AUTOMORPHISMS OF FUNCTION FIELDS

BY

MAXWELL ROSENLICHT

1. Let K be an algebraic function field of one variable over the constant field k and let $g>0$ be the genus of K. Let $\mathcal{G}$ be the group of all automorphisms of K that leave the elements of k fixed (and that leave a given place P_0 of K/k fixed if $g=1$). A classical theorem due to Schwartz-Klein-Noether-Weierstrass-Poincaré-Hurwitz when $g>1$ (and older for $g=1$) says that $\mathcal{G}$ is finite if k is the field of complex numbers. From this one can easily deduce the same result if k is any field of characteristic zero. The theorem for k an algebraically closed field of characteristic $p\neq 0$ was proved by H. L. Schmid in 1938 [5], and a less computational proof for any algebraically closed k was given recently by Iwasawa and Tamagawa [3]. We intend to show how this result can be very easily proved by one of the classical arguments (given in essence, but somewhat imprecisely, in [1]) if we replace integration on the Riemann surface R of K by use of its jacobian variety J, and finally we shall show what the corresponding result is when k is an arbitrary field. The reasons for including here the easy case $g=1$ will become apparent in the last section.

The analytic proof we have in mind runs as follows: $\mathcal{G}$ is naturally isomorphic to the group of complex analytic homeomorphisms of R (that leave P_0 fixed if $g=1$). First consider the special case in which R is elliptic or hyperelliptic. R can then be considered (in one and only one way) as a two-sheeted covering surface of a Riemann sphere S (such that, if $g=1$, P_0 is a branch point of this covering). The elements of $\mathcal{G}$ give rise to analytic homeomorphisms of S that permute the ramification points of S. Since $g>0$, the ramification points are in finite number >2. The finiteness of $\mathcal{G}$ then follows from (1) any analytic homeomorphism of S leaving three distinct points fixed is the identity, and (2) any element of $\mathcal{G}$ that leaves all points of S fixed is either the identity or merely interchanges the sheets of R. On the other hand if K is not elliptic or hyperelliptic, then the ratios of the differentials of the first kind of K give rise to the canonical embedding of R in S_{g-1}, the complex projective space of dimension $(g-1)$, and the automorphisms of K/k correspond one-one to projective transformations of S_{g-1} that map R onto itself. It follows that $\mathcal{G}$ can be considered as a Lie group with a finite number of components that acts analytically on R (see the second lemma of §2 for details), so it remains only to show that the component of the identity G of $\mathcal{G}$ has only one point. Hence we have to show that if $\sigma_1, \sigma_2 \in \mathcal{G}$ are homotopic (as maps of R), then $\sigma_1=\sigma_2$. So let ω be any differential of the first kind on R

Presented to the Society, December 28, 1953; received by the editors January 16, 1954.

and let Γ be any 1-cycle on R. Then $\sigma_1^{-1}(\Gamma)$ is homologous to $\sigma_2^{-1}(\Gamma)$, and hence $\int_\Gamma \sigma_1(\omega) = \int_{\sigma_1^{-1}(\Gamma)}\omega = \int_{\sigma_2^{-1}(\Gamma)}\omega = \int_\Gamma \sigma_2(\omega)$. Thus all the periods of $\sigma_1(\omega) - \sigma_2(\omega)$ are zero, so $\sigma_1(\omega) = \sigma_2(\omega)$. Since this is true for each ω and since the quotients of the ω's generate K, we have $\sigma_1 = \sigma_2$. Q.E.D.

2. In this section k is supposed algebraically closed.

LEMMA. *If K/k is any algebraic function field of one variable, there exists a nonsingular algebraic curve C in a projective space S_n such that C is defined over k, its function field $k(C)$ is k-isomorphic to K, and each birational map of C onto itself (that leaves a given place P_0 of K fixed if $g=1$) is induced by a nonsingular projective transformation of S_n.*

We prove this lemma generally to avoid the necessity for special consideration of the hyperelliptic case, which is messy in the case of characteristic 2. We first assume $g>1$ and show that the tricanonical image of K will do the trick. Let W_1, W_2, W_3 be canonical divisors of K. Then $d(W_1W_2W_3) = 6g-6 > 2g-2$, so $i(W_1W_2W_3) = 0$ and the Riemann-Roch theorem gives $r(W_1W_2W_3) = 5g-5$. Let $f_1, \cdots, f_{5g-5} \in K$ be a basis for the vector space $L(W_1W_2W_3)$ of multiples of $(W_1W_2W_3)^{-1}$. Since any two canonical divisors of K are linearly equivalent, if we started with different canonical divisors W_1', W_2', W_3' we could replace $f_1, \cdots, f_{5g-5}$ by their multiples by a certain nonzero element of K. It follows that the algebraic curve C defined over k by the homogeneous generic point $(f_1, \cdots, f_{5g-5})$, which is embedded in the projective space S_{5g-6} of dimension $5g-6$, is invariantly defined by K to within nonsingular projective transformations with coefficients in k of S_{5g-6}. $k(C) = k(\{f_i/f_j\})$, $i, j = 1, \cdots, 5g-5$, so $k(C) \subseteq K$. We now show that $k(C) = K$. K has precisely g linearly independent differentials of the first kind, so we can find distinct places $P_1, \cdots, P_g$ of K such that $i(P_1 \cdots P_g) = 0$. For each $j = 1, \cdots, g$, we have $i(P_1 \cdots P_g P_j^{-1}) = 1$. Choose distinct places P', P'' that are distinct from the zeros of the differentials that are multiples of the various divisors $P_1 \cdots P_g P_j^{-1}$. Then each integral divisor of degree g that divides $P_1 \cdots P_g P'$ is nonspecial, and similarly for $P_1 \cdots P_g P''$. Hence, by Riemann-Roch, there exist functions $g_1, g_2 \in K$ whose polar divisors are $P_1 \cdots P_g P'$ and $P_1 \cdots P_g P''$ respectively. Now choose nonzero differentials of first kind $\omega_1, \omega_2, \omega_3$ such that $P_1 \cdots P_{g-1} | (\omega_1)$, $P_g | (\omega_2)$, $P' | (\omega_3)$. Setting $W_i = (\omega_i)$, $i = 1, 2, 3$, we get $P_1 \cdots P_g P' | W_1W_2W_3$. Hence $1, g_1 \in L(W_1W_2W_3)$, so $g_1 \in k(C)$. Similarly $g_2 \in k(C)$. For suitable $c \in k$, $g_1 + cg_2$ has polar divisor $P_1 \cdots P_g P'P''$; since $[K:k(g_1)] = g+1$, $[K:k(g_1+g_2)] = g+2$, we get $k(C) = K$. Next let P_1, P_2 be any places of K, not necessarily distinct, and choose integral canonical divisors W_1, W_2, W_3 prime to P_1. Then $d(W_1W_2W_3P_1^{-1}P_2^{-1}) = 6g-8 > 2g-2$, so $i(W_1W_2W_3P_1^{-1}P_2^{-1}) = 0$. Thus $r(W_1W_2W_3P_1^{-1}) = r(W_1W_2W_3P_1^{-1}P_2^{-1}) + 1$, and there exists $f \in L(W_1W_2W_3)$ such that $P_1 | (f)_0$, $P_1P_2 \nmid (f)_0$. Since each function in our present $L(W_1W_2W_3)$ is finite at P_1, this implies the nonsingularity of C. Any birational map of C

onto itself that is defined over k comes from a k-automorphism of K, which can merely permute the canonical divisors of K, so this birational map comes from a nonsingular projective transformation of S_{5g-6}; if we have a birational map of C onto itself that is not defined over k, we merely extend the constant field k to get the same result, and this finishes the case $g>1$. If $g=1$, we have $L(P_0^\nu)=\nu$ for $\nu>0$, so there exist $x, y\in K$ such that $(1, x)$ and $(1, x, y)$ are bases for $L(P_0^2)$ and $L(P_0^3)$ respectively. $[K:k(x)]=2$, $[K:k(y)]=3$, so $K=k(x, y)$. If C is the curve in S_2 having as homogeneous generic point over k the point $(1, x, y)$, then $k(C)=K$. The seven quantities $y^2, yx, y, x^3, x^2, x, 1\in L(P_0^6)$ (a space of dimension 6), so C is a cubic curve. C is nonsingular, for otherwise it would be rational. For any birational map σ of C onto itself such that $\sigma(P_0)=P_0$ each space $L(P_0^\nu)$ is invariant under σ, so $\sigma(x)=a+bx$, $\sigma(y)=c+dx+ey$, where $a, \cdots, e$ are constants and $be\neq 0$. This ends the case $g=1$. If $g=0$, take $C=S_1$. Q.E.D.

LEMMA. *If C is a nonsingular curve of genus g, there exists an algebraic group variety G which may be identified with a subgroup of finite index of the group of all birational transformations of C onto itself (that leave a given point $P_0\in C$ fixed if $g=1$) such that the map $\Psi: G\times C\to C$ defined by $\Psi(\sigma\times P)=\sigma(P)$ is an everywhere defined rational map.*

Let k be an algebraically closed field of definition for C and let C be the curve of the preceding lemma. Let $Y_0, \cdots, Y_n$ be projective coordinates of S_n. Then any birational map σ of C onto itself (which leaves P_0 fixed if $g=1$) is induced by a projective transformation $Y_i\to\sum_{j=0}^n c_{ij}Y_j$, where (c_{ij}) is a nonsingular matrix of order $(n+1)$ with constant coefficients. (So $|c_{ij}|\neq 0$.) Choose the integer N so large that the forms in $k[Y]$ of degree N which vanish on C actually define C, and let $F_1, \cdots, F_m, F_{m+1}, \cdots, F_M \in k[Y]$ be a basis for all forms of degree N such that the subspace spanned by $F_1, \cdots, F_m$ consists precisely of all forms of degree N vanishing on C. The matrix (c_{ij}) then gives rise to a linear transformation of the vector space with basis elements $F_1, \cdots, F_M$,

$$(c_{ij}): F_\beta\to\sum_{\alpha=1}^{M} A_{\beta\alpha}((c_{ij}))F_\alpha \qquad (\beta=1, \cdots, M),$$

where the $A_{\beta\alpha}$'s are forms in $k[\{c_{ij}\}]$. The conditions that (c_{ij}) map C into itself are then $A_{\beta\alpha}((c_{ij}))=0$, $\beta=1, \cdots, m$, $\alpha=m+1, \cdots, M$. Conversely, if $|c_{ij}|\neq 0$ and (c_{ij}) satisfies these last conditions it induces a birational map of C onto itself. (If $g=1$, we must add the further algebraic condition $(c_{ij}): P_0\to P_0$.) We may clearly assume that C spans S_n. Then two (c_{ij})'s give rise to the same birational transformation of C if and only if they are proportional. Thus the birational transformations of C (which leave P_0 fixed if $g=1$) may be identified with the points of an abstract algebraic variety G' (here an algebraic variety minus a subvariety) in $S_{(n+1)^2-1}$. G' is a group under matrix multiplication, which corresponds to the composition of birational maps. We have only to take G to be the component of the identity of G'. Q.E.D.

THEOREM. *Let K be an algebraic function field of one variable over the algebraically closed constant field k. If K has genus $g>0$, then the group $\mathcal{G}$ of all k-automorphisms of K (which leave a given place P_0 of K fixed if $g=1$) is finite.*

Let C be a nonsingular projective model of K/k. Then it suffices to show that the group of birational transformations of C onto itself (or the subgroup of these leaving P_0 fixed if $g=1$) is finite. It suffices to show that if C, G are as in the preceding lemma, then $G=e(=\text{the identity map})$. If $g>1$, fix some point $P_0\in C$. Let ϕ be the canonical map of C into its jacobian variety J, normalized so that $\phi(P_0)=0$ (cf. [7]). Since J is an abelian variety we can write $\phi\Psi(\sigma\times P)=\psi(\sigma)+\psi'(P)$, where ψ, ψ' are rational maps of G and C respectively into J, and where we may suppose that $\psi(e)=0$. Thus $\phi\sigma(P)=\psi(\sigma)+\psi'(P)$. Setting $\sigma=e$, we get $\psi'(P)=\phi(P)$. Setting $P=P_0$ gives $\psi(\sigma)=\phi\sigma(P_0)$. Hence

$$\phi\sigma(P) = \phi\sigma(P_0) + \phi(P).$$

If $\sigma(P_0)$ is not constant we get $\phi(C)+\phi(C)\subseteq\phi(C)$. Since $\phi(C)$ generates J, we must have $\phi(C)=J$. Since $\phi(C)$ is a curve and J has dimension g, we have a contradiction in the case $g>1$ unless $\sigma(P_0)=e(P_0)=P_0$; if $g=1$, we have $\sigma(P_0)=P_0$ by assumption. Thus $\phi\sigma(P)=\phi(P_0)+\phi(P)=\phi(P)$. Hence the divisor $\sigma(P)P^{-1}$ is principal. Since $g>0$, we must have $\sigma(P)=P$, so $\sigma=e$. Q.E.D.

[REMARK. The above argument can be modified slightly to give the following known result, which is the essence of our proof: An irreducible algebraic system of rational endomorphisms of an abelian variety consists of only one endomorphism.]

3. In this section we let K be a field of algebraic functions of one variable of genus $g>0$ over the arbitrary constant field k. Let $\mathcal{G}$ be the group of k-automorphisms of K if $g>1$; if $g=1$, let $\mathcal{G}$ be the group of k-automorphisms of K leaving fixed a given place P_0 of K. If $\mathcal{G}$ is infinite we say that K satisfies the *exceptional case*. We proceed to give a full account of the exceptional case.

LEMMA. *Let E be any field, $\mathcal{G}$ a group of automorphisms of E, and let F be the subfield of E consisting of all elements of E left fixed by each automorphism of $\mathcal{G}$. Then E is separably generated over F.*

This has content only if E has characteristic $p\neq 0$. We have to show that if we have a relation $\sum_{i=1}^{n} c_i f_i^p=0$, where each $c_i\in F$ and each $f_i\in E$ and where not all the c_i's are 0, then $f_1, \cdots, f_n$ are linearly dependent over F. Clearly we may take $n>1$. If $\sigma_1, \cdots, \sigma_n\in\mathcal{G}$, we have $\sum_{i=1}^{n} c_i\sigma_j(f_i^p)=0$, $j=1, \cdots, n$, so $|\sigma_j(f_i^p)|_{i,j=1,\cdots,n}=0$, and hence $|\sigma_j(f_i)|_{i,j=1,\cdots,n}=0$. Let r

be the maximal rank that $(\sigma_j(f_i))_{i,j=1,\cdots,n}$ can assume for $\sigma_1, \cdots, \sigma_n \in \mathcal{G}$; then $1 \leqq r < n$. Reorder the f_i's and choose $\sigma_1, \cdots, \sigma_r \in \mathcal{G}$ so that $|\sigma_j(f_i)|_{i,j=1,\cdots,r} \neq 0$. Hold $\sigma_1, \cdots, \sigma_r$ fixed and let $\sigma_{r+1} \in \mathcal{G}$ be arbitrary. Then $|\sigma_j(f_i)|_{i,j=1,\cdots,r+1} = 0$, so there exist $h_1, \cdots, h_r \in E$ such that $\sigma_j(f_{r+1}) = \sum_{i=1}^r h_i\sigma_j(f_i)$, $j = 1, \cdots, r+1$, and $h_1, \cdots, h_r$ are unique (i.e. independent of the choice of σ_{r+1}). Thus for any $\sigma \in \mathcal{G}$ we have $\sigma(f_{r+1}) = \sum_{i=1}^r h_i\sigma(f_i)$. If $\bar{\sigma} \in \mathcal{G}$, we have $\sigma(f_{r+1}) = \bar{\sigma}\bar{\sigma}^{-1}\sigma(f_{r+1}) = \bar{\sigma}\sum_{i=1}^r h_i\bar{\sigma}^{-1}\sigma(f_i) = \sum_{i=1}^r \bar{\sigma}(h_i)\sigma(f_i)$. By the unicity of $h_1, \cdots, h_r$, we have $\bar{\sigma}(h_i) = h_i$, so each $h_i \in F$. Hence $f_1, \cdots, f_n$ are linearly dependent over F.

COROLLARY. *If K is an arbitrary algebraic function field of one variable with constant field k (K possibly of genus zero) and if K possesses an infinite number of k-automorphisms, then K is separably generated over k.*

For the subfield of K left element-wise fixed by each k-automorphism of K must contain k and be of infinite index under K. Hence this subfield is k itself.

Now let K/k be such that the exceptional case holds. Then K is separably generated over k. If k' is any algebraic extension of k we can define $k'K$, which is a function field of one variable with constant field k'. Any place of $k'K$ lies over a unique place of K and over any place of K lies exactly one place of $k'K$. (By a place of K/k we mean a k-homomorphism of a valuation ring of K into a fixed algebraic closure of k.) Any automorphism $\sigma \in \mathcal{G}$ induces a k'-automorphism of $k'K$, so $k'K$ has an infinity of k'-automorphisms. Let the curve C be a projective model of K/k each point of which is simple with reference to k. Then C has only a finite number of points that are not absolutely simple, and these correspond to a finite number of distinct places $P_1, \cdots, P_s$ of K. Such places we call *singular places* of K; the residue class field of K at each place P_i, denoted by $k(P_i)$, must be inseparable over k (cf. [8]). Clearly the places $P_1, \cdots, P_s$ must be permuted among themselves by each $\sigma \in \mathcal{G}$. Thus each k'-automorphism of $k'K$ corresponding to any $\sigma \in \mathcal{G}$ must permute the places of $k'K$ lying over $P_1, \cdots, P_s$. The genus of $k'K$ is $\leqq g$, with equality if $s = 0$ or if k' is separable over k [4; 2], so that $k'K/k'$ either satisfies the exceptional case or has genus zero. But the exceptional case cannot arise if the constant field is algebraically closed, so $\bar{k}K/\bar{k}$ must be rational. ($\bar{k}$ denotes the algebraic closure of k.) Hence $s > 0$ and K has characteristic $p \neq 0$.

LEMMA. *Let K/k satisfy the exceptional case. Then there exists a place P of K and a subgroup Γ of the group of all k-automorphisms of K such that*

(1) *Γ is of finite index in the group of all k-automorphisms of K.*

(2) *Each $\sigma \in \Gamma$ leaves P fixed, and if $\sigma \in \Gamma$, $\sigma \neq e$, then P is the only place of K left fixed by σ.*

Proof. Let k' be any algebraic extension field of k such that $k'K/k'$ also satisfies the exceptional case. Suppose that P' is a place of $k'K$ and Γ' a subgroup of the group of all k'-automorphisms of $k'K$, such that (1) and (2) hold for $k'K$, P', Γ'. Then we have our theorem for K/k proved if we let P be the place of K lying below P' and let Γ consist of all $\sigma\in\Gamma'$ that come from k-automorphisms of K. Hence it suffices to prove our theorem for $k'K/k'$, provided $k'K/k'$ has genus >0. The genus of K drops to zero when we extend k to $\bar{k}$, hence when we extend k to $k^{p^{-\infty}}$, hence when we extend k to $k^{p^{-\nu}}$, for some integer ν. If we choose ν minimal and set $k'=k^{p^{-(\nu-1)}}$, then $k'K/k'$ has genus >0, while $(k')^{1/p}K/(k')^{1/p}$ has genus zero. Hence we may assume that $k^{1/p}K/k^{1/p}$ has genus zero. If we now let k' be the part of $\bar{k}$ that is separably over k, then $k'K$ has the same genus as K while $(k')^{1/p}K$ is still of genus zero. Hence we may assume to begin with that $k^{1/p}K$ has genus zero and that k is separable algebraically closed. Then $k^{1/p}K/k^{1/p}\cong kK^p/k$, so the subfield kK^p of K has genus zero. Since k is separably algebraically closed, K has a place of degree one, hence so has kK^p, so kK^p is rational. Write $kK^p=k(y)$, for some $y\in K$. If x is any separating variable for K/k then each element of K is both separable and purely inseparable over $k(x, y)$, so $K=k(x, y)$. $x\notin k(y)$, $x^p\in k(y)$, so $[K:k(y)]=p$. Any k-automorphism σ of K induces a k-automorphism of $kK^p=k(y)$, so $\sigma(y)=(ay+b)/(cy+d)$, where $a, b, c, d\in k$ and $ad\neq bc$. Furthermore, since $K^p\subseteq k(y)$, the action of σ on y completely determines σ. Let P be a fixed singular place of K. Then the group H of all k-automorphisms σ of K such that $\sigma(P)=P$ is of finite index in the group of all k-automorphisms of K, so we may restrict our σ's to H. First suppose that $P(y)=\alpha\notin(k, \infty)$. Then α is inseparable over k. For each $\sigma\in H$ we have $c\alpha^2+d\alpha=a\alpha+b$, so we must have $p=2$, $d=a$, $b=c\alpha^2$, $\alpha^2\in k$. Hence $\sigma(y)=(ay+c\alpha^2)/(cy+a)$. If $\sigma\in H$, $\sigma\neq e$, we have $c\neq 0$, so P is the only place of K left fixed by σ. Thus if we set $\Gamma=H$ we are done in our special case. Hence we may suppose that $P(y)\in(k, \infty)$, and hence that $P(y)=0$. Then for $\sigma\in H$ we have $\sigma(y)=ay/(1+cy)$, $a, c\in k$, $a\neq 0$. P is the only place of K lying over the place $(y=0)$ of $k(y)$, so if e, f are the ramification index and residue class field degree respectively of P over $k(y)$, then $ef=p$. If $f=1$, then P is a place of degree one of K, hence nonsingular, contrary to assumption. Thus $f=p$, $e=1$, so $v_P(y)=1$. We now choose $x\in K$ such that $x\notin k(y)$ and $x^p=f(y)\in k[y]$, where we suppose that the degree n of the polynomial $f(y)$ is minimal for all such x. $n>0$. If $\sigma\in H$, then

$$(\sigma(x))^p = f(\sigma(y)) = f\left(\frac{ay}{1+cy}\right).$$

Choose the integer i such that $(i-1)p<n\leqq ip$. Then $i>0$ and

$$((1+cy)^i\sigma(x))^p = (1+cy)^{pi}f\left(\frac{ay}{1+cy}\right)\in k[y].$$

Now $P((1+cy)^i\sigma(x))=P(\sigma(x))=P(x)$, since $\sigma\in H$, so $v_P((1+cy)^i\sigma(x)-x)>0$.

Hence the only pole of $((1+cy)^i\sigma(x)-x)/y$ is at $(y=\infty)$, and thus

$$\left(\frac{(1+cy)^i\sigma(x)-x}{y}\right)^p=\frac{(1+cy)^{pi}f(ay/(1+cy))-f(y)}{y^p}$$

$=$a polynomial in y of degree $\leqq pi-p<n$. By the minimality property of n, $((1+cy)^i\sigma(x)-x)/y\in k[y]$, so we can write $(1+cy)^i\sigma(x)=x+h(y)$, with $h(y)\in k[y]$, and we deduce

$$f(y)+(h(y))^p=(1+cy)^{ip}f\left(\frac{ay}{1+cy}\right).$$

Differentiating,

$$f'(y)=a(1+cy)^{ip-2}f'\left(\frac{ay}{1+cy}\right).$$

Since K is separably generated over k, $f'(y)\neq 0$, so we write $f'(y)=y^r u(y)$, where $r\geqq 0$ and $u(y)\in k[y]$, $u(0)\neq 0$. Thus

$$u(y)=a^{r+1}(1+cy)^{ip-2-r}u\left(\frac{ay}{1+cy}\right).$$

Setting $y=0$ gives $a^{r+1}=1$, so there are only a finite number of possibilities for a. If we let Γ consist of all $\sigma\in H$ with $a=1$, properties (1), (2) follow immediately. Q.E.D.

Lemma. *If K/k satisfies the exceptional case, then K has precisely one singular place P and the residue class field $k(P)$ is purely inseparable over k. $\mathcal{G}$ contains a normal subgroup G such that*

(1) *$\mathcal{G}/G$ is cyclic and of finite order prime to p.*

(2) *If $\sigma\in G$, $\sigma\neq e$, then $\sigma(P)=P$ and P is the only place of K left fixed by σ.*

(3) *G is commutative and each of its elements has order p.*

If $g=1$, then $P_0=P$ and $\mathcal{G}$ is the group of all k-automorphisms of K.

Proof. We already know that K has at least one singular place P, and at most a finite number, and that each k-automorphism of K permutes the singular places, so the preceding lemma implies the first statement. If $k(P)$ were not purely inseparable over k we could let k' be the separable part of $k(P)$ and then the field $k'K/k'$ would satisfy the exceptional case and have more than one singular place. The final statement also follows from the previous lemma. Since P is the only singular place of K, for each $\sigma\in\mathcal{G}$ we have $\sigma(P)=P$. We can write $\bar{k}K=\bar{k}(z)$, where z is infinite at P. Then $\sigma(z)=az+b$, where a, $b\in\bar{k}$, $a\neq 0$, and a, b completely determine σ. Let G be the kernel of the homomorphism $\sigma\rightarrow a$ of $\mathcal{G}$ into the multiplicative group of $\bar{k}$. Then G consists precisely of e and of all $\sigma\in\mathcal{G}$ such that P is the only place left fixed by σ, verifying (2). G contains the Γ of the previous lemma, which implies (1). If $\sigma\in G$, then $\sigma(z)=z+b$, which gives (3). Q.E.D.

Now let K/k be any function field satisfying the exceptional case, and let P, G be as in the last lemma. Let G_0 be a finite subgroup of G of order p^n and let $K_0\supset k$ be the field of elements of K left fixed by each automorphism of G_0. If $t\in K_0$, $\sigma_0\in G_0$, $\sigma\in G$, then $\sigma_0(\sigma(t))=\sigma(\sigma_0(t))=\sigma(t)$, so $\sigma(t)\in K_0$. Thus each $\sigma\in G$ induces an automorphism of K_0. Furthermore K is a normal separable extension of K_0 of degree p^n. Consider Zeuthen's formula, $2g-2=p^n(2g_0-2)+d(D)$, where g_0 is the genus of K_0 and D the different of K with respect to K_0. Let P_0 be the place of K_0 lying under P. If the place P' of K lies over P_0 and $P'\neq P$, then for any $\sigma_0\in G_0$ the place $\sigma_0(P')$ lies over P_0 and the various places $\sigma_0(P')$ (for σ_0 ranging over G_0) are distinct from each other and from P; this implies that at least (p^n+1) distinct places of K lie over P_0, contradicting $[K:K_0]=p^n$. Hence P is the only place of K lying over P_0. Next let P' be any place of K distinct from P. Then the various places $\sigma_0(P')$ (for σ_0 ranging over G_0) are distinct and in number p^n and all lie over the same place of K_0; it follows that each ramification index and each residue class field degree of each $\sigma_0(P')$ over K_0 is 1, so $P'\nmid D$. Hence we can write $D=P^r$, for some $r\geqq 0$. If e and f are the ramification index and residue class field degree respectively for P over P_0, then $ef=p^n$. If $n>0$ then either $p|f$ (so $k(P)$ is inseparable over $k(P_0)$) or $p|e$, and hence (by [2, p. 69]) $P^e|D$. Hence $D=P^r$, with $r\geqq e$. Thus $2g-2-p^n(2g_0-2)=r\,d(P)\geqq ef\,d(P_0)=p^nd(P_0)$. Hence $2g-2\geqq p^n(2g_0-2+d(P_0))$. Thus if n is sufficiently large we have $g_0=0$ and $d(P_0)\leqq 2$. Take n so large that this is true. Then if $d(P_0)=2$ we must have $p=2$, and we can find a subgroup G_0' of G such that $G_0'\supset G_0$ and G_0'/G_0 has order 2. Let K_0' be the subfield of K consisting of all elements left fixed by each $\sigma_0'\in G_0'$. Then K_0 is separable over K_0' and $[K_0:K_0']=2$. Let P_0' be the place of K_0' lying under P_0. P_0 is the only place of K_0 lying over P_0'. Let e', f' be the ramification index and residue class field degree respectively for P_0 over P_0', and let D' be the different of K_0/K_0'. By Zeuthen's formula, $d(D')=2$. If $e'=2$ then $P_0^2|D'$, so $d(D')\geqq 4$, which is false, so $e'\neq 2$. But $e'f'=2$, so we have $e'=1, f'=2$, so $d(P_0')=1$. As a result, if n is sufficiently large we certainly have $g_0=0$ and $d(P_0)=1$. Here we can write $K_0=k(x)$, where $v_{P_0}(x)=-1$.

Fix a subgroup G_0 of G of least possible order p^n such that the fixed field K_0 of G_0 is of the form $K_0=k(x)$, where $v_{P_0}(x)=-1$, P_0 being the place of K_0 under P, and let $\sigma_1, \cdots, \sigma_n$ be a set of generators for G_0. For $i=1, \cdots, n$ let G_i be the subgroup of G_0 generated by $\sigma_1, \cdots, \sigma_{i-1}, \sigma_{i+1}, \cdots, \sigma_n$, and let K_i be the fixed field of G_i. K_i is a normal extension of $k(x)$ of degree p and the restriction of σ_i to K_i generates the Galois group of K_i over $k(x)$. Hence we can find a $y_i\in K_i$ such that $\sigma_i(y_i)=y_i+1$, and we have $y_i^p-y_i=f_i(x)\in k(x)$. We wish to show that y_i can be chosen so as to give $f_i(x)$ a particularly simple form. Any $\sigma \in G$ induces an automorphism of each field $k(x)$, $K_1, \cdots, K_n$, and since $\sigma(P_0)=P_0$ we have $\sigma(x)=\alpha x+\beta$, with α, $\beta\in k$. Since $\sigma^p=e$, $\alpha=1$, so $\sigma(x)=x+\beta$. $\sigma(y_i)\in K_i$ and $\sigma_i(\sigma(y_i)-y_i)=\sigma(\sigma_i(y_i))-\sigma_i(y_i)=\sigma(y_i)-y_i$, so $\sigma(y_i)-y_i=g(x)\in k(x)$. But $(\sigma(y_i))^p-\sigma(y_i)=f_i(\sigma(x))$, so $(g(x))^p-g(x)=f_i(x+\beta)-f_i(x)$. There are an infinity of σ's so we can assume that σ is chosen so that P_0 is the only pole that $f_i(x)$ and $f_i(x+\beta)$ can have in common. Use partial fractions to write $g(x)=g_1(x)+g_2(x)$, where $g_1(x)$ has poles only at the poles of $f_i(x)$ and $g_2(x)$ has no pole in common with $f_i(x)$. Then $(g_1(x))^p-g_1(x)+f_i(x)=f_i(x+\beta)-(g_2(x))^p+g_2(x)$ has poles only at P_0, that is $(g_1(x))^p-g_1(x)+f_i(x)\in k[x]$. If we set $z_i=y_i+g_1(x)$ we get $\sigma_i(z_i)=z_i+1$ and $z_i^p-z_i\in k[x]$. Hence we may suppose y_i chosen so that $f_i(x)\in k[x]$.

We digress for a moment to prove the following contention: If u is an indeterminate and $\bar{k}(u, v)$ a field such that $v^p-v=f(u)\in\bar{k}[u]$, and if $\bar{k}(u, v)/\bar{k}$ has genus zero, then we can write $f(u)=(g(u))^p-g(u)+au+b$, where $g(u)\in\bar{k}[u]$ and a, $b\in\bar{k}$. First, if $v\in\bar{k}(u)$, then $v\in\bar{k}[u]$ and there is nothing to prove. So we may suppose that $[\bar{k}(u, v):\bar{k}(u)]=p$. Let $f(u)=cu^r+h(u)$, where $c\in\bar{k}$, $c\neq 0$, and where $h(u)$ has degree less than r. $r>0$. If $p\mid r$, say $r=ps$, then $(v-c^{1/p}u^s)^p-(v-c^{1/p}u^s)=h(u)+c^{1/p}u^s$, and it clearly suffices to prove our contention with $f(u)$ replaced by $h(u)+c^{1/p}u^s$, a polynomial of smaller degree. Repeating this process, we get that it suffices to prove the following: If $v^p-v=cu^r+h(u)$, where $c\in\bar{k}$, $c\neq 0$, $h(u)\in\bar{k}[u]$ of degree $<r$, and $r>1$ is prime to p, then $\bar{k}(u, v)/\bar{k}$ has genus >0. To do this consider the differential du of $\bar{k}(u, v)$. For any $\eta\in\bar{k}$ there are p distinct places of $\bar{k}(u, v)$ lying over the place $(u=\eta)$ of $\bar{k}(u)$, so that $u-\eta$ is a uniformizing parameter at each of these places; hence du has order zero at each place of $\bar{k}(u, v)$ not lying over the place $(u=\infty)$ of $\bar{k}(u)$. But if P is a place of $\bar{k}(u, v)$ such that $P(u)=\infty$, then $pv_P(v)=rv_P(u)$, so $v_P(u)=-p$, $v_P(v)=-r$. Hence $v_P(du)=v_P(dv/(cru^{r-1}+h'(u))$ $=-r-1-(r-1)(-p)=(p-1)(r-1)-2$. This is $\geqq 0$ unless $p=2$, $r=2$, which case is excluded by the condition $p\nmid r$. Hence du is a nonzero differential of the first kind of $\bar{k}(u, v)$. This proves our contention.

Returning to our discussion of K, fix some i $(i=1, \cdots, n)$ and suppose that $f_i(x)$ has degree N. Write $f_i(x)=F(x^{p^\nu})$ for some integer $\nu\geqq 0$, where F is a polynomial. Setting $u=x^{p^\nu}$, $y_i^p-y_i=F(u)$. $\bar{k}K$ is rational, so by Lüroth's theorem so is $\bar{k}(u, y_i)$. By the above contention we can write $F(u)=(g(u))^p-g(u)+au+b$, where $g(u)\in\bar{k}[u]$ and a, $b\in\bar{k}$, and where we can assume $g(0)=0$. Hence $F'(u)=-g'(u)+a$. $F(u)$ has degree N/p^ν so (assuming $g(u)\neq 0$) $g(u)$ has degree $N/p^{\nu+1}$, and hence $F'(u)$ has degree $\leqq N/p^{\nu+1}-1$. Hence we can find a polynomial $H(u)\in k[u]$ of degree $\leqq N/p^{\nu+1}$ such that $H'(u)=F'(u)$. Writing $z_i=y_i+H(u)$ we get $\sigma_i(z_i)=z_i+1$ and $z_i^p-z_i=F(u)+(H(u))^p-H(u)=$ a polynomial in $k[u]$ of degree $\leqq N/p^\nu$ with derivative zero. Hence $z_i^p-z_i=G(x^{p^{\nu+1}})$, where $G(x^{p^{\nu+1}})$ is a polynomial of degree $\leqq N$ with coefficients in k. Hence we could have assumed to begin with that $f_i(x)$

is a polynomial in $x^{p^{\nu+1}}$, and repeat this process, if possible, to replace $f_i(x)$ by another polynomial of degree $\leqq N$ that is a polynomial in $x^{p^{\nu+2}}$, etc. This process must come to an end, so finally we get $g(u)=0$. Then $y_i^p-y_i=ax^{p^\nu}+b$, with $a,\ b\in k$. If $\nu>0$ and $a\in k^p$, then $(y_i-a^{1/p}x^{p^{\nu-1}})^p-(y_i-a^{1/p}x^{p^{\nu-1}})$ $=a^{1/p}x^{p^{\nu-1}}+b$, so if we choose ν minimal we have either $\nu=0$ or $a\notin k^p$. But if $\nu=0$, then $y_i^p-y_i=ax+b$, so K_i is a rational field with the place under P rational, contradicting the minimality of n. Hence we can assume that for $i=1,\cdots,n$ we have $y_i^p-y_i=a_ix^{p^{m_i}}+b_i$, with $a_i,\ b_i\in k,\ a_i\notin k^p$, and $m_i>0$. The only automorphism of G_0 leaving each y_i fixed is e, so $K=k(x,y_1,\cdots,y_n)$. For any $\sigma\in G$ we have $\sigma(x)=x+\beta,\ \beta\in k$. Setting $\alpha_i=\sigma(y_i)-y_i$, we get $\alpha_i^p-\alpha_i=a_i\beta^{p^{m_i}}$, so $\alpha_i\in k$. Conversely suppose $\alpha_1,\cdots,\alpha_n,\ \beta\in k$ and that $\alpha_i^p-\alpha_i=a_i\beta^{p^{m_i}},\ i=1,\cdots,n$. Let $X,\ Y_1,\cdots,\ Y_n$ be indeterminates. Then the prime ideal in $k[X,\ Y]$ having $(x,y_1,\cdots,y_n)$ as generic zero is generated by the various polynomials $(Y_i^p-Y_i-a_iX^{p^{m_i}}-b_i)$, so setting $\sigma(X)=X+\beta$, $\sigma(Y_i)=Y_i+\alpha_i,\ i=1,\cdots,n$, gives an automorphism of this ring carrying our prime ideal onto itself, and hence we get an automorphism σ of $k[x,\ y_1,\cdots,y_n]$ (and hence of K) such that $\sigma(x)=x+\beta,\ \sigma(y_i)=y_i+\alpha_i$. We summarize as follows.

THEOREM. *Let K/k satisfy the exceptional case. Then there exist $x\in K$ such that $[K:k(x)]=p^n$, where $p\neq 0$ is the characteristic of K, elements $y_1,\cdots,y_n\in K,\ a_1,\cdots,a_n,\ b_1,\cdots,b_n\in k$, with $a_1,\cdots,a_n\notin k^p$, and strictly positive integers $m_1,\cdots,m_n$ such that $K=k(x,\ y_1,\cdots,y_n)$ and $y_i^p-y_i=a_ix^{p^{m_i}}+b_i$, $i=1,\cdots,n$. For each set of elements $\beta,\ \alpha_1,\cdots,\alpha_n\in k$ such that $\alpha_i^p-\alpha_i=a_i\beta^{p^{m_i}},\ i=1,\cdots,n$, we have an automorphism σ of K/k defined by $\sigma(x)=x+\beta,\ \sigma(y_i)=y_i+\alpha_i,\ i=1,\cdots,n$, and the set of all such automorphisms σ forms the normal subgroup G of the full group of automorphisms $\mathcal{G}$ of K/k such that $\mathcal{G}/G$ is cyclic of finite order prime to p.*

It is easy to establish a converse of this theorem: Let $a_1,\cdots,a_n$, $b_1,\cdots,b_n,\ m_1,\cdots,m_n$ be as above and let K be the splitting field over $k(x)$ of the polynomial $\prod_{i=1}^n(Y^p-Y-a_ix^{p^{m_i}}-b_i)$. By deleting some of the factors in the product if necessary, we can assume that $[K:k(x)]=p^n$. If we have an infinite number of sets $\beta,\alpha_1,\cdots,\alpha_n\in k$ satisfying $\alpha_i^p-\alpha_i=a_i\beta^{p^{m_i}},\ i=1,\cdots$, n, and if K has genus >0, then K/k satisfies the exceptional case.

If K/k is exceptional, then its genus g cannot be arbitrary. First, since the genus drops to zero when we extend k to $\bar{k}$, by a result of Tate [6] g must be a multiple of $(p-1)/2$. Second, Zeuthen's formula $2g-2=-2p^n+rd(P)$ implies $2g-2\equiv 0\ (p)$. Thus g is of the form $g=(sp-2)(p-1)/2$, where s is an integer. For example, if $K=k(x,\ y)$, where $y^p-y=ax^p,\ a\in k,\ a\notin k^p$, then the curve in the projective plane whose generic point over k is $(1,\ x,\ y)$ is immediately seen to be nonsingular with reference to k, so in this case g $=(p-1)(p-2)/2$. This last field K is clearly exceptional if $p>2$ and k is separably algebraically closed.

References

1. P. Appell and E. Goursat, *Théorie des fonctions algébriques et de leurs intégrales*, Paris, 1895.

2. C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, no. 6, 1951.

3. K. Iwasawa and T. Tamagawa, *On the group of automorphisms of a function field*, J. Math. Soc. Japan vol. 3 (1951) and vol. 4 (1952).

4. M. Rosenlicht, *Equivalence relations on algebraic curves*, Ann. of Math. vol. 56 (1952).

5. H. L. Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharacteristik*, J. Reine Angew. Math. vol. 179 (1938).

6. J. Tate, *Genus change in inseparable extensions of function fields*, Proc. Amer. Math. Soc. vol. 3 (1952).

7. A. Weil, *Variétés abéliennes et courbes algébriques*, Paris, 1948.

8. O. Zariski, *The concept of a simple point of an abstract algebraic variety*, Trans. Amer. Math. Soc. vol. 62 (1947).

Northwestern University,
Evanston, Ill.