PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 9, Pages 2511–2525
S 0002-9939(99)05400-3
Article electronically published on May 4, 1999

SEMILINEAR TRANSFORMATIONS

SHREERAM S. ABHYANKAR

(Communicated by Ron Donagi)

ABSTRACT. In previous papers, nice trinomial equations were given for unramified coverings of the once punctured affine line in nonzero characteristic p with the projective general group $\mathrm{PGL}(m,q)$ and the general linear group $\mathrm{GL}(m,q)$ as Galois groups where $m>1$ is any integer and $q>1$ is any power of p. These Galois groups were calculated over an algebraically closed ground field. Here we show that, when calculated over the prime field, as Galois groups we get the projective general semilinear group $\mathrm{P\Gamma L}(m,q)$ and the general semilinear group $\mathrm{\Gamma L}(m,q)$. We also obtain the semilinear versions of the local coverings considered in previous papers.

1. INTRODUCTION

In my 1957 paper [A02], I considered the algebraic fundamental group $\pi_A(L_k)$ of the affine line L_k over a field k of characteristic $p>0$, and conjectured that if k is algebraically closed, then $\pi_A(L_k)$ coincides with the set $Q(p)$ of all quasi-p groups; recall that $\pi_A(L_k)$ is defined to be the set of all Galois groups of finite unramified Galois coverings of L_k, and $Q(p)$ is defined to be the set of all finite groups G such that $G=p(G)$ where $p(G)$ denotes the subgroup of G generated by all of its p-Sylow subgroups. In [A02], I also conjectured that if k is algebraically closed and $t\geq 0$ is any integer, then $\pi_A(L_{k,t})=Q_t(p)$, where $L_{k,t}=L_k$ punctured at t points, and $Q_t(p)=$ the set of all quasi-(p,t) groups, i.e., finite groups G such that $G/p(G)$ is generated by t generators; more generally, if k is algebraically closed and C_g is a projective nonsingular curve of genus g over k, then for any integer $w\geq 0$, upon letting $C_{g,w}=C_g$ minus $w+1$ points, we have $\pi_A(C_{g,w})=Q_{2g+w}(p)$. Now that these **Geometric Conjectures** have been settled affirmatively by Raynaud [Ray] and Harbater [Har], it is time to turn our attention to the arithmetic case of affine curves over the prime field $\mathrm{GF}(p)$ of cardinality p. As in the geometric case of curves over an algebraically closed ground field, here too the evidence suggests that the algebraic fundamental group should be "as large as possible." Specifically, as an **Arithmetical Conjectural Question** we ask whether $\pi_A(L_{\mathrm{GF}(p)})=Q_1(p)$.

The above Geometric Conjectures were inspired by the **Local Conjecture** which was implicit in my 1955 paper [A01] and was made explicit in [A06]. The said Local Conjecture predicts that if k is algebraically closed, then for all integers $r\geq 2$ and $t\geq 1$ we have $\pi_A^L(N_{k,t}^r)=P_t(p)$. Here $N_{k,t}^r$ represents a neighborhood of a simple

Received by the editors March 5, 1997 and, in revised form, July 2, 1997.
1991 *Mathematics Subject Classification.* Primary 12F10, 14H30, 20D06, 20E22.
This work was partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-97-1-0010.

point on an r-dimensional algebraic variety over k from which we have deleted a divisor having a t-fold normal crossing at the simple point. The local algebraic fundamental group $\pi_A^L(N_{k,t}^r)$ is defined to be the set of all inertia groups above the simple point coming from finite Galois coverings of the variety with branch locus at the simple point contained in the normal crossing divisor. Moreover, $P_t(p)$ is defined to be the set of all (p,t)-groups, i.e., finite groups G such that $G/p(G)$ is an abelian group on t generators. Note that $Q_t(p) = P_t(p)$ for $t \leq 1$, but $Q_t(p)$ is much larger than $P_t(p)$ for $t > 1$.

To provide evidence towards these conjectures, in [A01] to [A06], we considered the trinomials $F^* = F^*(Y) = Y^{n^*} + XY + (-1)^{n^*}$ and $F^{**} = F^{**}(Y) = Y^{n^*} + Y + X$ and $F^{\bullet\bullet} = F^{\bullet\bullet}(Y) = Y^{n^*} + ZY + X$ in indeterminates X, Y, Z over the field k, where $m > 1$ is any integer, $q > 1$ is any power of p, and $n^* = 1 + q + \cdots + q^{m-1}$. We also considered the trinomials obtained by changing Y to Y^{q-1} in these, i.e., the trinomials $\Phi^*(Y) = F^*(Y^{q-1})$ and $\Phi^{**}(Y) = F^{**}(Y^{q-1})$ and $\Phi^{\bullet\bullet}(Y) = F^{\bullet\bullet}(Y^{q-1})$. By taking Y-derivatives, we easily see that F^* and Φ^* give unramified coverings of the affine X-line, F^{**} and Φ^{**} give unramified coverings of the once punctured affine X-line, and $F^{\bullet\bullet}$ and $\Phi^{\bullet\bullet}$ give coverings of the affine (X,Z)-plane with the line $X = 0$ as the branch locus.

Recall that the general linear group $\mathrm{GL}(m,q)$ is the group of all nonsingular m by m matrices over the Galois Field $\mathrm{GF}(q)$ of cardinality q. Moreover, the special linear group $\mathrm{SL}(m,q)$ is the subgroup of this consisting of matrices of determinant 1. Now $\mathrm{GL}(m,q)$ may be regarded as the group of all nonsingular linear transformations of the vector space $\mathrm{GF}(q)^m$, and then it becomes a subgroup of the general semilinear group $\Gamma\mathrm{L}(m,q)$ = the group of all nonsingular semilinear transformations of $\mathrm{GF}(q)^m$, i.e., those additive bijections β of $\mathrm{GF}(q)^m$ for which we have $\beta(\zeta z) = \beta'(\zeta)\beta(z)$ for all $\zeta \in \mathrm{GF}(q)$ and $z \in \mathrm{GF}(q)^m$ where β' is an automorphism of $\mathrm{GF}(q)$ which depends only on β and not on ζ or z. Finally note that $\mathrm{PGL}(m,q)$, $\mathrm{PSL}(m,q)$ and $\mathrm{P}\Gamma\mathrm{L}(m,q)$ are the respective factor groups of $\mathrm{GL}(m,q)$, $\mathrm{SL}(m,q)$ and $\Gamma\mathrm{L}(m,q)$ modulo scalar matrices.

In [A03], [A04] it was shown that if k is algebraically closed, then $\mathrm{Gal}(\Phi^*, k(X))$ $= \mathrm{SL}(m,q)$ and $\mathrm{Gal}(F^*, k(X)) = \mathrm{PSL}(m,q)$;[1] we shall now show that this is so under the weaker assumption that $\mathrm{GF}(q) \subset k$.

For every divisor d of $q-1$, let $\Phi^{*(d)}$ and $F^{*(d)}$ be obtained by substituting $(-1)^{n^*}X^d$ for X in Φ^{**} and F^{**} respectively, let $\mathrm{GL}^{(d)}(m,q)$ be defined by the condition that $\mathrm{SL}(m,q) \lhd \mathrm{GL}^{(d)}(m,q) \lhd \mathrm{GL}(m,q)$ with $\mathrm{GL}(m,q)/\mathrm{GL}^{(d)}(m,q) = Z_d$,[2] let $\mathrm{PGL}^{(d)}(m,q)$ = the image of $\mathrm{GL}^{(d)}(m,q)$ under the canonical epimorphism of $\mathrm{GL}(m,q)$ onto $\mathrm{PGL}(m,q)$, and note that then $\mathrm{PGL}^{(d)}(m,q)$ is uniquely characterized by the condition that $\mathrm{PSL}(m,q) \lhd \mathrm{PGL}^{(d)}(m,q) \lhd \mathrm{PGL}(m,q)$ with $\mathrm{PGL}(m,q)/\mathrm{PGL}^{(d)}(m,q) = Z_{\mathrm{GCD}(m,d)}$.[3] In [A04] and [A05] it was shown that if

[1] Here we regard $\mathrm{SL}(m,q)$ as acting on nonzero vectors. For the polynomial $\widehat{\Phi}^*(Y) = Y\Phi^*(Y)$ we then have $\mathrm{Gal}(\widehat{\Phi}^*, k(X)) = \mathrm{SL}(m,q)$ regarded as acting on the entire vector space $\mathrm{GF}(q)^m$. The polynomials Φ^* and $\widehat{\Phi}^*$ may respectively be called the subvectorial and vectorial associates of the projective polynomial F^*. For generalities about projective, subvectorial, and vectorial polynomials, and their Galois groups, see Sections 2 and 3.

[2] Since $\mathrm{SL}(m,q) \lhd \mathrm{GL}(m,q)$ with $\mathrm{GL}(m,q)/\mathrm{SL}(m,q) = Z_{q-1}$, we see that this uniquely characterizes the intermediate group $\mathrm{GL}^{(d)}(m,q)$. Note that, as usual, $<$ and $\lhd$ denote subgroup and normal subgroup respectively, and Z_d denotes a cyclic group of order d.

[3] In view of the previous footnote, this follows from the fact that $[\mathrm{PGL}(m,q) : \mathrm{PSL}(m,q)] = \mathrm{GCD}(m, q-1)$.

$\mathrm{GF}(q) \subset k$, then $\mathrm{Gal}(\Phi^{**}, k(X)) = \mathrm{GL}(m,q)$ and $\mathrm{Gal}(F^{**}, k(X)) = \mathrm{PGL}(m,q)$; we shall now extend this result by showing that, if $\mathrm{GF}(q) \subset k$, then, for every divisor d of $q-1$, we have $\mathrm{Gal}(\Phi^{*(d)}, k(X)) = \mathrm{GL}^{(d)}(m,q)$ and $\mathrm{Gal}(F^{*(d)}, k(X)) = \mathrm{PGL}^{(d)}(m,q)$. In [A05] it was also shown that if $\mathrm{GF}(q) \subset k$, then $\mathrm{Gal}(\Phi^{\bullet\bullet}, k((X,Z))) = \mathrm{GL}(m,q)$ and $\mathrm{Gal}(F^{\bullet\bullet}, k((X,Z))) = \mathrm{PGL}(m,q)$;[4] we shall now extend this result by showing that if $\mathrm{GF}(q) \subset k$, then, for every divisor d of $q-1$, we have $\mathrm{Gal}(\Phi^{\bullet(d)}, k((X,Z))) = \mathrm{GL}^{(d)}(m,q)$ and $\mathrm{Gal}(F^{\bullet(d)}, k((X,Z))) = \mathrm{PGL}^{(d)}(m,q)$ where $\Phi^{\bullet(d)}$ and $F^{\bullet(d)}$ are obtained by substituting $(-1)^{n^*}X^d$ for X in $\Phi^{\bullet\bullet}$ and $F^{\bullet\bullet}$ respectively.

To extend the above results further by removing the assumption that $\mathrm{GF}(q) \subset k$, let us note that $\mathrm{GL}(m,q) \lhd \Gamma\mathrm{L}(m,q)$ and, upon letting u be the unique integer with $q = p^u$, we have $\Gamma\mathrm{L}(m,q)/\mathrm{GL}(m,q) = Z_u$. For every divisor δ of u, let $\Gamma\mathrm{L}_\delta(m,q)$ be defined by the condition that $\mathrm{GL}(m,q) \lhd \Gamma\mathrm{L}_\delta(m,q) \lhd \Gamma\mathrm{L}(m,q)$ with $\Gamma\mathrm{L}_\delta(m,q)/\mathrm{GL}(m,q) = Z_\delta$, and let us define $\mathrm{P}\Gamma\mathrm{L}_\delta(m,q) =$ the image of $\Gamma\mathrm{L}_\delta(m,q)$ under the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{P}\Gamma\mathrm{L}(m,q)$. Also let $\Gamma\mathrm{SL}_\delta(m,q)$ be the set of all subgroups I of $\Gamma\mathrm{L}_\delta(m,q)$ such that $I \cap \mathrm{GL}(m,q) = \mathrm{SL}(m,q) \lhd I$ with $I/\mathrm{SL}(m,q) = Z_\delta$, and let $\mathrm{P}\Gamma\mathrm{SL}_\delta(m,q)$ be the set of images of the various members of $\Gamma\mathrm{SL}_\delta(m,q)$ under the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{P}\Gamma\mathrm{L}(m,q)$.[5] Likewise, for every divisor d of $q-1$, let $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ be the set of all subgroups J of $\Gamma\mathrm{L}_\delta(m,q)$ such that $J \cap \mathrm{GL}(m,q) = \mathrm{GL}^{(d)}(m,q) \lhd J$ with $J/\mathrm{GL}^{(d)}(m,q) = Z_\delta$ and $I < J$ for some I in $\Gamma\mathrm{SL}_\delta(m,q)$, and let $\mathrm{P}\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ be the set of images of the various members of $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ under the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{P}\Gamma\mathrm{L}(m,q)$.[6]

Upon letting $\delta(k)$ be the unique divisor of u such that $\mathrm{Gal}(Y^q - Y, k) = Z_{\delta(k)}$, we shall show that $\mathrm{Gal}(\Phi^*, k(X)) \in \Gamma\mathrm{SL}_{\delta(k)}(m,q)$ and $\mathrm{Gal}(F^*, k(X)) \in \mathrm{P}\Gamma\mathrm{SL}_{\delta(k)}(m,q)$, and moreover $\mathrm{Gal}(\Phi^{**}, k(X)) = \Gamma\mathrm{L}_{\delta(k)}(m,q)$ and $\mathrm{Gal}(F^{**}, k(X)) = \mathrm{P}\Gamma\mathrm{L}_{\delta(k)}(m,q)$. Similarly we shall show that

$$\mathrm{Gal}(\Phi^{\bullet\bullet}, k((X,Z))) = \Gamma\mathrm{L}_{\delta(k)}(m,q) \quad \text{and} \quad \mathrm{Gal}(F^{\bullet\bullet}, k((X,Z))) = \mathrm{P}\Gamma\mathrm{L}_{\delta(k)}(m,q).$$

Likewise, for every divisor d of $q-1$, we shall show that $\mathrm{Gal}(\Phi^{*(d)}, k(X)) \in \Gamma\mathrm{L}_{\delta(k)}^{(d)}(m,q)$ and $\mathrm{Gal}(F^{*(d)}, k(X)) \in \mathrm{P}\Gamma\mathrm{L}_{\delta(k)}^{(d)}(m,q)$, and similarly we show that $\mathrm{Gal}(\Phi^{\bullet(d)}, k((X,Z))) \in \Gamma\mathrm{L}_{\delta(k)}^{(d)}(m,q)$ and $\mathrm{Gal}(F^{\bullet(d)}, k((X,Z))) \in \mathrm{P}\Gamma\mathrm{L}_{\delta(k)}^{(d)}(m,q)$.

As we shall indicate in Section 2, the trinomials $\Phi^*, \Phi^{**}, \Phi^{*(d)}, \Phi^{\bullet\bullet}, \Phi^{\bullet(d)}, F^*, F^{**}, F^{*(d)}, F^{\bullet\bullet}, F^{\bullet(d)}$ are members of more general families of polynomials which have the same Galois groups as these special members, and which give unramified

---

[4] As usual, $k((X,Z))$ denotes the field of meromorphic functions. In case of $\mathrm{Gal}(\Phi^{**}, k(X))$ and $\mathrm{Gal}(\Phi^{\bullet\bullet}, k((X,Z)))$ we regard $\mathrm{GL}(m,q)$ as acting on nonzero vectors. For the polynomials $\widehat{\Phi}^{**}(Y) = Y\Phi^{**}(Y)$ and $\widehat{\Phi}^{\bullet\bullet}(Y) = Y\Phi^{\bullet\bullet}(Y)$ we then have $\mathrm{Gal}(\widehat{\Phi}^{**}, k(X)) = \mathrm{GL}(m,q)$ and $\mathrm{Gal}(\widehat{\Phi}^{\bullet\bullet}, k((X,Z))) = \mathrm{GL}(m,q)$ regarded as acting on the entire vector space $\mathrm{GF}(q)^m$.

[5] It can be seen that $\Gamma\mathrm{SL}_\delta(m,q)$ is a nonempty complete set of conjugate subgroups of $\Gamma\mathrm{L}(m,q)$, and every I in $\Gamma\mathrm{SL}_\delta(m,q)$ is a split extension of $\mathrm{SL}(m,q)$ (i.e., some subgroup of I is mapped isomorphically onto $I/\mathrm{SL}(m,q)$ by the residue class map of I onto $I/\mathrm{SL}(m,q)$) such that $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\mathrm{SL}(m,q)$ and I. See Remark (4.1.1).

[6] It can be seen that $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ is a nonempty complete set of conjugate subgroups of $\Gamma\mathrm{L}(m,q)$, and every J in $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ is a split extension of $\mathrm{GL}^{(d)}(m,q)$ such that $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\mathrm{GL}(m,q)$ and J. It can also be seen that $\Gamma\mathrm{L}_\delta^{(q-1)}(m,q) = \Gamma\mathrm{SL}_\delta(m,q)$ and $\Gamma\mathrm{L}_\delta^{(1)}(m,q) = \{\Gamma\mathrm{L}_\delta(m,q)\}$. See Remark (4.1.1).

coverings of the affine space, the affine line minus a hyperplane, and the local affine space minus a normal crossing divisor.

In Section 2 we shall state the results about the Galois groups of these general families of polynomials assuming that the ground field contains $\mathrm{GF}(q)$, and we shall prove them in Section 3. In Section 4 we shall state and prove the sharper forms of these results without this assumption; it will turn out that the Galois groups then get enlarged into their semilinear versions.

As in [A02] to [A06], our calculation of the Galois groups will mainly be based on MTR = the Method of Throwing away Roots and RGT = Recognition Theorems for Groups. To explain MTR, if $F = F(Y) \in K[Y]$ is separable monic of degree n, then the Galois group $\mathrm{Gal}(F, K)$ is a transitive subgroup G of the symmetric group S_n on n letters, and its one-point stabilizer G_1 is the Galois group $\mathrm{Gal}(F', K(y))$ where y is a root of F and the "twisted derivative" F' of F is obtained by "throwing away" y, i.e., $F'(Y) = F(Y)/(Y - y)$; frequently, properties of G and G_1 can be read off from each other. As an example of RTG, we shall use the result of Cameron-Kantor [CaK] which gives a condition for a subgroup of $\mathrm{GL}(m, q)$ with $m > 2$ to contain $\mathrm{SL}(m, q)$, and which we state as the Transitivity Lemma (2.1.4) in Section 2. We shall also use the Basic Extension Principle (see page 93 of [A03]) saying that, for any overfield K^* of K, the Galois group $\mathrm{Gal}(F, K^*)$ may be regarded as a subgroup of the Galois group $\mathrm{Gal}(F, K)$, and the Substitution Principle (see page 98 of [A03]) which applies this to the case when $K = k(X^d)$ and $K^* = k(X)$. Yet another fact which we shall use is the Specialization Principle (see footnote 8 of [AL1]) saying that if K is the quotient field of a regular local domain R with $F \in R[Y]$ and $\alpha : R \to \overline{R}$ is an epimorphism where $\overline{R}$ is an integral domain with quotient field $\overline{K}$ such that the polynomial $\overline{F}$ obtained by applying α to the coefficients of F is separable, then the Galois group $\mathrm{Gal}(\overline{F}, \overline{K})$ may be regarded as a subgroup of the Galois group $\mathrm{Gal}(F, K)$.

Note that $\pi_A(L_k)$ is the set of all finite quotients of the complete algebraic fundamental group $\pi_A^C(L_k)$ = the (highly infinite) Galois group of the compositum of all finite extensions of $k(X)$ in a fixed algebraic closure which are unramified over $k[X]$. We would like to point out that, even when k is algebraically closed, the structure of $\pi_A^C(L_k)$ remains a complete mystery. Indeed, my few attempts to describe it were immediately shot down by Serre, who has predicted a similar fate for any future attempts I might make.

It is a pleasure to thank Nick Inglis, Paul Loomis and Ganesh Sundaram for stimulating conversations concerning the material of this paper.

2. Notation and outline

Let $k_p \subset K$ be fields of characteristic $p > 0$, let $q > 1$ be any power of p, and let $m > 0$ be any integer.[7] To abbreviate frequently occurring expressions, for every integer $i \geq -1$ we put

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

Recall that $f^*(Y)$ (resp: $\phi^*(Y)$ or $\widehat{\phi}^*(Y)$) in $K[Y]$ is said to be a **projective** (resp: **subvectorial** or **vectorial**) q**-polynomial** of q**-prodegree** (resp: q**-subdegree** or q**-degree**) m^* (where $m^* \geq 0$ is an integer) in Y with coefficients in

[7] In the Abstract and the Introduction we assumed $m > 1$. But in the rest of the paper, unless stated otherwise, we only assume $m > 0$.

K if it is of the form $f^*(Y) = \sum_{i=0}^{m^*} a_i^* Y^{\langle m^*-1-i\rangle}$ (resp :$\phi^*(Y) = \sum_{i=0}^{m^*} a_i^* Y^{q^{m^*-i}-1}$ or $\widehat{\phi}^*(Y) = \sum_{i=0}^{m^*} a_i^* Y^{q^{m^*-i}}$) with $a_i^* \in K$ for all i and $a_0^* \neq 0$. The phrase "of q-prodegree (resp: q-subdegree or q-degree) m^* in Y with coefficients in K" may be dropped or may be abbreviated to something like "in Y over K." Also the reference to q may be dropped. Note that $f^*(Y)$ (resp: $\phi^*(Y)$ or $\widehat{\phi}^*(Y)$) is **monic** $\Leftrightarrow a_0^* = 1$, and note that $f^*(Y)$ (resp: $\phi^*(Y)$ or $\widehat{\phi}^*(Y)$) is **separable** (i.e., its Y-discriminant is nonzero) $\Leftrightarrow a_{m^*}^* \neq 0$, and note that $\widehat{\phi}_Y^*(Y) = \widehat{\phi}_Y^*(0) = a_{m^*}^*/a_0^* = a_{m^*}^*$ where $\widehat{\phi}_Y^*(Y)$ is the Y-derivative of $\widehat{\phi}^*(Y)$. Also note that $f^*(Y) \to \phi^*(Y) = f^*(Y^{q-1})$ and $\phi^*(Y) \to \widehat{\phi}^*(Y) = Y\phi^*(Y)$ give bijections of projectives to subvectorials (= their **subvectorial associates**) to vectorials (= their **vectorial associates**).

Now let

$$f = f(Y) = \sum_{i=0}^{m} a_i Y^{\langle m-1-i\rangle} \text{ with } a_i \in K \text{ and } a_0 \neq 0 \neq a_m$$

be a separable projective q-polynomial of q-prodegree m in Y over K, and let

$$\phi = \phi(Y) = f(Y^{q-1}) = \sum_{i=0}^{m} a_i Y^{q^{m-i}-1}$$

and

$$\widehat{\phi} = \widehat{\phi}(Y) = Y\phi(Y) = \sum_{i=0}^{m} a_i Y^{q^{m-i}}$$

be the subvectorial and vectorial associates of f respectively.

Concerning the Galois groups of projective and subvectorial polynomials, in (2.5)(i) and (2.5)(ii) of [A04] we observed the following:[8]

Linearity Lemma (2.1.1). *If* $\mathrm{GF}(q) \subset K$*, then for the Galois group* $\mathrm{Gal}(\phi, K)$ *of the subvectorial polynomial* ϕ *in a natural manner we have* $\mathrm{Gal}(\phi, K) < \mathrm{GL}(m, q)$,[9] *and for the Galois group* $\mathrm{Gal}(f, K)$ *of its projective associate* f *in a natural manner we have* $\mathrm{Gal}(f, K) =$ *the image of* $\mathrm{Gal}(\phi, K)$ *under the canonical epimorphism of* $\mathrm{GL}(m, q)$ *onto* $\mathrm{PGL}(m, q)$.

In connection with (2.1.1), the following four lemmas are significant; for (2.1.2) see (2.5)(iii) of [A04], for (2.1.3) see (2.3) of [A04], for (2.1.4) see Theorem I of Cameron-Kantor [CaK], and for (2.1.5) see Result 4 of [A02],

Root Extraction Lemma (2.1.2). *There exists an element* Λ *in the splitting field of* ϕ *over* K *such that* $\Lambda^{q-1} = (-1)^{\langle m-1\rangle} a_m/a_0$.

Transvection Lemma (2.1.3). *For any* $H < \mathrm{GL}(m, q)$ *we have:* $\mathrm{SL}(m, q) < H \Leftrightarrow \mathrm{PSL}(m, q) <$ *the image of* H *under the canonical epimorphism of* $\mathrm{GL}(m, q)$ *onto* $PGL(m, q)$.

Transitivity Lemma (2.1.4) (Cameron-Kantor)**.** *If* $m > 2$ *and* $H < \mathrm{GL}(m, q)$ *is such that its image under the canonical epimorphism of* $\mathrm{GL}(m, q)$ *onto* $PGL(m, q)$ *is doubly transitive, then either* $\mathrm{SL}(m, q) < H$*, or* $(q, m) = (4, 2)$ *with* $A_7 \approx H <$

[8] In [A04] we assumed $m > 1$, but the following Lemmas (2.1.1) to (2.1.3) are obviously true for $m = 1$.

[9] The Galois group $\mathrm{Gal}(\widehat{\phi}, K)$ essentially equals the Galois group $\mathrm{Gal}(\phi, K)$ except that the former acts on the entire vector space of the roots of $\widehat{\phi}$ while the latter acts on the nonzero vectors of that vector space.

$\mathrm{SL}(4,2) = \mathrm{GL}(4,2) \approx A_8$ *(where* $\approx$ *denotes isomorphism, and* A_7 *and* A_8 *are the alternating groups on* 7 *and* 8 *letters respectively).*

Quasi-p Lemma (2.1.5). *If* $K = k_p(X)$ *with* X *an indeterminate and* k_p *algebraically closed,* $a_m/a_0 \in k_p$*, and* $a_i/a_0 \in k_p[X]$ *for* $1 \le i \le m-1$*, then* $\mathrm{Gal}(\phi, K)$ *and* $\mathrm{Gal}(f, K)$ *are quasi-p groups.*

To apply these lemmas to special families of polynomials, let $Y, X, T_1, T_2, \dots$ be indeterminates over k_p. For every $e \ge 0$ let

$$K_e = k_p(X, T_1, \dots, T_e) \tag{i}$$

and

$$\widetilde{K}_e = \begin{cases} \text{the quotient field of an } (e+1)-\text{dimensional regular local} \\ \text{domain } R_e \text{ with } k_p \subset R_e \text{ and } M(R_e) = (X, T_1, \dots, T_e)R_e \end{cases} \tag{ii}$$

where as usual $M(R_e)$ is the maximal ideal of R_e, and for every $e \ge 1$ and $0 \ne \tau \in k_p(T_1)$ let

$$K_{(e,\tau)} = k_p(X, \tau, T_2, \dots, T_e). \tag{iii}$$

For $0 \le e \le m-1$, consider the monic separable projective q-polynomial

$$f_e^{**} = f_e^{**}(Y) = Y^{\langle m-1 \rangle} + X + \sum_{i=1}^{e} T_i Y^{\langle i-1 \rangle}$$

of q-prodegree m in Y over K_e, and its subvectorial associate

$$\phi_e^{**} = \phi_e^{**}(Y) = f_e^{**}(Y^{q-1}) = Y^{q^m-1} + X + \sum_{i=1}^{e} T_i Y^{q^i-1}$$

and, for every divisor d of $q-1$, let $f_e^{*(d)}$ and $\phi_e^{*(d)}$ be obtained by substituting $(-1)^{\langle m-1 \rangle} X^d$ for X in f_e^{**} and ϕ_e^{**} respectively, i.e., let

$$f_e^{*(d)} = f_e^{*(d)}(Y) = Y^{\langle m-1 \rangle} + (-1)^{\langle m-1 \rangle} X^d + \sum_{i=1}^{e} T_i Y^{\langle i-1 \rangle}$$

and

$$\phi_e^{*(d)} = \phi_e^{*(d)}(Y) = Y^{q^m-1} + (-1)^{\langle m-1 \rangle} X^d + \sum_{i=1}^{e} T_i Y^{q^i-1}.$$

For $1 \le e \le m-1$ and every $0 \ne \tau \in k_p(T_1)$ let $f_{(e,\tau)}^{**}$ and $\phi_{(e,\tau)}^{**}$ be obtained by substituting τ for T_1 in f_e^{**} and ϕ_e^{**} respectively, i.e., let

$$f_{(e,\tau)}^{**} = f_{(e,\tau)}^{**}(Y) = Y^{\langle m-1 \rangle} + X + \tau Y + \sum_{i=2}^{e} T_i Y^{\langle i-1 \rangle}$$

and

$$\phi_{(e,\tau)}^{**} = \phi_{(e,\tau)}^{**}(Y) = Y^{q^m-1} + X + \tau Y^{q-1} + \sum_{i=2}^{e} T_i Y^{q^i-1}$$

and, for every divisor d of $q-1$, let $f^{*(d)}_{(e,\tau)}$ and $\phi^{*(d)}_{(e,\tau)}$ be obtained by substituting $(-1)^{\langle m-1\rangle}X^d$ for X in $f^{**}_{(e,\tau)}$ and $\phi^{**}_{(e,\tau)}$ respectively, i.e., let

$$f^{*(d)}_{(e,\tau)} = f^{*(d)}_{(e,\tau)}(Y) = Y^{\langle m-1\rangle} + (-1)^{\langle m-1\rangle}X^d + \tau Y + \sum_{i=2}^{e} T_i Y^{\langle i-1\rangle}$$

and

$$\phi^{*(d)}_{(e,\tau)} = \phi^{*(d)}_{(e,\tau)}(Y) = Y^{q^m-1} + (-1)^{\langle m-1\rangle}X^d + \tau Y^{q-1} + \sum_{i=2}^{e} T_i Y^{q^i-1}.$$

Finally, for $1 \le e \le m-1$ and every $0 \ne \tau \in k_p(T_1)$ let $f^{*}_{(e,\tau)}$ and $\phi^{*}_{(e,\tau)}$ be obtained by substituting $((-1)^{\langle m-1\rangle}\tau^{q-1}, X)$ for (X, T_1) in f^{**}_e and ϕ^{**}_e respectively, i.e., let

$$f^{*}_{(e,\tau)} = f^{*}_{(e,\tau)}(Y) = Y^{\langle m-1\rangle} + (-1)^{\langle m-1\rangle}\tau^{q-1} + XY + \sum_{i=2}^{e} T_i Y^{\langle i-1\rangle}$$

and

$$\phi^{*}_{(e,\tau)} = \phi^{*}_{(e,\tau)}(Y) = Y^{q^m-1} + (-1)^{\langle m-1\rangle}\tau^{q-1} + XY^{q-1} + \sum_{i=2}^{e} T_i Y^{q^i-1}.$$

The following Results (2.2.1) to (2.2.3) were respectively proved in Propositions (5.1)[10] to (5.3)[11] of [A05] by first establishing the double transitivity of the Galois groups of the respective projective q-polynomials, and then making some ramification considerations and using above Lemmas (2.1.1) to (2.1.4) but not (2.1.5).

Result (2.2.1). *If $m > 1$ and $\mathrm{GF}(q) \subset k_p$, then in a natural manner we have $\mathrm{SL}(m,q) < \mathrm{Gal}(\phi^{*}_{(1,1)}, K_0) < \mathrm{GL}(m,q)$ and $\mathrm{PSL}(m,q) < \mathrm{Gal}(f^{*}_{(1,1)}, K_0) < \mathrm{PGL}(m,q)$.*

Result (2.2.2). *If $m > 1$ and $\mathrm{GF}(q) \subset k_p$, then in a natural manner we have $\mathrm{Gal}(\phi^{**}_{(1,1)}, K_0) = \mathrm{GL}(m,q)$ and $\mathrm{Gal}(f^{**}_{(1,1)}, K_0) = \mathrm{PGL}(m,q)$.*

Result (2.2.3). *If $m > 1$ and $\mathrm{GF}(q) \subset k_p$, then in a natural manner we have $\mathrm{Gal}(\phi^{**}_{1}, \widetilde{K}_1) = \mathrm{GL}(m,q)$ and $\mathrm{Gal}(f^{**}_{1}, \widetilde{K}_1) = \mathrm{PGL}(m,q)$.*

From Results (2.2.1) to (2.2.3), by using Lemmas (2.1.1) to (2.1.4) but not (2.1.5), in Section 3 we shall deduce the following Theorems (2.3.1) to (2.3.5),[12] where $\widetilde{K}_e$ and $K_{(e,\tau)}$ are as in (ii) and (iii) above.

Theorem (2.3.1). *If $\mathrm{GF}(q) \subset k_p$, then, for $1 \le e \le m-1$ and every element $0 \ne \tau \in k_p(T_1)$, in a natural manner we have $\mathrm{Gal}(\phi^{*}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{SL}(m,q)$ and $\mathrm{Gal}(f^{*}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{PSL}(m,q)$.*

[10] In view of above Lemma (2.1.3), the $m = 2$ case of Result (2.2.1) follows from part (5.1.3) of Proposition (5.1) of [A05]. The $m > 2$ case of Result (2.2.1) follows from Proposition (3.2) of [A04] which was the original source for Proposition (5.1) of [A05]. By using above Lemma (2.1.5), in Proposition (3.2) of [A04] and Proposition (5.1) of [A05] it was shown that if k_p is algebraically closed, then $\mathrm{Gal}(\phi^{*}_{(1,1)}, K_0) = \mathrm{SL}(m,q)$ and $\mathrm{Gal}(f^{*}_{(1,1)}, K_0) = \mathrm{PSL}(m,q)$.

[11] As a misprint correction, in the last line of the proof of Proposition (5.3) of [A05], the reference to Lemma (4.6) should be changed to a reference to Lemma (3.6).

[12] In connection with (2.3.4) and (2.3.5) we note that, in the situation of Lemma (2.1.1), if K' is any field between K and the splitting field of ϕ over K, then the usual way of regarding $\mathrm{Gal}(\phi, K')$ to be a subgroup of $\mathrm{Gal}(\phi, K)$ is coherent with the natural manner, described in Lemma (2.1.1), of regarding these groups as subgroups of $\mathrm{GL}(m,q)$.

Theorem (2.3.2). *If* $\mathrm{GF}(q) \subset k_p$*, then, for* $1 \leq e \leq m-1$ *and every element* $0 \neq \tau \in k_p(T_1)$*, in a natural manner we have* $\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{GL}(m,q)$ *and* $\mathrm{Gal}(f^{**}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{PGL}(m,q)$*.*

Theorem (2.3.3). *If* $\mathrm{GF}(q) \subset k_p$*, then, for* $1 \leq e \leq m-1$ *and every integer* $\epsilon \geq e$*, in a natural manner we have* $\mathrm{Gal}(\phi^{**}_e, \widetilde{K}_\epsilon) = \mathrm{GL}(m,q)$ *and* $\mathrm{Gal}(f^{**}_e, \widetilde{K}_\epsilon) = \mathrm{PGL}(m,q)$*.*

Theorem (2.3.4). *If* $\mathrm{GF}(q) \subset k_p$*, then, for* $1 \leq e \leq m-1$ *and every element* $0 \neq \tau \in k_p(T_1)$ *and every divisor* d *of* $q-1$*, in a natural manner we have* $\mathrm{SL}(m,q) = \mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}(\Theta_d)) \lhd \mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{GL}^{(d)}(m,q)$ *and* $\mathrm{PSL}(m,q) = \mathrm{Gal}(f^{*(d)}_{(e,\tau)}, K_{(e,\tau)}(\Theta_d)) \lhd \mathrm{Gal}(f^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{PGL}^{(d)}(m,q)$ *for some element* Θ_d *in the splitting field of* $\phi^{*(d)}_{(e,\tau)}$ *over* $K_{(e,\tau)}$ *with* $\Theta_d^{(q-1)/d} = X$*.*

Theorem (2.3.5). *If* $\mathrm{GF}(q) \subset k_p$*, then, for* $1 \leq e \leq m-1$ *and every integer* $\epsilon \geq e$ *and every divisor* d *of* $q-1$*, in a natural manner we have*

$$\mathrm{SL}(m,q) = \mathrm{Gal}(\phi^{*(d)}_e, \widetilde{K}_\epsilon(\widetilde{\Theta}_d)) \lhd \mathrm{Gal}(\phi^{*(d)}_e, \widetilde{K}_\epsilon) = \mathrm{GL}^{(d)}(m,q)$$

and

$$\mathrm{PSL}(m,q) = \mathrm{Gal}(f^{*(d)}_e, \widetilde{K}_\epsilon(\widetilde{\Theta}_d)) \lhd \mathrm{Gal}(f^{*(d)}_e, \widetilde{K}_\epsilon) = \mathrm{PGL}^{(d)}(m,q)$$

for some element $\widetilde{\Theta}_d$ *in the splitting field of* $\phi^{*(d)}_e$ *over* $\widetilde{K}_\epsilon$ *with* $\widetilde{\Theta}_d^{(q-1)/d} = X$*.*

In Section 4 we shall refine these theorems into their semilinear versions without assuming $\mathrm{GF}(q) \subset k_p$.

Remark (2.4.1). Note that the equations $\phi^*_{(e,\tau)} = 0$ and $f^*_{(e,\tau)} = 0$ give unramified coverings of the affine line. Likewise the equations $\phi^{*(d)}_{(e,\tau)} = 0$ and $f^{*(d)}_{(e,\tau)} = 0$ give unramified coverings of the once punctured affine line. Finally the equations $\phi^{*(d)}_e = 0$ and $f^{*(d)}_e = 0$ give unramified coverings of the local affine space minus a normal crossing divisor. See [A06].

Remark (2.4.2). Note that by taking $k_p = k$ we get $(f^*_{(1,1)}, K_{(1,1)}) = (f^*_{(1,1)}, K_0) = (F^*, k(X))$ and $(f^{**}_{(1,1)}, K_{(1,1)}) = (f^{**}_{(1,1)}, K_0) = (F^{**}, k(X))$. Also note that by taking $(k_p, T_1, R_1) = (k, Z, k[[X,Z]])$ we get $(f^{**}_1, \widetilde{K}_1) = (F^{\bullet\bullet}, k((X,Z)))$.

Remark (2.4.3). The sign $(-1)^{\langle m-1\rangle}$ in Theorems (2.3.1) to (2.3.3) is important. For instance, by Lemma (2.1.2) and Theorem (2.3.2) we see that for odd $m > 1$ and $q = 3$ we have

$$\begin{aligned}&\mathrm{Gal}(Y^{q^m-1} + XY^{q-1} - 1, \mathrm{GF}(q)(X))\\ &\quad = \mathrm{SL}(m,q) \lhd \mathrm{GL}(m,q) = \mathrm{Gal}(Y^{q^m-1} + XY^{q-1} + 1, \mathrm{GF}(q)(X))\end{aligned}$$

with $\mathrm{GL}(m,q)/\mathrm{SL}(m,q) = Z_2$, but $\mathrm{Gal}(Y^{\langle m-1\rangle} + XY - 1, \mathrm{GF}(q)(X)) = \mathrm{PSL}(m,q) = \mathrm{PGL}(m,q) \lhd \mathrm{Gal}(Y^{\langle m-1\rangle} + XY + 1, \mathrm{GF}(q)(X))$.

3. Linear groups

To prove Theorems (2.3.1) to (2.3.5), assume that $\mathrm{GF}(q) \subset k_p$ and let there be given $1 \leq e \leq m-1$.

First let us consider $\mathrm{Gal}(\phi^{*}_{(e,\tau)}, K_{(e,\tau)})$ and $\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)})$ with $0 \neq \tau \in k_p(T_1)$. By applying the obvious epimorphism $k_p(\tau)[X, T_2, \ldots, T_e] \to k_p(\tau)[X]$ with kernel $(T_2, \ldots, T_e)k_p(\tau)[X, T_2, \ldots, T_e]$ to the coefficients of $\phi^{*}_{(e,\tau)}(Y) \in K_{(e,\tau)}[Y]$ and $\phi^{**}_{(e,\tau)}(Y) \in K_{(e,\tau)}[Y]$ we get $\phi^{*}_{(1,\tau)}(Y) \in K_{(1,\tau)}[Y]$ and $\phi^{**}_{(1,\tau)}(Y) \in K_{(1,\tau)}[Y]$ respectively, and hence by the Specialization Principle (see footnote 8 of [AL1]) we see that $\mathrm{Gal}(\phi^{*}_{(1,\tau)}, K_{(1,\tau)}) \lessapprox \mathrm{Gal}(\phi^{*}_{(e,\tau)}, K_{(e,\tau)})$ and $\mathrm{Gal}(\phi^{**}_{(1,\tau)}, K_{(1,\tau)}) \lessapprox \mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)})$.[13] We can take elements τ' and τ'' in an overfield of $k_p(X)$ with $\tau'^{\langle m-1\rangle} = \tau$ and $\tau''^{q-q^m} = \tau$ and then upon letting $k'_p = k_p(\tau')$ and $k''_p = k_p(\tau'')$ we have $K_{(1,\tau)} \subset k'_p(X)$ and $K_{(1,\tau)} \subset k''_p(X)$, and therefore by the Basic Extension Principle (cf. page 93 of [A03]) we see that $\mathrm{Gal}(\phi^{*}_{(1,\tau)}, k'_p(X)) \lessapprox \mathrm{Gal}(\phi^{*}_{(1,\tau)}, K_{(1,\tau)})$ and $\mathrm{Gal}(\phi^{**}_{(1,\tau)}, k''_p(X)) \lessapprox \mathrm{Gal}(\phi^{**}_{(1,\tau)}, K_{(1,\tau)})$, and hence we get $\mathrm{Gal}(\phi^{*}_{(1,\tau)}, k'_p(X)) \lessapprox \mathrm{Gal}(\phi^{*}_{(e,\tau)}, K_{(e,\tau)})$ and $\mathrm{Gal}(\phi^{**}_{(1,\tau)}, k''_p(X)) \lessapprox \mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)})$. Now $\phi^{*}_{(1,\tau)}(Y) = \tau'^{q^m-1}\phi'^{*}_{(1,1)}(Y)$ where $\phi'^{*}_{(1,1)}(Y)$ is obtained by substituting $(\tau'^{q-q^m}X, \tau'^{-1}Y)$ for (X, Y) in $\phi^{*}_{(1,1)}(Y)$ and hence $\mathrm{Gal}(\phi^{*}_{(1,\tau)}, k'_p(X)) \approx \mathrm{Gal}(\phi^{*}_{(1,1)}, k'_p(X))$; by (2.2.1) we have $\mathrm{SL}(m, q) < \mathrm{Gal}(\phi^{*}_{(1,1)}, k'_p(X))$; therefore we get $\mathrm{SL}(m, q) \lessapprox \mathrm{Gal}(\phi^{*}_{(e,\tau)}, K_{(e,\tau)})$; by (2.1.1) we know that in a natural manner we have $\mathrm{Gal}(\phi^{*}_{(e,\tau)}, K_{(e,\tau)}) < \mathrm{GL}(m, q)$ and hence (say by quasi-p considerations)[14] we see that in a natural manner we have $\mathrm{SL}(m, q) < \mathrm{Gal}(\phi^{*}_{(e,\tau)}, K_{(e,\tau)}) < \mathrm{GL}(m, q)$. Similarly $\phi^{**}_{(1,\tau)}(Y) = \tau''^{1-q^m}\phi''^{**}_{(1,1)}(Y)$ where $\phi''^{**}_{(1,1)}(Y)$ is obtained by substituting $(\tau''^{q^m-1}X, \tau''Y)$ for (X, Y) in $\phi^{**}_{(1,1)}(Y)$ and hence $\mathrm{Gal}(\phi^{**}_{(1,\tau)}, k''_p(X)) \approx \mathrm{Gal}(\phi^{**}_{(1,1)}, k''_p(X))$; this time by (2.2.2) we have $\mathrm{Gal}(\phi^{**}_{(1,1)}, k''_p(X)) = \mathrm{GL}(m, q)$ and therefore we get $\mathrm{GL}(m, q) \lessapprox \mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)})$; by (2.1.1) we know that in a natural manner we have $\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}) < \mathrm{GL}(m, q)$ and hence (say by order considerations) we see that in a natural manner we have $\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{GL}(m, q)$. This completes the proof of (2.3.2). Given any divisor d of $q-1$, by (2.1.2) there exists an element Λ_d in the splitting field of $\phi^{**}_{(e,\tau)}$ over $K_{(e,\tau)}$ such that $\Lambda_d^d = (-1)^{\langle m-1\rangle}X$, and hence by the Substitution Principle on page 98 of [A03] we may regard $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}(\Lambda_d)) \triangleleft \mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)})$ with $\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)})/\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}(\Lambda_d)) = Z_d$, and therefore[15] it follows that in a natural manner we have $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{GL}^{(d)}(m, q)$. Again by (2.1.2) there exists an element Θ_d in the splitting field of $\phi^{*(d)}_{(e,\tau)}$ over $K_{(e,\tau)}$ with $\Theta_d^{(q-1)/d} = X$, and by the usual Galois correspondence $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}(\Theta_d)) \triangleleft \mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)})$ with $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)})/\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}(\Theta_d)) = Z_{(q-1)/d}$ and hence (see the previous footnote) in a natural manner we have $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}(\Theta_d))$

[13] We are using $\lessapprox$ as an abbreviation for "is isomorphic to a subgroup of."

[14] The quasi-p part of a finite group G is denoted by $p(G)$ and is defined to be the subgroup of G generated by all of its p-Sylow subgroups. It can also be characterized as the subgroup of G generated by all of its elements of p-power order. Yet another characterization of it would be as the smallest normal subgroup of G which is the kernel of an epimorphism of G onto a group whose order is prime to p. It follows that $p(G) \lessapprox H < G \Rightarrow p(G) < H$. It only remains to note that $p(\mathrm{GL}(m, q)) = \mathrm{SL}(m, q)$ which is the crucial fact used in the proof of above Lemma (2.1.3) which is a reformulation of Lemma (2.3) of [A04].

[15] Say in view of the last footnote about the quasi-p part of $\mathrm{GL}(m, q)$ together with the fact that $\mathrm{SL}(m, q) \triangleleft \mathrm{GL}(m, q)$ with $\mathrm{GL}(m, q)/\mathrm{SL}(m, q) = Z_{q-1}$. Also note that for any $G < \mathrm{GL}(m, q)$ we have: $\mathrm{SL}(m, q) < G \Leftrightarrow \mathrm{SL}(m, q) < p(G) \Leftrightarrow \mathrm{SL}(m, q) = p(G)$.

$= \mathrm{SL}(m,q)$. This completes the proof of (2.3.4). In particular, in a natural manner we have $\mathrm{Gal}(\phi_{(e,T_1)}^{*(q-1)}, K_{(e,T_1)}) = \mathrm{GL}^{(q-1)}(m,q) = \mathrm{SL}(m,q)$. If $\tau \notin k_p$, then $(X, T_1, T_2, \ldots, T_e) \mapsto (\tau, X, T_2, \ldots, T_e)$ gives a k_p-isomorphism of $K_{(e,T_1)}$ onto $K_{(e,\tau)}$ which sends $\phi_{(e,T_1)}^{*(q-1)}$ to $\phi_{(e,\tau)}^{*}$; hence in a natural manner we have $\mathrm{Gal}(\phi_{(e,\tau)}^{*}, K_{(e,\tau)})$ $= \mathrm{SL}(m,q)$. If $\tau \in k_p$, then $(X, T_1, T_2, \ldots, T_e) \mapsto (\tau, X, T_2, \ldots, T_e)$ gives a k_p-epimorphism of $k_p[X, T_1, T_2, \ldots, T_e]$ onto $k_p[X, T_2, \ldots, T_e]$ which sends $\phi_{(e,T_1)}^{*(q-1)}$ to $\phi_{(e,\tau)}^{*}$ and hence by the Specialization Principle (see footnote 8 of [AL1]) we see that $\mathrm{Gal}(\phi_{(e,\tau)}^{*}, K_{(e,\tau)}) \lessapprox \mathrm{SL}(m,q)$; since we have already seen that in a natural manner we have $\mathrm{SL}(m,q) < \mathrm{Gal}(\phi_{(e,\tau)}^{*}, K_{(e,\tau)}) < \mathrm{GL}(m,q)$, by order considerations we conclude that in a natural manner we have $\mathrm{Gal}(\phi_{(e,\tau)}^{*}, K_{(e,\tau)}) = \mathrm{SL}(m,q)$. This completes the proof of (2.3.1).

Now let us consider $\mathrm{Gal}(\phi_e^{**}, \widetilde{K}_\epsilon)$ with $\epsilon \geq e$. Let $\theta\colon R_\epsilon \to \overline{R}_1 = R_\epsilon/(T_2, \ldots, T_\epsilon)R_\epsilon$ be the canonical epimorphism. Then $\overline{R}_1$ is a 2-dimensional regular local domain whose maximal ideal is generated by $\theta(X)$ and $\theta(T_1)$. Let $\overline{K}_1$ be the quotient field of $\overline{R}_1$, and let $\overline{\phi}_1^{**}(Y) \in \overline{K}_1[Y]$ be obtained by applying θ to the coefficients of $\phi_e^{**}(Y)$. Then by the Specialization Principle (see footnote 8 of [AL1]) we see that $\mathrm{Gal}(\overline{\phi}_1^{**}, \overline{K}_1) \lessapprox \mathrm{Gal}(\phi_e^{**}, \widetilde{K}_\epsilon)$, and by (2.2.3) we see that $\mathrm{Gal}(\overline{\phi}_1^{**}, \overline{K}_1) \approx \mathrm{GL}(m,q)$; by (2.1.1) in a natural manner we have $\mathrm{Gal}(\phi_e^{**}, \widetilde{K}_\epsilon) < \mathrm{GL}(m,q)$, and hence (say by order considerations) we conclude that in a natural manner we have $\mathrm{Gal}(\phi_e^{**}, \widetilde{K}_\epsilon) = \mathrm{GL}(m,q)$. This completes the proof of (2.3.3). Given any divisor d of $q-1$, by (2.1.2) there exists an element $\widetilde{\Lambda}_d$ in the splitting field of ϕ_e^{**} over $\widetilde{\Lambda}_d^d = (-1)^{\langle m-1\rangle}X$ and hence, by the Substitution Principle on page 98 of [A03], in the *affine case*, i.e., when $\widetilde{R}_\epsilon$ is the localization of $k_p[X, T_1, \ldots, T_\epsilon]$ at the maximal ideal generated by $(X, T_1, \ldots, T_\epsilon)$, we may regard $\mathrm{Gal}(\phi_e^{*(d)}, K_\epsilon) = \mathrm{Gal}(\phi_e^{**}, K_\epsilon(\widetilde{\Lambda}_d)) \triangleleft \mathrm{Gal}(\phi_e^{**}, K_\epsilon)$ with $\mathrm{Gal}(\phi_e^{**}, K_\epsilon)/\mathrm{Gal}(\phi_e^{**}, K_\epsilon(\widetilde{\Lambda}_d)) = Z_d$, and therefore (see the previous footnote) in a natural manner we have $\mathrm{Gal}(\phi_e^{*(d)}, K_\epsilon) = \mathrm{GL}^{(d)}(m,q)$. Referring to the proof of the Substitution Principle on page 98 of [A03], we see that the only special property of the affine case which we used in the last sentence was the existence of a k_p-isomorphism $k_p[X, T_1, \ldots, T_\epsilon] \to k_p[(-1)^{\langle m-1\rangle}X, T_1, \ldots, T_\epsilon] \subset k_p[X, T_1, \ldots, T_\epsilon]$ sending $(X, T_1, \ldots, T_\epsilon)$ to $((-1)^{\langle m-1\rangle}X, T_1, \ldots, T_\epsilon)$. Now upon letting $\widehat{R}_\epsilon$ to be the completion of R_ϵ and $\widehat{K}_\epsilon$ to be the quotient field of $\widehat{R}_\epsilon$, we see that $\widehat{R}_\epsilon = \widehat{k}_p[[X, T_1, \ldots, T_\epsilon]]$ where $\widehat{k}_p$ is an overfield of k_p, and clearly there exists a $\widehat{k}_p$-isomorphism $\widehat{k}_p[[X, T_1, \ldots, T_\epsilon]] \to \widehat{k}_p[[(-1)^{\langle m-1\rangle}X, T_1, \ldots, T_\epsilon]] \subset \widehat{k}_p[[X, T_1, \ldots, T_\epsilon]]$ sending $(X, T_1, \ldots, T_\epsilon)$ to $((-1)^{\langle m-1\rangle}X, T_1, \ldots, T_\epsilon)$. Therefore in a natural manner we have $\mathrm{Gal}(\phi_e^{*(d)}, \widehat{K}_\epsilon) = \mathrm{GL}^{(d)}(m,q)$. Since $\phi_e^{*(d)}(Y) \in K_\epsilon[Y]$ and $K_\epsilon \subset \widetilde{K}_\epsilon \subset \widehat{K}_\epsilon$, by the Basic Extension Principle (cf. page 93 of [A03]) we see that $\mathrm{Gal}(\phi_e^{*(d)}, \widehat{K}_\epsilon) \lessapprox \mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon) \lessapprox \mathrm{Gal}(\phi_e^{*(d)}, K_\epsilon)$. By (2.1.1) we also know that in a natural manner we have $\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon) < \mathrm{GL}(m,q)$. Therefore (see the previous footnote) in a natural manner we have $\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon) = \mathrm{GL}^{(d)}(m,q)$. Again by (2.1.2) there exists an element $\widetilde{\Theta}_d$ in the splitting field of $\phi_e^{*(d)}$ over $\widetilde{K}_\epsilon$ with $\widetilde{\Theta}_d^{(q-1)/d} = X$, and by the usual Galois correspondence $\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon(\widetilde{\Theta}_d)) \triangleleft \mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon)$ with $\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon)/\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon(\widetilde{\Theta}_d)) = Z_{(q-1)/d}$ and hence (see the previous footnote) in a natural manner we have $\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon(\widetilde{\Theta}_d)) = \mathrm{SL}(m,q)$. This completes the proof of (2.3.5).

4. Semilinear groups

In this section we shall generalize the results of the preceding sections to the case when the ground field does not necessarily contain the field $\mathrm{GF}(q)$ of q elements.

To recapitulate and refine the Linearity Lemma (2.1.1), let V be the set of all roots of $\widehat{\phi}$ in an algebraic closure Ω of K, and note that then V is an m-dimensional $\mathrm{GF}(q)$-vector-subspace of Ω.[16] Let $\overline{V}$ be the set of all roots of f in Ω. Then $V \setminus \{0\}$ is the set of all roots of ϕ in Ω, and $y \mapsto y^{q-1}$ gives a surjective map $V \setminus \{0\} \to \overline{V}$ whose fibers are punctured 1-spaces, i.e., 1-spaces minus the zero vector. So we may identify $\overline{V}$ with the projective space associated with V. In particular, fixing $0 \neq y \in V$ and letting y' vary over all elements of V with $y'^{q-1} = y^{q-1}$ we see that $y'/y \in K(V)$ varies over all nonzero elements of $\mathrm{GF}(q)$, and hence $\mathrm{GF}(q) \subset K(V) =$ the splitting field of $\widehat{\phi}$ over $K =$ the splitting field of ϕ over K. It follows that any $g \in \mathrm{Gal}(K(V), K)$ induces an automorphism g' of $\mathrm{GF}(q)$, and for all $z \in V$ and $\zeta \in \mathrm{GF}(q)$ we clearly have $g(\zeta z) = g'(\zeta)g(z)$; since g is clearly additive on V, we see that g induces on V a semilinear transformation, i.e., an element of $\Gamma\mathrm{L}(V) = \Gamma\mathrm{L}(m, q)$, and moreover this element belongs to $\mathrm{GL}(V) = \mathrm{GL}(m, q) \Leftrightarrow g'$ is identity. Thus in a natural manner $\mathrm{Gal}(\widehat{\phi}, K) < \Gamma\mathrm{L}(m, q)$. Clearly g' is identity for all $g \in \mathrm{Gal}(K(V), K) \Leftrightarrow \mathrm{GF}(q) \subset K$, and hence in the above identification $\mathrm{Gal}(\widehat{\phi}, K) < \mathrm{GL}(m, q) \Leftrightarrow \mathrm{GF}(q) \subset K$. Note that the Galois group $\mathrm{Gal}(\phi, K)$ essentially equals the Galois group $\mathrm{Gal}(\widehat{\phi}, K)$ except that the former acts on nonzero vectors while the latter acts on the entire vector space. Thus, in view of the relevant considerations of Lemmas (2.4) and (2.5) of [A04], we get the following:

Semilinearity Lemma (4.1.1). $\mathrm{GF}(q)$ *is contained in the splitting field of* $\widehat{\phi}$ *over* K *(which is the same thing as the splitting field of* ϕ *over* K*) and in a natural manner we may identify* $\mathrm{Gal}(\widehat{\phi}, K)$ *with a subgroup of* $\Gamma\mathrm{L}(m, q)$*; under this identification we have* $\mathrm{Gal}(\widehat{\phi}, K) < \mathrm{GL}(m, q) \Leftrightarrow \mathrm{GF}(q) \subset K$*. Likewise, we may identify* $\mathrm{Gal}(f, K)$ *with a subgroup of* $\mathrm{P}\Gamma\mathrm{L}(m, q)$ *and then* $\mathrm{Gal}(f, K)$ *becomes the image of* $\mathrm{Gal}(\widehat{\phi}, K)$ *under the canonical epimorphism of* $\Gamma\mathrm{L}(m, q)$ *onto* $\mathrm{P}\Gamma\mathrm{L}(m, q)$*. The Galois group* $\mathrm{Gal}(\phi, K)$ *essentially equals the Galois group* $\mathrm{Gal}(\widehat{\phi}, K)$ *except that the former acts on nonzero vectors while the latter acts on the entire vector space of roots of* $\widehat{\phi}$*.*

Let u be the unique integer with $q = p^u$, and let δ be any divisor of u. Let the groups $\Gamma\mathrm{L}_\delta(m, q)$ and $\mathrm{P}\Gamma\mathrm{L}_\delta(m, q)$, and the sets of groups $\Gamma\mathrm{SL}_\delta(m, q)$, $\mathrm{P}\Gamma\mathrm{SL}_\delta(m, q)$, $\Gamma\mathrm{L}_\delta^{(d)}(m, q)$, and $\mathrm{P}\Gamma\mathrm{L}_\delta^{(d)}(m, q)$, be defined as in Section 1. By (4.1.1) we know that $K(V)$ contains the splitting field $K(\mathrm{GF}(q))$ of $Y^q - Y$ over K, and hence $K(V)$ also contains the splitting field $K(\mathrm{GF}(p^{u/\delta}))$ of $Y^{p^{u/\delta}} - Y$ over K. According to the notation introduced in Section 1, $\delta(K)$ is defined to be the unique divisor of u such that

$$\mathrm{Gal}(Y^q - Y, K) = Z_{\delta(K)} \quad \text{i.e. equivalently} \quad [K(\mathrm{GF}(q)) : K] = \delta(K) \tag{4.1.2}$$

and we note that then[17]

$$K \cap \mathrm{GF}(q) = \mathrm{GF}(p^{u/\delta(K)}). \tag{4.1.3}$$

[16] This is so without assuming $\mathrm{GF}(q) \subset K$, although in [A04] we made that assumption.

[17] To see this, let $H(Y)$ be the minimal monic polynomial of a primitive element η of $\mathrm{GF}(q)$ over $K \cap \mathrm{GF}(q)$, and let $H'(Y)$ be the minimal monic polynomial of η over K. Then $H'(Y)$ divides $H(Y)$ and hence $H'(Y) \in \mathrm{GF}(q)[Y]$. But also $H'(Y) \in K[Y]$ and hence $H'(Y) \in (K \cap \mathrm{GF}(q))[Y]$. Therefore $H'(Y) = H(Y)$ and hence $K \cap \mathrm{GF}(q) = \mathrm{GF}(p^{u/\delta(K)})$.

For a moment let V be any m-dimensional vector space over $\mathrm{GF}(q)$. As above, for every $g \in \Gamma\mathrm{L}(V) = \Gamma\mathrm{L}(m,q)$ let g' be the unique element in $\mathrm{Aut}(\mathrm{GF}(q)) = Z_u$ such that for all $z \in V$ and $\zeta \in \mathrm{GF}(q)$ we have $g(\zeta z) = g'(\zeta)g(z)$. Then $g \mapsto g'$ gives an epimorphism $\Gamma\mathrm{L}(m,q) \to \mathrm{Aut}(\mathrm{GF}(q))$ whose kernel is $\mathrm{GL}(m,q)$. The group $\Gamma\mathrm{L}_\delta(m,q)$ can be characterized by saying that $\Gamma\mathrm{L}_\delta(m,q) = \{g \in \Gamma\mathrm{L}(m,q) : g' \in \mathrm{Gal}(\mathrm{GF}(q), \mathrm{GF}(p^{u/\delta}))\}$. Again letting V denote the vector space of roots of $\widehat{\phi}$, for any $g \in \mathrm{Gal}(\phi, K)$ we have $g' = g|_{\mathrm{GF}(q)}$ where $|$ denotes restriction,[18] and hence $\mathrm{Gal}(\phi,K) \cap \Gamma\mathrm{L}_\delta(m,q) = \{g \in \mathrm{Gal}(\phi,K) : g' \in \mathrm{Gal}(\mathrm{GF}(q), \mathrm{GF}(p^{u/\delta}))\} = \mathrm{Gal}(\phi, K(\mathrm{GF}(p^{u/\delta})))$;[19] by the usual Galois correspondence $\mathrm{Gal}(\phi, K(\mathrm{GF}(p^{u/\delta}))) \lhd \mathrm{Gal}(\phi,K)$ with $\mathrm{Gal}(\phi,K)/\mathrm{Gal}(\phi, K(\mathrm{GF}(p^{u/\delta}))) = \mathrm{Gal}(K(\mathrm{GF}(p^{u/\delta})), K)$, and therefore

$$\text{(4.1.4)} \qquad \begin{cases} \mathrm{Gal}(\phi,K) \cap \Gamma\mathrm{L}_\delta(m,q) = \mathrm{Gal}(\phi, K(\mathrm{GF}(p^{u/\delta}))) \lhd \mathrm{Gal}(\phi,K) \\ \text{with } \mathrm{Gal}(\phi,K)/\mathrm{Gal}(\phi, K(\mathrm{GF}(p^{u/\delta}))) = \mathrm{Gal}(K(\mathrm{GF}(p^{u/\delta})), K) \end{cases}$$

and this gives rise to the implication

$$\text{(4.1.5)} \qquad \mathrm{Gal}(\phi,K) < \Gamma\mathrm{L}_\delta(m,q) \Leftrightarrow \mathrm{GF}(p^{u/\delta}) \subset K,$$

which generalizes the implication $\Leftrightarrow$ of (4.1.1). In view of (4.1.2) and (4.1.3), by taking $\delta = 1$ in (4.1.4) and $\delta = \delta(K)$ in (4.1.5) we get:

Proposition (4.2.1). *We have*

$$\mathrm{Gal}(\phi,K) \cap \mathrm{GL}(m,q) = \mathrm{Gal}(\phi, K(\mathrm{GF}(q))) \lhd \mathrm{Gal}(\phi,K) < \Gamma\mathrm{L}_{\delta(K)}(m,q)$$

with $\mathrm{Gal}(\phi,K)/\mathrm{Gal}(\phi, K(\mathrm{GF}(q))) = Z_{\delta(K)}$.

By (4.2.1) we immediately get:

Proposition (4.2.2). *If* $\mathrm{Gal}(\phi, K(\mathrm{GF}(q))) = \mathrm{GL}^{(d)}(m,q)$ *where* d *is a divisor of* $q-1$*, then we have* $\mathrm{Gal}(\phi,K) \cap \mathrm{GL}(m,q) = \mathrm{GL}^{(d)}(m,q) \lhd \mathrm{Gal}(\phi,K) < \Gamma\mathrm{L}_{\delta(K)}(m,q)$ *with* $\mathrm{Gal}(\phi,K)/\mathrm{GL}^{(d)}(m,q) = Z_{\delta(K)}$.

Since $\mathrm{GL}^{(q-1)}(m,q) = \mathrm{SL}(m,q)$, in view of (4.1.1), by taking $d = q-1$ in (4.2.2) we get:

Proposition (4.2.3). *If* $\mathrm{Gal}(\phi, K(\mathrm{GF}(q))) = \mathrm{SL}(m,q)$*, then we have* $\mathrm{Gal}(\phi,K) \in \Gamma\mathrm{SL}_{\delta(K)}(m,q)$ *and* $\mathrm{Gal}(f,K) \in \mathrm{P}\Gamma\mathrm{SL}_{\delta(K)}(m,q)$.

Since $\mathrm{GL}^{(1)}(m,q) = \mathrm{GL}(m,q)$ and $[\Gamma\mathrm{L}_{\delta(K)}(m,q) : \mathrm{GL}(m,q)] = \delta(K)$, in view of (4.1.1), by taking $d = 1$ in (4.2.2) we get:

Proposition (4.2.4). *If* $\mathrm{Gal}(\phi, K(\mathrm{GF}(q))) = \mathrm{GL}(m,q)$*, then we have* $\mathrm{Gal}(\phi,K) = \Gamma\mathrm{L}_{\delta(K)}(m,q)$ *and* $\mathrm{Gal}(f,K) = \mathrm{P}\Gamma\mathrm{L}_{\delta(K)}(m,q)$.

Because of the usual Galois correspondence (see the previous footnote), by (4.2.3) and (4.2.4) we get:

[18] Strictly speaking $g' = \widetilde{g}|_{\mathrm{GF}(q)}$ where $\widetilde{g} \in \mathrm{Gal}(K(V), K)$ is such that $g = \widetilde{g}|_{V \setminus \{0\}}$.

[19] For any field K' with $K \subset K' \subset K(V)$, the usual way of regarding $\mathrm{Gal}(\phi, K')$ to be a subgroup of $\mathrm{Gal}(\phi,K)$ is coherent with the natural manner, described in (4.1.1), of regarding these groups as subgroups of $\Gamma\mathrm{L}(V)$.

Proposition (4.2.5). *If* $\mathrm{Gal}(\phi, K(\mathrm{GF}(q))) = \mathrm{GL}^{(d)}(m,q)$ *where* d *is a divisor of* $q-1$*, and for some field* K' *between* K *and the splitting field of* ϕ *over* K *we have* $\delta(K') = \delta(K)$ *and* $\mathrm{Gal}(\phi, K'(\mathrm{GF}(q))) = \mathrm{SL}(m,q)$*, then* $\mathrm{Gal}(\phi, K) \in \Gamma\mathrm{L}^{(d)}_{\delta(K)}(m,q)$ *and* $\mathrm{Gal}(f, K) \in \mathrm{P}\Gamma\mathrm{L}^{(d)}_{\delta(K)}(m,q)$*.*

In view of the above propositions, from Theorems (2.3.1) to (2.3.5) we shall now deduce the following Theorems (4.3.1) to (4.3.5), where $\widetilde{K}_e$ and $K_{(e,\tau)}$ are as in (ii) and (iii) above.

Theorem (4.3.1). *For* $1 \leq e \leq m-1$ *and every element* $0 \neq \tau \in k_p(T_1)$*, upon letting* $\delta = \delta(k_p)$*, we have* $\mathrm{Gal}(\phi^*_{(e,\tau)}, K_{(e,\tau)}) \in \Gamma\mathrm{SL}_\delta(m,q)$ *and* $\mathrm{Gal}(f^*_{(e,\tau)}, K_{(e,\tau)}) \in \mathrm{P}\Gamma\mathrm{SL}_\delta(m,q)$*.*

Theorem (4.3.2). *For* $1 \leq e \leq m-1$ *and every element* $0 \neq \tau \in k_p(T_1)$*, upon letting* $\delta = \delta(k_p)$*, we have* $\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}) = \Gamma\mathrm{L}_\delta(m,q)$ *and* $\mathrm{Gal}(f^{**}_{(e,\tau)}, K_{(e,\tau)}) = \mathrm{P}\Gamma\mathrm{L}_\delta(m,q)$*.*

Theorem (4.3.3). *For* $1 \leq e \leq m-1$ *and every integer* $\epsilon \geq e$*, upon letting* $\delta = \delta(\widetilde{K}_\epsilon)$*, we have* $\mathrm{Gal}(\phi^{**}_e, \widetilde{K}_\epsilon) = \Gamma\mathrm{L}_\delta(m,q)$ *and* $\mathrm{Gal}(f^{**}_e, \widetilde{K}_\epsilon) = \mathrm{P}\Gamma\mathrm{L}_\delta(m,q)$*. [Note that if either* $R_\epsilon = k_p[[X, T_1, \ldots, T_\epsilon]]$ *or* $R_\epsilon =$ *the localization of* $k_p[X, T_1, \ldots, T_\epsilon]$ *at the maximal ideal generated by* $(X, T_1, \ldots, T_\epsilon)$*, then* $\delta(\widetilde{K}_\epsilon) = \delta(k_p)$*.]*

Theorem (4.3.4). *For* $1 \leq e \leq m-1$ *and every element* $0 \neq \tau \in k_p(T_1)$ *and every divisor* d *of* $q-1$*, upon letting* $\delta = \delta(k_p)$*, we have* $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) \in \Gamma\mathrm{L}^{(d)}_\delta(m,q)$ *and* $\mathrm{Gal}(f^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) \in \mathrm{P}\Gamma\mathrm{L}^{(d)}_\delta(m,q)$*.*

Theorem (4.3.5). *For* $1 \leq e \leq m-1$ *and every integer* $\epsilon \geq e$ *and every divisor* d *of* $q-1$*, upon letting* $\delta = \delta(\widetilde{K}_\epsilon)$*, we have* $\mathrm{Gal}(\phi^{*(d)}_e, \widetilde{K}_\epsilon) \in \Gamma\mathrm{L}^{(d)}_\delta(m,q)$ *and* $\mathrm{Gal}(f^{*(d)}_e, \widetilde{K}_\epsilon) \in \mathrm{P}\Gamma\mathrm{L}^{(d)}_\delta(m,q)$*. [Note that if either* $R_\epsilon = k_p[[X, T_1, \ldots, T_\epsilon]]$ *or* $R_\epsilon =$ *the localization of* $k_p[X, T_1, \ldots, T_\epsilon]$ *at the maximal ideal generated by* $(X, T_1, \ldots, T_\epsilon)$*, then* $\delta(\widetilde{K}_\epsilon) = \delta(k_p)$*.]*

To prove (4.3.1), (4.3.2) and (4.3.4), let $1 \leq e \leq m-1$ and $0 \neq \tau \in k(T_1)$ be given, and note that then clearly $K_{(e,\tau)}(\mathrm{GF}(q)) = k_p(\mathrm{GF}(q))(X, \tau, T_2, \ldots, T_e)$ and $\delta(K_{(e,\tau)}) = \delta(k_p)$. By (2.3.1) we know that $\mathrm{Gal}(\phi^*_{(e,\tau)}, K_{(e,\tau)}(\mathrm{GF}(q))) = \mathrm{SL}(m,q)$, and hence by taking $(\phi^*_{(e,\tau)}, K_{(e,\tau)})$ for (ϕ, K) in (4.2.3) we get (4.3.1). Similarly by (2.3.2) we know that $\mathrm{Gal}(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}(\mathrm{GF}(q))) = \mathrm{GL}(m,q)$, and hence by taking $(\phi^{**}_{(e,\tau)}, K_{(e,\tau)})$ for (ϕ, K) in (4.2.4) we get (4.3.2). Given any divisor d of $q-1$, by (2.3.4) we know that $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}(\mathrm{GF}(q))) = \mathrm{GL}^{(d)}(m,q)$ and $\mathrm{Gal}(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}(\mathrm{GF}(q))(\Theta_d)) = \mathrm{SL}(m,q)$ for some element Θ_d in the splitting field of $\phi^{*(d)}_{(e,\tau)}$ over $K_{(e,\tau)}(\mathrm{GF}(q))$ with $\Theta_d^{(q-1)/d} = X$, and clearly $\delta(K_{(e,\tau)}) = \delta(K_{(e,\tau)}(\Theta_d))$, and hence by taking $(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}, K_{(e,\tau)}(\Theta_d))$ for (ϕ, K, K') in (4.2.5) we get (4.3.4).

To prove (4.3.3) and (4.3.5), let $1 \leq r \leq m-1$ and $\epsilon \geq e$ be given, and note that then, upon letting $\widetilde{K}^\dagger_\epsilon = \widetilde{K}_\epsilon(\mathrm{GF}(q))$ and $R^\dagger_\epsilon =$ the localization of the integral closure of R_ϵ in $\widetilde{K}^\dagger_\epsilon$ at a maximal ideal in it, we see that $R^\dagger_\epsilon$ is an $(\epsilon+1)$-dimensional regular local domain whose maximal ideal is generated by $(X, T_1, \ldots, T_\epsilon)$ and whose quotient field is $\widetilde{K}^\dagger_\epsilon$. Therefore by (2.3.3) we see that $\mathrm{Gal}(\phi^{**}_e, \widetilde{K}_\epsilon(\mathrm{GF}(q))) = \mathrm{GL}(m,q)$,

and hence by taking $(\phi_e^{**}, \widetilde{K}_\epsilon)$ for (ϕ, K) in (4.2.4) we get (4.3.3). Likewise, given any divisor d of $q-1$, by (2.3.5) we see that $\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon(\mathrm{GF}(q))) = \mathrm{GL}^{(d)}(m,q)$ and $\mathrm{Gal}(\phi_e^{*(d)}, \widetilde{K}_\epsilon(\mathrm{GF}(q))(\Theta_d)) = \mathrm{SL}(m,q)$ for some element $\widetilde{\Theta}_d$ in the splitting field of $\phi_e^{*(d)}$ over $\widetilde{K}_\epsilon(\mathrm{GF}(q))$ with $\widetilde{\Theta}_d^{(q-1)/d} = X$, and clearly $\delta(\widetilde{K}_\epsilon) = \delta(\widetilde{K}_\epsilon(\widetilde{\Theta}_d))$, and hence by taking $(\phi_e^{*(d)}, \widetilde{K}_\epsilon, \widetilde{K}_\epsilon(\widetilde{\Theta}_d))$ for (ϕ, K, K') in (4.2.5) we get (4.3.5).

Remark (4.4.1). Recall that $q = p^u > 1$ is any power of prime p, and $m > 0$ is any integer. For every divisor d of $q-1$, we are letting $\mathrm{GL}^{(d)}(m,q)$ be the unique subgroup of $\mathrm{GL}(m,q)$ containing $\mathrm{SL}(m,q)$ such that $\mathrm{GL}(m,q)/\mathrm{GL}^{(d)}(m,q) = Z_d$, and we are letting $\mathrm{PGL}^{(d)}(m,q)$ be the image of $\mathrm{GL}^{(d)}(m,q)$ under the canonical epimorphism of $\mathrm{GL}(m,q)$ onto $\mathrm{PGL}(m,q)$. Likewise, for every divisor δ of u, we are letting $\Gamma\mathrm{L}_\delta(m,q)$ be the unique subgroup of $\Gamma\mathrm{L}(m,q)$ containing $\mathrm{GL}(m,q)$ such that $\Gamma\mathrm{L}_\delta(m,q)/\mathrm{GL}(m,q) = Z_\delta$, and we are letting $\mathrm{P}\Gamma\mathrm{L}_\delta(m,q)$ be the image of $\Gamma\mathrm{L}_\delta(m,q)$ under the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{P}\Gamma\mathrm{L}(m,q)$. We are also letting $\Gamma\mathrm{SL}_\delta(m,q)$ be the set of all subgroups I of $\Gamma\mathrm{L}_\delta(m,q)$ such that $I \cap \mathrm{GL}(m,q) = \mathrm{SL}(m,q) \lhd I$ with $I/\mathrm{SL}(m,q) = Z_\delta$, and we are letting $\mathrm{P}\Gamma\mathrm{SL}_\delta(m,q)$ be the set of images of the various members of $\Gamma\mathrm{SL}_\delta(m,q)$ under the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{P}\Gamma\mathrm{L}(m,q)$. Finally we are letting $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ be the set of all subgroups J of $\Gamma\mathrm{L}_\delta(m,q)$ such that $J \cap \mathrm{GL}(m,q) = \mathrm{GL}^{(d)}(m,q) \lhd J$ with $J/\mathrm{GL}^{(d)}(m,q) = Z_\delta$ and $I < J$ for some I in $\Gamma\mathrm{SL}_\delta(m,q)$, and we are letting $\mathrm{P}\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ be the set of images of the various members of $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ under the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{P}\Gamma\mathrm{L}(m,q)$. Note that clearly $\Gamma\mathrm{L}_\delta^{(q-1)}(m,q) = \Gamma\mathrm{SL}_\delta(m,q)$ and $\Gamma\mathrm{L}_\delta^{(1)}(m,q) = \{\Gamma\mathrm{L}_\delta(m,q)\}$. Also note that the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{Aut}(\mathrm{GF}(q)) = Z_u$ with kernel $\mathrm{GL}(m,q)$ splits; to see this, as on page 79 of [A03], we may identify $\Gamma\mathrm{L}(m,q)$ with pairs (g,α) with $g \in \mathrm{Aut}(\mathrm{GF}(q))$ and $\alpha \in \mathrm{GL}(m,q)$, and now upon letting $\Gamma(m,q) = \{(g,1) : g \in \mathrm{Aut}(\mathrm{GF}(q))\}$ we see that $\Gamma(m,q)$ is a subgroup of $\Gamma\mathrm{L}(m,q)$ which is mapped isomorphically onto $\mathrm{Aut}(\mathrm{GF}(q))$ by the canonical epimorphism of $\Gamma\mathrm{L}(m,q)$ onto $\mathrm{Aut}(\mathrm{GF}(q))$. Let $\Gamma_\delta(m,q)$ be the unique subgroup of $\Gamma(m,q)$ of order δ. Then clearly $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\Gamma_\delta(m,q)$ and $\mathrm{GL}(m,q)$. Upon letting $I_\delta(m,q)$ be the subgroup of $\Gamma\mathrm{L}_\delta(m,q)$ generated by $\Gamma_\delta(m,q)$ and $\mathrm{SL}(m,q)$ we see that $I_\delta(m,q) \in \Gamma\mathrm{SL}_\delta(m,q)$. Likewise, upon letting $J_\delta^{(d)}(m,q)$ be the subgroup of $\Gamma\mathrm{L}_\delta(m,q)$ generated by $\Gamma_\delta(m,q)$ and $\mathrm{GL}^{(d)}(m,q)$ we see that $I_\delta(m,q) < J_\delta^{(d)}(m,q) \in \Gamma\mathrm{L}_\delta^{(d)}(m,q)$. Now $(g,\alpha) \mapsto (g, \det\alpha)$ gives an epimorphism σ of $\Gamma\mathrm{L}(m,q)$ onto $\Gamma\mathrm{L}(1,q)$ with kernel $\mathrm{SL}(m,q)$. Hence σ induces the usual bijection between the set of subgroups of $\Gamma\mathrm{L}(m,q)$ containing $\mathrm{SL}(m,q)$ and the set of all subgroups of $\Gamma\mathrm{L}(1,q)$. In particular $\Gamma\mathrm{L}_\delta^{(d)}(m,q) = \{J < \Gamma\mathrm{L}(m,q) : \sigma(J) \in \Gamma\mathrm{L}_\delta^{(d)}(1,q)\}$. Also $\sigma(\Gamma\mathrm{SL}_\delta(m,q)) = \Gamma\mathrm{SL}_\delta(1,q)$ and $\sigma(\Gamma\mathrm{L}_\delta^{(d)}(m,q)) = \Gamma\mathrm{L}_\delta^{(d)}(1,q)$. It is easy to see that $\Gamma\mathrm{SL}_\delta(1,q)$ is the set of all conjugates of $I_\delta(1,q)$ in $\Gamma\mathrm{L}(1,q)$, and $\Gamma\mathrm{L}_\delta^{(d)}(1,q)$ is the set of all conjugates of $J_\delta^{(d)}(1,q)$ in $\Gamma\mathrm{L}(1,q)$. From this it follows that $\Gamma\mathrm{SL}_\delta(m,q)$ is the set of all conjugates of $I_\delta(m,q)$ in $\Gamma\mathrm{L}(m,q)$, and $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ is the set of all conjugates of $J_\delta^{(d)}(m,q)$ in $\Gamma\mathrm{L}(m,q)$. Clearly $I_\delta(m,q)$ is a split extension of $\mathrm{SL}(m,q)$ such that $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\mathrm{GL}(m,q)$ and $I_\delta(m,q)$, and likewise $J_\delta^{(d)}(m,q)$ is a split extension of $\mathrm{GL}^{(d)}(m,q)$ such that $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\mathrm{GL}(m,q)$ and $J_\delta^{(d)}(m,q)$.

Therefore $\Gamma\mathrm{SL}_\delta(m,q)$ is a nonempty complete set of conjugate subgroups of $\Gamma\mathrm{L}(m,q)$, and every I in $\Gamma\mathrm{SL}_\delta(m,q)$ is a split extension of $\mathrm{SL}(m,q)$ such that $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\mathrm{GL}(m,q)$ and I, and likewise $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ is a nonempty complete set of conjugate subgroups of $\Gamma\mathrm{L}(m,q)$, and every J in $\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ is a split extension of $\mathrm{GL}^{(d)}(m,q)$ such that $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\mathrm{GL}(m,q)$ and J.

Recalling that $m>0$ is any integer, we conclude with the following four theorems, where $\widetilde{K}_e$ and $K_{(e,\tau)}$ are as in (ii) and (iii) above.

Theorem (4.4.2). *We have* $\mathrm{Gal}(\phi_{m-1}^{**},K_{m-1})=\Gamma\mathrm{L}_\delta(m,q)$ *and* $\mathrm{Gal}(f_{m-1}^{**},K_{m-1})=\mathrm{P}\Gamma\mathrm{L}_\delta(m,q)$ *where* $\delta=\delta(k_p)$.

Theorem (4.4.3). *We have* $\mathrm{Gal}(\phi_{m-1}^{**},\widetilde{K}_{m-1})=\Gamma\mathrm{L}_\delta(m,q)$ *and* $\mathrm{Gal}(f_{m-1}^{**},\widetilde{K}_{m-1})=\mathrm{P}\Gamma\mathrm{L}_\delta(m,q)$ *where* $\delta=\delta(\widetilde{K}_{m-1})$. *[Note that if* $R_{m-1}=k_p[[X,T_1,\dots,T_{m-1}]]$ *or* $R_{m-1}=$ *the localization of* $k_p[X,T_1,\dots,T_{m-1}]$ *at the maximal ideal generated by* $(X,T_1,\dots,T_{m-1})$, *then* $\delta(\widetilde{K}_{m-1})=\delta(k_p)$.*]*

Theorem (4.4.4). *We have* $\mathrm{Gal}(\phi_{m-1}^{*(d)},K_{m-1})\in\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ *and* $\mathrm{Gal}(f_{m-1}^{*(d)},K_{m-1})\in\mathrm{P}\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ *where* d *is any divisor of* $q-1$ *and* $\delta=\delta(k_p)$.

Theorem (4.4.5). *We have* $\mathrm{Gal}(\phi_{m-1}^{*(d)},\widetilde{K}_{m-1})\in\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ *and* $\mathrm{Gal}(f_{m-1}^{*(d)},\widetilde{K}_{m-1})\in\mathrm{P}\Gamma\mathrm{L}_\delta^{(d)}(m,q)$ *where* d *is any divisor of* $q-1$ *and* $\delta=\delta(\widetilde{K}_{m-1})$. *[Note that if either* $R_{m-1}=k_p[[X,T_1,\dots,T_{m-1}]]$ *or* $R_{m-1}=$ *the localization of* $k_p[X,T_1,\dots,T_{m-1}]$ *at the maximal ideal generated by* $(X,T_1,\dots,T_{m-1})$, *then* $\delta(\widetilde{K}_{m-1})=\delta(k_p)$.*]*

Namely, for $m>1$, Theorems (4.4.2) to (4.4.5) are special cases of Theorems (4.3.2) to (4.3.5) respectively. Also obviously for $m=1$ we have $\mathrm{Gal}(\phi_0^{**},K_0)=\mathrm{GL}(1,q)$ and $\mathrm{Gal}(\phi_0^{**},\widetilde{K}_0)=\mathrm{GL}(1,q)$, and from this the $m=1$ case of Theorems (4.4.2) to (4.4.5) follows as in the proof of Theorems (4.3.2) to (4.3.5).

References

[A01] S. S. Abhyankar, *On the ramification of algebraic functions*, American Journal of Mathematics **77** (1955), 572-592. MR **17:**193c

[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, *Projective polynomials*, Proceedings of the American Mathematical Society **125** (1997), 1643-1650. MR **98a:**12001

[A06] S. S. Abhyankar, *Local fundamental groups of algebraic varieties*, Proceedings of the American Mathematical Society **125** (1997), 1635-1641. MR **97h:**14032

[AL1] S. S. Abhyankar and P. A. Loomis, *Once more nice equations for nice groups*, Proceedings of the American Mathematical Society, **126** (1998), 1885-1896. MR **98k:**12003

[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

[Har] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, Inventiones Mathematicae **117** (1994), 1-25. MR **95i:**14029

[Ray] M. Raynaud, *Revêtment de la droit affine en charactéristic* $p>0$ *et conjecture d'Abhyankar*, Inventiones Mathematicae **116** (1994), 425-462. MR **94m:**14034

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

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