ISRAEL JOURNAL OF MATHEMATICS 88 (1994), 1–23

NICE EQUATIONS FOR NICE GROUPS

BY

SHREERAM S. ABHYANKAR*

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

ABSTRACT

Nice trinomial equations are given for unramified coverings of the affine line in nonzero characteristic p with $\mathrm{PSL}(m,q)$ and $\mathrm{SL}(m,q)$ as Galois groups. Likewise, nice trinomial equations are given for unramified coverings of the (once) punctured affine line in nonzero characteristic p with $\mathrm{PGL}(m,q)$ and $\mathrm{GL}(m,q)$ as Galois groups. Here $m > 1$ is any integer and $q > 1$ is any power of p.

1. Introduction

Given a bivariate polynomial

$$F = F(X,Y) = Y^N + \sum_{i=1}^{N} B_i(X)Y^{N-i} \quad \text{with } B_i(X) \in k[X]$$

where k is an algebraically closed field, let $\mathrm{Disc}_Y(F) \in k[X]$ be the Y-discriminant of F; recall that by definition $\mathrm{Disc}_Y(F)$ equals the Y-resultant $\mathrm{Res}_Y(F, F_Y)$ of F and its Y-derivative F_Y. As observed by Galois (or maybe Riemann), assuming $\mathrm{char}\, k = 0$ (where char stands for characteristic), if $\mathrm{Disc}_Y(F)$ is a nonzero constant, i.e., if $0 \neq \mathrm{Disc}_Y(F) \in k$, then F factors into linear factors in Y, i.e., $F = \prod_{i=1}^{N}(Y - \Phi_i(X))$ with $\Phi_i(X) \in k[X]$. In terms of Galois theory this says that, assuming $\mathrm{char}\, k = 0$, if $\mathrm{Disc}_Y(F)$ is a nonzero constant then the Galois group $\mathrm{Gal}(F, k(X))$ is the identity group; recall that if $\mathrm{Disc}_Y(F) \neq 0$ then $\mathrm{Gal}(F, k(X))$ is the permutation representation of the Galois group of the

* This work was partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-92-H-3035.
Received September 12, 1993 and in revised form January 11, 1994

splitting field of F over $k(X)$ acting on the roots of F. Moreover, again assuming $\operatorname{char} k = 0$, if $\operatorname{Disc}_Y(F)$ has at most one root in k, then $\operatorname{Gal}(F, k(X))$ is cyclic. In case of $k = \mathbb{C}$ these assertions respectively follow from the facts that the plane $\mathbb{R}^2 = \mathbb{C}$ is simply connected and the fundamental group of the punctured plane, $\mathbb{R}^2 -$ a point, is cyclic. These assertions can also be deduced from the Riemann-Hurwitz genus formula (cf. [Ab3]) and upon letting $G = \operatorname{Gal}(F, k(X))$, in case of $\operatorname{char} k = p \neq 0$, this deduction shows that if $\operatorname{Disc}_Y(F)$ is a nonzero constant then G is a **quasi-p group**, i.e., $G = p(G)$ where $p(G)$ denotes the subgroup of G generated by all its p-Sylow subgroups, and if $\operatorname{Disc}_Y(F)$ has at most one root then G is **quasi-p by cyclic**, i.e., $G/p(G)$ is cyclic.

Everything in the above paragraph remains valid (cf. Result 4 on page 841 of [Ab1]) if we replace **discriminant points**, i.e., roots of $\operatorname{Disc}_Y(F)$ in k, by branch points of the equation $F = 0$ in k. To recall what is a branch point, given any value of X in k, say $X = \lambda \in k$, we can write $F(X + \lambda, Y) = f_1(X, Y)^{d_1} \dots f_h(X, Y)^{d_h}$ where $d_1, \dots, d_h$ are positive integers and $f_1(X, Y), \dots, f_h(X, Y)$ are pairwise distinct monic irreducible polynomials of degrees $e_1 > 0, \dots, e_h > 0$ in Y with coefficients in the (formal) power series ring $k[[X]]$; note that if $\operatorname{Disc}_Y(F) \neq 0$ then $d_1 = \cdots = d_h = 1$. Now $X = \lambda$ is a **branch point** if $d_i e_i > 1$ for some i. By Hensel's Lemma (cf. [Ab3]) $f_i(0, Y) = (Y - \mu_i)^{e_i}$ for some $\mu_i \in k$. Since $\operatorname{Disc}_Y(F) = \operatorname{Res}_Y(F, F_Y)$, we also see that $X = \lambda \in k$ is a discriminant point iff the equation $F(\lambda, Y) = 0$ has less than N roots. It follows that every branch point is a discriminant point but not conversely, as seen by taking $F = Y^N - X^N$ with $1 < N \neq \operatorname{char} k$ and $X = \lambda = 0$. Let us recall that a branch point $X = \lambda$ is **tame** if $e_1, \dots, e_h$ are all nondivisible by $\operatorname{char} k$; otherwise it is **wild**.

If the equation $F = 0$ has no branch point in k, then we say that the equation $F = 0$ gives an **unramified covering of the affine line L_k over k**. If the equation $F = 0$ has no branch point in k other than possibly $X = 0$, then we say that the equation $F = 0$ gives an **unramified covering of the (once) punctured affine line $L_{k,1}$**. If the equation $F = 0$ has no branch point in k other than possibly $X = 0$, which is tame in case it is branched, then we say that the equation $F = 0$ gives a **tamely unramified covering of the (once) punctured affine line $L_{k,1}$**. Finally, if the polynomial F is irreducible in $k(X)[Y]$ and the equation $F = 0$ gives ... covering ... , then we say that the equation $F = 0$ gives an **irreducible ... covering ....**

Contrary to the characteristic zero situation, in nonzero characteristic p, there are plenty of unramified coverings of L_k and $L_{k,1}$. Indeed, as conjectured in [Ab1], their Galois groups should span all quasi-p groups and all quasi-p by cyclic groups respectively.

To exhibit interesting examples of such coverings, **henceforth we assume that k is an algebraically closed field with** $\operatorname{char} k = p \neq 0$, and we consider the trinomial

$$F^* = F^*(X, Y) = Y^n - aX^rY^t + bX^s$$

where

$$n > t > 0 \text{ and } r \geq 0 \leq s \text{ in } \mathbb{Z} \quad \text{and} \quad a \neq 0 \neq b \text{ in } k \text{ (for instance } a = 1 = b).$$

We are particularly interested in the equation $F^* = 0$ in the three cases: (1*) n is nondivisible by p but $n - t$ is divisible by p; (2*) n is nondivisible by p but t is divisible by p; (3*) n is divisible by p but t is nondivisible by p. We are especially interested in the three special cases: (1′) $s = 0$ and (1*) holds; (2′) $s = 0$ and (2*) holds; (3′) $r = 0$ and s is divisible by t and (3*) holds.

Now if (1*) holds then $F^* - t^{-1}YF_Y^* = bX^s$ and hence $\operatorname{Disc}_Y(F^*) = b^*X^{s^*}$ with $0 \neq b^* \in k$ and $0 \leq s^* \in s\mathbb{Z}$ and therefore the equation $F^* = 0$ gives an unramified covering of $L_{k,1}$. Likewise, if (2*) holds then $F_Y^* = nY^{n-1}$ and hence $\operatorname{Disc}_Y(F^*) = b^*X^{s^*}$ with $0 \neq b^* \in k$ and $0 \leq s^* \in s\mathbb{Z}$ and therefore the equation $F^* = 0$ gives an unramified covering of $L_{k,1}$. Finally, if (3*) holds then $F_Y^* = -taX^rY^{t-1}$ and hence $\operatorname{Disc}_Y(F^*) = b^*X^{s^*}$ with $0 \neq b^* \in k$ and $0 \leq s^* \in \mathbb{Z}$ and therefore the equation $F^* = 0$ gives an unramified covering of $L_{k,1}$.

It follows that in cases (1*), (2*) and (3*), the equation $F^* = 0$ gives an unramified covering of $L_{k,1}$; in these cases we let

$$G^* = \operatorname{Gal}(F^*, k(X)).$$

It also follows that in cases (1′), (2′) and (3′), the equation $F^* = 0$ gives an unramified covering of L_k. Cases (1′) and (2′) can be converted into each other by reciprocation, i.e., by sending Y to Y^{-1} and then multiplying by Y^n. In the 1957 paper [Ab1], the equation $F^* = 0$ in cases (1′) and (3′) was written down (cf. Propositions 1 and 2 of [Ab1]) and it was suggested that the Galois groups of the corresponding unramified coverings of L_k be computed. In [Ab4], [Ab5], [Ab6], [Ab7], [APS], [AOS], [AY1] and [AY2], where cases (1′) and (3′)

were respectively called bar and tilde, this was done for several values of n and t. Here we continue the project by doing it for a few more values.

In particular we shall prove the following Theorems 1.1 and 1.2 which further illustrate case (1*). Recall that $<$ and $\lhd$ denote subgroup and normal subgroup respectively. To avoid repetition, **henceforth let q be any positive power of p, i.e., $q = p^u$ for some positive integer u.**

THEOREM 1.1: *Assume that $n = 1 + q + \cdots + q^{m-1}$ where $m > 1$ is an integer. Also assume that $t = 1 + q + \cdots + q^{\mu-1}$ where $1 \leq \mu < m$ is an integer with $\mathrm{GCD}(n, t) = 1$ (for instance $\mu = 1$ and $t = 1$). Then we have the following.*

(1.1.1) *If $s \in n\mathbb{Z}$ and $r > s(n-t)/n$ (for instance if $r > 0 = s$), then the equation $F^* = 0$ gives an irreducible unramified covering of the affine line L_k with Galois group $G^* = \mathrm{PSL}(m, q)$.*

(1.1.2) *If $\mathrm{GCD}(s, m, q-1) = 1$ and $r > s(n-t)/n$ (for instance if $r = 1 = s$), then the equation $F^* = 0$ gives an irreducible tamely unramified covering of the punctured affine line $L_{k,1}$ with Galois group $G^* = \mathrm{PGL}(m, q)$.*

(1.1.3) *If $r \neq s(n-t)/n$, then the equation $F^* = 0$ gives an irreducible unramified covering of the punctured affine line $L_{k,1}$ with $\mathrm{PSL}(m, q) < G^* < \mathrm{PGL}(m, q)$.*

THEOREM 1.2: *Assume that $n = q^m - 1$ where $m > 1$ is an integer. Also assume that $t = q^\mu - 1$ where $1 \leq \mu < m$ is an integer with $\mathrm{GCD}(n, t) = q - 1$ (for instance $\mu = 1$ and $t = q - 1$). Then we have the following.*

(1.2.1) *If $s \in n\mathbb{Z}$ and $r > s(n-t)/n$ (for instance if $r > 0 = s$), then the equation $F^* = 0$ gives an irreducible unramified covering of the affine line L_k with Galois group $G^* = \mathrm{SL}(m, q)$.*

(1.2.2) *If $\mathrm{GCD}(s, q-1) = 1$ and $r > s(n-t)/n$ (for instance if $r = 1 = s$), then the equation $F^* = 0$ gives an irreducible tamely unramified covering of the punctured affine line $L_{k,1}$ with Galois group $G^* = \mathrm{GL}(m, q)$.*

(1.2.3) *If $r \neq s(n-t)/n$, then the equation $F^* = 0$ gives an irreducible unramified covering of the punctured affine line $L_{k,1}$ with $\mathrm{SL}(m, q) < G^* < \mathrm{GL}(m, q)$.*

The proof of Theorem 1.1 will be a slight modification of the "ascending" proof of $\mathrm{PSL}(2, q)$ coverings given in Section 21 of [Ab4] (cf. Footnote 85 of page 122 of [Ab4]), the main difference being that in addition to the Zassenhaus–Feit–Suzuki Theorem (cf. pages 83 and 114 of [Ab4]) we shall also use Theorem I of the Cameron–Kantor paper [CaK]. Theorem 1.2 will be deduced from Theo-

rem 1.1. Note that $\mathrm{PGL}(m,q) = \mathrm{GL}(m,q)/(\text{scalar matrices})$ and $\mathrm{PSL}(m,q) = \mathrm{SL}(m,q)/(\text{scalar matrices of determinant } 1)$, where $\mathrm{GL}(m,q)$ is the group of all m by m matrices whose entries are in the field $\mathrm{GF}(q)$ of q elements and whose determinant is nonzero and $\mathrm{SL}(m,q)$ is the subgroup of $\mathrm{GL}(m,q)$ consisting of those matrices whose determinant is 1. Also note that $\mathrm{PGL}(m,q)$ and $\mathrm{PSL}(m,q)$ are regarded as permutation groups on an $m-1$ dimensional projective space over $\mathrm{GF}(q)$, and the cardinality of such a projective space is $(q^m-1)/(q-1) = 1+q+\cdots+q^{m-1}$. Likewise, $\mathrm{GL}(m,q)$ and $\mathrm{SL}(m,q)$ are permutation groups on an m dimensional vector space over $\mathrm{GF}(q)$; alternatively $\mathrm{GL}(m,q)$ and $\mathrm{SL}(m,q)$ are regarded as permutation groups on the set of nonzero vectors in an m dimensional vector space over $\mathrm{GF}(q)$, and the cardinality of such a set is q^m-1; the first or the second meaning is taken when subgroups of $\mathrm{GL}(m,q)$ are regarded as Galois groups of equations of degree q^m or q^m-1 respectively.

From the above Theorems 1.1 and 1.2, by "reciprocation" we shall deduce the following Theorems 1.3 and 1.4 which illustrate case (2*).

THEOREM 1.3: *Assume that $n = 1+q+\cdots+q^{m-1}$ where $m>1$ is an integer. Also assume that $t = q^\mu + q^{\mu+1} + \cdots + q^{m-1}$ where $1 \le \mu < m$ is an integer with $\mathrm{GCD}(n,t) = 1$ (for instance $\mu = 1$ and $t = n-1$). Then we have the following.*

(1.3.1) *If $s \in n\mathbb{Z}$ and $r > s(n-t)/n$ (for instance if $r > 0 = s$), then the equation $F^* = 0$ gives an irreducible unramified covering of the affine line L_k with Galois group $G^* = \mathrm{PSL}(m,q)$.*

(1.3.2) *If $\mathrm{GCD}(s,m,q-1) = 1$ and $r > s(n-t)/n$ (for instance if $r = 1 = s$), then the equation $F^* = 0$ gives an irreducible tamely unramified covering of the punctured affine line $L_{k,1}$ with Galois group $G^* = \mathrm{PGL}(m,q)$.*

(1.3.3) *If $r \ne s(n-t)/n$, then the equation $F^* = 0$ gives an irreducible unramified covering of the punctured affine line $L_{k,1}$ with $\mathrm{PSL}(m,q) < G^* < \mathrm{PGL}(m,q)$.*

THEOREM 1.4: *Assume that $n = q^m - 1$ where $m > 1$ is an integer. Also assume that $t = q^m - q^\mu$ where $1 \le \mu < m$ is an integer with $\mathrm{GCD}(n,t) = q-1$ (for instance $\mu = 1$ and $t = q^m - q$). Then we have the following.*

(1.4.1) *If $s \in n\mathbb{Z}$ and $r > s(n-t)/n$ (for instance if $r > 0 = s$), then the equation $F^* = 0$ gives an irreducible unramified covering of the affine line L_k with Galois group $G^* = \mathrm{SL}(m,q)$.*

(1.4.2) *If $\mathrm{GCD}(s,q-1) = 1$ and $r > s(n-t)/n$ (for instance if $r = 1 = s$), then*

the equation $F^* = 0$ gives an irreducible tamely unramified covering of the punctured affine line $L_{k,1}$ with Galois group $G^* = \mathrm{GL}(m,q)$.

(1.4.3) *If $r \neq s(n-t)/n$, then the equation $F^* = 0$ gives an irreducible unramified covering of the punctured affine line $L_{k,1}$ with $\mathrm{SL}(m,q) < G^* < \mathrm{GL}(m,q)$.*

As an illustration of case (3*) we shall prove the following Theorem 1.5, where we note that $\mathrm{AGL}(1,q)$ is the group of all affine transformations of the affine line over $\mathrm{GF}(q)$, i.e., the group of all permutations $x \mapsto \alpha x + \beta$ of $\mathrm{GF}(q)$, with $0 \neq \alpha \in \mathrm{GF}(q)$ and $\beta \in \mathrm{GF}(q)$.

THEOREM 1.5: *Assume that $n = q$, $t = q-1$, $r = 0$ and $s = 1$. Then the equation $F^* = 0$ gives an irreducible tamely unramified covering of the punctured affine line $L_{k,1}$ with Galois group $G^* = \mathrm{AGL}(1,q)$.*

2. Some lemmas

Recall that $|\ |$ denotes cardinality, and $[:]$ denotes index as well as field degree. Note that $\mathrm{GF}(q)^*$ and $\mathrm{GF}(q)^+$ respectively denote the underlying multiplicative and additive groups of $\mathrm{GF}(q)$.

TRANSITIVITY LEMMA 2.1: *In this lemma (where we reprove and slightly generalize the double transitivity results of* [Ab4] *and* [Ab7]*), without assuming* $\mathrm{char}\, k$ *to be nonzero, but assuming* $\mathrm{GCD}(n,t) = 1$*, we consider the two cases $r-1 = 0 = s$ and $r = 0 = s-1$ and in these two cases we let F^* be denoted by $\bar{F}$ and $\widetilde{F}$ respectively, and we take a subfield k_0 such that k is an algebraic closure of k_0 and the elements a and b belong to k_0. In other words, just in this lemma, let $a \neq 0 \neq b$ be elements in a field k_0 which need not be algebraically closed and whose characteristic may or may not be zero, let k be an algebraic closure of k_0, let $n > t > 0$ be integers with $\mathrm{GCD}(n,t) = 1$, and consider the trinomials*

$$\bar{F} = \bar{F}(X,Y) = Y^n - aXY^t + b$$

and

$$\widetilde{F} = \widetilde{F}(X,Y) = Y^n - aY^t + bX.$$

For every integer $u > 0$ let $f_{u-1}(Y)$ be the monic polynomial of degree $u-1$ in Y with coefficients in k_0 given by

$$f_{u-1}(Y) = Y^{-1}[(Y+1)^u - 1]$$

and consider the monic polynomials $\bar{F}'$ *and* $\widetilde{F}'$ *of degree* $n-1$ *in* Y *with coefficients in* $k_0[X]$ *given by*

$$\bar{F}' = \bar{F}'(X,Y) = f_{n-1}(Y) - (1+bX^n)f_{t-1}(Y)$$

and

$$\widetilde{F}' = \widetilde{F}'(X,Y) = f_{n-1}(Y) - aX^{n-t}f_{t-1}(Y).$$

By the discriminant calculation on pages 103–105 of [Ab4] *we have*

$$\mathrm{Disc}_Y(\bar{F}) = n^n b^{n-1} - (n-t)^{n-t}t^t a^n b^{t-1}X^n$$

and

$$\mathrm{Disc}_Y(\widetilde{F}) = n^n b^{n-1}X^{n-1} - (n-t)^{n-t}t^t a^n b^{t-1}X^{t-1}.$$

Consequently, $\mathrm{Disc}_Y(\bar{F}) \neq 0 \neq \mathrm{Disc}_Y(\widetilde{F})$ *and hence the Galois groups* $\bar{G} = \mathrm{Gal}(\bar{F}, k_0(X))$ *and* $\widetilde{G} = \mathrm{Gal}(\widetilde{F}, k_0(X))$ *are defined. Concerning these Galois groups we have the following.*

(2.1.1) $\bar{G}$ *and* $\widetilde{G}$ *are transitive. Moreover,* $\mathrm{Disc}_Y(\bar{F}') \neq 0 \neq \mathrm{Disc}_Y(\widetilde{F}')$, *and* $\mathrm{Gal}(\bar{F}', k_0(X))$ *and* $\mathrm{Gal}(\widetilde{F}', k_0(X))$ *are the 1-point stabilizers of* $\bar{G}$ *and* $\widetilde{G}$ *respectively.*

(2.1.2) $\bar{G}$ *is doubly transitive.*

(2.1.3) *If* $t \neq 1$ *then* $\widetilde{G}$ *is doubly transitive. Likewise, if* $t = 1$ *and* n *is not a power of* $\mathrm{char}\, k$ *then* $\widetilde{G}$ *is doubly transitive.*

(2.1.4) *If* $t = 1$ *and* n *is a power of* $\mathrm{char}\, k$ *and* $\mathrm{GF}(n) \subset k_0$ *and* $\alpha^{n-1} = a$ *for some* $\alpha \in k_0$ *then, (as proved in* [Ab7]*),* $\widetilde{G} = \mathrm{GF}(n)^+$ *(and hence* $\widetilde{G}$ *is sharply 1-transitive and therefore it is not doubly transitive unless* $n = 2$*).*

(2.1.5) *If* $t = n-1$ *and* n *is a power of* $\mathrm{char}\, k$ *and* $\mathrm{GF}(n) \subset k_0$ *then* $\widetilde{G} = \mathrm{AGL}(1,n)$. *[It will be observed in the proof that cases (2.1.4) and (2.1.5) go over into each other by "modified reciprocation" which exhibits the* $\widetilde{G}$ *of (2.1.4) as a normal subgroup of the* $\widetilde{G}$ *of (2.1.5) in a natural way so that the factor group is* $\mathrm{GF}(n)^*$*].*

(2.1.6) *If* $t = 1$ *and* $n-1$ *is a positive power of* $\mathrm{char}\, k$ *and* $\mathrm{GF}(n-1) \subset k_0$ *then* $\widetilde{G} = \mathrm{PGL}(2, n-1)$. *[As will be explained in the proof, the* $\widetilde{G}$ *of (2.1.5) is the 1-point stabilizer of the* $\widetilde{G}$ *of (2.1.6)].*

(2.1.7) *If* $n-1$ *is a positive power of* $\mathrm{char}\, k$ *and either* $t = 1$ *or* $t = n-1$ *then, (as proved in* [Ab4]*),* $\mathrm{PSL}(2, n-1) < \bar{G}$, *and if also* $k_0 = k$ *then* $\bar{G} = \mathrm{PSL}(2, n-1)$.

Proof: $\bar{F}$ and $\widetilde{F}$ are irreducible because they are linear in X. Therefore $\bar{G}$ and $\widetilde{G}$ are transitive. To find the 1-point stabilizers of $\bar{G}$ and $\widetilde{G}$ we use the twisted derivative method of throwing away roots as illustrated in Sections 18 to 21 of [Ab4]. By solving $\bar{F} = 0$ we get $X = a^{-1}Y^{n-t} + a^{-1}bY^{-t} \in k_0(Y)$ and hence upon letting

$$\bar{f}'(Y,Z) = Z^{-1}[\bar{F}(a^{-1}Y^{n-t} + a^{-1}bY^{-t}, Z+Y) - \bar{F}(a^{-1}Y^{n-t} + a^{-1}bY^{-t}, Y)]$$

we see that $\mathrm{Disc}_Z(\bar{f}'(Y,Z)) \neq 0$ and $\mathrm{Gal}(\bar{f}'(Y,Z), k_0(Y))$ is the 1-point stabilizer of $\bar{G}$. Likewise, by solving $\widetilde{F} = 0$ we get $X = -b^{-1}Y^n + b^{-1}aY^t \in k_0(Y)$ and hence upon letting

$$\widetilde{f}'(Y,Z) = Z^{-1}[\widetilde{F}(-b^{-1}Y^n + b^{-1}aY^t, Z+Y) - \widetilde{F}(-b^{-1}Y^n + b^{-1}aY^t, Y)]$$

we see that $\mathrm{Disc}_Z(\widetilde{f}'(Y,Z)) \neq 0$ and $\mathrm{Gal}(\widetilde{f}'(Y,Z), k_0(Y))$ is the 1-point stabilizer of $\widetilde{G}$. Upon letting $F_{u-1}(Y,Z) = Z^{-1}[(Z+Y)^u - Y^u]$ for every integer $u > 0$, in view of the defining equations of $\bar{F}$ and $\widetilde{F}$, by the above two displayed equations we get

$$\bar{f}'(Y,Z) = F_{n-1}(Y,Z) - (Y^{n-t} + bY^{-t})F_{t-1}(Y,Z)$$

and

$$\widetilde{f}'(Y,Z) = F_{n-1}(Y,Z) - aF_{t-1}(Y,Z).$$

By comparing the above two equations with the defining equations of $\bar{F}'$ and $\widetilde{F}'$, we get

$$\bar{F}'(Y,Z) = Y^{n-1}\bar{f}'(Y^{-1}, Y^{-1}Z)$$

and

$$\widetilde{F}'(Y,Z) = Y^{n-1}\widetilde{f}'(Y^{-1}, Y^{-1}Z).$$

Now by writing (X,Y) for (Y,Z) we see that $\mathrm{Disc}_Y(\bar{F}'(X,Y)) \neq 0 \neq \mathrm{Disc}_Y(\widetilde{F}'(X,Y))$, and $\mathrm{Gal}(\bar{F}'(X,Y), k_0(X))$ and $\mathrm{Gal}(\widetilde{F}'(X,Y), k_0(X))$ are the 1-point stabilizers of $\bar{G}$ and $\widetilde{G}$ respectively. This completes the proof of (2.1.1).

Let $\bar{\xi}(Y) = -bf_{t-1}(Y)$ and $\bar{\eta}(Y) = f_{n-1}(Y) - f_{t-1}(Y)$. Also let $\widetilde{\xi}(Y) = -af_{t-1}(Y)$ and $\widetilde{\eta}(Y) = f_{n-1}(Y)$.

Since $\mathrm{GCD}(n,t) = 1$, for any $y \in k$ with $y^n = 1 = y^t$ we must have $y = 1$. Therefore 1 is the only common root of $Y^n - 1$ and $Y^t - 1$ in k. It follows $(Y-1)^{-1}(Y^n - 1)$ and $(Y-1)^{-1}(Y^t - 1)$ are nonzero coprime polynomials in

$k[Y]$. Therefore by applying the k-automorphism $Y \mapsto Y+1$ of $k[Y]$ we see that $f_{n-1}(Y)$ and $f_{t-1}(Y)$ are nonzero coprime polynomials in $k[Y]$. It follows that $\bar{\xi}(Y)$ and $\bar{\eta}(Y)$ are nonzero coprime polynomials in $k[Y]$. It also follows that $\widetilde{\xi}(Y)$ and $\widetilde{\eta}(Y)$ are nonzero coprime polynomials in $k[Y]$.

It is clear that if n is nondivisible by $\operatorname{char} k$ then (Y^n-1) is devoid of multiple roots in k, and hence so is $(Y-1)^{-1}(Y^n-1)$. On the other hand, if n is divisible by but not a power of $\operatorname{char} k$ then $Y^n-1=(Y^{n''}-1)^{n'}$ with integer $n''>1$ nondivisible by $\operatorname{char} k$ and integer $n'>1$ which is a power of $\operatorname{char} k$, and we can take a root $z\neq 1$ of $Y^{n''}-1$ in k and for any such root, in $k[Y]$, the polynomial $(Y-1)^{-1}(Y^n-1)$ is divisible by $(Y-z)^{n'}$ but not by $(Y-z)^{1+n'}$.

Since $n>1$, by applying the k-automorphism $Y\mapsto Y+1$ of $k[Y]$ we can find a monic polynomial $\psi_n(Y)\in k[Y]$ of degree 1 (hence irreducible) such that upon letting n^* to be the largest integer for which $\psi_n(Y)^{n^*}$ divides $f_{n-1}(Y)$ in $k[Y]$ we have that: if n is nondivisible by $\operatorname{char} k$ then $n^*=1$, whereas if n is divisible by but not a power of $\operatorname{char} k$ then $n^*=$ the highest power of $\operatorname{char} k$ which divides n; note that since $\operatorname{GCD}(n,t)=1$, in both the situations we have $\operatorname{GCD}(n-t,n^*)=1$; also note that n^* is the largest integer for which $\psi_n(Y)^{n^*}$ divides $\widetilde{\xi}(Y)\widetilde{\eta}(Y)$ in $k[Y]$. Similarly, in case $t\neq 1$, we can find a monic polynomial $\psi_t(Y)\in k[Y]$ of degree 1 (hence irreducible) such that upon letting t^* to be the largest integer for which $\psi_t(Y)^{t^*}$ divides $f_{t-1}(Y)$ in $k[Y]$ we have that: if t is nondivisible by $\operatorname{char} k$ then $t^*=1$, whereas if t is divisible by but not a power of $\operatorname{char} k$ then $t^*=$ the highest power of $\operatorname{char} k$ which divides t; note that since $\operatorname{GCD}(n,t)=1$, in both the situations we have $\operatorname{GCD}(n-t,t^*)=1=\operatorname{GCD}(n,t^*)$; also note that t^* is the largest integer for which $\psi_t(Y)^{t^*}$ divides $\widetilde{\xi}(Y)\widetilde{\eta}(Y)$ in $k[Y]$, and t^* is the largest integer for which $\psi_t(Y)^{t^*}$ divides $\bar{\xi}(Y)\bar{\eta}(Y)$ in $k[Y]$.

If $t=1$ and $n-t$ is a power of $\operatorname{char} k$ then clearly $\bar{\eta}(Y)=Y^{n-2}(Y+1)$ and hence, in $k[Y]$, the polynomial $\bar{\xi}(Y)\bar{\eta}(Y)$ is divisible by $(Y+1)$ but not by $(Y+1)^2$. Now upon letting $(\bar{\phi}(Y),N)=(\psi_t(Y),t^*)$ or $(Y+1,1)$ according as $t\neq 1$ and t is not a power of $\operatorname{char} k$ or $t=1$ and $n-t=$ is a power of $\operatorname{char} k$, in both the situations we see that $\operatorname{GCD}(n,t)=1$ and $\bar{\phi}(Y)$ is a non-constant irreducible polynomial in $k[Y]$ and N is the largest integer for which $\bar{\phi}(Y)^N$ divides $\bar{\xi}(Y)\bar{\eta}(Y)$ in $k[Y]$, and therefore by taking $(X,Y,n,0,\bar{\xi},\bar{\eta},\bar{\phi},N)$ for $(Y,Z,\lambda,\mu,\xi,\eta,\phi_1,\nu_1)$ in the First Irreducibility Lemma on page 101 of [Ab4] we conclude that the polynomial $\bar{F}'(X,Y)$ is irreducible in $k(X)[Y]$ and hence also in $k_0(X)[Y]$. Consequently, in view of (2.1.1), we see that

(1) if $t \neq 1$ and t is not a power of $\operatorname{char} k$ then $\bar{G}$ is doubly transitive,

and also that

(2) if $t = 1$ and $n - t$ is a power of $\operatorname{char} k$ then $\bar{G}$ is doubly transitive.

Note that (1) implies that

(3) if $1 < t \not\equiv 0 \pmod{\operatorname{char} k}$ then $\bar{G}$ is doubly transitive,

and (2) implies (the trivial assertion) that

(4) if $n = 2$ then $\bar{G}$ is doubly transitive.

By reciprocation (i.e., by sending Y to Y^{-1}) we see that $\operatorname{Gal}(Y^n - aXY^t + b, k_0(X))$ and $\operatorname{Gal}(Y^n - aXY^{n-t} + b, k_0(X))$ are isomorphic to each other, and $\operatorname{GCD}(n,t) = 1$ implies that $\operatorname{GCD}(n, n-t) = 1$ and either $t \not\equiv 0 \pmod{\operatorname{char} k}$ or $n - t \not\equiv 0 \pmod{\operatorname{char} k}$; therefore in view of (3) we see that

(5) if $1 < t < n - 1$ then $\bar{G}$ is doubly transitive.

Again by reciprocation, in view of (1), we see that

(6) if $n - t \neq 1$ and $n - t$ is not a power of $\operatorname{char} k$ then $\bar{G}$ is doubly transitive.

By (2), (4) and (6) we conclude that

(7) if $t = 1$ then $\bar{G}$ is doubly transitive.

By reciprocation, in view of (7), we see that

(8) if $t = n - 1$ then $\bar{G}$ is doubly transitive.

By (5), (7) and (8) we get (2.1.2).

Now $\operatorname{GCD}(n,t) = 1$ implies that if n is a power of $\operatorname{char} k$ then t cannot be divisible by $\operatorname{char} k$. Consequently, upon letting $(\tilde{\phi}(Y), T) = (\psi_n(Y), n^*)$ or $(\psi_t(Y), t^*)$ according as n is not a power of $\operatorname{char} k$ or $t \neq 1$ and n is a power of $\operatorname{char} k$, we see that $\operatorname{GCD}(n - t, T) = 1$ and $\tilde{\phi}(Y)$ is a nonconstant irreducible polynomial in $k[Y]$ and T is the largest integer such that $\tilde{\phi}(Y)^T$ divides $\tilde{\xi}(Y)\tilde{\eta}(Y)$ in $k[Y]$, and therefore by taking $(X, Y, n-t, 0, \tilde{\xi}, \tilde{\eta}, \tilde{\phi}, T)$ for $(Y, Z, \lambda, \mu, \xi, \eta, \phi_1, \nu_1)$ in the First Irreducibility Lemma on page 101 of [Ab4] we conclude that the polynomial $\tilde{F}'(X,Y)$ is irreducible in $k(X)[Y]$ and hence also in $k_0(X)[Y]$. Consequently, in view of (2.1.1), we see that (1*) if $t \neq 1$ then $\tilde{G}$ is doubly transitive, and also that (2*) if $t = 1$ and n is not a power of $\operatorname{char} k$ then $\tilde{G}$ is doubly transitive. By (1*) and (2*) we get (2.1.3).

If $t = 1$, n is a power of $\operatorname{char} k$, $\operatorname{GF}(n) \subset k_0$, and $\alpha^{n-1} = a$ for some $\alpha \in k_0$, then

$$\alpha^{-n}\tilde{F}(X, \alpha Y) = Y^n - Y + \alpha^{-n}bX$$

and hence by taking $(n, \alpha^{-n}bX)$ for (p^m, x) in (7.1**) of Section 7 of [Ab7] we get $\tilde{G} = \operatorname{GF}(n)^+$; since $\tilde{G}$ is abelian, it must be sharply 1-transitive and hence it

cannot be doubly transitive unless $n = 2$. This proves (2.1.4).

To prove (2.1.5), for a moment assume that $t = n-1$ and n is a power of $\operatorname{char} k$ and $\mathrm{GF}(n) \subset k_0$. Let

$$\widehat{F} = \widehat{F}(X,Y) = Y^n - aXY + X \quad \text{and} \quad \widehat{F}' = \widehat{F}'(X,Y) = Y^{n-1} - aX^n(aX-1)^{-1}.$$

Then

$$\widehat{F}(X,Y) = XY^n\widetilde{F}(b^{-1}X^{-1}, Y^{-1})$$

and by solving $\widehat{F} = 0$ we get $X = Y^n(aY-1)^{-1}$ and we have

$$\widehat{F}'(Y,Z) = Z^{-1}[\widehat{F}(Y^n(aY-1)^{-1}, Z+Y) - \widehat{F}(Y^n(aY-1)^{-1}, Y)].$$

Therefore $\mathrm{Disc}_Y(\widehat{F}) \neq 0$ and $\mathrm{Gal}(\widehat{F}, k_0(X)) = \widetilde{G}$, and $\mathrm{Disc}_Y(\widehat{F}') \neq 0$ and $\mathrm{Gal}(\widehat{F}', k_0(X))$ is the 1-point stabilizer of $\mathrm{Gal}(\widehat{F}, k_0(X))$. By the First Irreducibility Lemma on page 101 of [Ab4] we see that $\widehat{F}'$ is irreducible in $k_0(X)[Y]$. Moreover, since $\mathrm{GF}(n) \subset k_0$, we get $\mathrm{Gal}(\widehat{F}', k_0(X)) = \mathrm{GF}(n)^*$. Therefore $\mathrm{Gal}(\widehat{F}', k_0(X))$ is sharply 1-transitive. Consequently $\widetilde{G}$ is sharply 2-transitive and hence by Zassenhaus' Theorem (see page 78 of [Ab4]) $\widetilde{G} = \mathrm{AGLNF}(1, \Psi)$ for some finite near-field Ψ. Now the 1-point stabilizer of $\mathrm{AGLNF}(1, \Psi)$ is the underlying multiplicative group Ψ^* of Ψ; moreover Ψ^* is abelian if and only if Ψ is a field. Since the 1-point stabilizer of $\widetilde{G}$ is abelian, we must have $\widetilde{G} = \mathrm{AGL}(1, n)$. This proves (2.1.5). To explain the bracketed remark in (2.1.5), note that $X^n\widehat{F}(X^{1-n}, X^{-1}Y) = Y^n - aY + X$ and hence, by the Substitutional Principle on page 98 of [Ab4], we have $\mathrm{Gal}(Y^n - aY + X, k_0(X)) \triangleleft \widetilde{G}$ with $\widetilde{G}/\mathrm{Gal}(Y^n - aY + X, k_0(X)) = \mathrm{GF}(n)^*/M$ for some $M \triangleleft \mathrm{GF}(n)^*$ and, assuming $\alpha^{n-1} = a$ for some $\alpha \in k_0$, by (2.1.4) we get $\mathrm{Gal}(Y^n - aY + X) = \mathrm{GF}(n)^+$ and therefore we must have $M = 1$.

To prove (2.1.6) and (2.1.7), henceforth assume that $t = 1$ and $n - 1 = q = p^u$ with positive integer u and $\operatorname{char} k = p \neq 0$. Now $\widetilde{F}' = Y^q + Y^{q-1} + 1 - aX^q$ and hence (either obviously or by the Substitutional Principle on page 98 of [Ab4]) we see that $\widetilde{G}' = \mathrm{Gal}(\widetilde{F}', k_0(X)) = \mathrm{Gal}(Y^q + Y^{q-1} + 1 - aX, k_0(X)) = \mathrm{Gal}(Y^q + Y^{q-1} + X, k_0(X))$ and therefore by (2.1.5) we get $\widetilde{G}' = \mathrm{AGL}(1, q)$. Consequently $\widetilde{G}$ is sharply 3-transitive and hence by the Zassenhaus–Feit–Suzuki Theorem (see page 83 of [Ab4]) we see that either $\widetilde{G} = \mathrm{PGL}(2, q)$ or q is an even power of an odd prime p and $\widetilde{G} = \mathrm{PML}(2, q)$. By the description given on

page 163 of [HuB] we see that the 2-point stabilizer of $\mathrm{PML}(2,q)$ is nonabelian. Therefore we must have $\widetilde{G} = \mathrm{PGL}(2,q)$. In Section 21 of [Ab4] it is proved that

$$\mathrm{Gal}(Y^{q+1} - XY + 1, k(X)) = \mathrm{PSL}(2,q).$$

Since $b^{-1}\bar{F}(a^{-1}b^{q/(q+1)}X, b^{1/(q+1)}Y) = Y^{q+1} - XY + 1$, we get $\mathrm{Gal}(\bar{F}, k(X)) = \mathrm{Gal}(Y^{q+1} - XY + 1, k(X))$. Since $k_0 \subset k$, we also get $\mathrm{Gal}(\bar{F}, k(X)) < \mathrm{Gal}(\bar{F}, k_0(X))$. Therefore $\mathrm{PSL}(2,q) = \mathrm{Gal}(\bar{F}, k(X)) < \bar{G}$. Finally, by reciprocation we get $\mathrm{Gal}(Y^{q+1} - aXY^q + b, k_0(X)) = \mathrm{Gal}(Y^{q+1} - ab^{-1}XY + b^{-1}, k_0(X)) = \bar{G}$. This completes the proof of (2.1.6) and (2.1.7).

SYLOW SUBGROUP LEMMA 2.2: *Let $H < A_7$ with $|H| \equiv 0 \pmod{14}$ where A_7 is the alternating group on $\{1,2,\ldots,7\}$. Then a 2-Sylow subgroup P of H cannot be normal in H.*

Proof: Since $14 \equiv 0 \pmod 7$, H contains a seven cycle σ. Since $14 \equiv 0 \pmod 2$, we have $P \neq 1$. Since the order of P is a power of 2, P is contained in a 2-Sylow subgroup Q of A_7. Let A_6^i be the alternating group on $\{1,\ldots,i-1,i+1,\ldots,7\}$ regarded as a subgroup of A_7, and let P' be a 2-Sylow subgroup of A_6^1. Since $[A_7\colon A_6^1] = 7 \not\equiv 0 \pmod 2$, P' is a 2-Sylow subgroup Q' of A_7. Therefore $Q = \tau^{-1}Q'\tau$ for some $\tau \in A_7$. Let $j = \tau(1)$. Then $Q \subset A_6^j$. Since $P \neq 1$, we can find $\pi \in P$ and $l \in \{1,2,\ldots,7\}$ such that $\pi(l) \neq l$. Since σ is a seven cycle, for some integer e we have $\sigma^e(l) = j$. It follows that $(\sigma^{-1}\pi\sigma)(j) \neq j$, and hence $\sigma^{-1}\pi\sigma \notin A_6^j$. Since $P \subset Q \subset A_6^j$, we get $\sigma^{-1}\pi\sigma \notin P$. Since $\pi \in P$ and $\sigma \in H$, P cannot be normal in H.

TRANSVECTION LEMMA 2.3: *Given any integer $m > 1$, let ϕ: $\mathrm{GL}(m,q) \to \mathrm{PGL}(m,q)$ be the canonical epimorphism. Then for any $H < \mathrm{GL}(m,q)$ we have that: $\mathrm{SL}(m,q) < H \Leftrightarrow \mathrm{PSL}(m,q) < \phi(H)$.*

Proof: $\Rightarrow$ is obvious. To prove $\Leftarrow$ let any $H < \mathrm{GL}(m,q)$ with $\mathrm{PSL}(m,q) < \phi(H)$ be given. We are going to use the well-known fact (cf. Theorem 9.2 on page 74 of [Suz]) that the transvections $\{I + \lambda E_{ij}\colon i \neq j, \lambda \in \mathrm{GF}(q)\}$ generate $\mathrm{SL}(m,q)$, where I is the m by m identity matrix and E_{ij} is the m by m matrix with 1 in the (i,j)-th spot and zero elsewhere. Fix $i \neq j$, and let $D = \{cI\colon 0 \neq c \in \mathrm{GF}(q)\}$ and $D_{ij} = \{I + \lambda E_{ij}\colon \lambda \in \mathrm{GF}(q)\}$. For all c, c', λ, λ' in $\mathrm{GF}(q)$ we clearly have $(cI + \lambda E_{ij})(c'I + \lambda' E_{ij}) = cc'I + (c\lambda' + c'\lambda)E_{ij}$. It follows that $D = \ker\phi < \mathrm{GL}(m,q)$ and $D_{ij} < \mathrm{SL}(m,q)$, and $c \mapsto cI$ and $\lambda \mapsto I + \lambda E_{ij}$ give isomorphisms

$\mathrm{GF}(q)^* \to D$ and $\mathrm{GF}(q)^+ \to D_{ij}$ respectively. Let

$$J_{ij} = \{cI + \lambda E_{ij} \colon 0 \neq c \in \mathrm{GF}(q), \lambda \in \mathrm{GF}(q)\}.$$

Then $J_{ij} = \{c[I+\lambda E_{ij}] \colon 0 \neq c \in \mathrm{GF}(q), \lambda \in \mathrm{GF}(q)\}$ and for all c, c', λ, λ' in $\mathrm{GF}(q)$ with $c \neq 0 \neq c'$ we have $(c[I + \lambda E_{ij}])(c'[I + \lambda' E_{ij}]) = cc'I + cc'(\lambda + \lambda')E_{ij}$, and hence $J_{ij} = DD_{ij} = D \times D_{ij} < \mathrm{GL}(m, q)$ where $D \times D_{ij}$ is internal direct product. Let $\psi \colon J_{ij} \to D_{ij}$ be the projection map. Since $|D| = q - 1$ and $|D_{ij}| = q$, we have $\mathrm{GCD}(|D|, |D_{ij}|) = 1$. Consequently by the General Subgroup Lemma (cf. [Ab8] or (4.19) on page 141 of [Suz]), every subgroup of J_{ij} whose image under ψ is D_{ij} must contain D_{ij}. Since $\ker \phi = \ker \psi$ and $\phi(J_{ij}) < \mathrm{PSL}(m, q) < \phi(H)$, we get $H \cap J_{ij} < J_{ij}$ with $\psi(H \cap J_{ij}) = D_{ij}$, and hence $D_{ij} < (H \cap J_{ij})$. Therefore $D_{ij} < H$. This being so for all $i \neq j$, we conclude that $\mathrm{SL}(m, q) < H$.

COMPOSITE POLYNOMIAL LEMMA 2.4: *Let $V = V(Y)$, $W = W(Y)$, $E = E(Y)$ be monic polynomials of degrees $v > 0$, $w > 0$, $e > 0$ in Y with coefficients in a field K, respectively, such that $\mathrm{Disc}_Y(V) \neq 0$ and $V(Y) = W(E(Y))$. Let R_V and R_W be the roots of V and W in an algebraic closure $\bar{K}$ of K, respectively. Then we have the following.*

(1) $\mathrm{Disc}_Y(W) \neq 0$ *(equivalently $|R_W| = w$), and upon letting $R_W = \{\Theta_i \colon 1 \leq i \leq w\}$ and $\Lambda_i = \{S \in \bar{K} \colon E(S) = \Theta_i\}$ we have that $R_V = \bigcup_{i=1}^{w} \Lambda_i$ is a disjoint partition of R_V with $|R_V| = v = we$ and $|\Lambda_i| = e$ for $1 \leq i \leq w$.*

(2) *$K(R_V) \supset K(R_W)$ where these are the respective splitting fields of V and W over K in $\bar{K}$. Thinking of $\mathrm{Gal}(K(R_V), K)$ and $\mathrm{Gal}(K(R_W), K)$ as the group of all K-automorphisms of $K(R_V)$ and $K(R_W)$ respectively, for every $g \in \mathrm{Gal}(K(R_V), K)$ we have $g(K(R_W)) = K(R_W)$ and, upon letting g^* to be the bijection of $K(R_W)$ onto itself such that $g^*(S) = g(S)$ for all $S \in K(R_W)$, we have $g^* \in \mathrm{Gal}(K(R_W), K)$. Moreover $g \mapsto g^*$ gives the usual Galois theory group epimorphism whose kernel is $\mathrm{Gal}(K(R_V), K(R_W))$.*

(3) *Thinking of $\mathrm{Gal}(V, K)$ as a permutation group on R_V, given any $g \in \mathrm{Gal}(K(R_V), K)$ we have $g(R_V) = R_V$ and, upon letting g_V to be the permutation of R_V such that $g_V(S) = g(S)$ for all $S \in R_V$, we have $g_V \in \mathrm{Gal}(V, K)$. Moreover $g \mapsto g_V$ gives a group isomorphism $\mathrm{Gal}(K(R_V), K) \to \mathrm{Gal}(V, K)$ (which is the usual permutation representation).*

(4) *Thinking of $\mathrm{Gal}(W, K)$ as a permutation group on R_W, given any $g \in \mathrm{Gal}(K(R_W), K)$ we have $g(R_W) = R_W$ and, upon letting g_W to be the permutation of R_W such that $g_W(S) = g(S)$ for all $S \in R_W$, we have $g_W \in$*

$\mathrm{Gal}(W, K)$. *Moreover* $g \mapsto g_W$ *gives a group isomorphism* $\mathrm{Gal}(K(R_W), K) \to \mathrm{Gal}(W, K)$ *(which is the usual permutation representation).*

(5) *Given any* $g \in \mathrm{Gal}(K(R_V), K)$ *we have* $g(R_W) = R_W$ *and upon letting* $g_{V,W}$ *to be the permutation of* R_W *such that* $g_{V,W}(S) = g(S)$ *for all* $S \in R_W$, *we have* $g_{V,W} \in \mathrm{Gal}(W, K)$. *Moreover* $g \mapsto g_{V,W}$ *gives a group epimorphism* $\mathrm{Gal}(K(R_V), K) \to \mathrm{Gal}(W, K)$ *whose kernel is* $\mathrm{Gal}(K(R_V), K(R_W))$.

(6) *Given any* $\gamma \in \mathrm{Gal}(V, K)$, *for every* $i \in \{1, \ldots, w\}$ *we have* $\gamma(\Lambda_i) = \Lambda_j$ *for some* $j \in \{1, \ldots, w\}$ *and, upon letting* γ' *to be the permutation of* R_W *such that* $\gamma'(\Theta_i) = \Theta_j$ *for all* $i \in \{1, \ldots, w\}$, *we have* $\gamma' \in \mathrm{Gal}(W, K)$. *Moreover* $\gamma \mapsto \gamma'$ *gives a group epimorphism* $\mathrm{Gal}(V, K) \to \mathrm{Gal}(W, K)$ *whose kernel is* $\mathrm{Gal}(V, K(R_W))$.

(7) *For every* $g \in \mathrm{Gal}(K(R_V), K)$ *we have* $g_{V,W} = (g^*)_W = (g_V)'$.

(8) *If* $E(Y) = Y^e$ *then for some* $\Lambda \in K(R_V)$ *we have* $\Lambda^e = (-1)^w V(0)$.

Proof: We can first write $W(Y) = \prod_{i=1}^{w}(Y - \Theta_i')$ with $\Theta_i' \in \bar{K}$, and then we can write $E(Y) - \Theta_i' = \prod_{j=1}^{e}(Y - \Lambda_{ij})$ with $\Lambda_{ij} \in \bar{K}$. Since $V(Y) = W(E(Y))$, we get $V(Y) = \prod_{j=1}^{e}\prod_{i=1}^{w}(Y - \Lambda_{ij})$. Since $\mathrm{Disc}_Y(V) \neq 0$, we must have $\Lambda_{ij} \neq \Lambda_{i'j'}$ whenever $(i, j) \neq (i', j')$. This proves (1) with $\Theta_i = \Theta_i'$ and $\Lambda_i = \{\Lambda_{ij} \colon 1 \leq j \leq e\}$ for $1 \leq i \leq w$.

Since $E(Y) \in K[Y]$ and $\{E(S) \colon S \in R_V\} = R_W$, we get $K(R_V) \supset K(R_W)$ and then the rest of (2) is obvious.

Items (3) to (5) are obvious. Items (6) and (7) follow from items (1) to (5).

If $E(Y) = Y^e$ then upon letting $\Lambda = \Lambda_{11} \cdots \Lambda_{w1}$ we get $\Lambda \in K(R_V)$ with $\Lambda^e = \Theta_1' \cdots \Theta_w' = (-1)^w V(0)$ which proves (8).

PROJECTIVE SPACE LEMMA 2.5: *In the situation of 2.4, assume that* K *is an overfield of* $\mathrm{GF}(q)$. *Also assume that* $E(Y) = Y^{q-1}$, *and assume that upon letting* $U(Y) = YV(Y)$ *we have* $U = U(Y) = Y^{q^m} + \sum_{i=1}^{m} C_i Y^{q^{m-i}}$ *where* $m > 1$ *is an integer and* $C_1, \ldots, C_m$ *are elements in* K *with* $C_m \neq 0$. *Let* R_U *be the roots of* U *in* $\bar{K}$ *and note that then* $R_U = \{0\} \cup R_V$ *is a disjoint partition of* R_U, *and we have* $K(R_U) = K(R_V)$. *Let* $K(R_U)$ *be equipped with the structure of a vector space over* $\mathrm{GF}(q)$ *acquired in virtue of its being an overfield of* $\mathrm{GF}(q)$. *Then we have the following.*

(i) R_U *is an* m*-dimensional vector subspace of* $K(R_U)$ *and upon letting* $\mathrm{GL}(R_U)$ *to be the group of all vector space isomorphisms of* R_U, *which we regard as a permutation group on the nonzero vectors* R_V, *we have*

$\mathrm{Gal}(V, K) < \mathrm{GL}(R_U)$.

(ii) *For an m-dimensional vector space D over $\mathrm{GF}(q)$, let $D^* = D \setminus \{0\}$ be called an m-*__dimensional punctured vector space__ *over $\mathrm{GF}(q)$, and recall that an $(m-1)$-dimensional projective space over $\mathrm{GF}(q)$ is a set Δ together with a surjective map ψ: $D^* \to \Delta$ such that the inverse images of the points of Δ are exactly all the 1-dimensional punctured vector subspaces of D^*, and also recall that a projective transformation of Δ is a permutation of Δ induced by a vector space isomorphism of D and the set of all these permutations is the group $\mathrm{PGL}(\Delta)$, and finally recall that this gives a canonical group epimorphism ϕ: $\mathrm{GL}(D) \to \mathrm{PGL}(\Delta)$ whose kernel is $\mathrm{GF}(q)^*$. With all this in mind, we claim that $\Lambda_1, \ldots, \Lambda_w$ are exactly all the distinct 1-dimensional punctured vector subspaces of the m-dimensional punctured vector space R_V over $\mathrm{GF}(q)$, and by putting $\psi(S) = E(S) = S^{q-1}$ for all $S \in R_V$ we get a surjective map ψ: $R_V \to R_W = \{\Theta_1 \ldots, \Theta_w\}$ with $\psi^{-1}(\Theta_i) = \Lambda_i$ for $1 \leq i \leq w$ which makes R_W into an $(m-1)$-dimensional projective space over $\mathrm{GF}(q)$, and finally with this structure we have $\phi(\mathrm{Gal}(V, K)) = \mathrm{Gal}(W, K) < \mathrm{PGL}(R_W)$ where ϕ: $\mathrm{GL}(R_U) \to \mathrm{PGL}(R_W)$ is the canonical group epimorphism.*

(iii) *Without assuming K to be an overfield of $\mathrm{GF}(q)$, for some $\Lambda \in K(R_V)$ we have $\Lambda^{q-1} = (-1)^{1+q+\cdots+q^{m-1}} C_m$.*

Proof: Clearly $U(Y + Z) = U(Y) + U(Z)$ and for every $S \in \mathrm{GF}(q)$ we have $U(SY) = SU(Y)$. Therefore R_U is a vector subspace of $K(R_U)$. Since $|R_U| = q^m = |\mathrm{GF}(q)|^m$, the dimension of the said subspace must be m. The rest of (i) now follows from (3) of Lemma 2.4.

Now a 1-dimensional punctured vector subspace of $K(R_U)$ is a subset of $K(R_U)$ of the form $\{ST\colon 0 \neq S \in \mathrm{GF}(q)\}$ with $0 \neq T \in K(R_U)$. Equivalently, it is a set of the form $\{S \in \bar{K}\colon E(S) = T\} \subset K(R_U)$ with $0 \neq T \in K(R_U)$. Therefore (ii) follows from (i) and Lemma 2.4.

Finally, (iii) follows from (8) of Lemma 2.4.

COROLLARY 2.6: *A part of (2.1.7) can be strengthened by saying that, in the situation of 2.1, if $n-1$ is a positive power of* char k *and $\mathrm{GF}(n-1) \subset k_0$ and either $t = 1$ or $t = n-1$ then $\mathrm{PSL}(2, n-1) < \bar{G} < \mathrm{PGL}(2, n-1)$.*

Proof: Follows from (2.1.7) and part (ii) of Lemma 2.5.

3. Additive polynomials

Let K be a field of characteristic $p \neq 0$, let q be a positive power of p, let $m > 1$ be an integer, let $C_1, \ldots, C_m$ be elements in K with $C_m \neq 0$, and consider the polynomials

$$U = U(Y) = Y^{q^m} + \sum_{i=1}^{m} C_i Y^{q^{m-i}}$$

and

$$V = V(Y) = Y^{q^m-1} + \sum_{i=1}^{m} C_i Y^{q^{m-i}-1}$$

and

$$W = W(Y) = Y^{(q^m-1)/(q-1)} + \sum_{i=1}^{m} C_i Y^{(q^{m-i}-1)/(q-1)}.$$

Here U is an **additive polynomial**, i.e., a polynomial such that $U(Y+Z) = U(Y) + U(Z)$. Moreover, V is obtained by dividing U by Y, and W is obtained by substituting $Y^{1/(q-1)}$ for Y in V. Clearly $V + YV_Y = C_m = W - YW_Y$ with $0 \neq C_m \in K$, and hence $\mathrm{Disc}_Y(V) \neq 0 \neq \mathrm{Disc}_Y(W)$, and therefore $\mathrm{Gal}(V, K)$ and $\mathrm{Gal}(W, K)$ are well defined. Concerning these Galois groups we have the following.

PROPOSITION 3.1: *For some Λ in the splitting field of V over K we have $\Lambda^{q-1} = (-1)^{\nu} C_m$ where $\nu = 1 + q + \cdots + q^{m-1}$. Moreover, if $\mathrm{GF}(q) \subset K$ then, in a natural manner, we may regard $\mathrm{Gal}(V, K) < \mathrm{GL}(m, q)$ and $\mathrm{Gal}(W, K) < \mathrm{PGL}(m, q)$ in such a manner that $\phi(\mathrm{Gal}(V, K)) = \mathrm{Gal}(W, K)$ where ϕ: $\mathrm{GL}(m, q) \to \mathrm{PGL}(m, q)$ is the canonical epimorphism.*

Proof: Let R_U, R_V and R_W be the roots of U, V and W in an algebraic closure $\bar{K}$ of K, respectively. Now everything follows from Lemma 2.5 by identifying $\mathrm{GL}(R_U)$ and $\mathrm{PGL}(R_W)$ with $\mathrm{GL}(m, q)$ and $\mathrm{PGL}(m, q)$ respectively.

As a consequence of Lemmas 2.1–2.3 and Proposition 3.1 we shall now prove the following.

PROPOSITION 3.2: *Recall that k is an algebraically closed field of characteristic p, and let k_0 be a subfield of k such that k is an algebraic closure of k_0 and $\mathrm{GF}(q) \subset k_0$. Assume that $K = k_0(X)$. Let $1 \leq \mu < m$ be an integer such that $\mathrm{GCD}(\nu, \tau) = 1$ where $\nu = 1 + q + \cdots + q^{m-1}$ and $\tau = 1 + q + \cdots + q^{\mu-1}$. Assume that $C_{m-\mu} = -aX^{\rho}$ and $C_m = bX^{\sigma}$ where a and b are nonzero elements in k_0, and ρ and σ are integers such that $\rho \neq \sigma(\nu - \tau)/\nu$ (for instance $\rho \neq 0 = \sigma$ or*

$\rho = 0 \neq \sigma$). Also assume that $C_1 = \cdots = C_{m-\mu-1} = C_{m-\mu+1} = \cdots = C_{m-1} = 0$. Then we have the following.

(3.2.1) *We have* $\mathrm{PSL}(m,q) < \mathrm{Gal}(W,k(X)) < \mathrm{Gal}(W,k_0(X)) < \mathrm{PGL}(m,q)$ *and we have*

$$[\mathrm{Gal}(W,k(X))\colon \mathrm{PSL}(m,q)] \equiv 0 \quad \left(\mathrm{mod}\ \frac{\mathrm{GCD}(m,q-1)}{\mathrm{GCD}(\sigma,m,q-1)}\right).$$

Moreover, if $\sigma \in \nu\mathbb{Z}$ then $\mathrm{Gal}(W,k(X)) = \mathrm{PSL}(m,q)$. Likewise, if $\mathrm{GCD}(\sigma,m,q-1) = 1$ then $\mathrm{Gal}(W,k_0(X)) = \mathrm{PGL}(m,q)$.

(3.2.2) *The polynomial W is irreducible in $k(X)[Y]$, and $X = 0$ and $X = \infty$ are the only valuations of $k(X)/k$ which are possibly ramified in the splitting field of W over $k(X)$. Moreover, if $\rho > \sigma(\nu-\tau)/\nu$ and the valuation $X = 0$ of $k(X)/k$ is ramified in the splitting field of W over $k(X)$ then it is tamely ramified. Finally, if $\rho > \sigma(\nu-\tau)/\nu$ and $\sigma \in \nu\mathbb{Z}$ then $X = \infty$ is the only valuation of $k(X)/k$ which is ramified in the splitting field of W over $k(X)$.*

(3.2.3) *We have* $\mathrm{SL}(m,q) < \mathrm{Gal}(V,k(X)) < \mathrm{Gal}(V,k_0(X)) < \mathrm{GL}(m,q)$ *and we have* $[\mathrm{Gal}(V,k(X)) : \mathrm{SL}(m,q)] \equiv 0 \pmod{(q-1)/\mathrm{GCD}(\sigma,q-1)}$. *Moreover, if $\sigma \in (q-1)\nu\mathbb{Z}$ then $\mathrm{Gal}(V,k(X)) = \mathrm{SL}(m,q)$. Likewise, if $\mathrm{GCD}(\sigma,q-1) = 1$ then $\mathrm{Gal}(V,k_0(X)) = \mathrm{GL}(m,q)$.*

(3.2.4) *The polynomial V is irreducible in $k(X)[Y]$, and $X = 0$ and $X = \infty$ are the only valuations of $k(X)/k$ which are possibly ramified in the splitting field of V over $k(X)$. Moreover, if $\rho > \sigma(\nu-\tau)/\nu$ and the valuation $X = 0$ of $k(X)/k$ is ramified in the splitting field of V over $k(X)$ then it is tamely ramified. Finally, if $\rho > \sigma(\nu-\tau)/\nu$ and $\sigma \in (q-1)\nu\mathbb{Z}$ then $X = \infty$ is the only valuation of $k(X)/k$ which is ramified in the splitting field of V over $k(X)$.*

Proof: For a moment assume that $\rho = 1$ and $\sigma = 0$. If $m = 2$ then by (2.1.7) we get $\mathrm{Gal}(W,k(X)) = \mathrm{PSL}(2,q)$. So for a moment also assume that $m > 2$. Then by Proposition 3.1 we have $\mathrm{Gal}(W,k(X)) < \mathrm{PGL}(m,q)$, and by (2.1.2) we see that $\mathrm{Gal}(W,k(X))$ is 2-transitive. Now Theorem I of [CaK] says that: if G is a subgroup of the group $\Gamma\mathrm{L}(m,q)$ of semilinear transformations with $m > 2$ and if G is 2-transitive on the set of points of the projective space $\mathrm{PG}(m-1,q)$, then either $\mathrm{SL}(m,q) < G$ or G is A_7 inside $\mathrm{SL}(4,2)$. Therefore either $\mathrm{PSL}(m,q) < \mathrm{Gal}(W,k(X))$ or $(m,q) = (4,2)$ and $\mathrm{Gal}(W,k(X)) = A_7(15)$

where $A_7(15)$ is the representation of A_7 as a transitive permutation group of degree 15. If $(m,q) = (4,2)$ then $\nu = 15$ and, because $\mathrm{GCD}(\nu,\tau) = 1$, we have $\tau = 1$ or 7; now (obviously or by Proposition 1 on page 831 of [Ab1]) the $X = \infty$ valuation of $k(X)$ splits into the valuations $Y = \infty$ and $Y = 0$ of the root field of W over $k(X)$ and their respective ramification exponents are 14 and 1 in case $\tau = 1$, and 8 and 7 in case $\tau = 7$; in both the cases the order of an inertia group H of an extension of the $X = 0$ valuation to the splitting field of W over $k(X)$ is divisible by 14; also the inertia group H has a unique 2-Sylow subgroup P which is hence normal in H; therefore by Lemma 2.2 we cannot have $\mathrm{Gal}(W,k(X)) = A_7(15)$. Thus $\mathrm{PSL}(m,q) < \mathrm{Gal}(W,k(X)) < \mathrm{PGL}(m,q)$. Since $W - YW_Y = b$, we see that $X = \infty$ is the only valuation of $k(X)/k$ which is ramified in the splitting field of W and hence $\mathrm{Gal}(W,k(X))$ is quasi-p. But no group between $\mathrm{PSL}(m,q)$ and $\mathrm{PGL}(m,q)$, other than $\mathrm{PSL}(m,q)$, can be quasi-p. Therefore we must have $\mathrm{Gal}(W,k(X)) = \mathrm{PSL}(m,q)$. So we have shown that:

(1) If $\rho = 1$ and $\sigma = 0$ then $\mathrm{Gal}(W,k(X)) = \mathrm{PSL}(m,q)$.

Now $\mathrm{PSL}(m,q)$ is a nonabelian simple group except when $m = 2$ and $q = 2$ or 3 in which cases it equals S_3 and A_4 respectively. Therefore, in view of Corollaries (3.3), (3.4) and (3.8) of the Substitutional Principle on pages 99 and 100 of [Ab4], by (1) we get that:

(2) If $\rho \neq 0 = \sigma$ then $\mathrm{Gal}(W,k(X)) = \mathrm{PSL}(m,q)$.

In the general case, if $\sigma \in \nu\mathbb{Z}$, then upon letting $\rho' = \rho - \sigma(\nu - \tau)/\nu$ we have $0 \neq \rho' \in \mathbb{Z}$ and $X^{-\sigma}W(X^{\sigma/\nu}Y) = Y^\nu - aX^{\rho'}Y^\tau + b$ and hence $\mathrm{Gal}(W,k(X)) = \mathrm{Gal}(Y^\nu - aX^{\rho'}Y^\tau + b, k(X))$. Therefore by (2) we see that:

(3) If $\sigma \in \nu\mathbb{Z}$ then $\mathrm{Gal}(W,k(X)) = \mathrm{PSL}(m,q)$.

In the completely general case, upon letting $\rho'' = \nu\rho$ and $\sigma'' = \nu\sigma$ we have $\rho'' \in \mathbb{Z}$ and $\sigma'' \in \nu\mathbb{Z}$ with $\rho'' \neq \sigma''(\nu - \tau)/\nu$ and hence, in view of Corollary (3.1) of the Substitutional Principle on page 99 of [Ab4], by (3) we get $\mathrm{PSL}(m,q) = \mathrm{Gal}(Y^\nu - aX^{\rho''}Y^\tau + bX^{\sigma''}, k(X)) < \mathrm{Gal}(W,k(X))$. Since $k_0 \subset k$, we also have $\mathrm{Gal}(W,k(X)) < \mathrm{Gal}(W,k_0(X))$. Since $\mathrm{GF}(q) \subset k_0$, by Proposition 3.1 we get $\mathrm{Gal}(W,k_0(X)) < \mathrm{PGL}(m,q)$. Thus:

(4) $\mathrm{PSL}(m,q) < \mathrm{Gal}(W,k(X)) < \mathrm{Gal}(W,k_0(X)) < \mathrm{PGL}(m,q)$.

By (4) it follows that:

(5) The polynomial W is irreducible in $k(X)[Y]$.

Since $W - YW_Y = bX^\sigma$, we see that:

(6) $X = 0$ and $X = \infty$ are the only valuations of $k(X)/k$ which are possibly

ramified in the splitting field of W over $k(X)$.

Since $W - YW_Y = bX^\sigma$, we also see that:

(7) If $\rho > 0 = \sigma$ then $X = \infty$ is the only valuation of $k(X)/k$ which is possibly ramified in the splitting field of W over $k(X)$.

If $\rho > \sigma(\nu - \tau)/\nu$ and $\sigma \in \nu\mathbb{Z}$ then upon letting $\rho' = \rho - \sigma(\nu - \tau)/\nu$ we have $0 < \rho' \in \mathbb{Z}$ and $X^{-\sigma}W(X^{\sigma/\nu}Y) = Y^\nu - aX^{\rho'}Y^\tau + b$. Hence by (7) we see that:

(8) If $\rho > \sigma(\nu - \tau)/\nu$ and $\sigma \in \nu\mathbb{Z}$ then $X = \infty$ is the only valuation of $k(X)/k$ which is ramified in the splitting field of W over $k(X)$.

By (8) we see that if $\rho > \sigma(\nu - \tau)/\nu$ then the valuation $X = 0$ of $k(X)/k$ is unramified in the splitting field of $Y^\nu - aX^{\nu\rho}Y^\tau + bX^{\nu\sigma}$ over $k(X)$. From this it follows that:

(9) If $\rho > \sigma(\nu - \tau)/\nu$ and the valuation $X = 0$ of $k(X)/k$ is ramified in the splitting field of W over $k(X)$ then it is tamely ramified.

In view of Proposition 3.1, by (4) we see that:

(10) $\mathrm{SL}(m, q) < \mathrm{Gal}(V, k(X)) < \mathrm{Gal}(V, k_0(X)) < \mathrm{GL}(m, q)$.

By (10) it follows that:

(11) The polynomial V is irreducible in $k(X)[Y]$.

Since $V + YV_Y = bX^\sigma$, we see that:

(12) $X = 0$ and $X = \infty$ are the only valuations of $k(X)/k$ which are possibly ramified in the splitting field of V over $k(X)$.

Since $V + YV_Y = bX^\sigma$, we also see that:

(13) If $\rho > 0 = \sigma$ then $X = \infty$ is the only valuation of $k(X)/k$ which is ramified in the splitting field of V over $k(X)$.

If $\rho > \sigma(\nu - \tau)/\nu$ and $\sigma \in (q-1)\nu\mathbb{Z}$ then upon letting $\rho' = \rho - \sigma(\nu - \tau)/\nu$ we have $0 < \rho' \in \mathbb{Z}$ and $X^{-\sigma}V(X^{\sigma/((q-1)\nu)}Y) = Y^{(q-1)\nu} - aX^{\rho'}Y^{(q-1)\tau} + b$. Hence by (13) we see that:

(14) If $\rho > \sigma(\nu - \tau)/\nu$ and $\sigma \in (q-1)\nu\mathbb{Z}$ then $X = \infty$ is the only valuation of $k(X)/k$ which is ramified in the splitting field of V over $k(X)$.

By (14) we see that if $\rho > \sigma(\nu - \tau)/\nu$ then the valuation $X = 0$ of $k(X)/k$ is unramified in the splitting field of $Y^{(q-1)\nu} - aX^{(q-1)\nu\rho}Y^{(q-1)\tau} + bX^{(q-1)\nu\sigma}$ over $k(X)$. From this it follows that:

(15) If $\rho > \sigma(\nu - \tau)/\nu$ and the valuation $X = 0$ of $k(X)/k$ is ramified in the splitting field of V over $k(X)$ then it is tamely ramified.

If $\rho > \sigma(\nu - \tau)/\nu$ and $\sigma \in (q-1)\nu\mathbb{Z}$ then by (14) we see that $\mathrm{Gal}(V, k(X))$ is quasi-p. But no group between $\mathrm{SL}(m, q)$ and $\mathrm{GL}(m, q)$, other than $\mathrm{SL}(m, q)$, can

be quasi-p. Therefore, in view of (10), we conclude that:

(16) If $\rho > \sigma(\nu-\tau)/\nu$ and $\sigma \in (q-1)\nu\mathbb{Z}$ then $\mathrm{Gal}(V, k(X)) = \mathrm{SL}(m,q)$.

By Proposition 3.1 there exists an element X' in a splitting field of V over $k(X)$ with $X'^d = X$ where $d = (q-1)/\mathrm{GCD}(\sigma, q-1)$. Let $V' = V'(Y) = Y^{(q-1)\nu} - aX'^{d\rho}Y^{(q-1)\tau} + bX'^{d\sigma}$. Then $k(X')/k(X)$ is a Galois extension whose Galois group is the cyclic group Z_d of order d, and we have $\mathrm{Gal}(V', k(X')) \lhd \mathrm{Gal}(V, k(X))$ with $\mathrm{Gal}(V, k(X))/\mathrm{Gal}(V', k(X')) = \mathrm{Gal}(k(X'), k(X))$. By (10) we also have $\mathrm{SL}(m,q) < \mathrm{Gal}(V', k(X')) \lhd \mathrm{Gal}(V, k(X)) < \mathrm{Gal}(V, k_0(X)) < \mathrm{GL}(m,q)$. Therefore $[\mathrm{Gal}(V, k(X)) : \mathrm{SL}(m,q)] \equiv 0 \pmod{d}$. Thus:

(17) $[\mathrm{Gal}(V, k(X)) : \mathrm{SL}(m,q)] \equiv 0 \pmod{(q-1)/\mathrm{GCD}(\sigma, q-1)}$.

Since $\mathrm{GL}(m,q)/\mathrm{SL}(m,q) = Z_{q-1}$, by (10) and (17) we see that:

(18) If $\mathrm{GCD}(\sigma, q-1) = 1$ then $\mathrm{Gal}(V, k_0(X)) = \mathrm{GL}(m,q)$.

Since $\mathrm{GL}(m,q)/\mathrm{SL}(m,q) = Z_{q-1}$ and $\mathrm{PGL}(m,q)/\mathrm{PSL}(m,q) = Z_l$ with $l = \mathrm{GCD}(m, q-1)$, in view of Proposition 3.1, by (10) and (17) we see that:

(19) $[\mathrm{Gal}(W, k(X)) : \mathrm{PSL}(m,q)] \equiv 0 \pmod{\mathrm{GCD}(m, q-1)/\mathrm{GCD}(\sigma, m, q-1)}$.

Since $\mathrm{PGL}(m,q)/\mathrm{PSL}(m,q) = Z_l$, by (4) and (19) we see that:

(20) If $\mathrm{GCD}(\sigma, m, q-1) = 1$ then $\mathrm{Gal}(W, k_0(X)) = \mathrm{PGL}(m,q)$.

This completes the proof of the proposition.

From the above proposition, by reciprocation, we shall now deduce the following.

PROPOSITION 3.3: *Recall that k is an algebraically closed field of characteristic p, and let k_0 be a subfield of k such that k is an algebraic closure of k_0 and $\mathrm{GF}(q) \subset k_0$. Assume that $K = k_0(X)$. Let $1 \le \mu < m$ be an integer such that $\mathrm{GCD}(\nu, \tau^*) = 1$ where $\nu = 1 + q + \cdots + q^{m-1}$ and $\tau^* = q^\mu + q^{\mu+1} + \cdots + q^{m-1}$. Let a^* and b^* be nonzero elements in k_0, and let ρ^* and σ^* be integers such that $\rho^* \not\equiv \sigma^*(\nu-\tau^*)/\nu$ (for instance $\rho^* \not\equiv 0 \equiv \sigma^*$ or $\rho^* \equiv 0 \not\equiv \sigma^*$). Let $W^* = W^*(Y) = Y^\nu - a^*X^{\rho^*}Y^{\tau^*} + b^*X^{\sigma^*}$ and $V^* = V^*(Y) = Y^{(q-1)\nu} - a^*X^{\rho^*}Y^{(q-1)\tau^*} + b^*X^{\sigma^*}$. Then we have the following.*

(3.3.1) *We have*

$$\mathrm{PSL}(m,q) < \mathrm{Gal}(W^*, k(X)) < \mathrm{Gal}(W^*, k_0(X)) < \mathrm{PGL}(m,q)$$

and we have

$$[\mathrm{Gal}(W^*, k(X)) : \mathrm{PSL}(m,q)] \equiv 0 \quad \left(\mathrm{mod}\ \frac{\mathrm{GCD}(m, q-1)}{\mathrm{GCD}(\sigma^*, m, q-1)}\right).$$

Moreover, if $\sigma^* \in \nu\mathbb{Z}$ *then* $\mathrm{Gal}(W^*, k(X)) = \mathrm{PSL}(m,q)$. *Likewise, if* $\mathrm{GCD}(\sigma^*, m, q-1) = 1$ *then* $\mathrm{Gal}(W^*, k_0(X)) = \mathrm{PGL}(m,q)$.

(3.3.2) *The polynomial* W^* *is irreducible in* $k(X)[Y]$, *and* $X = 0$ *and* $X = \infty$ *are the only valuations of* $k(X)/k$ *which are possibly ramified in the splitting field of* W^* *over* $k(X)$. *Moreover, if* $\rho^* > \sigma^*(\nu - \tau^*)/\nu$ *and the valuation* $X = 0$ *of* $k(X)/k$ *is ramified in the splitting field of* W^* *over* $k(X)$ *then it is tamely ramified. Finally, if* $\rho^* > \sigma^*(\nu - \tau^*)/\nu$ *and* $\sigma^* \in \nu\mathbb{Z}$ *then* $X = \infty$ *is the only valuation of* $k(X)/k$ *which is ramified in the splitting field of* W^* *over* $k(X)$.

(3.3.3) *We have* $\mathrm{SL}(m,q) < \mathrm{Gal}(V^*, k(X)) < \mathrm{Gal}(V^*, k_0(X)) < \mathrm{GL}(m,q)$ *and we have* $[\mathrm{Gal}(V^*, k(X)) : \mathrm{SL}(m,q)] \equiv 0 \pmod{(q-1)/\mathrm{GCD}(\sigma^*, q-1)}$. *Moreover, if* $\sigma^* \in (q-1)\nu\mathbb{Z}$ *then* $\mathrm{Gal}(V^*, k(X)) = \mathrm{SL}(m,q)$. *Likewise, if* $\mathrm{GCD}(\sigma^*, q-1) = 1$ *then* $\mathrm{Gal}(V^*, k_0(X)) = \mathrm{GL}(m,q)$.

(3.3.4) *The polynomial* V^* *is irreducible in* $k(X)[Y]$, *and* $X = 0$ *and* $X = \infty$ *are the only valuations of* $k(X)/k$ *which are possibly ramified in the splitting field of* V^* *over* $k(X)$. *Moreover, if* $\rho^* > \sigma^*(\nu - \tau^*)/\nu$ *and the valuation* $X = 0$ *of* $k(X)/k$ *is ramified in the splitting field of* V^* *over* $k(X)$ *then it is tamely ramified. Finally, if* $\rho^* > \sigma^*(\nu - \tau^*)/\nu$ *and* $\sigma \in (q-1)\nu\mathbb{Z}$ *then* $X = \infty$ *is the only valuation of* $k(X)/k$ *which is ramified in the splitting field of* V^* *over* $k(X)$.

Proof: Let $\tau = \nu - \tau^*$ and $\rho = \rho^* - \sigma^*$ and $\sigma = -\sigma^*$. Now, since $\mathrm{GCD}(\nu, \tau^*) = 1$, we get $\mathrm{GCD}(\nu, \tau) = 1$, and since $\rho^* \neq \sigma^*(\nu - \tau^*)/\nu$, we get $\rho \neq \sigma(\nu - \tau)/\nu$. Clearly $\mathrm{GCD}(\sigma^*, q-1) = \mathrm{GCD}(\sigma, q-1)$ and $\mathrm{GCD}(\sigma^*, m, q-1) = \mathrm{GCD}(\sigma, m, q-1)$. Also clearly: $\rho^* > \sigma^*(\nu - \tau^*)/\nu \Leftrightarrow \rho > \sigma(\nu - \tau)/\nu$. Likewise: $\sigma^* \in \nu\mathbb{Z} \Leftrightarrow \sigma \in \nu\mathbb{Z}$. Similarly: $\sigma^* \in (q-1)\nu\mathbb{Z} \Leftrightarrow \sigma \in (q-1)\nu\mathbb{Z}$. Let $a = a^* b^{*-1}$ and $b = b^{*-1}$, and let W and V be as in Proposition 3.2. Then $W(Y) = b^{*-1} X^{-\sigma^*} Y^{\nu} W^*(Y^{-1})$ and $V(Y) = b^{*-1} X^{-\sigma^*} Y^{(q-1)\nu} V^*(Y^{-1})$. Therefore Proposition 3.3 follows from Proposition 3.2.

Remark 3.4: We have deduced the "Likewise" in (3.2.1), and hence also the "Likewise" in (3.3.1), from the "Likewise" in (3.2.3). In case of $m = 2$, the "Likewise" in (3.2.1), and hence also the "Likewise" in (3.3.1), can be deduced directly from (2.1.6) by interposing the following material in the proof of Proposition 3.2 between (9) and (10):

For a moment suppose that $m = 2$ and $\sigma \not\equiv 0 \pmod 2$. If $p = 2$ then

$\mathrm{PSL}(2,q) = \mathrm{PGL}(2,q)$ and hence by (4) we get $\mathrm{Gal}(W, k_0(X)) = \mathrm{PGL}(2,q)$. So also suppose that $p \neq 2$. Upon letting $W' = W'(Y) = Y^{q+1} - aX^{q\rho}Y + bX^{q\sigma}$ we obviously have $\mathrm{Gal}(W', k(X)) = \mathrm{Gal}(W, k(X))$. Upon letting $\sigma' = q\sigma - (q+1)\rho$ we have $X^{-(q+1)\rho}W'(X^\rho Y) = Y^{q+1} - aY + bX^{\sigma'}$ and hence $\mathrm{Gal}(W', k(X)) = \mathrm{Gal}(Y^{q+1} - aY + bX^{\sigma'}, k(X))$. Clearly $\sigma' \not\equiv 0 \pmod 2$ and $[\mathrm{PGL}(2,q)\colon \mathrm{PSL}(2,q)] = 2$, and by (4) we have

$$\mathrm{PSL}(2,q) < \mathrm{Gal}(Y^{q+1} - aY + bX^{\sigma'}, k(X)) < \mathrm{PGL}(2,q),$$

and by (2.1.6) we have $\mathrm{Gal}(Y^{q+1} - aY + bX, k(X)) = \mathrm{PGL}(2,q)$; therefore, in view of Corollary (3.1) of the Substitutional Principle on page 99 of [Ab4], we get $\mathrm{Gal}(Y^{q+1} - aY + bX^{\sigma'}, k(X)) = \mathrm{PGL}(2,q)$. Therefore $\mathrm{Gal}(W, k(X)) = \mathrm{PGL}(2,q)$, and hence by (4) we get $\mathrm{Gal}(W, k_0(X)) = \mathrm{PGL}(2,q)$. Thus: If $m = 2$ and $\sigma \not\equiv 0 \pmod 2$ then $\mathrm{Gal}(W, k_0(X)) = \mathrm{PGL}(2,q)$.

4. Proof of Theorems 1.1 to 1.5

Theorems 1.1 and 1.2 follow from Proposition 3.2. Theorems 1.3 and 1.4 follow from Proposition 3.3. Theorem 1.5 follows from (2.1.5).

References

[Ab1] S. S. Abhyankar, *Coverings of algebraic curves,* American Journal of Mathematics **79** (1957), 825–856.

[Ab2] S. S. Abhyankar, *Ramification Theoretic Methods in Algebraic Geometry,* Princeton University Press, Princeton, 1959.

[Ab3] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers,* American Mathematical Society, Providence, RI, 1990.

[Ab4] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic,* Bulletin of the American Mathematical Society **27** (1992), 68–133.

[Ab5] S. S. Abhyankar, *Mathieu group coverings in characteristic two,* Comptes Rendus de l'Academie des Sciences, Paris **316** (1993), 267–271.

[Ab6] S. S. Abhyankar, *Alternating group coverings of the affine line in characteristic greater than two,* Mathematische Annalen **296** (1993), 63–68.

[Ab7] S. S. Abhyankar, *Fundamental group of the affine line in positive characteristic,* Proceedings of the 1992 Bombay International Colloquium on Geometry and Analysis held at the Tata Institute of Fundamental Research, to appear.

[Ab8] S. S. Abhyankar, *Wreath products and enlargements of groups*, Discrete Mathematics, to appear.

[AOS] S. S. Abhyankar, J. Ou and A. Sathaye, *Alternating group coverings of the affine line in characteristic two*, Discrete Mathematics, to appear.

[APS] S. S. Abhyankar, H. Popp and W. K. Seiler, *Mathieu-group coverings of the affine line*, Duke Mathematical Journal **68** (1992), 301–311.

[AY1] S. S. Abhyankar and I. Yie, *Small degree coverings of the affine line in characteristic two*, Discrete Mathematics, to appear.

[AY2] S. S. Abhyankar and I. Yie, *Some more Mathieu group coverings of the affine line in characteristic two*, Proceedings of the American Mathematical Society, to appear.

[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.

[HuB] B. Huppert and N. Blackburn, *Finite Groups III*, Springer-Verlag, New York, 1983.

[Suz] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.