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 \( \text{PSp}(2m, q) \) and the (vectorial) symplectic isometry group \( \text{Sp}(2m, q) \) 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 \( \text{PGSp}(2m, q) \) and the (vectorial) symplectic similitude group \( \text{GSp}(2m, q) \) 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
\[
F = F(Y) = Y^n + T^qY^u + XY^v + TY^w + 1
\]
in indeterminates \( T, X, Y \) over a field \( k \) of characteristic \( p \), where
\[
n = 1 + q + \cdots + q^{2m-1},
\]
\[
u = 1 + q + \cdots + q^{m-1},
\]
\[
w = 1 + q + \cdots + q^{m-2},
\]
and consider its Galois group \( \text{Gal}(F, k(X, T)) \) and the Galois group \( \text{Gal}(\Phi, k(X, T)) \) of its subvectorial associate \( \Phi = \Phi(Y) = F(Y^{q-1}) \). Also consider the deformation
\[
F^\sharp = F^\sharp(Y) = Y^n + T^qY^u + XY^v + S^wTY^w + 1
\]
in indeterminates \( T, X, S, Y \), where \( S \) is another indeterminate, and consider its Galois group \( \text{Gal}(F^\sharp, k(X, S, T)) \) and the Galois group \( \text{Gal}(\Phi^\sharp, k(X, S, T)) \).

1. Here we regard \( \text{Sp}(2m, q) \) as acting on nonzero vectors. For the vectorial associate \( \hat{\Phi}(Y) = Y^q\Phi(Y) \) we then have \( \text{Gal}(\hat{\Phi}, k(X, T)) = \text{Sp}(2m, q) \) regarded as acting on the entire vector space \( \text{GF}(q)^{2m} \).

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

©1998 American Mathematical Society
[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 $\Phi$ 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 $\Phi^d$, 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 $\text{GSp}(2m,q)/\text{GSp}^d(2m,q) = \mathbb{Z}_d$, and upon letting $F(d)$ be obtained by substituting $S^d$ for $S$ in $F^d$, we have $\text{Gal}(F(d), k(X,S,T)) = \text{PGSp}^d(2m,q)$ where we define $\text{PGSp}^d(2m,q) = \text{image of GSp}^d(2m,q)$ 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. As noted in [A06], the polynomials $\Phi$ and $F$ are specializations of more general polynomials $\phi_e$ 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 $\phi_e^d, \phi_e(d), f_e^d, f_e(d)$ 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. To abbreviate frequently occurring expressions, for every

---

3Since $\text{Sp}(2m,q)\triangleleft \text{GSp}(2m,q)$ with $\text{GSp}(2m,q)/\text{Sp}(2m,q) = \mathbb{Z}_{q-1}$ (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, $\triangleleft$ and $\triangleleft$ denote subgroup and normal subgroup respectively, and $\mathbb{Z}_d$ denotes a cyclic group of order $d$.

4In view of the previous footnote, this follows from the fact that $\text{PGSp}(2m,q)/\text{PSp}(2m,q) = \mathbb{Z}_2$ or $\mathbb{Z}_1$ 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

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

Let

$$f^\flat = f^\flat(Y) = S^r(Y) XY^{\langle m-1 \rangle} + \sum_{i=1}^{m} \left( S^r(Y) Y^{\langle m-i \rangle} T_i + S^r(Y) Y^{\langle m-i \rangle} t_i \right),$$

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

$$r(2m) = 0$$

such that for some nonnegative integer $t$ we have

(**)

$$q^i r(m-i) = r(m+i) + t q^i (m-i) \quad \text{for } 0 \leq i \leq m$$

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

$$\hat{\phi}^\flat = \hat{\phi}^\flat(Y) = f^\flat(Y^{\langle r \rangle})$$

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

and

$$\hat{\phi}^\flat = \hat{\phi}^\flat(Y) = Y^\flat f^\flat(Y)$$

$$= S^r(Y) XY^{q^m} + \sum_{i=1}^{m} \left( S^r(Y) Y^{q^m+i} + S^r(Y) Y^{q^m+i} \right).$$

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

$$f_e^\flat = f_e^\flat(Y) = Y^{\langle 2m-1 \rangle) + S^r(Y) + S^r(Y) X Y^{\langle m-1 \rangle}$$

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

and note that then $f_e^\flat$ 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 $k_p[X, S, T_1, \ldots, T_e]$. Now the constant term of $f_e^\flat$ is $S^r(0)$ and the $Y$-exponent of every other term in $f_e^\flat$ is 1 modulo $p$, and hence $f_e^\flat - Y f_e^\flat Y = S^r(0)$ where $f_e^\flat Y$ is the $Y$-derivative of $f_e^\flat$. Therefore\(^6\) $\text{Disc}_Y(f_e^\flat) = S^r(0)(q^{2m-2})$ where $\text{Disc}_Y(f_e^\flat)$ is the $Y$-discriminant of $f_e^\flat$, and hence the Galois group $\text{Gal}(f_e^\flat, k_p(X, S, T_1, \ldots, T_e))$ is well-defined as a subgroup of the symmetric group $\text{Sym}_{2(m-1)}$, and the equation $f_e^\flat = 0$ gives an unramified covering of the once punctured affine line over $k_p(X, T_1, \ldots, T_e)$. Since $f_e^\flat$ is linear in $X$, by the Gauss Lemma it follows that $f_e^\flat$ is irreducible in $k_p(X, S, T_1, \ldots, T_e)[Y]$, and

\(^6\)See 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 \( \phi^e_c \) and \( \overline{\phi}^e_c \) be obtained by putting \( T_m = 1 \) and \( T_1 = 0 \) for \( e < i < m \) in \( \phi^e \) and \( \overline{\phi}^e \) respectively, and note that then

\[
\phi^e_c = \phi^e_c(Y) = f^e_c(Y^{q-1}) = Yq^{2m-1} + S^{(0)} + S^{(r)}XYq^{m-1} + \sum_{i=1}^{e} \left( S^{(m+i)}T_i Yq^{m+i-1} + S^{(m-i)}T_i Yq^{m-1} \right)
\]

and

\[
\overline{\phi}^e_c = \overline{\phi}^e_c(Y) = Y \phi^e_c(Y) = Yq^{2m} + S^{(0)}Y + S^{(m)}XYq^m + \sum_{i=1}^{e} \left( S^{(m+i)}T_i Yq^{m+i} + S^{(m-i)}T_i Yq^{m-1} \right)
\]

are the subvectorial and vectorial associates of \( f^e_c \) respectively. By a similar calculation, \( Disc_Y(\phi^e_c) = (-1)^{q^m-1}S^{(0)(q^m-2)} \) and \( Disc_Y(\overline{\phi}^e_c) = S^{(0)q^2m} \), and hence the Galois groups \( \text{Gal}(\phi^e_c, k_p(X, S, T_1, \ldots, T_e)) \) and \( \text{Gal}(\overline{\phi}^e_c, k_p(X, S, T_1, \ldots, T_e)) \) are well-defined as subgroups of the symmetric groups on \( q^{2m} - 1 \) and \( q^{2m} \) letters respectively, and the equations \( \phi^e_c = 0 \) and \( \overline{\phi}^e_c = 0 \) give unramified coverings of the once punctured affine line over \( k_p(X, T_1, \ldots, T_e) \).

For every divisor \( d \) of \( q - 1 \), let \( \phi^{d(e)}_c, \phi^{d(e)}_c, \overline{\phi}^{d(e)}_c \) be obtained by substituting \( S^d \) for \( S \) in \( f^e_c, \phi^e_c, \overline{\phi}^e_c \) respectively and note that then, as above, the Galois group \( \text{Gal}(f^{(d)}_c, k_p(X, S, T_1, \ldots, T_e)) \) is a well-defined transitive subgroup of \( \text{Sym}(2m-1) \), the Galois groups

\[
\text{Gal}(\phi^{(d)}_c, k_p(X, S, T_1, \ldots, T_e)) \quad \text{and} \quad \text{Gal}(\overline{\phi}^{(d)}_c, k_p(X, S, T_1, \ldots, T_e))
\]

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

For \( 0 \leq e \leq m - 1 \), let \( \phi^e_c \) and \( f^e_c \) be obtained by putting \( S = 1 \) in \( \phi^e_c \) and \( f^e_c \) respectively. Note that, for \( 1 \leq e \leq m - 1 \), these \( \phi^e_c \) and \( f^e_c \) are the same as those considered in [A06], and if \( m > 1 \), then \( \phi^{m-1}_c \) and \( f^{m-1} \) respectively coincide with \( \phi \) and \( f \) of [A06]. For \( 0 \leq e \leq m - 1 \), let \( K_c = k_p(X, T_1, \ldots, T_e) \), let \( G_c \) and \( PG_c \) be the Galois groups of \( \phi^e_c \) and \( f^e_c \) over \( K_c \), respectively, and let \( G^{d(e)}_c \) and \( PG^{d(e)}_c \) be the Galois groups of \( \phi^{d(e)}_c \) and \( f^{d(e)}_c \) over \( K_c(S) \) respectively. Likewise, for \( 0 \leq e \leq m - 1 \), and for every divisor \( d \) of \( q - 1 \), let \( G^{(d)}_c \) and \( PG^{(d)}_c \) be the Galois groups of \( \phi^{(d)}_c \) and \( f^{(d)}_c \) over \( K_c(S) \) respectively.

In Section 3, we apply the Mantra of [A08] to the twisted derivative of \( f^g \) and thereby we prove the Symplectic Rank Theorem (3.6) which says that \( PG^{d}_c \) 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 \( \phi^e_c \) over \( K_c(S) \) contains a \( (q - 1) \)-th root of its modified constant term \( S^{q^e} \); 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 \( GF(q) \subset k_p \) 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 \( \text{Sp}(2m, q) = G_c \circ GSp^{(d)}(2m, q) = G^{(d)}_c \circ G^{d}_c = GSp(2m, q) \)
and \( \text{PSp}(2m, q) = \text{PG} \triangleleft \text{PGSp}^{(d)}(2m, q) = \text{PG}^{(d)} \triangleleft \text{PGSp}(2m, q) \). Note that

\[
\begin{dcases}
\text{if } r(i) = (2m - 1) - (i - 1) \text{ for } 0 \leq i \leq 2m, \\
\text{then conditions } (*) \text{ and } (**) \text{ are satisfied with } t = q^m + 1
\end{dcases}
\]

and

\[
\begin{dcases}
\text{if } r(m + i) = 0 \text{ and } r(m - i) = q^{m-i}(i - 1) \text{ for } 0 \leq i \leq m, \\
\text{then conditions } (*) \text{ and } (**) \text{ are satisfied with } t = 1.
\end{dcases}
\]

Case (') arises when we homogenize \( f_e \), i.e., when we put \( f_e^2(Y) = S^{(2m-1)}f_e(Y/S) \), and so we may call it the \textit{homogeneous case}; we shall deal with this in greater detail elsewhere. By analogy, case ("') may be called the \textit{twisted homogeneous case}. In the twisted homogeneous case ("'), if \( m > 2 \) and \( \text{GF}(q) \subset k_p \), then by taking \( k = k_p \) and \( T_1 = T \in \phi_1^* \) and \( f_1^* \) we get \( \Phi^d \) and \( F^d \) respectively, and hence by the above result we have \( \text{Gal}(\Phi^d, k(X, S, T)) = \text{GSp}(2m, q) \) and \( \text{Gal}(F^d, k(X, S, T)) = \text{PGSp}(2m, q) \), and for every divisor \( d \) of \( q - 1 \) we have \( \text{Gal}(\Phi^{(d)}, k(X, S, T)) = \text{GSp}^{(d)}(2m, q) \) and \( \text{Gal}(F^{(d)}, k(X, S, T)) = \text{PGSp}^{(d)}(2m, q) \). By applying the above result to case ("') we also see that if \( m > 2 \) and \( \text{GF}(q) \subset k_p \), then for \( 1 \leq c \leq m - 1 \) we have \( G_e = \text{Sp}(2m, q) \) and \( \text{PG} = \text{PSp}(2m, q) \) which shows that the results of [A06] remain valid without assuming \( k_p \) algebraically closed.

3. Twisted derivative and its factorization

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

\[
S^{r(m)}X = \sum_{i=1}^{m} \left( S^{r(m+i)}T_i^* Y^{m-1+i} + S^{r(m-i)}T_i Y^{m-1-i} \right)
\]

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

\[
f^{rb}(Y, Z) = \frac{f^x(Z) - f^x(Y)}{Z - Y} \quad \text{(def of the twisted derivative } f^{rb} \text{ of } f^x) \\
= \sum_{i=1}^{m} \left( S^{r(m+i)}T_i^* Y^{m-1+i} + S^{r(m-i)}T_i Y^{m-1-i} \right)
\]

\[
\times \left( Z^{m-1} - Y^{m-1} \right)
\]

\[
+ \sum_{i=1}^{m} \left( S^{r(m+i)}T_i^* Z^{m-1+i} - Y^{m-1+i} \right)
\]

\[
+ S^{r(m-i)}T_i Z^{m-1-i} - Y^{m-1-i} \right)
\]
and therefore

\[ g^b = g^b(Y, Z) = Y^{(2m-1)-1} f^b(1/Y, Z/Y) \]  
(def of polynomial \( g^b \) obtained

by dividing roots of \( f^b \) by \( Y \) and then changing \( Y \) to \( 1/Y \))

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

\[ - \sum_{i=1}^{m} S^{r(m-i)}T_i \left( \frac{Z^{(m-1)} - Z^{(m-1-i)}}{Z - 1} \right) Y^{(2m-1) - (m-1-i)} \]

By simplifying \( g^b \) we get

\[ g^b = \sum_{i=1}^{m} S^{r(m+i)}T_i^q \left( \frac{Z^{(m-1+i)} - Z^{(m-1)}}{Z - 1} \right) Y^{(2m-1) - (m-1+i)} \]

\[ - \sum_{i=1}^{m} S^{r(m-i)}T_i \left( \frac{Z^{(m-1)} - Z^{(m-1-i)}}{Z - 1} \right) Y^{(2m-1) - (m-1-i)} \]

\[ = \sum_{i=1}^{m} \frac{Z^{(m-1)} (Zq^{m(i-1)} - 1)}{Z - 1} Y q^{m+i(m-1-i)} S^{r(m+i)}T_i^q \]

\[ - \sum_{i=1}^{m} \frac{Z^{(m-1-i)} (Zq^{m-i(i-1)} - 1)}{Z - 1} Y q^{m-i} S^{r(m-i)}T_i \]

\[ = \sum_{i=1}^{m} \frac{G_i^{r(m-1-i)} H_i^q (Z(Z - 1)^{q-1})^{(i-1)} Y q^{m+i} S^{r(m+i)}T_i^q}{Y^{(1+q^m)}q^m (i-1)} \]

\[ - \sum_{i=1}^{m} G_i^{r(m-1-i)} H_i Y q^{m-i} S^{r(m-i)}T_i \]

where for \( 1 \leq i \leq m \) we have

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

Hence in view of (***) we see that

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

and for \( 1 \leq i \leq m \) we have

\[ B_i^* = G_i^{r(m-1-i)} H_i Y q^{m-i} S^{r(m-i)}T_i \]
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
\[ G_i^{(m-1-i)}H_i^{q^i} (Z(Z - 1)^{q-1})^{(j-1)} = G_i^{(m-1-i+j)}H_i. \]
Hence upon letting
\[ g^b = \frac{\Gamma^*}{(Y^{q^m+1}S^t)^{q^m-1}} \]
we get
\[ g^b = \sum_{i=1}^{m} \sum_{j=0}^{i-1} G_i^{(m-1-i+j)}H_iY^{a(i,j)}S^{b(i,j)}T_i^q \]
where, for \(0 \leq j < i \leq m\), the integers \(a(i, j)\) and \(b(i, j)\) are given by
\[
\begin{align*}
  a(i, j) &= q^{m+j}(m - 2 - j) + q^{m-i+j}(i - j - 2) \\
  b(i, j) &= q^jr(m - i) - tq^m(j - 1) - tq^{m-1}
\end{align*}
\]
and out of these \(a(i, j)\) is obviously nonnegative and \(b(i, j)\) is also nonnegative because by (**) we have
\[ b(i, j) = q^{j-i}r(m + i) + tq^{m+j-i}(i - j - 2) \geq 0. \]
It follows that
\[ g^b \in GF(p)[Z, Y, S, T_1, \ldots, T_m] \]
and hence upon letting
\[ g^b = Z(Z - 1)^{q-1}(g^b)^{q-1} - Y^{(q^m+1)q^{m-1}}S^{q^m-1} \]
we have
\[ g^b \in GF(p)[Z, Y, S, T_1, \ldots, T_m] \]
and, in view of the defining equations of \(A\) and \(g^b\), by the factorization \(g^r = \Gamma(\Lambda^q - 1)\) we get the factorization
\[ g^b = g^b g^b. \]
By the definitions of \(G_i\) and \(H_i\) we see that
\[ \deg G_m^{(m-2)}H_m = q(2m - 3) > q(m - 2 + j) = \deg G_i^{(m-1-i+j)}H_i \]
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 \(q(2m - 3)\) in \(Z\) with coefficients in \(GF(p)[Y, S, T_1, \ldots, T_m]\) and in it the coefficient of the highest \(Z\)-degree term is \(T_q^{q-1}\). By the definition of \(g^b\) it now follows that \(g^b\) is a polynomial of degree \(1+(q-1)+(q-1)q(2m-3) = q^{2m-1}\) in \(Z\) with coefficients in \(GF(p)[Y, S, T_1, \ldots, T_m]\) and in it the coefficient of the highest \(Z\)-degree term is \(T_{(q-1)q}^{q-1}\). Now, upon
letting $g^e_x, g^m_x, g'^m_x$ be obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in $g^b, g^b_y, g^b_s$ respectively, we see that

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

(3.2)

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

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

(3.3)

Substituting $g'^m_x$ and $g^m_x$ for $g'^b$ and $g^b$ in the defining equation of $g'_{m,s}$ we see that

$$g'^m_x = Z (Z - 1) g^m_x Y^{-1} - Y^{q+m+1} S t q^{m-1}.$$

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

$$g'^m_x = Z \left( E''_x - (Z^{m-1} - 1) N'' \right) q^{-1} - Y^{q+m+1} S t q^{m-1}.$$

Using the geometric series identity

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

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

$$\begin{cases}
\text{for } 0 \leq e \leq m - 1 \text{ we have } \\
g'^m_x = \left( \sum_{t=1}^{q} Z (Z^{m-1} - 1)^{t-1} N''^{t-1} E''_{t} q^{-t} \right) - Y^{q+m+1} S t q^{m-1} \\
\text{where } E''_t = \sum_{i=1}^e \sum_{j=0}^{i-1} G_{i}^j(m-1-i+j) (Z^{i-1} - 1) Y^{a(i,j)} S^{b(i,j)} T_i^{q^j} \\
\text{and } N'' = -\sum_{\mu=0}^{m-1} G_m^{(m-2-\mu)} Y^{q+m+1} S t q^{m-1} - Y^{q+m+1} S t q^{m-1}
\end{cases}
$$

(3.4)

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 $g^m_x$ and $g'^m_x$ respectively. Since, for $1 \leq e \leq m - 1$, the polynomials $g^e_x$ and $g'^e_x$ of [A06] were obtained by putting $T_i = 0$ for $e < i < m$ in the polynomials $g^b$ and $g'^b$ respectively, it follows that $g^e_x$ and $g'^e_x$ can also be obtained by putting $S = 1$ in $g^m_x$ and $g'^m_x$ respectively.

\(^7\)As 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 $(q^m + 1)(q^m - 1)$ to $(q^m + 1)q^{m-1}$.\(\)
Therefore by the irreducibility of \( g'_c \) and \( g''_c \) proved in (4.5) of [A06] we conclude that

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

For \( 1 \leq e \leq m - 1 \), as we have noted, \( f^e_c \) is irreducible in \( K_c(S)[Y] \) where \( K_c = k_p(X, T_1, \ldots, T_e) \), its twisted derivative is \( f'^e_c(Y, Z) \), and \( g''_c \) is obtained by dividing the \( Z \)-roots of \( f'^e_c(Y, Z) \) 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 \( PG^e_c \) of \( f^e_c \) over \( K_c(S) \) 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 \( GF(q) \subseteq k_p \), then, for \( 0 \leq e \leq m - 1 \), for the respective Galois groups \( G^e_c \) and \( PG^e_c \) of \( f^e_c \) and \( f^e_c \) over \( K_c(S) \), in a natural manner we have \( G^e_c < GL(2m, q) \) and \( \Theta_{2m}(G^e_c) = PG^e_c < PGL(2m, q) \) where \( \Theta_{2m} \) is the canonical epimorphism of \( GL(2m, q) \) onto \( PGL(2m, q) \).

Recall that

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

is the vectorial associate of \( f^e(Y) \), and let

\[
\psi^e(Y, Z) = Y q^m \phi^e(Z) - Z q^m \phi^e(Y).
\]

Then in view of (**) we see that

\[
\psi^e(Y, Z) = \sum_{i=1}^{m} \left( A^i B^i(Y, Z) q^i - B^i(Y, Z) \right) \quad \text{where} \quad A^i = \frac{1}{S^{q(m)}}
\]

and for \( 1 \leq i \leq m \) we have

\[
B^i(Y, Z) = \left( Z q^m Y q^{m-i} - Y q^m Z q^{m-i} \right) S^{r(m-i)} T_i.
\]

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

\[
\psi^e(Y, Z) = A^i \Gamma^e(Y, Z) q^i - \Gamma^e(Y, Z) \quad \text{where} \quad \Gamma^e(Y, Z) = \sum_{i=1}^{m} \sum_{j=0}^{i-1} A^i B^i(Y, Z) q^j.
\]

Substituting the values of \( A^i \) and \( B^i \) in the defining equation for \( \Gamma^e \) we get

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

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

Recall that, for \( 0 \leq e \leq m - 1 \), the vectorial associate of \( f^e_c(Y) \) is \( \phi^e_c(Y) \) and let

\[
\psi^e_c(Y, Z) = Y q^m \phi^e_c(Z) - Z q^m \phi^e_c(Y).
\]
Then $\psi^e\phi^e$ can be obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in the defining equation of $\psi^e$, and hence by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in the above expression of $\psi^e$ in terms of $\Gamma^e$ we get

$$
\psi^e(\hat{Y}, \hat{Z}) = S^{-tq^m} \Gamma^e(\hat{Y}, \hat{Z}) - \Gamma^e_s(\hat{Y}, \hat{Z})
$$

where

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

Again, $\Gamma^e_s$ is obtained by putting $T_m = 1$ and $T_i = 0$ for $e < i < m$ in $\Gamma^e$, and hence

$$
\Gamma^e_s
$$

is a polynomial of degree $q^{2m-1}$ in $Z$

with coefficients in $GF(p)[Y, S, T_1, \ldots, T_e]$ and in it

the coefficient of the highest $Z$-degree term is $(YS^t)^{q^m-1}$.

For $0 \leq e \leq m - 1$, since $\deg \psi(\hat{Y}) = q^{2m}$ and $\Disc \psi(\hat{Y}) = S^{r(0)q^{2m}}$, in view of (3.8), (3.9) and (3.11), we see that there exists a nonzero root $y_e$ of $\hat{\phi}^e(\hat{Y})$ in any splitting field $\hat{L}_e^\prime$ of $\hat{\phi}^e(\hat{Y})$ over $K_e(S)$ where $K_e = k(X, T_1, \ldots, T_e)$, and given any such $y_e$ there exists a root $z_e$ of $\hat{\phi}^e(\hat{Y})$ in $L_e^\prime$ such that $\Gamma^e_s(y_e, z_e) \neq 0$, and for every such $z_e$ we have $\Gamma^e_s(y_e, z_e)q = S^{q^m}$. Clearly $\GCD(qm, q-1) = \GCD(t, q-1)$, and hence for any divisor $d$ of $(q-1)/\GCD(q-1)$, we can find integers $\sigma, \tau$ with $\sigma tq^m + \tau(q-1) = (q-1)/d$, and for any such roots $y_e, z_e$ and any such integers $\sigma, \tau$,

upon letting $\Lambda_e = \Gamma^e_s(y_e, z_e)^{S^{\tau}}$ we see that $\Lambda_e^{q-1} = S^{(q-1)/d}$ with $\Lambda_e \in L^\prime_e$. If also $GF(q) \subset k_p$, then we can find $\lambda \in GF(q) \subset k_p$ such that upon letting $\Lambda_e = \lambda \Lambda_e$ we have $\Lambda_e^q = S^{\tau}$ and $\Lambda_e \in L^\prime_e$, and now, because $L^\prime_e$ is also a splitting field of $\phi^e(\hat{Y})$ over $K_e(S)$, by the Substitution Principle on page 98 of [A03], for the Galois groups $G^{(d)}_e$ and $G^{(d)}_e$ of $\phi^{(d)}_e$ and $\phi^{(d)}_e$ over $K_e(S)$ respectively, in a natural manner we have $G^{(d)}_e = \Gal(\phi^e, K_e(\Lambda_e)) \subset G^{(d)}_e$ with $G^{(d)}_e/G^{(d)}_e = \Gal(K_e(\Lambda_e), K_e(S)) = Z_d$.

For $0 \leq e \leq m - 1$, let $R = k_p[X, S, T_1, \ldots, T_e]$ and $\overline{R} = k_p[X, T_1, \ldots, T_e]$, 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 $\phi^{(d)}_e$ is a monic polynomial in $Y$ with coefficients in $R$, and by applying $\alpha$ to the coefficients of $\phi^{(d)}_e$ we get the polynomial $\phi_e$ which is such that $\Disc \phi_e \neq 0$, and therefore, for the Galois group $G_e$ of $\phi_e$ over $K_e$ in a natural manner we have $G_e < G^{(d)}_e$.
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 $\hat{\phi}_e(Y)$ in any splitting field $L_e^1$ of $\hat{\phi}_e(Y)$ over $K_e(S)$ where $K_e = k_p(X, T_1, \ldots, T_e)$, and given any such $y_e$ there exists a root $z_e$ of $\hat{\phi}_e(Y)$ in $L_e^1$ such that $\Gamma_e^2(y_e, z_e) \neq 0$, and for every such $z_e$ we have $\Gamma_e^2(y_e, z_e)^{q-1} = S^{q^m}$ (note that for any $y_e \in L_e^1$ and $z_e \in L_e^1$ we obviously have $\Gamma_e^2(y_e, z_e) \in L_e^1$).

Moreover, for every divisor $d$ of $(q - 1)/\gcd(t, q - 1)$, there exist integers $\sigma, \tau$ with $\sigma q^m + \tau(q - 1) = (q - 1)/d$, and if $\text{GF}(q) \subset k_p$, then, given any such roots $y_e, z_e$ and any such integers $\sigma, \tau$, there exists $\lambda \in \text{GF}(q) \subset k_p$, such that for $\Lambda_e = \lambda \Gamma_e^2(y_e, z_e)^{\sigma q^m}$ we have $\Lambda_e \in L_e^1$ with $\Lambda_e^d = S$, and for the respective Galois groups $G_e, G_e^{(d)}, G_e^d$ of $\phi_e, \phi_e^{(d)}, \phi_e^d$ over $K_e, K_e(S), K_e(S)$ respectively, in a natural manner we have $G_e < G_e^{(d)} < G_e^d$ with $G_e^d/G_e^{(d)} = Z_d$.

4. Galois groups

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

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

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 $(q - 1)/\gcd(t, q - 1)$, in a natural manner we have

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

and

$$\text{PSp}(2m, q) \triangleleft \text{PG}_e \triangleleft \text{PG}_e^{(d)} < \text{PG}_e^d \triangleleft \text{PGSp}(2m, q)$$

where we recall that $G_e, G_e^{(d)}, G_e^d, \text{PG}_e, \text{PG}_e^{(d)}, \text{PG}_e^d$ are the Galois groups of $\phi_e, \phi_e^{(d)}, \phi_e^d$ over $K_e, K_e(S), K_e(S)$ respectively with $K_e = k_p(X, T_1, \ldots, T_e)$.

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

\[
\begin{cases}
\text{if } m > 2 \text{ and } \text{GF}(q) \subset k_p \text{ and } \gcd(t, q - 1) = 1, \text{ then for } 1 \leq e \leq m - 1 \text{ we have} & \\
\text{Sp}(2m, q) = G_e \triangleleft G_e^d = \text{GSp}(2m, q) \text{ and } \text{PSp}(2m, q) = \text{PG}_e \triangleleft \text{PG}_e^d = \text{PGSp}(2m, q)
\end{cases}
\]

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

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

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

and

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

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], $\text{Gal}(\phi, k_p(X, T_1, \ldots, T_e))$ and $\text{Gal}(f, k_p(X, T_1, \ldots, T_m))$ should be changed to $\text{Gal}(\phi, k_p(X, T_1, \ldots, T_{m-1}))$ and $\text{Gal}(f, k_p(X, T_1, \ldots, T_{m-1}))$ respectively.
where we recall that $G_e, G_e^{(d)}, G_e^1, PG_e, PG_e^{(d)}, PG_e^1$ are the Galois groups of $\phi_e, \phi_e^{(d)}, f_e, f_e^{(d)}, f_e^1$ over $K_e, K_e(S), K_e(S), K_e, K_e(S), K_e(S)$ respectively with $K_e = k_p(X, T_1,\ldots,T_e)$.

Remark (4.3). By applying (4.2) to case ("") we see that if $m > 2$ and $GF(q) \subset k_p$, then, for $1 \leq e \leq m - 1$, in a natural manner we have $\text{Gal}(\phi_e, k_p(X, T_1,\ldots,T_e)) = \text{Sp}(2m, q)$ and $\text{Gal}(f_e, k_p(X, T_1,\ldots,T_e)) = \text{PSp}(2m, q)$, 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


