GALOIS THEORY OF SEMILINEAR TRANSFORMATIONS*

By
Shreeram S. Abhyankar
Mathematics Department, Purdue University, West Lafayette, IN 47907, USA;
e-mail: ram@cs.purdue.edu

Abstract. The general linear groups $\mathrm{GL}(m,q)$ can be realized as Galois groups of certain vectorial (= q-additive) polynomials over rational function fields when the ground field contains $\mathrm{GF}(q)$, where $m > 0$ is any integer and $q > 1$ is any power of any prime p. When calculated over the prime field as the ground field, these Galois groups get enlarged into the semilinear groups $\Gamma\mathrm{L}(m,q)$. Similarly, for any integer $n > 0$, the Galois groups of the n-th iterates of these vectorials get enlarged from $\mathrm{GL}(m,q,n)$ to $\Gamma\mathrm{L}(m,q,n)$ where $\mathrm{GL}(m,q,n)$ is the general linear group of the free module of rank m over the local ring $\mathrm{GF}(q)[T]/T^n$ and $\Gamma\mathrm{L}(m,q,n)$ is its semilinearization. Likewise, a corresponding enlargement to the semilinear symplectic groups $\Gamma\mathrm{Sp}(2m,q)$ happens when dealing with suitable vectorials having the symplectic similitude groups $\mathrm{GSp}(2m,q)$ as Galois groups. Much of this continues to hold when, instead of over rational function fields, the vectorials are considered over meromorphic function fields. A similar semilinear enlargement takes place when dealing with Galois groups between $\mathrm{SL}(m,q)$ and $\mathrm{GL}(m,q)$ or between $\mathrm{Sp}(2m,q)$ and $\mathrm{GSp}(2m,q)$. The calculation of these various Galois groups leads to a determination of the algebraic closures of the ground fields in the splitting fields of the corresponding vectorial polynomials.

Section 1: Introduction

Throughout this paper, let $k_p \subset K \subset \Omega$ be fields of characteristic $p > 0$ where Ω is an algebraic closure of K, let $q = p^u > 1$ be any power of p, let $m > 0$ be any integer, and to abbreviate frequently occurring expressions, for every integer $i \geq -1$, let us put

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

Moreover, for any nonconstant $\phi = \phi(Y) \in K[Y]$ we let

$$\mathrm{SF}(\phi, K) = \text{the } \textbf{splitting field} \text{ of } \phi \text{ over } K \text{ in } \Omega$$

and

$$\mathrm{AC}(k_p, \phi, K) = \text{the } \textbf{algebraic closure} \text{ of } k_p \text{ in } \mathrm{SF}(\phi, K).$$

For various classes of separable ϕ, we shall determine the group $\mathrm{Gal}(\phi, K)$ and the field $\mathrm{AC}(k_p, \phi, K)$. Here K will mostly be a rational function field over k_p or a formal meromorphic series field over k_p. Also ϕ will mostly be a projective or subvectorial or vectorial polynomial over K.

*1991 Mathematical Subject Classification: 12F10, 14H30, 20D06, 20E22. This work was partly supported by NSF Grant DMS 91-01424 and NSA grant MDA 904-97-1-0010.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Recall that $f^*(Y)$ (resp: $\phi^*(Y)$ or $\phi^*(Y)$) 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 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 $\phi^*(Y) = \sum_{i=0}^{m^*} a_i^* Y^{q^{m^*-i}}$) 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 $\phi^*(Y)$) is **monic** $\Leftrightarrow a_0^* = 1$, and note that $f^*(Y)$ (resp: $\phi^*(Y)$ or $\phi^*(Y)$) is **separable** (i.e., its Y-discriminant is nonzero) $\Leftrightarrow a_{m^*}^* \neq 0$, and note that $\phi_Y^*(Y) = \phi_Y^*(0) = a_{m^*}^*$ where $\phi_Y^*(Y)$ is the Y-derivative of $\phi^*(Y)$. Also note that $f^*(Y) \to \phi^*(Y) = f^*(Y^{q-1})$ and $\phi^*(Y) \to \phi^*(Y) = Y\phi^*(Y)$ give bijections of projectives to subvectorials (= their **subvectorial associates**) to vectorials (= their **vectorial associates**).

To review what was said in Lemmas (2.4) and (2.5) of [A03] and Lemma (4.1.1) of [A08], for a moment let $f = f(Y)$ be a separable projective q-polynomial of q-prodegree m over K, let $\phi = \phi(Y) = f(Y^{q-1})$ and $\phi = \phi(Y) = Y\phi(Y)$, and let V be the set of all roots of ϕ in Ω, and note that then V is an m-dimensional $\mathrm{GF}(q)$-vector-subspace of Ω; to see this, it suffices to observe that the cardinality of V is q^m and for all y, z in Ω and $\zeta \in \mathrm{GF}(q)$ we have $\phi(y+z) = \phi(y) + \phi(z)$ and $\phi(\zeta z) = \zeta\phi(z)$. 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 $\mathrm{GF}(q) \subset K(V) = \mathrm{SF}(\phi, K) = \mathrm{SF}(\phi, K)$. 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 $\mathrm{Gal}(\phi, K) < \Gamma\mathrm{L}(m, q)$. 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 $\mathrm{Gal}(\phi, K) < \mathrm{GL}(m, q) \Leftrightarrow \mathrm{GF}(q) \subset K$. Thus we have the following:

Semilinearity Lemma (1.1). *Let $f = f(Y)$ be a separable projective q-polynomial of q-prodegree m in Y over K, let $\phi = \phi(Y) = f(Y^{q-1})$ and $\phi = \phi(Y) = Y\phi(Y)$, and let V be the set of all roots of ϕ in Ω. Then V is an m-dimensional $GF(q)$-vector-subspace of Ω with $GF(q) \subset K(V) = SF(\phi, K) = SF(\phi, K)$, and in a natural manner we may identify $Gal(\phi, K)$ with a subgroup of $\Gamma L(V) = \Gamma L(m, q)$; under this identification we have*

$Gal(\phi, K) < GL(m,q) \Leftrightarrow GF(q) \subset K$. Likewise, we may identify $Gal(f, K)$ with a subgroup of $P\Gamma L(m,q)$ and then $Gal(f, K)$ becomes the image of $Gal(\phi, K)$ under the canonical epimorphism of $\Gamma L(m,q)$ onto $P\Gamma L(m,q)$. The Galois group $Gal(\phi, K)$ essentially equals the Galois group $Gal(\phi, K)$ except that the former acts on nonzero vectors while the latter acts on the entire vector space V.

This lemma will be used tacitly. In particular, the said Galois groups will be regarded as subgroups of $\Gamma L(V) = \Gamma L(m,q)$ and its projectivization. In Section 2 we shall deal with vectorials whose Galois groups are between $SL(m,q)$ and $\Gamma L(m,q)$; this will be based on [A08]. In Section 3 we shall deal with iterates of some of the vectorials considered in Section 2; this will be based on [AS1]. In Section 4 we shall deal with vectorials whose Galois groups are between $Sp(2m,q)$ and $\Gamma Sp(2m,q)$; this will be based on [A04], [AL1] and [AL2]. For relevant general discussion about Galois Theory, see [A01], [A02] and [A07]. As a supplement to (1.1), in (2.5)(iii) of [A03] we proved the following:

Root Extraction Lemma (1.2). *Given any monic subvectorial q-polynomial $\phi = \phi(Y)$ of q-subdegree m in Y over K, there exists $\Lambda \in SF(\phi, K)$ such that $\Lambda^{q-1} = (-1)^{(m-1)}\phi(0)$.*

When $GF(q) \subset K$, the Galois groups of the vectorials over K to be considered in Section 2 will be between $SL(m,q)$ and $GL(m,q)$. Note that $SL(m,q) \triangleleft GL(m,q)$ with $GL(m,q)/SL(m,q) = Z_{q-1}$ and hence for every divisor d of $q-1$ there is a unique group $GL^{(d)}(m,q)$ such that $SL(m,q) < GL^{(d)}(m,q) < GL(m,q)$ and $[GL(m,q) : GL^{(d)}(m,q)] = d$ where, as usual, $<$ and $\triangleleft$ denote subgroup and normal subgroup respectively, Z_{q-1} denotes a cyclic group of order $q-1$, and $:$ denotes index. Upon letting $PGL^{(d)}(m,q)$ to be the image of $GL^{(d)}(m,q)$ under the canonical epimorphism of $GL(m,q)$ onto $PGL(m,q)$ we see that $PGL^{(d)}(m,q)$ is the unique group between $PSL(m,q)$ and $PGL(m,q)$ such that $[PGL(m,q) : PGL^{(d)}(m,q)] = GCD(m,d)$.

Likewise $GL(m,q) \triangleleft \Gamma L(m,q)$ with $\Gamma L(m,q)/GL(m,q) = Z_u$ and hence for every divisor δ of u there is a unique group $\Gamma L_\delta(m,q)$ such that $GL(m,q) < \Gamma L_\delta(m,q) < \Gamma L(m,q)$ and $[\Gamma L_\delta(m,q) : GL(m,q)] = \delta$, where $P\Gamma L_\delta(m,q)$ is the image of $\Gamma L_\delta(m,q)$ under the canonical epimorphism of $\Gamma L(m,q)$ onto $P\Gamma L(m,q)$. Also we let $\Gamma SL_\delta(m,q)$ be the set of all subgroups I of $\Gamma L_\delta(m,q)$ such that $I \cap GL(m,q) = SL(m,q) \triangleleft I$ with $I/SL(m,q) = Z_\delta$, and we let $P\Gamma SL_\delta(m,q)$ be the set of images of the various members of $\Gamma SL_\delta(m,q)$ under the canonical epimorphism of $\Gamma L(m,q)$ onto $P\Gamma L(m,q)$; in Remark (4.4.1) of [A08] we have shown that $\Gamma SL_\delta(m,q)$ is a nonempty complete set of conjugate subgroups of $\Gamma L(m,q)$, and every I in $\Gamma SL_\delta(m,q)$ is a **split extension** of $SL(m,q)$ (i.e., some subgroup of I is mapped isomorphically onto $I/SL(m,q)$ by the residue class map of I onto $I/SL(m,q)$) such that

$\Gamma L_\delta(m,q)$ is generated by $GL(m,q)$ and I. Finally we let $\Gamma L_\delta^{(d)}(m,q)$ be the set of all subgroups J of $\Gamma L_\delta(m,q)$ such that $J \cap GL(m,q) = GL^{(d)}(m,q) \triangleleft J$ with $J/GL^{(d)}(m,q) = Z_\delta$ and $I < J$ for some I in $\Gamma SL_\delta(m,q)$, and we let $P\Gamma L_\delta^{(d)}(m,q)$ be the set of images of the various members of $\Gamma L_\delta^{(d)}(m,q)$ under the canonical epimorphism of $\Gamma L(m,q)$ onto $P\Gamma L(m,q)$; in Remark (4.4.1) of [A08] we have shown that $\Gamma L_\delta^{(d)}(m,q)$ is a nonempty complete set of conjugate subgroups of $\Gamma L(m,q)$, and every J in $\Gamma L_\delta^{(d)}(m,q)$ is a split extension of $GL^{(d)}(m,q)$ such that $\Gamma L_\delta(m,q)$ is generated by $GL(m,q)$ and J; note that clearly $\Gamma L_\delta^{(q-1)}(m,q) = \Gamma SL_\delta(m,q)$ and $\Gamma L_\delta^{(1)}(m,q) = \{\Gamma L_\delta(m,q)\}$.

To determine the Galois groups when $GF(q)$ is not contained in K, we note that $SF(Y^q - Y, K) = K(GF(q))$ and we **let $\delta(K)$ be the unique divisor** of u such that

(1.3)
$$\mathrm{Gal}(Y^q - Y, K) = Z_{\delta(K)} \quad \text{i.e. equivalently} \quad [K(GF(q)) : K] = \delta(K)$$

and we note that then (see Footnote 17 of [A08])

(1.4)
$$K \cap GF(q) = GF(p^{u/\delta(K)}).$$

Concerning $\delta(K)$, the following lemma is easily proved; see Propositions (4.2.3) to (4.2.5) of [A08].

Linear Enlargement Lemma (1.5). *For any separable projective q-polynomial $f = f(Y)$ of q-prodegree m in Y over K and its subvectorial associate $\phi = \phi(Y) = f(Y^{q-1})$ we have the following.*

(1.5.1) If $Gal(\phi, K(GF(q))) = SL(m,q)$, then $Gal(\phi, K) \in \Gamma SL_{\delta(K)}(m,q)$ and $Gal(f,K) \in P\Gamma SL_{\delta(K)}(m,q)$.

(1.5.2) If $Gal(\phi, K(GF(q))) = GL(m,q)$, then $Gal(\phi, K) = \Gamma L_{\delta(K)}(m,q)$ and $Gal(f,K) = P\Gamma L_{\delta(K)}(m,q)$.

(1.5.3) If $Gal(\phi, K(GF(q))) = GL^{(d)}(m,q)$ where d is a divisor of $q-1$, and for some field K' between K and $SF(\phi, K)$ we have $\delta(K') = \delta(K)$ and $Gal(\phi, K'(GF(q))) = SL(m,q)$, then $Gal(\phi, K) \in \Gamma L_{\delta(K)}^{(d)}(m,q)$ and $Gal(f,K) \in P\Gamma L_{\delta(K)}^{(d)}(m,q)$.

In determining $AC(k_p, \phi, K)$ we shall use the following obvious:

Algebraic Closure Lemma (1.6). *Just in this lemma let $k_p \subset K \subset \Omega$ be fields of any characteristic, which may or may not be zero, such that Ω is an algebraic closure of K. Let $\phi = \phi(Y)$ be a nonconstant separable polynomial in Y with coefficients in K, and let k^* be an algebraic field extension of k_p in $SF(\phi, K)$ such that for every finite algebraic field extension k' of k^* in $SF(\phi, K)$ we have $[K(k') : K(k^*)] = [k' : k^*]$ and $|Gal(\phi, K(k'))| = |Gal(\phi, K(k^*))|$. Then $AC(k_p, \phi, K) = k^*$.*

As a matter of terminology, we recall that a (noetherian) local ring S' is said to **dominate** a local ring S if S is a subring of S' and the **maximal**

ideal $M(S)$ of S is contained in the maximal ideal $M(S')$ of S', and we note that then the **residue field** $S/M(S)$ of S may be identified with a subfield of the residue field $S'/M(S')$ of S'; if under this identification, $S/M(S)$ coincides with $S'/M(S')$ then S' is said to be **residually rational** over S; thus in particular S' is residually rational over a subfield means that the subfield gets mapped isomorphically onto $S'/M(S')$ under the canonical epimorphism $S' \to S'/M(S')$.

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

Section 2: Linear Groups

In this Section, to write down families of polynomials whose Galois groups are between $\mathrm{SL}(m,q)$ and $\Gamma\mathrm{L}(m,q)$, let $Y, X, T_1, T_2, \dots$ be indeterminates over k_p. For every $e \geq 0$ let

$$K_e = k_p(X, T_1, \dots, T_e)$$

and

$$K_e = \text{the quotient field of an } (e+1)\text{-dimensional regular local domain } R_e \text{ with } k_p \subset R_e \text{ and } M(R_e) = (X, T_1, \dots, T_e)R_e$$

and for every $e \geq 1$ and $0 \neq \tau \in k_p(T_1)$ let

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

We shall apply the considerations of Section 1 by taking $K = K_e$ or K_e or $K_{(e,\tau)}$ with suitable e and τ.

First, for $0 \leq e \leq m-1$, 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

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

Next, for $1 \leq e \leq m-1$ and every $0 \neq \tau \in k_p(T_1)$ 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 $f_{(e,\tau)}^{*(d)}$ and $\phi_{(e,\tau)}^{*(d)}$ 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

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

and

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

Finally, for $1 \leq e \leq m-1$ and every $0 \neq \tau \in k_p(T_1)$ 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

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

Concerning these polynomials, by MRT (= the Method of Ramification Theory) and MTR (= the Method of Throwing Away Roots), supplemented by Theorem I of [CaK] which we restate as Theorem (2.1*) below, in Theorems (2.3.1) to (2.3.5) of [A08] we respectively proved parts (2.1.1) to (2.1.5) of the following Theorem (2.1).

Theorem (2.1*) [Cameron-Kantor]. *If $m > 2$ and $H < GL(m,q)$ is such that its image under the canonical epimorphism of $GL(m,q)$ onto $PGL(m,q)$ is doubly transitive, then either $SL(m,q) < H$, or $(q,m) = (4,2)$ with $A_7 \approx H < SL(4,2) = GL(4,2) \approx A_8$ (where $\approx$ denotes isomorphism, and A_7 and A_8 are the alternating groups on 7 and 8 letters respectively).*

Theorem (2.1). *For $1 \leq e \leq m-1$ we have the following.*

(2.1.1) If $GF(q) \subset k_p$, then for every element $0 \neq \tau \in k_p(T_1)$ we have $Gal(\phi^*_{(e,\tau)}, K_{(e,\tau)}) = SL(m,q)$.

(2.1.2) If $GF(q) \subset k_p$, then for every element $0 \neq \tau \in k_p(T_1)$ we have $Gal(\phi^{**}_{(e,\tau)}, K_{(e,\tau)}) = GL(m,q)$.

(2.1.3) If $GF(q) \subset k_p$, then for every integer $\epsilon \geq e$ we have $Gal(\phi^{**}_e, K_\epsilon) = GL(m,q)$.

(2.1.4) If $GF(q) \subset k_p$, then for every element $0 \neq \tau \in k_p(T_1)$ and every divisor d of $q-1$ we have $Gal(\phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) = GL^{(d)}(m,q)$.

(2.1.5) If $GF(q) \subset k_p$, then for every integer $\epsilon \geq e$ and every divisor d of $q-1$ we have $Gal(\phi^{*(d)}_e, K_\epsilon) = GL^{(d)}(m,q)$.

By using the Algebraic Closure Lemma (1.6), we shall now deduce the following consequences of the above Theorem.

Theorem (2.2). *For $1 \leq e \leq m-1$ we have the following.*

(2.2.1) For every element $0 \neq \tau \in k_p(T_1)$ we have $AC(k_p, \phi^*_{(e,\tau)}, K_{(e,\tau)}) = k_p(GF(q))$.

(2.2.2) For every element $0 \neq \tau \in k_p(T_1)$ we have $AC(k_p, \phi^{**}_{(e,\tau)}, K_{(e,\tau)}) = k_p(GF(q))$.

(2.2.3) If $\epsilon \geq e$ is any integer such that R_ϵ is residually rational over k_p, then we have $AC(k_p, \phi^{**}_e, K_\epsilon) = k_p(GF(q))$.

(2.2.4) For every element $0 \neq \tau \in k_p(T_1)$ and every divisor d of $q-1$, we have $AC(k_p, \phi^{*(d)}_{(e,\tau)}, K_{(e,\tau)}) = k_p(GF(q))$.

(2.2.5) If $\epsilon \geq e$ is any integer such that R_ϵ is residually rational over k_p, then for every divisor d of $q-1$ we have $AC(k_p, \phi^{*(d)}_e, K_\epsilon) = k_p(GF(q))$.

To prove (2.2.1) or (2.2.2) or (2.2.4), let $1 \leq e \leq m-1$ and $0 \neq \tau \in k(T_1)$ be given, and respectively let $(\phi, G) = (\phi^*_{(e,\tau)}, \mathrm{SL}(m,q))$ or $(\phi^{**}_{(e,\tau)}, \mathrm{GL}(m,q))$ or $(\phi^{*(d)}_{(e,\tau)}, \mathrm{GL}^{(d)}(m,q))$ where in the last case d is any divisor of $q-1$. Upon letting $K = K_{(e,\tau)}$ and $k^* = k_p(\mathrm{GF}(q))$, by (1.1) we see that $k^* \subset \mathrm{SF}(\phi, K)$. Now we have $K(k^*) = k^*(X, \tau, T_2, \ldots, T_e)$ with $\tau \in k^*(T_1)$ and $\mathrm{GF}(q) \subset k^*$, and given any finite algebraic field extension k' of k^* in $\mathrm{SF}(\phi, K)$ we also have $K(k') = k'(X, \tau, T_2, \ldots, T_e)$ with $\tau \in k'(T_1)$ and $\mathrm{GF}(q) \subset k'$, and hence respectively by (2.1.1) or (2.1.2) or (2.1.4) we see that $\mathrm{Gal}(\phi, K(k')) = G = \mathrm{Gal}(\phi, K(k^*))$. For any finite algebraic field extension k' of k^* in $\mathrm{SF}(\phi, K)$ we clearly have $[K(k') : K(k^*)] = [k' : k^*]$. Therefore by (1.6) we conclude that $\mathrm{AC}(k_p, \phi, K) = k^*$.

To prove (2.2.3) or (2.2.5), let $1 \leq r \leq m-1$ and $\epsilon \geq e$ be given, and respectively let $(\phi, G) = (\phi_e^{**}, \mathrm{GL}(m,q))$ or $(\phi_e^{*(d)}, \mathrm{GL}^{(d)}(m,q))$ where in the second case d is any divisor of $q-1$. Upon letting $K = K_\epsilon$ and $k^* = k_p(\mathrm{GF}(q))$, by (1.1) we see that $k^* \subset \mathrm{SF}(\phi, K)$. Moreover, upon letting R_ϵ^* to be the localization of the integral closure of R_ϵ in $K(k^*)$ at a maximal ideal in it we see that R_ϵ^* is an $(\epsilon+1)$-dimensional regular local domain whose maximal ideal is generated by $(X, T_1, \dots, T_\epsilon)$ and whose quotient field is $K(k^*)$, and we clearly have $\mathrm{GF}(q) \subset K(k^*)$, and given any finite algebraic field extension k' of k^* in $\mathrm{SF}(\phi, K)$, upon letting R'_ϵ to be the localization of the integral closure of R_ϵ^* in $K(k')$ at a maximal ideal in it we see that R'_ϵ is an $(\epsilon+1)$-dimensional regular local domain whose maximal ideal is generated by $(X, T_1, \dots, T_\epsilon)$ and whose quotient field is $K(k')$, and we clearly have $\mathrm{GF}(q) \subset K(k')$, and hence respectively by (2.1.3) or (2.1.5) we see that $\mathrm{Gal}(\phi, K(k')) = G = \mathrm{Gal}(\phi, K(k^*))$. Now, assuming R_ϵ to be residually rational over k_p, we see that R_ϵ^* is the integral closure of R_ϵ in $K(k^*)$, and R_ϵ^* is residually rational over k^*, and given any finite algebraic field extension k' of k^* in $\mathrm{SF}(\phi, K)$, we see that R'_ϵ is the integral closure of R_ϵ^* in $K(k')$, and R'_ϵ is residually rational over k', and also $[K(k') : K(k^*)] = [k' : k^*]$. Therefore again by (1.6) we conclude that $\mathrm{AC}(k_p, \phi, K) = k^*$.

In Theorems (4.3.1) to (4.3.5) of [A08] we deduced the following consequences of parts (2.1.1) to (2.1.5) of the above Theorem (2.1) together with the Linear Enlargement Lemma (1.5).

Theorem (2.3). *For $1 \leq e \leq m-1$ we have the following.*

(2.3.1) For every element $0 \neq \tau \in k_p(T_1)$, upon letting $\delta = \delta(k_p)$, we have Gal$(\phi_{(e,\tau)}^*, K_{(e,\tau)}) \in \Gamma SL_\delta(m,q)$ and Gal$(f_{(e,\tau)}^*, K_{(e,\tau)}) \in P\Gamma SL_\delta(m,q)$.

(2.3.2) For every element $0 \neq \tau \in k_p(T_1)$, upon letting $\delta = \delta(k_p)$, we have Gal$(\phi_{(e,\tau)}^{**}, K_{(e,\tau)}) = \Gamma L_\delta(m,q)$ and Gal$(f_{(e,\tau)}^{**}, K_{(e,\tau)}) = P\Gamma L_\delta(m,q)$.

(2.3.3) For every integer $\epsilon \geq e$, upon letting $\delta = \delta(K_\epsilon)$, we have Gal$(\phi_e^{**}, K_\epsilon) = \Gamma L_\delta(m,q)$ and Gal$(f_e^{**}, K_\epsilon) = P\Gamma L_\delta(m,q)$. [Note that if either $R_\epsilon = k_p[[X, T_1, \dots, T_\epsilon]]$ or $R_\epsilon =$ the localization of $k_p[X, T_1, \dots, T_\epsilon]$ at the maximal ideal generated by $(X, T_1, \dots, T_\epsilon)$ then R_ϵ is residually rational over k_p and we have $\delta(K_\epsilon) = \delta(k_p)$.]

(2.3.4) For 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 Gal$(\phi_{(e,\tau)}^{*(d)}, K_{(e,\tau)}) \in \Gamma L_\delta^{(d)}(m,q)$ and Gal$(f_{(e,\tau)}^{*(d)}, K_{(e,\tau)}) \in P\Gamma L_\delta^{(d)}(m,q)$.

(2.3.5) For every integer $\epsilon \geq e$ and every divisor d of $q-1$, upon letting $\delta = \delta(K_\epsilon)$, we have Gal$(\phi_e^{*(d)}, K_\epsilon) \in \Gamma L_\delta^{(d)}(m,q)$ and Gal$(f_e^{*(d)}, K_\epsilon) \in P\Gamma L_\delta^{(d)}(m,q)$. [Note that if either $R_\epsilon = k_p[[X, T_1, \dots, T_\epsilon]]$ or $R_\epsilon =$ the localization of $k_p[X, T_1, \dots, T_\epsilon]$ at the maximal ideal generated by $(X, T_1, \dots, T_\epsilon)$ then R_ϵ is residually rational over k_p and we have $\delta(K_\epsilon) = \delta(k_p)$.]

Remark (2.4) [Local Surface Coverings].

(2.4.1). For $m > 1 = e$ we get the trinomials $f_1^{**} = Y^{\langle m-1 \rangle} + T_1 Y + X$ and $\phi_1^{**} = Y^{q^m} + T_1 Y^q + XY$, giving local coverings above a normal crossing of the branch locus in the local (X, T_1)-plane, dealt with in [A07] and [A08]; this is particularly significant with $R_2 = k_p[[X, T_1]]$; the above Theorems (2.2.3), (2.2.5), (2.3.3) and (2.3.5) give generalizations for the local $(\epsilon + 1)$-dimensional space; the following Theorems (2.4.3) and (2.4.5) are special cases of this. For $m > 1 = e$ and $\tau = 1$ we get the trinomials $f^*_{(1,1)} = Y^{\langle m-1 \rangle} + XY + (-1)^{\langle m-1 \rangle}$ and $\phi^*_{(1,1)} = Y^{q^m} + XY^q + (-1)^{\langle m-1 \rangle} Y$ giving unramified coverings of the affine line, and the trinomials $f^{**}_{(1,1)} = Y^{\langle m-1 \rangle} + Y + X$ and $\phi^{**}_{(1,1)} = Y^{q^m} + Y^q + XY$ giving unramified coverings of the once punctured affine line, dealt with in [A03] and [A08].

Remembering that now $m > 0$ is any integer, we conclude with the following consequences of the above theorems:

(2.4.2). *We have* $Gal(\phi^{**}_{m-1}, K_{m-1}) = \Gamma L_\delta(m, q)$ *and* $Gal(f^{**}_{m-1}, K_{m-1}) = P\Gamma L_\delta(m, q)$ *where* $\delta = \delta(k_p)$, *and we have* $AC(k_p, \phi^{**}_{m-1}, K_{m-1}) = k_p(GF(q))$.

(2.4.3). *We have* $Gal(\phi^{**}_{m-1}, K_{m-1}) = \Gamma L_\delta(m, q)$ *and* $Gal(f^{**}_{m-1}, K_{m-1}) = P\Gamma L_\delta(m, q)$ *where* $\delta = \delta(K_{m-1})$, *and moreover if* R_{m-1} *is residually rational over* k_p *then we have* $AC(k_p, \phi^{**}_{m-1}, K_{m-1}) = k_p(GF(q))$. *[Note that if either* $R_{m-1} = k_p[[X, T_1, \ldots, T_{m-1}]]$ *or* $R_{m-1} =$ *the localization of* $k_p[X, T_1, \ldots, T_{m-1}]$ *at the maximal ideal generated by* $(X, T_1, \ldots, T_{m-1})$ *then* R_{m-1} *is residually rational over* k_p *and we have* $\delta(K_{m-1}) = \delta(k_p)$.*]*

(2.4.4). *We have* $Gal(\phi^{*(d)}_{m-1}, K_{m-1}) \in \Gamma L^{(d)}_\delta(m, q)$ *and* $Gal(f^{*(d)}_{m-1}, K_{m-1}) \in P\Gamma L^{(d)}_\delta(m, q)$ *where* d *is any divisor of* $q - 1$ *and* $\delta = \delta(k_p)$, *and we have* $AC(k_p, \phi^{*(d)}_{m-1}, K_{m-1}) = k_p(GF(q))$.

(2.4.5). *We have* $Gal(\phi^{*(d)}_{m-1}, K_{m-1}) \in \Gamma L^{(d)}_\delta(m, q)$ *and* $Gal(f^{*(d)}_{m-1}, K_{m-1}) \in P\Gamma L^{(d)}_\delta(m, q)$ *where* d *is any divisor of* $q-1$ *and* $\delta = \delta(K_{m-1})$, *and moreover if* R_{m-1} *is residually rational over* k_p *then we have* $AC(k_p, \phi^{*(d)}_{m-1}, K_{m-1}) = k_p(GF(q))$. *[Note that if either* $R_{m-1} = k_p[[X, T_1, \ldots, T_{m-1}]]$ *or* $R_{m-1} =$ *the localization of* $k_p[X, T_1, \ldots, T_{m-1}]$ *at the maximal ideal generated by* $(X, T_1, \ldots, T_{m-1})$ *then* R_{m-1} *is residually rational over* k_p *and we have* $\delta(K_{m-1}) = \delta(k_p)$.*]*

Namely, everything except the assertions about AC was noted as Theorems (4.4.2) to (4.4.5) of [A08]. For $m > 1$, the assertions about AC are special cases of Theorems (2.2.2) to (2.2.5) respectively. For $m = 1$, it is easy to see that if $\mathrm{GF}(q) \subset k_p$ then $\mathrm{Gal}(\phi_0^{**}, K_0) = \mathrm{GL}(1, q) = \mathrm{Gal}(\phi_0^{**}, K_0)$ and $\mathrm{Gal}(\phi_0^{*(d)}, K_0) = \mathrm{GL}^{(d)}(1, q) = \mathrm{Gal}(\phi_0^{*(d)}, K_0)$ for every divisor d of $q - 1$, and from this the assertions about AC follow as in the proofs of Theorems (2.2.2) to (2.2.5).

Note (2.5) [From Local Surface Coverings to Affine Line Coverings]. As hinted in (2.4.1), the family of projective polynomials f_e^{**} was generalized from the $m > 1 = e$ case with $R_2 = k_p[[X, T_1]]$ when it is reduced to the trinomial $f_1^{**} = Y^{\langle m-1\rangle} + T_1 Y + X$, giving a local covering above a normal crossing of the branch locus in the local (X, T_1)-plane, dealt with in [A07] and [A08]. Likewise, the families of projective polynomials $f^{**}_{(e,\tau)}$ and $f^{*}_{(e,\tau)}$ were generalized from the $m > 1 = e = \tau$ case when they are reduced to the trinomials $f^*_{(1,1)} = Y^{\langle m-1\rangle} + XY + (-1)^{\langle m-1\rangle}$ and $f^{**}_{(1,1)} = Y^{\langle m-1\rangle} + Y + X$, giving unramified coverings of the affine line and the once punctured affine line respectively, dealt with in [A03] and [A08]. Out of this, the $m = 2$ and $q = p$ case of $f^*_{(1,1)}$, i.e., the trinomial $Y^{1+p} + XY + 1$, corresponds to the $t = 1$ case of the family of trinomials $Y^{p+t} + XY^t + 1$, where t is a positive integer prime to p, giving unramified coverings of the affine line, which was our starting point in [A01] and [A02].

Section 3: Iterated Linear Groups

In this Section, let

$$(3.1) \qquad E = E(Y) = Y^{q^m} + \sum_{i=1}^{m} X_i Y^{q^{m-i}} \quad \text{with} \quad X_i \in K \text{ and } X_m \neq 0$$

be a monic separable vectorial q-polynomial of q-degree m in Y over K, where the elements $X_1, \dots, X_m$ need not be algebraically independent over k_p. When we want to assume that the elements $X_1, \dots, X_m$ are algebraically independent over k_p and $K = k_p(X_1, \dots, X_m)$, we may express this by saying that we are in the **generic** case. In the **general** (= not necessarily generic) case, let V be the set of all roots of E in Ω, and note that then V is an m-dimensional GF(q)-vector-subspace of Ω. Let $X_{1,1}, \dots, X_{m,1}$ be a GF(q)-basis of V. Then

$$(3.2) \quad Y^{q^m} + \sum_{i=1}^{m} X_i Y^{q^{m-i}} = \prod_{(\lambda_1,\dots,\lambda_m)\in \mathrm{GF}(q)^m} (Y - \lambda_1 X_{1,1} - \dots - \lambda_m X_{m,1})$$

and hence

$$(3.3) \qquad k_p[X_1, \dots, X_m] \subset k_p(\mathrm{GF}(q))[X_{1,1}, \dots, X_{m,1}]$$

and

$$(3.4) \qquad \mathrm{SF}(E, K) = K(V) = K(\mathrm{GF}(q))(X_{1,1}, \dots, X_{m,1}).$$

As noted in (1.1), we also have

$$(3.5) \qquad \mathrm{Gal}(E, K(\mathrm{GF}(q))) < \mathrm{GL}(V) = \mathrm{GL}(m, q)$$