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

AGAIN NICE EQUATIONS FOR NICE GROUPS

SHREERAM S. ABHYANKAR

(Communicated by Ronald M. Solomon)

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

1. INTRODUCTION

Let $m > 1$ be any integer, let $q' > 1$ be any power of a prime p, let $q = q'^2$, consider the polynomials $F^\dagger = F^\dagger(Y) = Y^{n'} + X^{q'}Y^v + XY^w + 1$ and $F'^* = F'^*(Y) = Y^{n'^*} + XY + 1$ in indeterminates X, Y over an algebraically closed field k of characteristic p, where $n' = 1 + q + \cdots + q^{2m-2}$, $v = 1 + q + \cdots + q^{m-1}$, $w = 1 + q + \cdots + q^{m-2}$, $n'^* = 1 + q' + \cdots + q'^{m-1}$, and consider their respective Galois groups $\mathrm{Gal}(F^\dagger, k(X))$ 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 [CKa] on antiflag transitive collineation groups, I proved that $\mathrm{Gal}(F'^*, k(X)) =$ the projective special linear group $\mathrm{PSL}(\nu, q')$; the $m = 2$ case of this was actually proved in my Feit-Serre-Email paper [A03] as a consequence of the Zassenhaus-Feit-Suzuki Theorem. In the present paper, as a consequence of Liebeck's characterization of classical groups by orbit sizes [Li2], I shall show that $\mathrm{Gal}(F^\dagger, k(X)) =$ the projective special unitary group $\mathrm{PSU}(2m-1, q')$. Note that Liebeck's orbit size characterization depends on the Rank 3 characterization of Liebeck [Li1] and the primitive divisor characterization of Penttila-Praeger-Saxl [PPS], which in turn are based on CT = the Classification Theorem of Finite Simple Groups. Also note that, in the present paper, I only use the two-orbit case of Liebeck's orbit size characterization which, as Liebeck points out in the Introduction of [Li2], depends only on Liebeck's 1987 paper [Li1] and not on the Penttila-Praeger-Saxl paper [PPS].

As a corollary of the above-mentioned theorem that the Galois group of $F^\dagger$ is $\mathrm{PSU}(2m-1, q')$, I shall show that the Galois group of a more general polynomial $f^\dagger$ is also $\mathrm{PSU}(2m-1, q')$. Moreover, by slightly changing $f^\dagger$ and $F^\dagger$, I shall show that we get polynomials $\phi^\dagger$ and $\phi_1^\dagger$ whose Galois group is the special unitary group $\mathrm{SU}(2m-1, q')$. The polynomials $f^\dagger, \phi^\dagger$ and $\phi_1^\dagger$ are also special cases of the families of

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.

polynomials giving unramified coverings of the affine line in nonzero characteristic written down in [A01].

It is a pleasure to thank Martin Liebeck for having promptly produced [Li2] at my request, and Ulrich Meierfrankenfeld for inspiring conversations.

2. Notation and outline

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

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

We shall frequently use the geometric series identity

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

and its corollary

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

Let

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

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

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

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

and note that then $f^\dagger_e$ is a monic polynomial of degree $\langle 2m-2 \rangle = 1 + q + q^2 + \cdots + q^{2m-2}$ in Y with coefficients in the polynomial ring $k_p[T_1, \ldots, T_e]$ and, as above, $\mathrm{Disc}_Y(f^\dagger_e) = 1$ and the Galois group $\mathrm{Gal}(f^\dagger_e, k_p(T_1, \ldots, T_e))$ is a subgroup of $\mathrm{Sym}_{\langle 2m-2 \rangle}$. Note that if $k = k_p =$ an algebraically closed field (of characteristic $p > 0$), then $F^\dagger$ is obtained by substituting X for T_1 in $f^\dagger_1$ and hence $\mathrm{Gal}(F^\dagger, k(X)) = \mathrm{Gal}(f^\dagger_1, k_p(T_1))$.

In Section 3, we factor $f^\dagger$ as $f^\dagger = \overline{f} f^*$ where $\overline{f} = \overline{f}(Y)$ and $f^* = f^*(Y)$ are monic polynomials of degrees $(q' q^{m-1} + 1)\langle m-2 \rangle$ and $q^{m-1}(q\langle m-2 \rangle - q'\langle m-2 \rangle + 1)$ in Y with coefficients in $k_p[T_1, \ldots, T_{m-1}]$ respectively. In Section 4, we show that $\overline{f}$ and f^* are irreducible in $k_p(T_1, \ldots, T_{m-1})[Y]$, and hence $\mathrm{Gal}(f^\dagger, k_p(T_1, \ldots, T_{m-1}))$ may be regarded as a subgroup of $\mathrm{PGL}(2m-1, q)$ having 2 orbits of sizes $(q' q^{m-1} + 1)\langle m-2 \rangle$ and $q^{m-1}(q\langle m-2 \rangle - q'\langle m-2 \rangle + 1)$. Given any e with $1 \leq e \leq m-1$, by putting $T_i = 0$ for all $i > e$ in $\overline{f}$ and f^* we get $f^\dagger_e = \overline{f}_e f^*_e$ where $\overline{f}_e$ and f^*_e are monic polynomials of degrees $(q' q^{m-1} + 1)\langle m-2 \rangle$

and $q^{m-1}(q\langle m-2\rangle - q'\langle m-2\rangle + 1)$ in Y with coefficients in $k_p[T_1,\ldots,T_e]$ respectively. In Section 4, we also show that $\overline{f}_e$ and f_e^* are irreducible in $k_p(T_1,\ldots,T_e)[Y]$, and hence $\mathrm{Gal}(f_e^\dagger, k_p(T_1,\ldots,T_e))$ may be regarded as a subgroup of $\mathrm{PGL}(2m-1,q)$ having 2 orbits of sizes $(q'q^{m-1}+1)\langle m-2\rangle$ and $q^{m-1}(q\langle m-2\rangle - q'\langle m-2\rangle+1)$. In Section 6, from this orbit description, we deduce the result that if k_p is algebraically closed, then $\mathrm{Gal}(f^\dagger, k_p(T_1,\ldots,T_{m-1})) = \mathrm{Gal}(f_e^\dagger, k_p(T_1,\ldots,T_e)) = \mathrm{PSU}(2m-1,q')$ for $1\le e\le m-1$.

Consider the monic polynomials

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

and

$$\begin{aligned}\phi_e^\dagger = \phi_e^\dagger(Y) = {} & Y^{q^{2m-1}-1}+1\\ & + \sum_{i=1}^{e}\left(T_i^{q'q^{i-1}}Y^{q^{m-1+i}-1} - T_iY^{q^{m-i}-1}\right) \quad \text{for } 1\le e\le m-1\end{aligned}$$

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

In Section 5, we give a review of linear algebra including definitions of $\mathrm{PSU}(2m-1,q')$ and $\mathrm{SU}(2m-1,q')$.

3. Factorization of the basic equation

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

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

by telescopically putting

$$h_m(Y) = \sum_{\mu=0}^{m-1} Y^{\alpha(m,\mu)} - \sum_{\mu=0}^{m-2} Y^{\alpha'(m,\mu)},$$

where

$$\alpha(m,\mu) = (q'q^{m-1}+1)\langle m-2-\mu\rangle \quad \text{for} \quad 0\le\mu\le m-1$$

and

$$\alpha'(m,\mu) = (q^m+1)\langle m-3-\mu\rangle + q^{m-2-\mu}[1+(q-q')\langle\mu\rangle] \quad \text{for} \quad 0\le\mu\le m-2,$$

and checking that then

$$\begin{aligned}&1+(q-q')\langle m-2\rangle + q'\alpha(m,0)\\ &= 1+(q-q')\langle m-2\rangle + q'(q'q^{m-1}+1)\langle m-2\rangle\\ &= \langle 2m-2\rangle\end{aligned}$$

and, for $0 \le \mu < m-1$,

$$\begin{aligned} &1+(q-q')\langle m-2\rangle + q'\alpha(m,\mu+1) \\ &= 1+(q-q')\langle m-2\rangle + q'(q'q^{m-1}+1)\langle m-3-\mu\rangle \\ &= 1+q\langle m-2\rangle + q^m\langle m-3-\mu\rangle - q'\langle m-2\rangle + q'\langle m-3-\mu\rangle \\ &= q^{m-2-\mu}(1+q\langle\mu\rangle) + (q^m+1)\langle m-3-\mu\rangle - q'q^{m-2-\mu}\langle\mu\rangle \\ &= (q^m+1)\langle m-3-\mu\rangle + q^{m-2-\mu}[1+(q-q')\langle\mu\rangle] \\ &= \alpha'(m,\mu) \end{aligned}$$

and, for $0 \le \mu < m-1$,

$$\begin{aligned} &1+(q-q')\langle m-2\rangle + q'\alpha'(m,\mu) \\ &= 1+(q-q')\langle m-2\rangle + q'(q^m+1)\langle m-3-\mu\rangle + q'q^{m-2-\mu}[1+(q-q')\langle\mu\rangle] \\ &= \langle m-2-\mu\rangle + q'[-\langle m-2\rangle + (q^m+1)\langle m-3-\mu\rangle + q^{m-2-\mu}\langle\mu+1\rangle] \\ &= (q'q^{m-1}+1)\langle m-2-\mu\rangle \\ &= \alpha(m,\mu) \end{aligned}$$

and

$$\alpha(m,m-1)=0$$

and hence

$$\begin{aligned} &Y^{1+(q-q')\langle m-2\rangle} h_m(Y)^{q'} + h_m(Y) \\ &= \sum_{\mu=0}^{m-1} Y^{1+(q-q')\langle m-2\rangle + q'\alpha(m,\mu)} - \sum_{\mu=0}^{m-2} Y^{1+(q-q')\langle m-2\rangle + q'\alpha'(m,\mu)} \\ &\quad + \sum_{\mu=0}^{m-1} Y^{\alpha(m,\mu)} - \sum_{\mu=0}^{m-2} Y^{\alpha'(m,\mu)} \\ &= Y^{\langle 2m-2\rangle} + 1. \end{aligned}$$

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

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

by telescopically putting

$$h_i(Y,T_i) = \sum_{\mu=0}^{i-1} Y^{\alpha(i,\mu)} T_i^{q^{i-1-\mu}} - \sum_{\mu=0}^{i-2} Y^{\alpha'(i,\mu)} T_i^{q'q^{i-2-\mu}},$$

where

$$\alpha(i,\mu) = q^{i-1-\mu}\langle m-1-i\rangle + (q'q^{m-1}+1)\langle i-2-\mu\rangle \quad \text{for} \quad 0 \le \mu \le i-1$$

and

$$\begin{aligned} \alpha'(i,\mu) &= \langle m-3-\mu\rangle \\ &\qquad + q^m\langle i-3-\mu\rangle + q^{m-2-\mu}[1+(q-q')\langle\mu\rangle] \quad \text{for} \quad 0 \le \mu \le i-2, \end{aligned}$$

and checking that then

$$\begin{aligned}&1+(q-q')\langle m-2\rangle+q'\alpha(i,0)\\&=1+(q-q')\langle m-2\rangle+q'q^{i-1}\langle m-1-i\rangle+q'(q'q^{m-1}+1)\langle i-2\rangle\\&=\langle m-2+i\rangle\end{aligned}$$

and, for $0\le\mu<i-1$,

$$\begin{aligned}&1+(q-q')\langle m-2\rangle+q'\alpha(i,\mu+1)\\&=1+(q-q')\langle m-2\rangle+q'q^{i-2-\mu}\langle m-1-i\rangle+q'(q'q^{m-1}+1)\langle i-3-\mu\rangle\\&=1+q\langle m-2\rangle+q^m\langle i-3-\mu\rangle-q'\langle m-2\rangle+q'q^{i-2-\mu}\langle m-1-i\rangle+q'\langle i-3-\mu\rangle\\&=\langle m-3-\mu\rangle+q^{m-2-\mu}(1+q\langle\mu\rangle)+q^m\langle i-3-\mu\rangle-q'q^{m-2-\mu}\langle\mu\rangle\\&=\langle m-3-\mu\rangle+q^m\langle i-3-\mu\rangle+q^{m-2-\mu}[1+(q-q')\langle\mu\rangle]\\&=\alpha'(i,\mu)\end{aligned}$$

and, for $0\le\mu<i-1$,

$$\begin{aligned}&1+(q-q')\langle m-2\rangle+q'\alpha'(i,\mu)\\&=1+(q-q')\langle m-2\rangle+q'\langle m-3-\mu\rangle\\&\quad+q'q^m\langle i-3-\mu\rangle+q'q^{m-2-\mu}[1+(q-q')\langle\mu\rangle]\\&=\langle m-2-\mu\rangle+q'[-\langle m-2\rangle+\langle m-3-\mu\rangle+q^m\langle i-3-\mu\rangle+q^{m-2-\mu}\langle\mu+1\rangle]\\&=q^{i-1-\mu}\langle m-1-i\rangle+(q'q^{m-1}+1)\langle i-2-\mu\rangle\\&=\alpha(i,\mu)\end{aligned}$$

and

$$\alpha(i,i-1)=\langle m-1-i\rangle$$

and hence

$$\begin{aligned}&Y^{1+(q-q')\langle m-2\rangle}h_i(Y,T_i)^{q'}+h_i(Y,T_i)\\&=\sum_{\mu=0}^{i-1}Y^{1+(q-q')\langle m-2\rangle+q'\alpha(i,\mu)}T_i^{q'q^{i-1-\mu}}-\sum_{\mu=0}^{i-2}Y^{1+(q-q')\langle m-2\rangle+q'\alpha'(i,\mu)}T_i^{q^{i-1-\mu}}\\&\quad+\sum_{\mu=0}^{i-1}Y^{\alpha(i,\mu)}T_i^{q^{i-1-\mu}}-\sum_{\mu=0}^{i-2}Y^{\alpha'(i,\mu)}T_i^{q'q^{i-2-\mu}}\\&=T_i^{q'q^{i-1}}Y^{\langle m-2+i\rangle}+T_iY^{\langle m-1-i\rangle}.\end{aligned}$$

Summing the above equations for h_i with $0<i\le m$ we get

$$Y^{1+(q-q')\langle m-2\rangle}\overline{f}(Y)^{q'}+\overline{f}(Y)=f^\dagger(Y),$$

where we have put

$$\begin{aligned}\overline{f}=\overline{f}(Y)&=\sum_{\mu=0}^{m-1}Y^{\alpha(m,\mu)}-\sum_{\mu=0}^{m-2}Y^{\alpha'(m,\mu)}\\&\quad+\sum_{i=1}^{m-1}\sum_{\mu=0}^{i-1}Y^{\alpha(i,\mu)}T_i^{q^{i-1-\mu}}-\sum_{i=1}^{m-1}\sum_{\mu=0}^{i-2}Y^{\alpha'(i,\mu)}T_i^{q'q^{i-2-\mu}}.\end{aligned}$$

By factoring the LHS of the previous equation, it follows that

$$f^\dagger = \overline{f} f^*, \quad \text{where} \quad f^* = f^*(Y) = Y^{1+(q-q')\langle m-2\rangle}\overline{f}(Y)^{q'-1} + 1.$$

Note that the ($\mu = 0$) term in the above first summation is $Y^{(q'q^{m-1}+1)\langle m-2\rangle}$ and its exponent $(q'q^{m-1}+1)\langle m-2\rangle$ is strictly greater than the Y-exponent of every other term in the above four summations, and hence $\overline{f}$ is a monic polynomial of degree $(q'q^{m-1}+1)\langle m-2\rangle$ in Y with coefficients in $k_p[T_1, \dots, T_{m-1}]$, and therefore f^* is a monic polynomial of degree $1+(q-q')\langle m-2\rangle + (q'-1)(q'q^{m-1}+1)\langle m-2\rangle = q^{m-1}[1+(q-q')\langle m-2\rangle]$ in Y with coefficients in $k_p[T_1, \dots, T_{m-1}]$. Thus

$$(3.0) \qquad \begin{cases} f^\dagger = \overline{f} f^*, \text{ where } \overline{f} \text{ and } f^* \text{ are monic polynomials} \\ \text{of degrees } (q'q^{m-1}+1)\langle m-2\rangle \text{ and } q^{m-1}[1+(q-q')\langle m-2\rangle] \text{ in } Y \\ \text{with coefficients in } k_p[T_1, \dots, T_{m-1}] \text{ respectively.} \end{cases}$$

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

$$(3.1) \qquad \begin{cases} \text{for } 1 \le e \le m-1 \text{ we have } f_e^\dagger = \overline{f}_e f_e^*, \text{ where } \overline{f}_e \text{ and } f_e^* \text{ are} \\ \text{monic polynomials of degrees} \\ (q'q^{m-1}+1)\langle m-2\rangle \text{and } q^{m-1}(q\langle m-2\rangle - q'\langle m-2\rangle + 1) \text{ in } Y \\ \text{with coefficients in } k_p[T_1, \dots, T_e] \text{ respectively.} \end{cases}$$

4. Irreducibility

Now for $1 \le e \le m-1$ we have

$$f_e^\dagger = A_e T_1^{q'} - B_e T_1 + C_e,$$

where $0 \ne A_e = Y^{\langle m-1\rangle} \in k_p[Y], 0 \ne B_e = -Y^{\langle m-2\rangle} \in k_p[Y]$ and

$$C_e = Y^{\langle 2m-2\rangle} + 1 + \sum_{i=2}^{e} \left(T_i^{q'q^{i-1}} Y^{\langle m-2+i\rangle} + T_i Y^{\langle m-1-i\rangle} \right) \in k_p[Y, T_2, \dots, T_e],$$

and hence in particular $\deg_{T_1} f_e^\dagger = q'$. Also clearly $\deg_{T_1} \overline{f}_e = 1$ and hence $\deg_{T_1} f_e^* = q'-1$.

By letting I to be the Y-adic valuation of $Q = k_p(Y, T_2, \dots, T_e)$, i.e., the real discrete valuation whose valuation ring is the localization of $k_p[Y, T_2, \dots, T_e]$ at the principal prime ideal generated by Y, we see that $I(A_e) = \langle m-1\rangle$ and $I(B_e) = \langle m-2\rangle$; hence $I(B_e/A_e) = \langle m-2\rangle - \langle m-1\rangle = -q^{m-1}$ and therefore $\mathrm{GCD}(q'-1, I(B_e/A_e)) = 1$. Also obviously A_e and C_e have no nonconstant common factor in $k_p[Y, T_2, \dots, T_e]$. Therefore by Lemmas (4.2) and (4.3) of [A05],

(4.1) $\qquad \overline{f}_e$ and f_e^* are irreducible in $k_p(T_1, \dots, T_e)[Y]$ for $1 \le e \le m-1$.

By taking $e = m-1$ in (4.1) we see that,

(4.2) $\qquad \overline{f}$ and f^* are irreducible in $k_p(T_1, \dots, T_{m-1})[Y]$.

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

$$\Theta_m : \mathrm{GL}(m,q) \to \mathrm{PGL}(m,q) = \mathrm{GL}(m,q)/\mathrm{GF}(q)^*$$

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

Now, in view of Proposition 3.1 of [A04], by (3.0), (3.1), (4.1) and (4.2) we get the following:

Theorem (4.3). *Assuming $GF(q) \subset k_p$, for $1 \le e \le m-1$, in a natural manner we may regard*

$$Gal(\phi_e^\dagger, k_p(T_1,\dots,T_e)) < GL(2m-1,q)$$

and

$$Gal(f_e^\dagger, k_p(T_1,\dots,T_e)) < PGL(2m-1,q),$$

and then

$$\Theta_{2m-1}(Gal(\phi_e^\dagger, k_p(T_1,\dots,T_e))) = Gal(f_e^\dagger, k_p(T_1,\dots,T_e))$$

and $Gal(f_e^\dagger, k_p(T_1,\dots,T_e))$ has two orbits of sizes $(q'q^{m-1}+1)\langle m-2\rangle$ and $q^{m-1}(q\langle m-2\rangle - q'\langle m-2\rangle + 1)$. In particular, again assuming $GF(q) \subset k_p$, in a natural manner we may regard

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

and

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

and then

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

and $Gal(f^\dagger, k_p(T_1,\dots,T_{m-1}))$ has two orbits of sizes $(q'q^{m-1}+1)\langle m-2\rangle$ and $q^{m-1}(q\langle m-2\rangle - q'\langle m-2\rangle + 1)$.

Recall that a *quasi-p group* is a finite group which is generated by its p-Sylow subgroups. Since $\mathrm{Disc}_Y f_e^\dagger = 1 = \mathrm{Disc}_Y \phi_e^\dagger$ 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 (4.4). *If k_p is algebraically closed, then, for $1 \le e \le m-1$, $Gal(f_e^\dagger, k_p(T_1,\dots,T_e))$ and $Gal(\phi_e^\dagger, k_p(T_1,\dots,T_e))$ are quasi-p groups. Hence in particular, if k_p is algebraically closed, then $Gal(f^\dagger, k_p(T_1,\dots,T_{m-1}))$ and $Gal(\phi^\dagger, k_p(T_1,\dots,T_{m-1}))$ are quasi-p groups.*

5. Review of linear algebra

Dickson (page 131 of [Dic]) defines the *hyperorthogonal group* in $\mathrm{GF}(q)$ on m indices as the group of all $a = (a_{ij}) \in \mathrm{GL}(m,q)$ which leave the m-variate form

$$x_1^{q'+1} + \dots + x_m^{q'+1}$$

unchanged, i.e., for which

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{m} x_i a_{ij}\right)^{q'+1} = \sum_{i=1}^{m} x_i^{q'+1}$$

or equivalently (page 133 of [Dic]) [1]

$$\sum_{j=1}^{m} a_{ij}^{q'+1} = 1 \quad \text{for } 1 \le i \le m$$

and

$$\sum_{j=1}^{m} a_{ij} a_{lj}^{q'} = 0 \quad \text{for } 1 \le i \le m \text{ and } 1 \le l \le m \text{ with } i \ne l.$$

Dickson denotes this group by $G_{m,p,s}$, where $p^s = q'$, and calculates (page 134 of [Dic]) its order $\Omega_{m,p,s}$; Dickson allows $m = 1$ and notes that (page 137 of [Dic]) then it is a cyclic group of order $q' + 1$. In modern terminology, this group is called the *general unitary group* and is denoted by $\mathrm{GU}(m, q')$; see [LiK] where on the second line of Table 2.1C on page 19, Dickson's $\Omega_{m,p,s}$ is given as the order $|I|$. We also put $\mathrm{SU}(m, q') = \mathrm{GU}(m, q') \cap \mathrm{SL}(m, q)$ and we call this the *special unitary group*; Dickson denotes this (page 137 of [Dic]) by $H_{m,p,s}$. Finally, we put $\mathrm{PGU}(m, q') = \Theta_m(\mathrm{GU}(m, q'))$ and $\mathrm{PSU}(m, q') = \Theta_m(\mathrm{SU}(m, q'))$, and we call these the *projective general unitary group* and *projective special unitary group* respectively; Dickson (page 138 of [Dic]) denotes $\mathrm{PSU}(m, q')$ by $HO(m, q)$ and notes its simplicity provided $(m, q') \ne (2, 2), (2, 3), (3, 2)$ (note that we are always assuming $m > 1$).

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

$$\mathrm{SU}(m, q') < H \Leftrightarrow \mathrm{PSU}(m, q') < \Theta_m(H). \tag{5.1}$$

In case $(m, q') \ne (3, 2)$, this follows exactly as in the proof of Lemma 2.3 of [A04] because then by (22.4) of [Asc] $\mathrm{SU}(m, q')$ is generated by transvections. Now the order of every transvection is p or 1, and the said proof is based on the fact that the group is generated by elements of p-power order, i.e., equivalently, the fact that it is a quasi-p group. So (5.1) holds also for $(m, q') = (3, 2)$; namely, $\mathrm{SU}(3, 2)$ is a quasi-2 group because its transvections generate a subgroup of index 4 (see lines 13–14 on page 124 of [Tay]).

By (2.3.3), 2.10.4(ii) and 2.10.6(i) of [LiK], for any $H < \mathrm{GL}(m, q)$ we have

$$\mathrm{SU}(m, q') \triangleleft H \Leftrightarrow \mathrm{SU}(m, q') < H < \mathrm{GU}(m, q')\mathrm{GF}(q)^* \tag{5.2}$$

and by 2.1.C of [LiK] we have

$$[\mathrm{GU}(m, q')\mathrm{GF}(q)^* : \mathrm{SU}(m, q')] \not\equiv 0 \pmod{p}. \tag{5.3}$$

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

$$\mathrm{PSU}(m, q') \triangleleft G \Leftrightarrow \mathrm{PSU}(m, q') < G < \mathrm{PGU}(m, q') \tag{5.4}$$

and by (5.3) we get

$$[\mathrm{PGU}(m, q') : \mathrm{PSU}(m, q')] \not\equiv 0 \pmod{p}. \tag{5.5}$$

Finally, for any $H < \mathrm{GL}(m, q)$ we obviously have

$$H < \mathrm{GU}(m, q')\mathrm{GF}(q)^* \Leftrightarrow \Theta_m(H) < \mathrm{PGU}(m, q'). \tag{5.6}$$

[1] To make up for Dickson's unusual definition of the product of matrices (pages 76 and 88 of [Dic]), in his matrix (α_{ij}), the index i should be regarded as the column number and j the row number.

In view of (5.4), Theorem (a) of [Li2] may be stated thus:

Theorem (5.7) [Liebeck]. *$G < PGL(2m-1,q)$ has two orbits of sizes $(q'q^{m-1}+1)\langle m-2\rangle$ and $q^{m-1}(q\langle m-2\rangle - q'\langle m-2\rangle+1)$ if and only if after a suitable change of basis of $GF(q)^{2m-1}$ we have $PSU(2m-1,q') < G < PGU(2m-1,q')$.*

Let $\mathrm{PSU}(2m-1,q')_1$ denote $\mathrm{PSU}(2m-1,q')$ as it acts on the orbit of size $(q'q^{m-1}+1)\langle m-2\rangle$, and let $\mathrm{PSU}(2m-1,q')_2$ denote $\mathrm{PSU}(2m-1,q')$ as it acts on the orbit of size $(q'q^{m-1}+1)\langle m-2\rangle$. These actions are faithful for $(m,q)\neq(2,4)$ because $\mathrm{PSU}(2m-1,q')$ is simple, and for $(m,q)=(2,4)$ because the proper normal subgroups of $\mathrm{PSU}(3,2)$ have index 2, 4 or 8 (page 124 of [Tay]), and hence

$$\mathrm{PSU}(2m-1,q')_1 \approx \mathrm{PSU}(2m-1,q') \approx \mathrm{PSU}(2m-1,q')_2 \tag{5.8}$$

where $\approx$ denotes isomorphism of abstract groups.

6. Galois groups

By (4.3), (5.1), (5.6) and (5.7) we get the following:

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

$$SU(2m-1,q') < Gal(\phi_e^\dagger, k_p(T_1,\dots,T_e)) < GU(2m-1,q')GF(q)^*$$

and

$$PSU(2m-1,q') < Gal(f_e^\dagger, k_p(T_1,\dots,T_e)) < PGU(2m-1,q').$$

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

$$SU(2m-1,q') < Gal(\phi^\dagger, k_p(T_1,\dots,T_e)) < GU(2m-1,q')GF(q)^*$$

and

$$PSU(2m-1,q') < Gal(f^\dagger, k_p(T_1,\dots,T_e)) < PGU(2m-1,q').$$

By (3.0) to (3.1), (4.1), (4.2), (4.4), (5.2), (5.3), (5.4), (5.5), (5.8) and (6.1) we get the following:

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

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

and

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

and

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

and

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

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

[A05] S. S. Abhyankar, *More nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 3577–3591.

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

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

[Li1] M. W. Liebeck, *The affine permutation groups of rank three*, Proceedings of London Mathematical Society **54** (1987), 477–516. MR **88m:**20004

[Li2] M. W. Liebeck, *Characterization of classical groups by orbit sizes on the natural module*, Proceedings of the American Mathematical Society **124** (1996), 3561–3566.

[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

[PPS] T. Penttila, C. E. Praeger and J. Saxl, *Linear groups with orders divisible by certain large primes*, (To Appear).

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907

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