J. Aust. Math. Soc. **88** (2010), 301–312
doi:10.1017/S1446788710000108

FINITE GROUPS AS GALOIS GROUPS OF FUNCTION FIELDS WITH INFINITE FIELD OF CONSTANTS

C. ÁLVAREZ-GARCÍA and G. VILLA-SALVADOR✉

(Received 5 June 2009; accepted 15 January 2010)

Communicated by F. Calegari

Abstract

Let E/k be a function field over an infinite field of constants. Assume that $E/k(x)$ is a separable extension of degree greater than one such that there exists a place of degree one of $k(x)$ ramified in E. Let K/k be a function field. We prove that there exist infinitely many nonisomorphic separable extensions L/K such that $[L:K]=[E:k(x)]$ and $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong \mathrm{Aut}_{k(x)} E$.

2000 *Mathematics subject classification*: primary 12F12; secondary 11R58, 12F10, 14H05.

Keywords and phrases: automorphism groups, function fields, infinite field of constants, nonseparably generated function fields.

1. Introduction

Let K be an algebraic function field over a field k and let $\mathrm{Aut}_k K$ be its full group of automorphisms. For $k=\mathbb{C}$, Greenberg [4] proved in 1974 that given a nontrivial finite group G, there exist infinitely many Galois extensions L/K such that $\mathrm{Gal}(L/K)$ is isomorphic to G and that $\mathrm{Gal}(L/K)=\mathrm{Aut}_{\mathbb{C}} L$. This result of Greenberg gives a positive answer to the inverse problem in Galois theory for function fields $K/\mathbb{C}$.

In several other cases Greenberg's result can be extended to function fields K/k with k an algebraically closed field.

Madden and Valentini [6] proved that every finite group can be realized as the full automorphism group of an algebraic function field K/k. D'Mello and Madan [3] established the theorem of Greenberg in the case where G is a solvable group G and $K=k(x)$ is a rational function field.

The main result of Stichtenoth in [8] is that if $E/k(x)$ a finite separable extension of degree greater than one, then, for every function field K/k of genus greater than one, there exist infinitely many nonisomorphic separable extensions L/K such that

$$[E:k(x)]=[L:K] \quad \text{and} \quad \mathrm{Aut}_{k(x)} E \cong \mathrm{Aut}_K L = \mathrm{Aut}_k L.$$

The results of Stichtenoth and of D'Mello and Madan can be combined to obtain the analogous of Greenberg's theorem provided that the group G is solvable and the genus of K is larger than one.

Madan and Rosen [5] proved that Greenberg's result remains valid for an arbitrary function field K/k with k an algebraically closed field of arbitrary characteristic. This result gives a positive answer to the inverse problem of Galois theory for any field K over an algebraically closed field of constants.

Rzedowski and Villa [7] proved an analogue of Stichtenoth's result for congruence function fields without restriction on the genus, provided that in the extension $E/k(x)$ there exist prime divisors of degree one, one ramified and another unramified. In [1] we remove the ramification restrictions given in [7].

A natural question is what happens when the field of constants k of a function field is an arbitrary field. Some of the results are straightforward for separably generated function field extensions K/k, for instance, when k is a perfect field. If K/k is not a separably generated extension, some of the tools we have in the case where k is perfect are no longer available; for instance the Castelnuovo–Severi inequality, the difference of the extension, and so on. We also have to deal with the special behavior of new constants and so on.

The main goal of this paper is to establish an analogue of the main result of [7] for an infinite field of constants k now under one ramification restriction. We prove that given any infinite field k, if $E/k(x)$ is any separable extension, where k is the full field of constants of E, such that a place of $k(x)$ of degree one is ramified in E, then for any function field K/k, there exist infinitely many nonisomorphic function fields over k such that L/K is a separable extension of the same degree as $E/k(x)$ and $\mathrm{Aut}_K L = \mathrm{Aut}_k L \cong \mathrm{Aut}_{k(x)} E$. This is Theorem 4.3.

Given a function field K/k, we first choose a suitable $y \in K$ and construct a suitable C-improvement $E_1/k(y)$ of $E/k(x)$ (see [7]) such that the field of constants of $L = E_1 K$ is k, while $[L : K] = [K : k(y)]$ and the intermediate fields of L other than K have large enough genus (Proposition 3.5). With this condition, it follows that any element of the group of automorphisms of L over k restricts to an automorphism of K (Proposition 3.6). The next step is to find a ramification of the places in the support of $(y)_K$ in such a way that any automorphism of L over k fixes K elementwise. If the constant field is finite or algebraically closed then the extension $K/k(y)$ is separable. We use the C-improvements constructed in Proposition 4.1 to deal with the inseparable case.

The paper is organized as follows. In Section 2 we give several general results that will be used to find field extensions with suitable properties to be used in our construction. In Section 3 we find a bound for the genus of the compositum of fields. When K/k is separably generated, we have the Castelnuovo–Severi inequality. We find an analogue of this bound of the genus for general k. This is Proposition 3.5. As a consequence of this variant of the Castelnuovo–Severi inequality, we have the analogue of a result of Madden and Valentini [6] that establishes that if L/K is an extension such that every proper intermediate field has large enough genus, then for any automorphism σ of L, we have $\sigma(K) = K$.

Section 4 deals with function field extensions with a prime divisor of degree one ramified. Under this ramification restriction it is possible to prove our main result.

We use the following notation. The field k is an infinite field and K/k denotes a function field with full field of constants k. In a rational function field $k(x)$, P_f denotes the place defined by the irreducible polynomial f. For a field extension F/K, the group of automorphisms of L that fix K pointwise is denoted by $\operatorname{Aut}_K F$. For a function field E/k, let $(x)_E$ denote the principal divisor of x in E and deg P denote the degree of a place P of E. For an extension F/E, $\operatorname{Con}_{F/E}$ is the conorm map with respect to F/E. If F/E is a separable extension we write $D_{F/E}$ for the different of the extension.

2. Function fields over infinite field of constants

In this section we give some general results that will be needed to prove the main result of the paper.

LEMMA 2.1. *Let $F/k(x)$ be a Galois extension and let $k(y)$ be a rational function field such that $([F : k(x)], [k(y) : k(x)]) = 1$. If E/l is an intermediate field of $F/k(x)$, then the field of constants of $E(y)$ is l.*

PROOF. Let N be the field of constants of $E(y)$. Since N/l is a separable we have that $[E : l(x)] = [EN : N(x)]$. Since $[k(y) : k(x)] = [N(y) : N(x)]$, it follows that $([EN : N(x)], [N(y) : N(x)]) = 1$. Hence $[E(y) : N(y)] = [EN : N(x)]$.

$$\begin{array}{ccccc} l(y) & \text{---} & E(y) & \text{---} & F(y) \\ | & & | & & | \\ l(x) & \text{---} & E & \text{---} & F \end{array} \qquad \begin{array}{ccccc} N(y) & \text{---} & E(y) & \text{---} & FN(y) \\ | & & | & & | \\ N(x) & \text{---} & EN & \text{---} & FN \end{array}$$

Similarly $[E(y) : l(y)] = [E : l(x)]$, and so we obtain $[E(y) : N(y)] = [E(y) : l(y)]$. Therefore $N(y) = l(y)$ and $N = l$. □

The proof of Lemma 2.2 is similar to the proof in the case where the constant field is perfect [9].

LEMMA 2.2. *Suppose that F'/F is a finite separable extension of function fields. Let F_1, F_2 be intermediate fields of F'/F such that $F' = F_1F_2$. Then, for a place $P \in \mathbb{P}_F$:*

(1) *if P is completely decomposed in F_1/F and F_2/F, then P is completely decomposed in F'/F;*

(2) *if P is unramified and separable in F_1/F and F_2/F, then P is unramified and separable in F'/F.* □

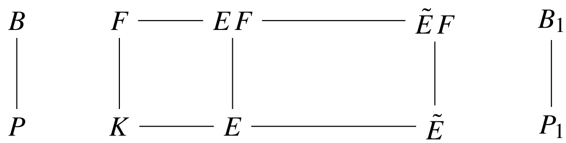
As a consequence of (2) of Lemma 2.2 we have the following lemma.

LEMMA 2.3. *Let K/k be a function field and let E/K be a finite separable extension with normal closure $\tilde{E}$. Assume that $P \in \mathbb{P}_K$ is ramified or inseparable in $\tilde{E}$. Then P is ramified or inseparable in E.* □

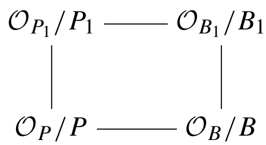
https://doi.org/10.1017/S1446788710000108 Published online by Cambridge University Press

LEMMA 2.4. *Suppose that E/K is a finite separable extension of function fields. Let P be a place of K ramified or inseparable in E. Then for a purely inseparable finite extension F/K the place B of F lying over P is ramified or inseparable in EF.*

PROOF. Let $\tilde{E}$ be the normal closure of E/K. Since $\tilde{E} \cap F = K$, the normal closure of EF/F is $\tilde{E}F$. Now we consider a place P_1 of $\tilde{E}$ lying over P and let B_1 be the extension of P_1 in $\tilde{E}F$. Since $B_1 \cap F$ is over P we have that $B_1 \cap F = B$.



Denote by $D(P_1|P)$ the decomposition group of P_1 and by $I(P_1|P)$ the inertia group. The restriction of an element in $D(B_1|B)$ to $\tilde{E}$ belongs to $D(P_1|P)$, so there is an embedding $\varphi : D(B_1|B) \to D(P_1|P)$ such that $\varphi(I(B_1|B)) \subseteq I(P_1|P)$. Since the place B_1 is the only extension of P_1 in $\tilde{E}F$, φ is an isomorphism.



On the other hand, $[\mathcal{O}_{B_1}/B_1 : \mathcal{O}_B/B]_s = [\mathcal{O}_{P_1}/P_1 : \mathcal{O}_P/P]_s$ since the extensions $(\mathcal{O}_B/B)/(\mathcal{O}_P/P)$, $(\mathcal{O}_{B_1}/B_1)/(\mathcal{O}_{P_1}/P_1)$ are purely inseparable. Hence

$$\begin{aligned}[D(P_1|P) : I(P_1|P)] &= [\mathcal{O}_{P_1}/P_1 : \mathcal{O}_P/P]_s = [\mathcal{O}_{B_1}/B_1 : \mathcal{O}_B/B]_s \\ &= [D(B_1|B) : I(B_1|B)].\end{aligned}$$

Therefore $\varphi(I(B_1|B)) = I(P_1|P)$, so B is ramified or inseparable in $\tilde{E}F/F$. Finally, from Lemma 2.3 we obtain that B is ramified or inseparable in EF/F. □

LEMMA 2.5. *Let E/K be a Galois extension of algebraic functions fields with field of constants k. Let $\sigma \in \mathrm{Gal}(E/K)$. Then if $\sigma \neq \mathrm{Id}$ the set $A_\sigma = \{B \in \mathbb{P}_E \mid \sigma(B) \neq B\}$ is infinite.*

PROOF. Suppose that A_σ is finite for some $\sigma \neq \mathrm{Id}$. Let K_1 be the fixed field of σ and $A_\sigma = \{B_1, \ldots, B_m\}$. Now $\sigma(B) = B$ for each place $B \in \mathbb{P}_E$ with $B \neq B_i$. Let $y_1 \in E \backslash K_1$ and $y_2 \in K_1$ be such that $v_{B_i}(y_2) > 0$. Then there exists j such that $v_{B_i}(y_1 y_2^j) > 0$ and $y_1 y_2^j \notin K_1$. Let c be a constant distinct from 1 and let $y = y_1 y_2^j + c$, $y \notin K_1$. Hence $v_{B_i}(y) = v_{B_i}(y + 1) = 0$. It follows that $\sigma(y) = y$, which implies that $\sigma(y) = ay$ with $a \in k$. Similarly, there exists $b \in k$ such that $\sigma(1 + y) = b(1 + y)$, then $1 + ay = b + by$. Since $y \notin k$ we obtain that $\sigma(y) = y$. Thus $y \in K_1$. This contradiction shows the result. □

https://doi.org/10.1017/S1446788710000108 Published online by Cambridge University Press

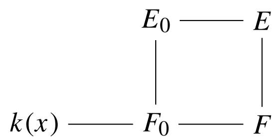
3. Bound for the genus of a compositum of fields

The Castelnuovo–Severi inequality is valid for separably generated extensions K/k. This inequality plays an important role in [7, 8]. In Proposition 3.5 we give an analogous inequality for K/k not necessarily separable generated. Then we deduce Proposition 3.6 which is the main result of this section. This is the analogue of the Madden–Valentini result in [6].

For a function field K/k of genus g_K, let $g'_K = \max\{g_K, 1\}$.

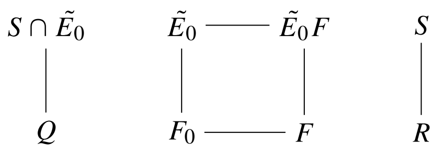
LEMMA 3.1. *Let F/k be a function field with separably closed field of constants. Given a separable geometric finite extension E/F, there exist infinitely many places in F that are completely decomposed in E/F. If $d = \min\{\deg P \mid P \in \mathbb{P}_F\}$ we can choose the places of degree less than or equal to $2g'_F d$.*

PROOF. Let P be a place of F such that $d = \deg P$. There exists $x \in F$ with pole divisor $P^{2g'_F}$. Denote by F_0 the separable closure of $k(x)$ in F and by E_0 the separable closure of $k(x)$ in E. Since E_0 and F are linearly disjoint over F_0 and $[E : k(x)]_i = [F : k(x)]_i$, then $E = E_0F$.



In the extension $E_0/k(x)$ there are a finite number of places which are either ramified or inseparable. Hence almost all places of degree one of $k(x)$ are unramified and separable in $E_0/k(x)$, so these places are completely decomposed in $E_0/k(x)$. Therefore there exist infinitely many places of degree one in F_0 which are completely decomposed in E_0.

Let Q be a place of degree one in F_0 completely decomposed in E_0 and let R be the place of F lying over Q. Let $\tilde{E}_0$ be a normal closure of E_0/F_0. Lemma 2.2 implies that Q is completely decomposed in $\tilde{E}_0/F_0$.



Since, given a place S of $\tilde{E}_0F$ lying over R, the decomposition group $D(S|R)$ embeds in the group $D(S \cap \tilde{E}_0|Q)$, then R is completely decomposed in E_0F/F. The relative degree $f(R|Q) = \deg R$ is less than or equal to $[F : k(x)] = 2g'_F d$. □

LEMMA 3.2. *Assume that k is separably closed, and consider a function field F/k such that F_1/k is a subfield of F such that F/F_1 is a separable extension of degree $n > 1$. Let $y \in F$ be an element such that $F = F_1(y)$ and $d_1 = \min\{\deg P \mid P \in \mathbb{P}_{F_1}\}$.*

https://doi.org/10.1017/S1446788710000108 Published online by Cambridge University Press

Then there exist infinitely many places $P \in \mathbb{P}_{F_1}$ of degree at most $2g'_{F_1} d_1$ having the following properties.

(1) *P has n distinct extensions $P_1, \ldots, P_n$ in F/F_1.*
(2) *The restrictions $P_1 \cap k(y), \ldots, P_n \cap k(y)$ are pairwise distinct places of $k(y)$.*

PROOF. Let $\varphi(z) = z^n + a_{n-1}z^{n-1} + \cdots + z_0 \in F_1[z]$ be the minimal polynomial of y over F_1. By Lemma 3.1 there are infinitely many places $P \in \mathbb{P}_{F_1}$ completely decomposed in F/F_1 and such that $\{1, \ldots, y^{n-1}\}$ is an integral basis of F/F_1 for almost all such places P. Since by Kummer's theorem the decomposition of the polynomial $\bar{\varphi}(z) \in (\mathcal{O}_P/P)[z]$ corresponds to the decomposition of P in F, we must have that $\bar{\varphi}(z) = \prod_{i=1}^{n}(z - c_i)$ with pairwise distinct elements $c_i \in \mathcal{O}_P/P$.

Let b_i be such that $c_i = b_i + P$. Again by Kummer's theorem we have that for $i = 1, \ldots, n$ there exists a unique place $P_i \in \mathbb{P}_F$ such that $P_i | P$ and $v_{P_i}(y - b_i) > 0$. There exist $\beta_i \in k$ and an integer $m \geq 0$ such that $b_i^{p^m} + P = \beta_i + P$. Hence

$$v_{P_i}(y^{p^m} - \beta_i) \geq \min\{v_{P_i}(y^{p^m} - b_i^{p^m}), v_{P_i}(b_i^{p^m} - \beta_i)\} > 0.$$

Since $\beta_i = \beta_j$ implies $c_i^{p^m} = c_j^{p^m}$, it follows that the elements β_i are pairwise distinct, so the restrictions $P_i \cap k(y^{p^m})$ are distinct. □

The following result can be found in [9].

LEMMA 3.3. *Let F_1/k be a subfield of F/k and let $[F : F_1] = n$. Assume that $\{z_1, \ldots, z_n\}$ is a basis of F/F_1 such that all $z_i \in L(C^{-1})$ for some divisor $C \in D_F$. Then $g_F \leq 1 + n(g_{F_1} - 1) + \deg C$.*

LEMMA 3.4. *Let F/k be a function field with separably closed field of constants. Suppose that F_1/k and F_2/k are subfields of F/k satisfying the following conditions.*

(1) *$F = F_1F_2$ and F/F_1 is separable.*
(2) *$[F : F_i] = n_i$ and F_i/k has genus g_i $(i = 1, 2)$.*

Then the genus g of F/k is bounded above by $1 + n_1(g_1 - 1) + 4n_1n_2g'_1g'_2d_1$, where $d_1 = \min\{\deg P \mid P \in \mathbb{P}_{F_1}\}$.

PROOF. Since $F = F_1F_2$ there are $y_1, \ldots, y_s \in F_2$ with $F = F_1(y_1, \ldots, y_s)$. The extension F/F_1 is separable, hence we can find $a_1, \ldots, a_s \in k$ such that the element $y = \sum a_j y_j \in F_2$ is a primitive element of F/F_1. Let $P \in \mathbb{P}_{F_1}$ be such that it has n_1 distinct extensions $P_1, \ldots, P_{n_1}$ in F and such that the restrictions $Q_i = P_i \cap F_2 \in \mathbb{P}_{F_2}$ are pairwise distinct (Lemma 3.1). We have that $\deg Q_i = 2g'_1 d_1$. There exists $u_i \in F_2$ with pole divisor $Q_i^{2g'_2}$. The elements $u_1, \ldots, u_{n_1}$ form a basis of F/F_1.

Suppose that $\sum x_i u_i = 0$ with $x_i \in F_1$ is a nontrivial linear combination. Let $j \in \{1, \ldots, n_1\}$ be such that $v_P(x_j) \leq v_P(x_i)$ for $i = 1, \ldots, n_1$. Then

$$v_{P_j}(x_j u_j) = v_{P_j}(x_j) + v_{P_j}(u_j) \leq v_P(x_j) - 2g'_2.$$

For $i \neq j$,

$$v_{P_j}(x_i u_i) = v_{P_j}(x_i) + v_{P_j}(u_i) \geq v_P(x_i),$$

hence $v_{P_j}(\sum x_i u_i) = v_{P_j}(x_j u_j) < \infty$, which is not possible. Now we consider the divisor $C = \mathrm{Con}_{F/F_2}(\sum Q_i^{2g_2'})$. Its degree is $2n_2 g_2' \sum \deg Q_i \leq 4n_1 n_2 g_1' g_2' d_1$. Since the elements $u_1, \ldots, u_{n_1}$ are in $L(C^{-1})$, we have $g \leq 1 + n_1(g_1 - 1) + 4n_1 n_2 g_1' g_2' d_1$ from Lemma 3.3. □

PROPOSITION 3.5. *Let F, F_1, F_2 be function fields with field of constants k such that $F = F_1 F_2$ and F/F_1 is a separable extension. Then*

$$g_F \leq 1 + [F : F_1](g_{F_1} - 1) + 4[F : F_1][F : F_2] g'_{F_1} g'_{F_2} d,$$

where $d = \min\{\deg P \mid P \in \mathbb{P}_{F_1}\}$.

PROOF. Consider a separable closure k_1 of k and let $\tilde{F} = F k_1$, $\tilde{F}_i = F_i k_1$, $i = 1, 2$. Since k_1/k is separable, $g_{\tilde{F}} = g_F$, $g_{\tilde{F}_i} = g_{F_i}$ and $n_i = [\tilde{F} : \tilde{F}_i] = [F : F_i]$, $i = 1, 2$. Let $d_1 = \min\{\deg R \mid R \in \mathbb{P}_{\tilde{F}_1}\}$. By Lemma 3.4,

$$\begin{aligned} g_F = g_{\tilde{F}} &\leq 1 + n_1(g_{\tilde{F}_1} - 1) + 4n_1 n_2 g'_{\tilde{F}_1} g'_{\tilde{F}_2} d_1 \\ &= 1 + [F : F_1](g_{F_1} - 1) + 4[F : F_1][F : F_2] g'_{F_1} g'_{F_2} d_1. \end{aligned}$$

We choose $P \in \mathbb{P}_{F_1}$ such that $\deg P = d$, and let R be a place in $\tilde{F}_1$ lying over P. Now $d = [\mathcal{O}_P/P : k] \geq [\mathcal{O}_R/R : k_1] \geq d_1$ since $\mathcal{O}_R/R$ is the composition of $\mathcal{O}_P/P$ and k_1 [2, p. 128], and the result follows. □

The following result is a consequence of Proposition 3.5 with $F_1 = K$, $F_2 = \sigma(K)$.

PROPOSITION 3.6. *If L/K is a finite separable extension of function fields with field of constants k such that, for each intermediate field M, $K \subset M \subseteq L$,*

$$g_M > 1 + [M : K](g_K - 1) + 4[M : K]^2 {g'_K}^2 d,$$

then for each $\sigma \in \mathrm{Aut}_k L$ we obtain that $\sigma(K) = K$.

4. Separable extensions with a prime divisor of degree one ramified

The next result is analogous to [8, Lemma 2] and [7, Lemma 2] and we will use it to find suitable C-improvements of a given finite separable extension $E/k(x)$.

PROPOSITION 4.1. *Assume that k is infinite and let $E/k(x)$ be a finite separable extension of function fields over k such that P_{x-1} is ramified in E and the zero Q_1 and the pole Q_2 of x in $k(x)$ are unramified and separable in E. Let $\tilde{E}/l$ be a normal closure of $E/k(x)$. Let $C, C_1, C_2 \in \mathbb{R}^+$ be arbitrary. Then there exists a finite extension $F/k(y)$ satisfying the following properties.*

(1) *There exists a subfield E_1/k of F/l such that*

$$[E:k(x)]=[E_1:k(y)], \quad [\tilde{E}:k(x)]=[F:k(y)],$$

$$\mathrm{Gal}(E/k(x))\cong \mathrm{Gal}(E_1/k(y))$$

and F is a normal closure of $E_1/k(y)$. Moreover, P_{y-1} is ramified in F and the pole of y in $k(y)$ is unramified and separable in F.

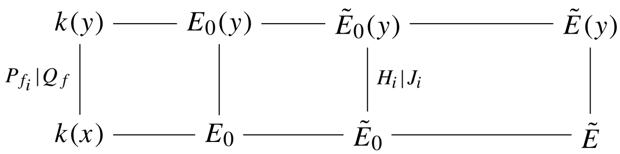
(2) *Let E_2 be an intermediate field, $k(y)\subset E_2\subseteq E_1$. Then either there is a place in $k(y)$ of degree greater than C_2 ramified or inseparable in $E_2/k(y)$ or there are more than C_1 places of $k(y)$ ramified or inseparable in $E_2/k(y)$.*

(3) *For each intermediate field $k\subseteq k_1\subseteq l$, the genus g_M of any field $k_1(y)\subset M\subseteq F$ with constant field k_1 is greater than C.*

(4) *Let N/k be a finite separable extension. If M/N is any intermediate field, $N(y)\subset M\subseteq FN$, then $g_M>C$.*

PROOF. First we prove (1) and (2). Choose an integer $m>0$ such that $m>\max\{C_1C_2, 2C+3\}$ and $(m, p[\tilde{E}:k(x)])=1$. Let $y^m=x$. Then $k(y)/k(x)$ is a separable extension of degree m. By the genus formula the only places of $k(x)$ which ramify in $k(y)/k(x)$ are Q_1 and Q_2, and there are no inseparable places. Let $F=\tilde{E}(y)$. Then F is the normal closure of $E_1=E(y)$, $[E_1:k(y)]=[E:k(x)]$, the constant field of E_1 is k and $\mathrm{Aut}_{k(y)} E_1\cong \mathrm{Aut}_{k(x)} E$ (Lemma 2.1).

Consider an intermediate field E_0, $k(x)\subset E_0\subseteq E$. By the genus formula there is a place Q_f of $k(x)$ ramified or inseparable in E_0. Let $\tilde{E}_0$ be the normal closure of $E_0/k(x)$ contained in $\tilde{E}$. Since Q_f is different from Q_1 and Q_2 it follows that Q_f is unramified in $k(y)/k(x)$; this implies that the polynomial $f(x)=f(y^m)$ splits into irreducible distinct factors $f_1(y),\ldots, f_h(y)$ in $k(y)$.



Let H_i be an extension of P_{f_i} in $\tilde{E}_0(y)$. Since $J_i=H_i\cap\tilde{E}_0$ lies over Q_f, then J_i is ramified or inseparable in $\tilde{E}_0/k(x)$, so $e(H_i|Q_i)f_i(H_i|Q_i)>1$. Since $P_{f_i}\cap k(x)$ is different from Q_1 and Q_2, the place P_{f_i} is unramified and separable in $k(y)/k(x)$, hence $e(H_i|P_{f_i})f_i(H_i|P_{f_i})>1$. Then P_{f_i} is ramified or inseparable in $E_0(y)/k(y)$ (Lemma 2.3). Since $P_{y-1}|Q_{x-1}$, it follows that P_{y-1} is ramified in F. Since Q_2 is unramified and separable in $\tilde{E}/k(x)$ (Lemma 2.2), the pole of y is unramified and separable in $F/k(y)$ by the correspondence between the inertia groups. If $\deg f_i\leq C_2$ for all i, the number h of factors is minimum when $\deg f_i=C_2$. In this case $hC_2=m\deg f>C_1C_2$, and it follows that $h>C_1$.

To prove (3), let k_1 be an intermediate field of l/k. Denote by R_1 the zero of x in $k_1(x)$ and by R_2 the pole of x in $k_1(x)$. The extension $k_1(x)/k(x)$ has degree equal to $f(R_1|Q_1) = f(R_2|Q_2)$. Therefore if a place $D_i \in \mathbb{P}_{k_1(y)}$ lies over R_i we obtain $e(D_i|R_i) = [k(y) : k(x)] = m$. Then in $k_1(y)$, $R_i = D_i^m$ with $i = 1, 2$.

$$\begin{array}{ccccc} k(y) & \text{---} & k_1(y) & & \\ {\scriptstyle P_0|Q_1}\ \Big| \ {\scriptstyle P_\infty|Q_2} & & \Big| \ {\scriptstyle D_i|R_i} & & \\ k(x) & \text{---} & k_1(x) & \text{------} & \tilde{E} \end{array} \qquad \begin{array}{ccccc} k_1(y) & \text{---} & M & \text{---} & \tilde{E}(y) \\ \Big| & & \Big| & & \Big| \\ k_1(x) & \text{---} & M_0 & \text{---} & \tilde{E} \end{array}$$

Let M/k_1 be such that $k_1(y) \subset M \subseteq \tilde{E}(y)$. If $M_0 = M \cap \tilde{E}$, then $k_1(x) \subset M_0 \subseteq \tilde{E}$. Let $T \in \mathbb{P}_M$ be such that $T|D_i$. Since $(m, [\tilde{E} : k(x)]) = 1$, then $e(T|T \cap M_0) \geq m$. Since $[M : M_0] = m$, it also follows that $e(T|T \cap M_0) = m$ and $f(T|T \cap M_0) = 1$. Since Q_1 is unramified in $\tilde{E}$ we have that in M_0, $R_1 = T_1 \cdots T_h$, where $h \geq 2$ or $f(T_1|R_1) \geq 2$.

$$\begin{array}{c} D_i \\ \Big| \\ R_i \end{array} \qquad \begin{array}{ccc} k_1(y) & \text{---} & M \\ \Big| & & \Big| \\ k_1(x) & \text{---} & M_0 \end{array} \qquad \begin{array}{c} T \\ \Big| \\ T \cap M_0 \end{array}$$

Then at least three places of M are fully ramified in M/M_0 or at least two places are fully ramified and one of them is of degree greater than or equal to two. From the genus formula we obtain that

$$\begin{aligned} g_M &= 1 + m(g_{M_0} - 1) + \tfrac{1}{2}\deg(D_{M/M_0}) \\ &\geq 1 - m + \tfrac{3}{2}(m - 1) = 1 + \tfrac{1}{2}(m - 3). \end{aligned}$$

Finally we prove (4). Let $k_1 = N \cap l$. Then $k_1(y) \subseteq N(y) \cap F$. If M/N is any intermediate field, $N(y) \subset M \subseteq FN$ and $M_1 = M \cap F$, then $N(y) \cap F \subset M_1 \subseteq F$.

$$\begin{array}{ccccccccc} & & & & N(y) & \text{---} & M & \text{---} & FN \\ & & & & \Big| & & \Big| & & \Big| \\ k(y) & \text{---} & k_1(y) & \text{---} & N(y) \cap F & \text{---} & M_1 & \text{---} & F \end{array}$$

The constant field of M_1 is k_1 and $M = M_1 N$. This implies that $g_M = g_{M_1}$, and by (3) it follows that $g_{M_1} > C$. □

PROPOSITION 4.2. *Suppose that K/k is a function field such that $K/k(y)$ is a finite extension, where K_0 is the separable closure of $k(y)$ in K. Let $C_0 \in \mathbb{R}^+$ and let n_s be the number of places P of $k(y)$ which are ramified or inseparable in $K_0/k(y)$. Assume that the degree of these places is less than d_s. Let $F/k(y)$ be an extension with the properties stated in Proposition 4.1 such that $C > g_{K_0}$ and $C_1 > n_s + 2(m + C_0)$, $C_2 > d_s, 2(m + C_0)$, where $m = [E : k(x)]$. Then the following hold.*

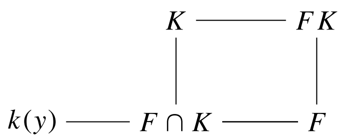
(1) *The constant field of $E_1 K$ is k.*

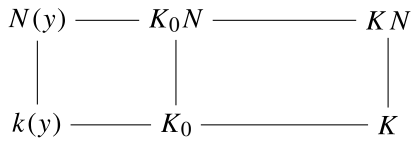
https://doi.org/10.1017/S1446788710000108 Published online by Cambridge University Press

(2) $[E_1 : k(y)] = [E_1K : K]$, *whence* $\mathrm{Aut}_{k(y)}\, E_1 \cong \mathrm{Aut}_K\, E_1K$ *and* FK *is the normal closure of* E_1K.

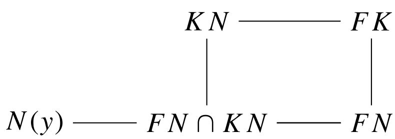
(3) *Each field* H *such that* $K \subset H \subseteq E_1K$ *has genus greater than* C_0.

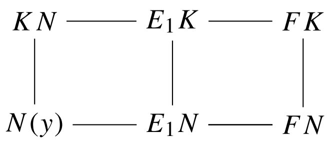
PROOF. First we prove (1) and (2). The constant field of $K \cap F$ is k and $K \cap F/k(y)$ is a separable extension, hence $g_{K\cap F} \leq g_{K_0} < C$. From Proposition 4.1 we obtain $K \cap F = k(y)$. Given that F is the normal closure of $E_1/k(y)$, assertion (2) follows from the Galois correspondence. Let N be the constant field of E_1K. Since E_1K/K is a separable extension, N/k is separable.





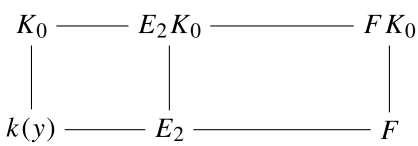
The separable closure of $N(y)$ in KN is K_0N, hence $FN \cap KN \subseteq K_0N$, so $g_{FN\cap KN} \leq g_{K_0N} = g_{K_0}$. From Proposition 4.1, the genus of each intermediate field M/N, $N(y) \subset M \subseteq FN$, is greater than C. Since N is the constant field of $FN \cap KN$, this implies that $FN \cap KN = N(y)$.

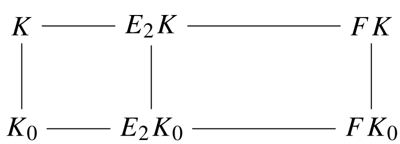




It follows that $[E_1K : KN] = [E_1NKN : KN] = [E_1N : N(y)]$. From (2), we deduce that $[E_1K : KN] = [E_1K : K]$, as $[E_1 : k(y)] = [E_1N : N(y)]$. Therefore $KN = K$.

Finally we prove (3). From Proposition 4.1, for every field E_2 such that $k(y) \subset E_2 \subseteq E_1$, either a place of $k(y)$ of degree greater than C_2 is ramified or inseparable in $E_2/k(y)$, or there are more than C_1 places of $k(y)$ ramified or inseparable in $E_2/k(y)$. Since $C_1 > n_s$ and $C_2 > d_s$, there exists a place of K_0 of degree greater than C_2 ramified or inseparable in E_2K_0/K_0, or K_0 has more than $C_1 - n_s$ ramified or inseparable places in E_2K_0/K_0.





Since K/K_0 is purely inseparable, by Lemma 2.4 it follows that in E_2K/K there exist more than $C_1 - n_s$ ramified or inseparable places, or a place of degree greater than C_2 is ramified or inseparable. Therefore

$$\begin{aligned} g_{E_2K} &= 1 + [E_2K : K](g_K - 1) + \tfrac{1}{2}\deg(D_{E_2K/K}) \\ &> -m + \tfrac{1}{2}2(m + C_0) = C_0. \end{aligned}$$ □

https://doi.org/10.1017/S1446788710000108 Published online by Cambridge University Press

We are now in a position to prove the main result of this paper. This is analogous to [8, Satz 1] and [7, Theorem 3].

THEOREM 4.3. *Let E/k be a function field with an infinite field of constants and let $E/k(x)$ be a separable extension of degree m such that a place of degree one of $k(x)$ is ramified in E. Let K/k be a function field. Then there exist infinitely many nonisomorphic fields L such that L/K is a separable extension of degree m and* $\operatorname{Aut}_K L = \operatorname{Aut}_k L \cong \operatorname{Aut}_{k(x)} E$.

PROOF. Let $\sigma_1, \ldots, \sigma_{n-1} \in \operatorname{Aut}_k K$, $\sigma_i \neq \mathrm{Id}$ and $|\operatorname{Aut}_k K| = n$. There exist pairwise distinct places $B_1, \ldots, B_{n-1}$ of K such that $\sigma_1(B_1), \ldots, \sigma_{n-1}(B_{n-1})$ are pairwise distinct and $B_i \neq \sigma_j(B_j)$ with $1 \leq i, j \leq n-1$. By the approximation theorem, there exists $w \in K$ such that $v_{\sigma_i(B_i)}(w) > 0$ and $v_{B_i}(w) = -1$. Denote by K_0 the separable closure of $k(w)$ in K and by n_s the number of places R of $k(w)$ ramified or inseparable in $K_0/k(w)$. Choose $d_s \in \mathbb{R}$ such that $\deg R \leq d_s$.

Let $C_0 = 1 + m(g_K - 1) + 4m^2 g_K^2 d$, where $d = \min\{\deg B \mid B \in \mathbb{P}_K\}$. We may assume that the place Q_{x-1} of $k(x)$ is ramified in $E/k(x)$ and that the zero and the pole of x in $k(x)$ are unramified and separable in $E/k(x)$. Consider the function field F/l of Proposition 4.1 with $C > g_{K_0}$, $C_1 > n_s + 2(m + C_0)$, $C_2 > d_s, 2(m + C_0)$. From (1) of Proposition 4.1 it follows that for $z = 1/y - 1$ the pole R_∞ of z is ramified in $F/k(z)$ and its zero R_0 is unramified and separable. The isomorphism $\varphi : k(w) \to k(z)$, given by $\varphi(f(w)) = f(z)$, can be extended to a homomorphism $\bar{\varphi}$ of K into an algebraic closure $\overline{k(z)}$ of $k(z)$. Therefore we may assume that K is an extension of $k(z)$, and that K_0 is the separable closure of $k(z)$ in K such that n_s is the number of ramified or inseparable places R of $k(z)$ in $K_0/k(z)$ and $\deg R \leq d_s$. Also may replace $\bar{\varphi}(B_i)$ by B_i and $\bar{\varphi}\sigma_i\bar{\varphi}^{-1}$ by σ_i in such a way that $v_{\sigma_i(B_i)}(z) > 0$ and $v_{B_i}(z) = -1$.

Define $L = E_1 K$. From Proposition 4.2, the field of constants of L is k, the degree of L/K is m and $\operatorname{Aut}_{k(z)} E_1 \cong \operatorname{Aut}_K L$. Consider an extension $H_i \in \mathbb{P}_{FK}$ of $\sigma_i(B_i)$ and the restriction $J_i = H_i \cap F$.

$$\begin{array}{ccccccc} K_1 & \text{———} & K & \text{———} & E_1 K & \text{———} & FK \\ & & {\scriptstyle \sigma_i(B_i)|R_0}\Big| & & \Big| & & \Big|{\scriptstyle H_i|J_i} \\ & & k(z) & \text{———} & E_1 & \text{———} & F \end{array}$$

Let $\sigma \in \operatorname{Aut}_k L$. From Propositions 3.6 and 4.2, $\sigma(K) = K$. Now, since R_∞ is ramified in $F/k(z)$ and the B_i are unramified in $K/k(z)$, it follows that each B_i is ramified in FK/K. Hence, from Lemma 2.3, each B_i is ramified or inseparable in E_1K/K. Since the inertia group $I(H_i|\sigma_i(B_i))$ embeds into the inertia group $I(J_i|R_0)$ and R_0 is unramified and separable in $F/k(z)$, the places $\sigma(B_1), \ldots, \sigma(B_{n-1})$ are unramified and separable in FK/K. Then $\sigma \neq \sigma_i$. Thus $\operatorname{Aut}_k L = \operatorname{Aut}_K L$.

Note that since g_L can be chosen arbitrarily large, there are infinitely many fields L satisfying the result. If $n = 1$ the extension L is obtained as before. □

https://doi.org/10.1017/S1446788710000108 Published online by Cambridge University Press

References

[1] C. Álvarez-García and G. Villa-Salvador, 'Groups of automorphisms of global function fields', *Int. J. Algebra* **2** (2008), 65–78.

[2] M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable*, Lecture Notes in Mathematics, 314 (Springer, Berlin, 1973).

[3] J. D'Mello and M. Madan, 'Algebraic function fields with solvable automorphism group in characteristic p', *Comm. Algebra* **11** (1983), 1187–1236.

[4] L. Greenberg, 'Maximal groups and signatures', in: *Discontinuous Groups and Riemann Surfaces (Proc. Conf. Univ. Maryland, College Park, MD, 1973)* pp. 207–226. Ann. of Math. Studies, No. 79 (Princeton University Press, Princeton, NJ, 1974).

[5] M. Madan and M. Rosen, 'The automorphism group of a function field', *Proc. Amer. Math. Soc.* **115** (1992), 923–929.

[6] D. J. Madden and R. C. Valentini, 'The group of automorphisms of algebraic function fields', *J. Reine Angew. Math.* **343** (1983), 162–168.

[7] M. Rzedowski-Calderón and G. Villa-Salvador, 'Automorphisms of congruence function fields', *Pacific J. Math.* **150** (1991), 167–178.

[8] H. Stichtenoth, 'Zur Realisierbarkeit endlicher Gruppen als Automorphismengruppen algebraischer Funktionenkörper', *Math. Z.* **187** (1984), 221–225.

[9] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext (Springer, Berlin, 1993).

C. ÁLVAREZ-GARCÍA, Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados del I.P.N.,
Av. Instituto Politécnico Nacional No. 2508,
Col San Pedro Zacatenco, C.P. 07360, México D. F., México
and
Departamento de Matemáticas,
Universidad Autónoma Metropolitana Iztapalapa, México
e-mail: calvarez@ctrl.cinvestav.mx

G. VILLA-SALVADOR, Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados del I.P.N.,
Av. Instituto Politécnico Nacional No. 2508,
Col San Pedro Zacatenco, C.P. 07360, México D. F., México
and
Departamento de Matemáticas,
Universidad Autónoma Metropolitana Iztapalapa, México
e-mail: gvilla@ctrl.cinvestav.mx