PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 6, June 1997, Pages 1643–1650
S 0002-9939(97)03939-7

PROJECTIVE POLYNOMIALS

SHREERAM S. ABHYANKAR

(Communicated by Ronald M. Solomon)

Dedicated to J-P. Serre for his Seventieth Birthday

Abstract. Certain nice trinomials have the projective linear groups as their Galois groups. This was proved using considerable group theory. Here is an easier proof based on the observation that the said trinomials are what may be called projective polynomials. It extends the results to a local situation.

1. Introduction

Let K be a field of characteristic $p > 0$. Let $q > 1$ be a power of p and let $m > 1$ be an integer. Let $A \neq 0 \neq B$ be elements in K and let

$$F(Y) = Y^{\langle m-1\rangle} + AY + B \quad \text{and} \quad \Phi(Y) = Y^{q^m-1} + AY^{q-1} + B$$

where, for every integer $i \geq -1$, we are using the **abbreviation** $\langle i\rangle = 1 + q + q^2 + \cdots + q^i$ with the conventions $\langle 0\rangle = 1$ and $\langle -1\rangle = 0$. In Propositions (5.1), (5.2) and (5.3) of Section 5, we shall respectively prove detailed versions of the following Claims (1.1), (1.2) and (1.3):

Claim (1.1). *If $K = k_p(X)$ for an algebraically closed field k_p, and $(A, B) = (X, 1)$, then $Gal(F, K) = PSL(m, q)$ and $Gal(\Phi, K) = SL(m, q)$.*

Claim (1.2). *If $K = k_p(X)$ for a field k_p with $GF(q) \subset k_p$, and $(A, B) = (1, X)$, then $Gal(F, K) = PGL(m, q)$ and $Gal(\Phi, K) = GL(m, q)$.*

Claim (1.3). *If K is the quotient field of a regular local domain R of dimension $d \geq 2$ with $GF(q) \subset R$, and $(A, B) = (Z, X)$ where $(X, Z, Z_3, \ldots, Z_d)$ is a basis of the maximal ideal of R, then $Gal(F, K) = PGL(m, q)$ and $Gal(\Phi, K) = GL(m, q)$.*

The first two Claims (1.1) and (1.2) were originally proved in [2] and [3]. The $m = 2$ case of (1.1) was also proved by Carlitz [11] and Serre (Appendix of [2]). Here we give a more direct proof of (1.1) and (1.2) which yields a proof of (1.3). Briefly, by the shape of F we see that it is a "projective polynomial" and hence, assuming $\mathrm{GF}(q) \subset K$, its Galois group $\mathrm{Gal}(F, K)$ may be regarded as a subgroup

Received by the editors January 5, 1996.
1991 *Mathematics Subject Classification.* Primary 12F10, 14H30, 20D06, 20E22.
This work was partly supported by NSF grant DMS 91–01424 and NSA grant MDA 904–92–H–3035.

of $\mathrm{PGL}(m,q)$. Next, by "throwing away a root" of F, we get the 2-transitivity of $\mathrm{Gal}(F,K)$. In case of $m>2$, in [3], we then invoke Cameron-Kantor Theorem I of [10] which characterizes 2-transitive collineation groups. The said Cameron-Kantor Theorem I says that, for $m>2$, a 2-transitive subgroup of $\mathrm{PGL}(m,q)$ either contains $\mathrm{PSL}(m,q)$ or it is the alternating group $A_7(15)$ inside $\mathrm{PSL}(4,2)$. In our original proof of the $m=2$ case of (1.1) given in [2], instead of Cameron-Kantor Theorem I, we invoked the Zassenhaus-Feit-Suzuki Theorem (see page 83 of [2]) which characterizes 2-transitive permutation groups in which only the identity fixes 3 points. In Section 4, we shall put in proper perspective the calculation of the first two "twisted derivatives" of F obtained by successively "throwing away" two roots of F, which was originally given in [2] and [3]. This yields an estimate for the order of $\mathrm{Gal}(F,K)$, and as we shall show in Section 5, coupled with the above observation that $\mathrm{Gal}(F,K)$ may be regarded as a subgroup of $\mathrm{PGL}(m,q)$, finishes off the proof of the $m=2$ case of (1.1) to (1.3) without invoking any further group theory. In Section 3, we recall Proposition (3.2) of [3] dealing with the $m>2$ case of (1.1) and (1.2). In the proof of this Proposition given in [3], the Sylow Subgroup Lemma (2.2) [3] was used for showing that $A_7(15)$ does not occur while applying Cameron-Kantor Theorem I to our situation. The refinements of this Lemma, needed for extending this to (1.3), are discussed in items (3.4) to (3.8) of Section 3.

To introduce the notion of a projective polynomial, let $f(Y)$, $\phi(Y)$ and $\widehat{\phi}(Y)$ be monic polynomials in Y with coefficients in a field K of characteristic p. We call $f(Y)$ a **projective q-polynomial** if it is of the form $f(Y)=Y^{\langle m-1\rangle}+\sum_{i=1}^{m}b_iY^{\langle m-1-i\rangle}$ with $b_i\in K$ and integer $m>0$; note that then: $f(Y)$ is separable (i.e., its Y-discriminant is nonzero) $\Leftrightarrow b_m\neq 0$. Likewise we call $\phi(Y)$ a **subvectorial q-polynomial** if it is of the form $\phi(Y)=Y^{q^m-1}+\sum_{i=1}^{m}b_iY^{q^{m-i}-1}$ with $b_i\in K$ and integer $m>0$; again note that then: $\phi(Y)$ is separable $\Leftrightarrow b_m\neq 0$. Now clearly $f(Y)\mapsto\phi(Y)=f(Y^{q-1})$ gives a bijection of projectives to subvectorials. Finally we call $\widehat{\phi}(Y)$ a **vectorial q-polynomial** if it is of the form $\widehat{\phi}(Y)=Y^{q^m}+\sum_{i=1}^{m}b_iY^{q^{m-i}}$ with $b_i\in K$ and integer $m>0$; note that then: $\widehat{\phi}(Y)$ is separable $\Leftrightarrow b_m\neq 0$. Obviously $\phi(Y)\mapsto\widehat{\phi}(Y)=Y\phi(Y)$ gives a bijection of subvectorials to vectorials. Note that the above polynomials $F(Y)$ and $\Phi(Y)$ are respectively projective and subvectorial q-polynomials.

In (2.5) of [3] I noted the well-known **Fact (1.F1)** that if $\phi(Y)$ is separable subvectorial and $\mathrm{GF}(q)$ is a subfield of K then, upon letting $\widehat{\phi}(Y)=Y\phi(Y)$, in a natural manner we have $\mathrm{Gal}(\phi,K)=\mathrm{Gal}(\widehat{\phi},K)<\mathrm{GL}(m,q)$ where $<$ denotes subgroup, and where in case of $\mathrm{Gal}(\phi,K)$ we regard $\mathrm{GL}(m,q)$ as acting on the nonzero vectors of $\mathrm{GF}(q)^m$ whereas in case of $\mathrm{Gal}(\widehat{\phi},K)$ we regard $\mathrm{GL}(m,q)$ as acting on the entire vector space $\mathrm{GF}(q)^m$. As a straightforward consequence of this, in (2.5) of [3] I deduced the **Fact (1.F2)** that if $f(Y)$ is separable projective and $\mathrm{GF}(q)$ is a subfield of K then in a natural manner we have $\mathrm{Gal}(f,K)<\mathrm{PGL}(m,q)$ in such a way that $\mathrm{Gal}(f,K)$ is the image of $\mathrm{Gal}(\phi,K)$ with $\phi(Y)=f(Y^{q-1})$ under the canonical map of $\mathrm{GL}(m,q)$ onto $\mathrm{PGL}(m,q)$. In (2.3) of [3] I also noted the easy to prove **Fact (1.F3)** that if $f(Y)$ is separable projective and $\mathrm{GF}(q)$ is a subfield of K then: $\mathrm{SL}(m,q)<\mathrm{Gal}(\phi,K)\Leftrightarrow\mathrm{PSL}(m,q)<\mathrm{Gal}(f,K)$ with $\phi(Y)=f(Y^{q-1})$. Finally in (2.5iii) of [3] I easily deduced the **Fact (1.F4)** that if $f(Y)$ is separable projective then $\Lambda^{q-1}=(-1)^{\langle m-1\rangle}f(0)$ for some element Λ in the splitting field of $f(Y^{q-1})$ over K.

2. Coverings

In my 1957 paper [1] I noted that the trinomial equation $F(Y) = 0$, with $(A, B) = (X, 1)$ and $K = k(X)$ where k is an algebraically closed field of characteristic $p > 0$, gives an unramified covering of the affine line L_k over k, and suggested that the Galois group $\mathrm{Gal}(F, k(X))$ be computed. My interest in Galois theory was revived when, in September 1988, Serre wrote me a letter saying that he could prove that if $(A, B) = (X, 1)$ and $m = 2$ then $\mathrm{Gal}(F, k(X)) = \mathrm{PSL}(2, q)$, i.e., he settled Claim (1.1) for $m = 2$. He called his proof a descending proof as opposed to the ascending proof which I later found. Both of these appeared in my 1992 paper [2]; while this paper was in press, Serre discovered that his proof was similar to the proof which Carlitz [11] had given in 1956. Now the Carlitz-Serre proof is based on "modular" considerations, whereas my proof was based on the Zassenhaus-Feit-Suzuki Theorem. Then, as said above, by replacing the Zassenhaus-Feit-Suzuki Theorem by Cameron-Kantor Theorem I, in my 1994 paper [3] I settled Claims (1.1) and (1.2). Note that the trinomial equation $\Phi(Y) = 0$, with $(A, B) = (1, X)$ and $K = k(X)$, also gives an unramified coverings of the affine line L_k. Also note that the trinomial equations $F(Y) = 0$ and $\Phi(Y) = 0$, with $(A, B) = (1, X)$ and $K = k(X)$, give unramified coverings of the (once) punctured affine line $L_{k,1}$ (punctured at $X = 0$). Thus in (1.1) we are dealing with unramified coverings of L_k, and in (1.2) we are dealing with unramified coverings of $L_{k,1}$.

Actually, in the 1957 paper [1] I wrote down several explicit families of equations giving unramified coverings of the affine line and higher dimensional affine spaces. Many of these are defined over the prime field $\mathrm{GF}(p)$, and indeed have $(0, 1, -1)$ as the only coefficients. In [3] to [8] I have shown that their Galois groups encompass all the alternating, symmetric, and Mathieu groups as well as all the symplectic, odd-dimensional unitary, and even-dimensional elliptic-type orthogonal groups over finite fields.

As said before, the extra dividend of the more direct proof of Claims (1.1) and (1.2) given in this paper is that it yields a proof of Claim (1.3). In the forthcoming paper [9] I shall show how (1.3) leads to some progress in the calculation of local fundamental groups. In brief, for $d \geq 2$, let P be the origin of the d-dimensional affine space L_k^d over k with coordinates $(X, Z, Z_3, \ldots, Z_d)$, let $R = k[[X, Z, Z_3, \ldots, Z_d]] =$ the completion of the local ring of P on L_k^d, and let $K = k((X, Z, Z_3, \ldots, Z_d)) =$ the quotient field of R. Now the equation $F(Y) = 0$ with $(A, B) = (Z, X)$ gives a covering of L_k^d whose branch locus is the hyperplane $M : X = 0$, and by (1.3) we get

$$\mathrm{Gal}(F, K) = \mathrm{GL}(m, q).$$

Thus $\mathrm{GL}(m, q)$ belongs to the local algebraic fundamental group of $L_k^d - M$ at P.

3. Core and inertia

Recall that K is a field of characteristic $p > 0$, and $q > 1$ is a power of p, and $m > 1$ is an integer. Let $b_1, \ldots, b_m$ be elements in K with $b_m \neq 0$, and consider the projective polynomial

$$f = f(Y) = Y^{(q^m-1)/(q-1)} + \sum_{i=1}^{m} b_i Y^{(q^{m-i}-1)/(q-1)}$$

and the corresponding subvectorial polynomial

$$\phi = \phi(Y) = Y^{q^m-1} + \sum_{i=1}^{m} b_i Y^{q^{m-i}-1}.$$

Concerning the Galois groups of these polynomials, in Proposition (3.1) of [3] we proved the following:

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

As a consequence of the above Proposition, together with Lemmas (2.1), (2.2) and (2.3) of [3], in Proposition (3.2) of [3] we proved 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 $GF(q) \subset k_0$. Assume that $K = k_0(X)$. Let $1 \le \mu < m$ be an integer such that $GCD(\nu,\tau) = 1$ where $\nu = 1+q+\cdots+q^{m-1}$ and $\tau = 1+q+\cdots+q^{\mu-1}$. Assume that $b_{m-\mu} = -aX^\rho$ and $b_m = bX^\sigma$ where a and b are nonzero elements in k_0, and ρ and σ are integers such that $\rho \ne \sigma(\nu-\tau)/\nu$ (for instance $\rho \ne 0 = \sigma$ or $\rho = 0 \ne \sigma$). Also assume that $b_1 = \cdots = b_{m-\mu-1} = b_{m-\mu+1} = \cdots = b_{m-1} = 0$. Then we have the following:*

(3.2.1) *We have $PSL(m,q) < Gal(f,k(X)) < Gal(f,k_0(X)) < PGL(m,q)$ and we have $[Gal(f,k(X)) : PSL(m,q)] \equiv 0 \bmod GCD(m,q-1)/GCD(\sigma,m,q-1)$. Also, if $\sigma \in \nu\mathbb{Z}$ then $Gal(f,k(X)) = PSL(m,q)$. Likewise, if $GCD(\sigma,m,q-1) = 1$ then $Gal(f,k_0(X)) = PGL(m,q)$.*

(3.2.2) *The polynomial f 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 f 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 f 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 f over $k(X)$.*

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

(3.2.4) *The polynomial ϕ 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 ϕ 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 ϕ 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 ϕ over $k(X)$.*

Remark (3.4). In the proof of Proposition (3.2) on page 19 of [3], in line 15, the reference to Proposition 3.1 should be changed to a reference to Lemma 2.3. Likewise, in the proof of Lemma 2.2 on page 12 of [3], the phrase "some integer e we have $\sigma^e(l) = j$" should be changed to "some power σ' of σ we have $\sigma'(l) = j$", and in the remaining three sentences everywhere change σ to σ'. Now replacing $(2,7)$ by (u,v) and replacing the alternating group A_n by the symmetric group S_n in the said proof we get:

Lemma (3.5). *If $u \neq v$ are primes and $H < S_v$ with $|H| \equiv 0 \bmod v$ then H cannot have a nonidentity normal subgroup whose order is a power of u.*

Recall that for a finite group H and prime u, the u-**core** $O_u(H)$ of H is defined by putting $O_u(H)$ = the intersection of all u-Sylow subgroups of H = the (unique) largest normal subgroup of H whose order is a power of u = the subgroup of H generated by all of its normal subgroups whose orders are powers of u. Clearly $O_u(H)$ is a characteristic subgroup of H, and hence: $H' \triangleleft H \Rightarrow O_u(H') \triangleleft H$ and $O_u(H') \triangleleft O_u(H)$, where $\triangleleft$ denotes normal subgroup. Also clearly: $O_u(H) = 1 \Leftrightarrow H$ has no nonidentity normal subgroup whose order is a power of u. Therefore by (3.5) we get:

Lemma (3.6). *If $u \neq v$ are primes and $H' \triangleleft H < S_v$ with $|H| \equiv 0 \bmod v$ then H' cannot have a nonidentity normal subgroup whose order is a power of u.*

From the above proof of (3.6) we also get the following variation of it:

Lemma (3.7). *If $w > 0$ is an integer which is nondivisible by a prime u and H is a transitive subgroup of S_w, then $O_u(H) = 1$ and more generally $O_u(H') = 1$ for every $H' \triangleleft H$.*

Remark (3.8). The fact that the **inertia** group H' of a valuation (of any rank) with residue characteristic $u > 0$ has a unique (and hence normal) u-Sylow subgroup can be restated by saying that $O_u(H')$ is a (and hence the only) u-Sylow subgroup of H'; since $H' \triangleleft H$ where H is the splitting group of the said valuation, we also get $O_u(H') \triangleleft H$.

4. Calculations

Recall that K is a field of characteristic $p > 0$, and $\langle m{-}1\rangle = 1{+}q{+}q^2{+}\cdots{+}q^{m-1}$ where $q > 1$ is a power of p and $m > 1$ is an integer. Also recall that $A \neq 0 \neq B$ are elements in K and

$$F(Y) = Y^{\langle m-1\rangle} + AY + B \quad \text{and} \quad \Phi(Y) = Y^{q^m-1} + AY^{q-1} + B. \tag{4.1}$$

Let V be a root of $F(Y)$ in an overfield of K. Let $F'(Y)$ be the twisted derivative of $F(Y)$ at V, i.e.,

$$F'(Y) = Y^{-1}[F(Y+V) - F(V)]. \tag{4.2}$$

Then $F'(Y) = Y^{-1}[(Y+V)^{\langle m-1\rangle} - V^{\langle m-1\rangle}] + A$ and hence

$$F'(Y) = Y^{q\langle m-2\rangle} + VY^{q\langle m-2\rangle-1} + \Big(\sum\nolimits^{*} V^i Y^{q\langle m-2\rangle-i}\Big) + (V^{q\langle m-2\rangle} + A) \tag{4.3}$$

where $\sum^*$ denotes summation over integers i which are in the range $1 < i < q\langle m{-}2\rangle$ and whose q-adic expansion contains only 0's and 1's, and where we note that if $m = 2$ then the summation $\sum^*$ is empty and hence its value is 0. Since $F(V) = 0$ we get

$$V^{\langle m-1\rangle} + AV + B = 0 \tag{4.4}$$

and hence

$$VF'(Y) = VY^{q\langle m-2\rangle} + V^2Y^{q\langle m-2\rangle-1} + \Big(\sum\nolimits^{*} V^{i+1}Y^{q\langle m-2\rangle-i}\Big) - B. \tag{4.5}$$

Let $E(Y)$ be obtained by reciprocating $F'(Y)$. Then

$$E(Y) = -B^{-1}VY^{q\langle m-2\rangle}F'(Y^{-1}) \tag{4.6}$$

and hence

$$E(Y) = Y^{q\langle m-2\rangle} - \Big(\sum\nolimits^{*} B^{-1}V^{i+1}Y^{i}\Big) - B^{-1}V^{2}Y - B^{-1}V. \tag{4.7}$$

Let W be a root of $E(Y)$ in an overfield of $K(V)$. Let $E'(Y)$ be the twisted derivative of $E(Y)$ at W, i.e.,

$$E'(Y) = Y^{-1}[E(Y+W) - E(W)]. \tag{4.8}$$

Let K^* be the splitting field of $E'(Y)$ over $K(V,W)$. Now clearly: **Description (4.9)** K^* is the splitting field of $F(Y)$ over K, and it is also the common splitting field of $F'(Y)$ and $E(Y)$ over $K(V)$; moreover the Galois groups of $F'(Y)$ and $E(Y)$ over $K(V)$ are isomorphic as permutation groups. Hence in particular

$$F'(Y) \text{ is irreducible over } K(V) \Leftrightarrow E(Y) \text{ is irreducible over } K(V). \tag{4.10}$$

Also clearly: **Description (4.11)** if $F(Y)$ and $E(Y)$ are irreducible over K and $K(V)$ respectively then $\mathrm{Gal}(F,K)$ is a 2-transitive subgroup of the symmetric group $S_{\langle m-1\rangle}$ and its 2-point stabilizer is $\mathrm{Gal}(E',K(V,W))$, and for their orders we have $|\mathrm{Gal}(F,K)| = (q+1)q|\mathrm{Gal}(E',K(V,W))|$. By (4.7) and (4.8) we see that

$$\text{if } m = 2 \text{ then } E'(Y) = Y^{q-1} - B^{-1}V^{2}. \tag{4.12}$$

5. Consequences

As consequences of the calculations of Section 4, we shall now prove the following three Propositions.

Proposition (5.1). *Assume that $K = k_p(X)$ for a subfield k_p, and $(A,B) = (X,1)$. Then we have the following:*

(5.1.1) *$F(Y)$ and $E(Y)$ are irreducible over K and $K(V)$ respectively, and we have $K(V) = k_p(V)$.*

(5.1.2) *The V-adic valuation J of $k_p(V)/k_p$ has a unique extension I to $K(V,W)$, and for it we have $I(V) = q\langle m-2\rangle$, and upon letting H to be the inertia group of an extension of J to K^* we have $H < Gal(E,K(V)) < Gal(F,K)$ with $|H| \equiv 0 \bmod q\langle m-2\rangle$ and H has a unique normal p-Sylow subgroup.*

(5.1.3) *If $m = 2$ and $GF(q) \subset k_p$ then $Gal(F,K) = PSL(2,q)$.*

(5.1.4) *If $m > 1$ and k_p is algebraically closed then $Gal(F,K) = PSL(m,q)$ and $Gal(\Phi,K) = SL(m,q)$.*

Proposition (5.2). *Assume that $K = k_p(X)$ for a subfield k_p, and $(A,B) = (1,X)$. Then we have the following:*

(5.2.1) *$F(Y)$ and $E(Y)$ are irreducible over K and $K(V)$ respectively, and we have $K(V) = k_p(V)$.*

(5.2.2) *If $m = 2$ then $E'(Y)$ is irreducible over $K(V,W)$.*

(5.2.3) *If $m = 2$ then the V-adic valuation J of $k_p(V)/k_p$ has a unique extension I to $K(V,W)$, and for it we have $I(V) = q$.*

(5.2.4) *If $m > 1$ and if $GF(q) \subset k_p$ then $Gal(F,K) = PGL(m,q)$ and $Gal(\Phi,K) = GL(m,q)$.*

Proposition (5.3). *Assume that K is the quotient field of a regular local domain R of dimension $d > 1$, and $(A,B) = (Z,X)$ where $(X,Z,Z_3,\dots,Z_d)$ is a basis of the maximal ideal $M(R)$ of R. Then we have the following:*

(5.3.1) *$F(Y)$ and $E(Y)$ are irreducible over K and $K(V)$ respectively; $R[V]$ is a d-dimensional regular local domain with $M(R[V]) = (V,Z,Z_3,\dots,Z_d)R[V]$.*

(5.3.2) *The real discrete valuation J of $K(V)$, whose valuation ring R_J is the localization of $R[V]$ at the prime ideal $VR[V]$, has a unique extension I to $K(V,W)$, and for it we have $I(V) = 1$, and upon letting H' and H to be the inertia and splitting groups of an extension of J to K^*, we have $H' \lhd H < Gal(E, K(V)) < Gal(F, K)$, with $|H| \equiv 0 \bmod q\langle m-2\rangle$ and $|H'| \equiv 0 \bmod q$, and H' has a unique normal p-Sylow subgroup.*

(5.3.3) *If $m = 2$ then $E'(Y)$ is irreducible over $K(V,W)$.*

(5.3.4) *If $m > 1$ and $GF(q) \subset R$ then $Gal(F,K) = PGL(m,q)$ and $Gal(\Phi, K) = GL(m,q)$.*

To prove (5.1), first assume that $K = k_p(X)$ for a subfield k_p, and $(A,B) = (X,1)$. Then $F(Y)$ is linear in X, and hence by Gauss's Lemma $F(Y)$ is irreducible over K, and we clearly have $K(V) = k_p(V)$. Let J be the V-adic valuation of $k_p(V)/k_p$, i.e., the unique real discrete valuation of $k_p(V)/k_p$ with $J(V) = 1$. Since $B = 1$, in view of (4.7), by Eisenstein's Criterion $E(Y)$ is irreducible over $K(V)$ and J has a unique extension I to $K(V,W)$, and for it we have $I(V) = q\langle m-2\rangle$, and upon letting H be the inertia group of an extension of J to K^* we have $H < \mathrm{Gal}(E, K(V)) < \mathrm{Gal}(F,K)$ with $|H| \equiv 0 \bmod q\langle m-2\rangle$ and H has a unique normal p-Sylow subgroup. If $m = 2$ then by (4.12) we get $E'(Y) = Y^{q-1} - V^2$, and clearly $\mathrm{GCD}(q-1, I(V^2)) = 1$ or 2 according as p is even or odd, and hence if also $\mathrm{GF}(q) \subset k_p$ then $\mathrm{Gal}(E'(Y), K(V,W))$ is a cyclic group of order $(q-1)$ or $(q-1)/2$ according as p is even or odd, and therefore by (4.11) we get $|\mathrm{Gal}(F,K)| = |\mathrm{PSL}(2,q)|$. Obviously $\mathrm{PSL}(2,q)$ is the only subgroup of $\mathrm{PGL}(2,q)$ whose order coincides with the order of $\mathrm{PSL}(2,q)$. Hence in view of Fact (1.F2) we see that if $m = 2$ and $\mathrm{GF}(q) \subset k_p$ then $\mathrm{Gal}(F,K) = \mathrm{PSL}(2,q)$. For the rest of (5.1.4) see Proposition (3.2).

To prove (5.2), next assume that $K = k_p(X)$ for a subfield k_p, and $(A,B) = (1,X)$. Then $F(Y)$ is linear in X, and hence by Gauss's Lemma $F(Y)$ is irreducible over K, and we clearly have $K(V) = k_p(V)$. Let J be the V-adic valuation of $k_p(V)$. Let $E^*(Y) = E(Y-1)$. If $m = 2$ then by (4.4) and (4.7) we get $E^*(Y) = (Y-1)^q + (V^{1+q}+V)^{-1}V^2(Y-1) + (V^{1+q}+V)^{-1}V = Y^q + A^*Y + B^*$ where $A^* = -B^{-1}V^2 = (V^q+1)^{-1}V$ and $B^* = -1 - (V^q+1)^{-1}V + (V^q+1)^{-1} = -(V^q+1)^{-1}(V^{q-1}+1)V$, and hence $J(A^*) = J(B^*) = 1$, and so by Eisenstein's Criterion $E^*(Y)$ (and therefore $E(Y)$) is irreducible over $K(V)$ and J has a unique extension I to $K(V,W)$, and for it we have $I(A^*) = I(B^*) = I(V) = q$, and by (4.12) we get $E'(Y) = Y^{q-1} - B^{-1}V^2 = Y^{q-1} + A^*$, and clearly $\mathrm{GCD}(q-1, I(A^*)) = 1$, and hence $E'(Y)$ is irreducible over $K(V,W)$, and if also $\mathrm{GF}(q) \subset k_p$ then $\mathrm{Gal}(E', K(V,W))$ is a cyclic group of order $(q-1)$ and so by (4.11) we get $|\mathrm{Gal}(F,K)| = |\mathrm{PGL}(2,q)|$. Consequently in view of Fact (1.F2) we see that if $m = 2$ and $\mathrm{GF}(q) \subset k_p$ then $\mathrm{Gal}(F,K) = \mathrm{PGL}(2,q)$. For a proof of the irreducibility of $F'(Y)$ (and hence of $E(Y)$) over $K(V) = k_p(V)$ which is valid for all $m > 1$, note that $F'(VY) = Y^{-1}[(Y+1)^{\langle m-1\rangle} - 1]V^{q\langle m-2\rangle} + 1$ where $Y^{-1}[(Y+1)^{\langle m-1\rangle} - 1]$ is a product of $q\langle m-2\rangle > 0$ pairwise distinct monic linear factors in $\overline{k}_p[Y]$, where $\overline{k}_p$ is the algebraic closure of k_p, and hence $F'(VY)$ is irreducible in $k_p(Y)[V]$ and therefore by Gauss's Lemma it is irreducible in $k_p(V)[Y]$, and hence $F'(Y)$ is irreducible in $k_p(V)[Y]$. For the rest of (5.2.4) see Proposition (3.2).

To prove (5.3), finally assume that K is the quotient field of a regular local domain R of dimension $d > 1$, and $(A,B) = (Z,X)$ where $(X, Z, Z_3, \ldots, Z_d)$ is a basis of the maximal ideal $M(R)$ of R. Now by a Generalized Eisenstein Criterion

we see that $F(Y)$ is irreducible over K, and $R[V]$ is a d-dimensional regular local domain with $M(R[V]) = (V, Z, Z_3, \ldots, Z_d)R[V]$; also $R[V]$ is the integral closure of R in $K(V)$, and $K(V)$ is the quotient field of $R[V]$. Let J be the real discrete valuation of $K(V)$ whose valuation ring R_J is the localization of $R[V]$ at the prime ideal $VR[V]$. Let $t : R_J \to \overline{K} = R_J/M(R_J)$ be the residue class map. Then $\overline{K}$ is the quotient field of the $(d-1)$-dimensional regular local domain $\overline{R} = t(R[V])$ with $M(\overline{R}) = (t(Z), t(Z_3), \ldots, t(Z_d))\overline{R}$. By (4.3) we see that $F'(Y) \in S[Y]$ and upon letting $\overline{F}'(Y) \in \overline{K}[Y]$ be obtained by applying t to the coefficients of $F'(Y)$ we get $\overline{F}'(Y) = Y^{q\langle m-2\rangle} + t(Z)$. Now $t(Z) \in M(\overline{R}) \setminus M(\overline{R})^2$, and hence by Eisenstein's Criterion $\overline{F}'(Y)$ is irreducible over $\overline{K}$, and J has a unique extension I to $K(V, W)$, and for it we have $I(V) = 1$. Clearly the residue degree of I over J is $q\langle m-2\rangle$ out of which q is the purely inseparable part, and hence upon letting H' and H be the inertia and splitting groups of an extension of J to K^* we have $H' \lhd H < \mathrm{Gal}(E, K(V)) < \mathrm{Gal}(F, K)$, with $|H| \equiv 0 \bmod q\langle m-2\rangle$ and $|H'| \equiv 0 \bmod q$, and H' has a unique normal p-Sylow subgroup. By (4.4) we get $J(B^{-1}V) = 0$ and hence $I(B^{-1}V^2) = 1$. Therefore by (4.12) we conclude that if $m = 2$ then $E'(Y)$ is irreducible over $K(V, W)$, and if also $\mathrm{GF}(q) \subset R$ then $\mathrm{Gal}(E', K(V, W))$ is a cyclic group of order $(q-1)$ and hence by (4.11) we get $|\mathrm{Gal}(F, K)| = |\mathrm{PGL}(2, q)|$ and so by Fact (1.F2) we must have $\mathrm{Gal}(F, K) = \mathrm{PGL}(2, q)$. In view of Cameron-Kantor Theorem I and Facts (1.F1) to (1.F4) together with Lemma (4.6), the rest of (5.3.4) follows as in the proof of Proposition (3.2) given in [3].

References

[1] S. S. Abhyankar, *Coverings of algebraic curves*, Amer. J. Math. **79** (1957), 825-856. MR **20:**872

[2] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. A.M.S. **27** (1992), 68-133. MR **94a:**12004

[3] S. S. Abhyankar, *Nice equations for nice groups*, Israel J. Math. **88** (1994), 1-24. MR **96f:**12003

[4] S. S. Abhyankar, *Fundamental group of the affine line in positive characteristic*, Proceedings of the 1992 International Colloquium on Geometry and Analysis, Tata Institute of Fundamental Research, Bombay (1995), 1-26. CMP 96:01

[5] S. S. Abhyankar, *Mathieu group coverings and linear group coverings*, Contemporary Mathematics **186** (1995), 293-319. CMP 96:01

[6] S. S. Abhyankar, *Again nice equations for nice groups*, Proceedings of the American Mathematical Society, (To Appear). CMP 95:16

[7] S. S. Abhyankar, *More nice equations for nice groups*, Proceedings of the American Mathematical Society, (To Appear). CMP 95:16

[8] S. S. Abhyankar, *Further nice equations for nice groups*, Transactions of the American Mathematical Society, (To Appear). CMP 96:09

[9] S. S. Abhyankar, *Local fundamental groups of algebraic varieties*, pp. (To Appear). CMP 95:16

[10] P. J. Cameron and W. M. Kantor, *2-Transitive and antiflag transitive collineation groups of finite projective spaces*, J. of Algebra **60** (1979), 384-422. MR **81c:**20032

[11] L. Carlitz, *Resolvents of certain linear groups in a finite field*, Canad. J. Math. **8** (1956), 568-579. MR **18:**377f

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907
E-mail address: ram@cs.purdue.edu