, K_e(S), K_e(S), K_e, K_e(S), K_e(S)$ respectively with $K_e = k_p(X, T_1, \dots, T_e)$.

Remark (4.3). By applying (4.2) to case (") we see that if $m > 2$ and $\text{GF}(q) \subset k_p$, then, for $1 \leq e \leq m - 1$, in a natural manner we have $\text{Gal}(\phi_e, k_p(X, T_1, \dots, T_e)) = \text{Sp}(2m, q)$ and $\text{Gal}(f_e, k_p(X, T_1, \dots, T_e)) = \text{PSp}(2m, q)$, which is an improvement on Theorem (6.2) of [A06] as we no longer need the condition that k_p is algebraically closed. We shall discuss the $m \leq 2$ case of (4.2) elsewhere.

REFERENCES

- [A01] S. S. Abhyankar, *Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$* , Annals of Mathematics **63** (1956), 491-526. MR **17**:1134d
- [A02] S. S. Abhyankar, *Coverings of algebraic curves*, American Journal of Mathematics **79** (1957), 825-856. MR **20**:872
- [A03] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, 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 **96f**:12003
- [A05] S. S. Abhyankar, *Again nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2967-2976. MR **96m**:12004
- [A06] S. S. Abhyankar, *More nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2977-2991. MR **96m**:12005
- [A07] S. S. Abhyankar, *Further nice equations for nice groups*, Transactions of the American Mathematical Society **348** (1996), 1555-1577. MR **96m**:14021
- [A08] S. S. Abhyankar, *Factorizations over finite fields*, Finite Fields and Applications, London Mathematical Society, Lecture Note Series **233** (1996), 1-21. CMP 97:08
- [A09] S. S. Abhyankar, *Projective polynomials*, Proceedings of the American Mathematical Society **125** (1997), 1643-1650. CMP 97:07
- [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
- [Kan] W. M. Kantor, *Rank 3 characterizations of classical geometries*, Journal of Algebra **36** (1975), 309-313. MR **52**:8229
- [KLi] P. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, Cambridge, 1990. MR **91g**:20001
- [Tit] J. Tits, *Buildings of Spherical Type and Finite BN-Pairs*, Springer Lecture Notes In Mathematics Number 386, 1974. MR **57**:9866
- [Wae] B. L. van der Waerden, *Modern Algebra, vol I*, Frederick Ungar Publishing Co., New York, 1949. MR **10**:587b

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907

E-mail address: ram@cs.purdue.edu

E-mail address: loomisp@math.purdue.edu