International Journal of Pure and Applied Mathematics
Volume 78 No. 7 2012, 957-972
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

GALOIS GROUPS OF FUNCTION FIELDS WITH INFINITELY MANY AUTOMORPHISMS

C. Alvarez-Garcia[1], G. Villa-Salvador[2] §

[1]Universidad Autónoma Metropolitana-I
Departamento de Matemáticas
09340, México D.F., México

[2]CINVESTAV IPN
Departamento de Control Automático
Apartado postal 14-740
07000, México, D.F., México

Abstract: Let $E/k(x)$ be a separable geometric extension such that the pole divisor of x is ramified. Let K/k be a function field of genus at least one such that $\mathrm{Aut}_k K$ is infinite. If K/k is elliptic we suppose that the characteristic is zero. The main result of the paper is that there are infinitely many non-isomorphic function fields L over k such that L/K is a Galois extension and $\mathrm{Gal}(L/K) = \mathrm{Aut}_k L \cong \mathrm{Aut}_{k(x)} E$.

AMS Subject Classification: 11R58, 11R32, 12F12, 14H52
Key Words: inverse Galois problem, geometric extension, infinite automorphism group, moduli field, C-improvement

1. Introduction

The central problem in inverse Galois theory is to provide an answer to E. Noether question, the inverse Galois problem: is each finite group the Galois group of an extension of the field of rational numbers?

Received: February 15, 2012

§Correspondence author

When the group G is not finite the answer to Noehter's question is in general no, even in the abelian case. For instance, if $\mathbb{Z}_p$ is the ring of p–adic integers, then there does not exist an extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

There exist many papers dealing with this still unsolved problem and several of its analogues and generalizations.

In [8], Madden and Valentini proved the following theorem: Any finite group can be realized as the full group of automorphisms of an algebraic function field over an algebraically closed field k. This theorem was proved in [10] under the assumption that k is finite.

If K/k is a function field with group of automorphisms $\mathrm{Aut}_k K$ a finite group, from [1], [2] and [10] we obtain the following theorem.

Theorem 1. *For any finite separable non–trivial extension $E/k(x)$, where the pole divisor of x is ramified, there exist infinitely many non–isomorphic fields L such that L/K is a Galois extension and*

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K L = \mathrm{Aut}_k L \cong \mathrm{Aut}_{k(x)} E.$$

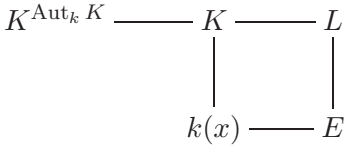
The purpose of this paper is to prove that Theorem 1 remains valid when $\mathrm{Aut}_k K$ is an infinite group and K has genus at least one (see Theorem 33).

Let us fix some notation to be maintained throughout the entire work. For an extension of fields L/F, $\mathrm{Aut}_F L$ denotes the group of automorphisms of L that fix F pointwise. Denote by L^H the fixed field of a subgroup H of $\mathrm{Aut}_F L$. If F/k is a function field and $x \in F^{\square}$, N_x is the pole divisor and $(x)_F$ is the principal divisor of x in F. The genus of F/k will be denoted by g_F. We write $\mathbb{P}_F$ for the set of places of F and $\mathbb{P}_F^1 = \{P \in \mathbb{P}_F | \deg P = 1\}$, $\deg P$ denotes the degree of the place. In the rational function field $k(x)$, $P_{f(x)}$ denotes the place corresponding to the irreducible polynomial $f(x)$. Let L/l be an extension of F/k. We say that L/F is a geometric extension if $l = k$. For a separable extension L/F of function fields $D_{L/F}$ denotes the different of L/F and $\mathrm{Con}_{L/F}$ the conorm homomorphism. Finally, $\bar{k}$ is an algebraic closure of an arbitrary field k.

2. Infinite Full Automorphism Group

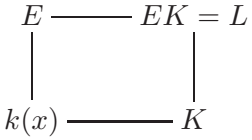
The technique used to prove Theorem 1 can be described as follows. Suppose that the intermediate fields in $E/k(x)$ have large genus (Definition 2, Lemma 7). In [1], [2] and [10] it was obtained an element $x \in K$ such that: 1) the field

of constants of $L = EK$ is k, 2) each $\sigma \in \mathrm{Aut}_k\, L$ satisfies $\sigma(K) = K$ and 3) the decomposition of the places in $(x)_K$ with respect to $K/K^{\mathrm{Aut}_k\, K}$ implies that $\sigma|_K = \mathrm{Id}$, so $\mathrm{Aut}_k\, L = \mathrm{Aut}_K\, L$.



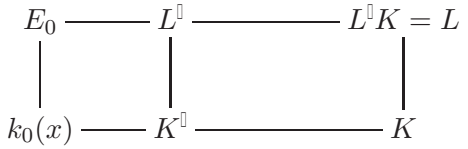
Suppose now that $\mathrm{Aut}_k\, K$ is infinite. The main difficulty for the application of the above technique is that $K^{\mathrm{Aut}_k\, K} = k$ [9, p. 5].

First we consider the case $g_K \geq 2$ (see Proposition 21). The proof follows closely the one for $\mathrm{Aut}_k\, K$ finite.



From the result of Rosenlicht [9, p. 10] K has infinitely many places of degree one. There is $x \in K$ such that the divisor N_x is a product of places $P_1, \ldots, P_t, P$ of degree one, $\mathrm{Aut}_K\, EK \cong \mathrm{Aut}_{k(x)}\, E$ and the field of constants of EK is k. We can assume (Lemma 20) that the intermediate fields in $E/k(x)$ have large genus and the pole divisor of x is the only place of degree one of $k(x)$ ramified in $E/k(x)$. Hence any $\sigma \in \mathrm{Aut}_k\, EK$ satisfies that $\sigma(K) = K$ (Lemma 4) and $\sigma\{P_1, \ldots, P_t, P\} = \{P_1, \ldots, P_t, P\}$. Therefore $\sigma = \mathrm{Id}$ (Lemma 12). Thus $\mathrm{Aut}_k\, EK = \mathrm{Aut}_K\, EK$.

Now let $g_K = 1$ (see Proposition 32). Let k_0 be a definition field of K. Using the concept of moduli field (Definition 14) and the above technique we find an extension $L^{\natural}/K^{\natural}$ of function fields over k_0 such that $L = L^{\natural}K$ satisfies Theorem 1.



More precisely, let $K^{\natural}/k_0$ such that $K = K^{\natural}k$. There exists $E_0/k_0(x)$ with the following properties. Let $L^{\natural} = E_0K^{\natural}$. Then $L^{\natural}/K^{\natural}$ is a geometric extension and if $\sigma \in \mathrm{Aut}_k\, L^{\natural}K$ there is l/k_0 finite such that $\sigma(K^{\natural}l) = K^{\natural}l$. The ramification in $L^{\natural}/K^{\natural}$ of the places in $\mathbb{P}^1_{K'}$ implies that $\sigma|_K = \mathrm{Id}$.

3. Improvements and Moduli Field

This section contains some results and definitions necessary for the rest of the paper. Throughout Section 3, k denotes an arbitrary field.

Definition 2. Let $E/k(x)$ be an extension of function fields and C be a real number. If a geometric extension $E_1/k(y)$ satisfies:
1) $[E : k(x)] = [E_1 : k(y)]$,
2) $\mathrm{Aut}_{k(x)} E \cong \mathrm{Aut}_{k(y)} E_1$,
3) if M is any intermediate field, $k(y) \subset M \subseteq E$, then $g_M \geq C$,
we say that $E_1/k(y)$ is a C-improvement of $E/k(x)$.

Lemma 3. *Let L, K, E be function fields with field of constants k and such that $L = EK$. Then $g_L \leq 1+[L : E](g_E-1)+4[L : E][L : K](g_E+1)(g_K+1)d$, where $d = \min\{\deg P | P \in \mathbb{P}_E\}$.*

Proof. See [2, p. 307]. □

Lemma 4. *If L/K is a finite extension of function fields with field of constants k and such that for any intermediate field M, $K \subset M \subseteq L$, it holds that $g_M > 4[M : K]^2(g_K+1)^2 d + [M : K](g_K-1)+1$ then for any $\sigma \in \mathrm{Aut}_k L$ we have $\sigma(K) = K$, where $d = \min\{\deg P | P \in \mathbb{P}_K\}$.*

Proof. See [2, p. 307]. □

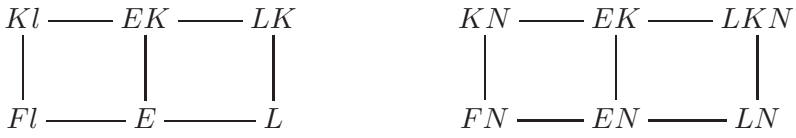
Lemma 5. *Let K/k be a function field and M/k be an algebraic extension. Let E/K be a geometric finite extension. If either E/K or M/k is separable then $[EM : KM] = [E : K]$.*

Proof. See [2, p. 303]. □

Lemma 6. *Let F/k be a function field. Let L/F be a Galois extension of function fields and K/F be a geometric finite extension such that $([L : F], [K : F]) = 1$. If E/l is an intermediate field of L/F, then the field of constants of EK is l.*

Proof. Let N be the field of constants EK. From Lemma 5 we have that $[E : Fl] = [EN : FN]$ (since l/k is separable, l is the constant field of Fl). Since $[K : F] = [KN : FN]$ (Lemma 5), it follows that $([EN : FN], [KN : FN]) = 1$.

Hence $[EK : KN] = [EN : FN]$.



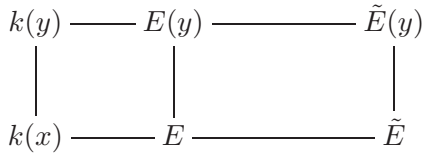
Similarly $[EK : Kl] = [E : Fl]$, so we obtain $[EK : KN] = [EK : Kl]$. Then $N = l$. □

Lemma 7. *Let $E/k(x)$ be a separable geometric extension. Let $\tilde{E}/l$ be a normal closure of $E/k(x)$ and $C \in \mathbb{R}^+$. Then there is a function field F/l, and $y \in F$ such that:*
1) *there is an intermediate field $k(y) \subset E_1 \subseteq F$ such that $E_1/k(y)$ is a C-improvement of $E/k(x)$. Moreover $F/k(y)$ is the normal closure of $E_1/k(y)$,*
2) *if the pole divisor of x ramifies in $\tilde{E}/k(x)$ then the pole divisor of y ramifies in $F/k(y)$,*
3) *let k_1 be such that $k \subseteq k_1 \subseteq l$. Then if M/k_1 is any intermediate field M/k_1, $k_1(y) \subset M \subseteq F$, we have $g_M \geq C$,*
4) *given a finite extension N/k, for all intermediate fields M/N, $N(y) \subset M \subseteq FN$, it holds that $g_M \geq C$.*

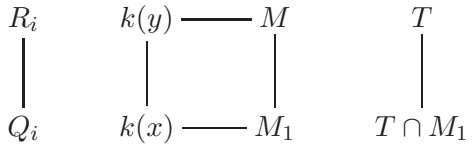
Proof. See [2, p. 307]. □

Lemma 8. *Let $E/k(x)$ be a separable geometric extension such that the pole divisor of x is ramified. Let $\tilde{E}$ be the normal closure of $E/k(x)$ and $C \in \mathbb{R}^+$. Then if $(m, [\tilde{E} : k(x)]) = 1$ and $y^m = x$ (m sufficiently large), the extension $E(y)/k(y)$ is a C-improvement of $E/k(x)$ such that the pole divisor of y is ramified in $E(y)/k(y)$.*

Proof. As $(m, [\tilde{E} : k(x)]) = 1$, the extension $E(y)/k(y)$ is geometric by Lemma 6. Moreover $E(y)/k(y)$ satisfies 1) and 2) of Definition 2. Denote by $Q_1, Q_2 \in \mathbb{P}_{k(x)}$ the zero divisor and the pole divisor of x. We may assume that Q_1 does not ramify in E. Let M/k be any intermediate field $k(y) \subset M \subseteq E(y)$. Then $M_1 = M \cap E$ satisfies $k(x) \subset M_1 \subseteq E$.



The zero divisor of y in $k(y)$ is R_1 and R_2 is its pole divisor. Let $T \in \mathbb{P}_M$ be such that $T|R_i$. Since $(m, [\tilde{E} : k(x)]) = 1$, it holds that $e(T|T \cap M_1) \geq m$. Since $[M : M_1] = m$, we have that $e(T|T \cap M_1) = m$ and $f(T|T \cap M_1) = 1$. The place Q_1 does not ramify in E. Hence $R_1 = T_1 \cdots T_h$ in M_1, where $h \geq 2$ o $f(T_1|R_1) \geq 2$.



Then at least three places of M are fully ramified in M/M_1 or at least two places are fully ramified and one of them is of degree larger than 2. From the genus formula

$$\begin{aligned} g_M &= 1 + m(g_{M_1} - 1) + \frac{1}{2}\deg(D_{M/M_1}) \\ &\geq 1 - m + \frac{3}{2}(m-1) = \frac{1}{2}(m-1). \end{aligned}$$

Thus $m \geq 2C + 1$ implies that $g_M \geq C$. □

Lemma 9. *Let K/k be a function field with at least one place P of degree one. Then each place of degree one of K has only one extension in $K\bar{k}$*

Proof. Let $P \in \mathbb{P}_K$ and let q be a large prime number. There exists $x \in K$ such that $N_x = P^q$ and $K/k(x)$ is separable. The pole divisor of x in $K\bar{k}$ has the form $(\mathrm{Con}_{K\bar{k}/K}P)^q$. Since $[K\bar{k} : \bar{k}(x)] = [K : k(x)]$ it follows that $q \deg \mathrm{Con}_{K\bar{k}/K}P = q$. Thus $\mathrm{Con}_{K\bar{k}/K}P$ is of degree one. Then $\mathrm{Con}_{K\bar{k}/K}P = R$, R a place of $K\bar{k}$. □

The following result is a theorem of Schmid (see Satz 9 of [11]).

Theorem 10. *Let $K/\bar{k}$ be a function field. Then each nontrivial $\sigma \in \mathrm{Aut}_{\bar{k}} K$ has at most $2_K + 2$ fixed prime divisors of K.*

Proof. See [13, p. 601]. □

Lemma 11. *Let K/k be a function field. Assume that K has at least $2g_K+3$ prime divisors P_i of degree one. Let $\sigma \in \mathrm{Aut}_k K$ be such that $\sigma(P_i) = P_i$ for all i, then σ is the identity.*

Proof. Let R_i the only place of $K\bar{k}$ lying over P_i (Lemma 9). Any $\sigma \in \mathrm{Aut}_k K$ induces a $\bar{k}$-automorphism $\bar{\sigma}$ of $K\bar{k}$. Thus $\bar{\sigma}(R_i) = R_i$ for all i and by Theorem 10 $\bar{\sigma} = \mathrm{Id}$. □

Lemma 12. *Let $K/\bar{k}$ be a function field and $T = \{P_1, \ldots, P_t\}$ be a set of places of K with $t > 2g_K + 3$. Then, for all but finitely many places P, the identity is the only element $\sigma \in Aut_{\bar{k}}K$ such that $\sigma(T \cup \{P\}) = T \cup \{P\}$.*

Proof. See [12, p. 44], [7, p. 924]. □

Lemma 13. *Let K/k be a function field defined over $k' \subseteq k$ and let K'/k' be such that K' has sufficiently many places of degree one, $K = K'k$. Let $T' = \{Q'_1, \ldots, Q'_t\} \subset \mathbb{P}_{K'}$ with $t > 2g_K+3$. Then, for all but finitely many places $Q' \in \mathbb{P}_{K'}$, the only $\sigma \in Aut_k K$ such that $\sigma(K') = K'$ and $\sigma|_{K'}(T' \cup \{Q'\}) = T' \cup \{Q'\}$ is the identity.*

Proof. From Lemma 9 there exist unique prime divisors Q_i, Q in $K\bar{k}$ lying over Q'_i, Q' (resp.). Thus the lemma follows from Lemma 12. □

Let $K/\bar{k}$ be a function field and $K/\bar{k}(x)$ be a separable extension. The action of $\mathrm{Gal}(\bar{k}/k)$ on $K/\bar{k}(x)$ is as follows. Given $\sigma \in \mathrm{Gal}(\bar{k}/k)$ we extend σ to a $k(x)$-automorphism $\bar{\sigma}$ of $\overline{k(x)}$. Define K^σ by $K^\sigma = \bar{\sigma}(K)$. This definition is independent of the extension $\bar{\sigma}$ up to $\bar{k}(x)$-isomorphism.

$$\begin{array}{ccccccc}
k(x) & \text{———} & \bar{k}(x) & \text{———} & K & \text{———} & \overline{k(x)} \\
\bar{\sigma}|_{k(x)}=\mathrm{Id}\,\big| & & \big| & & \big| & & \big|\,\bar{\sigma} \\
k(x) & \text{———} & \bar{\sigma}(\bar{k}(x)) & \text{———} & \bar{\sigma}(K) & \text{———} & \overline{k(x)}
\end{array}$$

Definition 14. Consider the subgroup H of $\mathrm{Gal}(\bar{k}/k)$ consisting of the $\sigma \in \mathrm{Gal}(\bar{k}/k)$ such that K and K^σ are isomorphic over $\bar{k}(x)$. The moduli field of $K/\bar{k}(x)$ relative to the extension $\bar{k}/k$ is defined to be the fixed field of H in $\bar{k}$.

The moduli field is a finite extension of k contained in each field of definition of $K/\bar{k}(x)$ containing k (Hammer and Herrlich [6, p. 6]). Although the moduli field need not be a field of definition, a field of definition k_1 of $K/\bar{k}$ is a moduli field relative to $\bar{k}/k_1$. Let $k_1(z, y)$ be such that $K = \bar{k}(z, y)$. Since $k_1(x)(z, y)/k_1(x)$ is separable there is w such that $k_1(x)(z, y) = k_1(x)(w)$. Hence, for each $\sigma \in \mathrm{Gal}(\bar{k}/k_1)$ we have that w, $\bar{\sigma}(w)$ are conjugate over $k_1(x)$. Then $K^\sigma = \bar{k}(x)(\bar{\sigma}(w))$ is isomorphic to K over $\bar{k}(x)$.

$$\begin{array}{ccccccc}
k_1(x) & \text{———} & k'(x)(w) & \text{———} & K = \bar{k}(z,y) & \text{———} & \overline{k(x)} \\
\bar{\sigma}|_{k_1(x)}=\mathrm{Id}\,\big| & & \big|\,\bar{\sigma} & & \big| & & \big|\,\bar{\sigma} \\
k_1(x) & \text{———} & k'(x)(\bar{\sigma}(w)) & \text{———} & K^\sigma & \text{———} & \overline{k(x)}
\end{array}$$

Theorem 15. *Let $K/\bar{k}(x)$ be a separable extension of function fields. Suppose that k is the moduli field of $K/\bar{k}(x)$ relative to $\bar{k}/k$. Then there exists a geometric extension $K^{\natural}/l(x)$ such that $K = K^{\natural}\bar{k}$ and $[l : k] \leq [K : \bar{k}(x)]$.*

Proof. See [3, p. 49]. □

4. Field of Genus Larger than One

In this section K/k denotes a function field of genus larger than one and whose full automorphism group is infinite. Rosenlicht [9, p. 5] proved that k is an imperfect field. For this reason, except in Lemma 16, we assume that k is imperfect of characteristic p.

Lemma 16. *Let k be a field of positive characteristic p and suppose that $f(x) \in k[x] \setminus k^p[x]$ is a monic irreducible polynomial. Then for each $m \geq 0$ $f(x^{p^m})$ is irreducible.*

Proof. See [5, p. 227]. □

Lemma 17. *Let k be an imperfect field of characteristic p. Let $f_1, \ldots, f_n \in k[x]$ such that $f_i \notin k[x]^p$. Then, there exists $a \in k$ such that $f_i(x + a) \notin k^p[x]$ for all $1 \leq i \leq n$.*

Proof. See [5, p. 227]. □

Lemma 18. *Let $E/k(x)$ be a separable geometric extension. Suppose that the pole divisor of x ramifies in $E/k(x)$. Then there exists a separable geometric extension $E_1/k(x)$ which satisfies $[E : k(x)] = [E_1 : k(x)]$, $Aut_{k(x)}E \cong Aut_{k(x)}E_1$ and the pole divisor of x ramifies in $E_1/k(x)$. Moreover for each place P_f of $k(x)$ either ramified or inseparable in $E_1/k(x)$ satisfies that $f \notin k^p[x]$.*

Proof. Let $P_{\infty}, P_{f_1}, \ldots, P_{f_n}$ be all the places of $k(x)$ either ramified or inseparable ($f_i \notin k[x]^p$) in $E/k(x)$. From Lemma 17, we have that there exists $a \in k$ such that $f_i(x + a) \notin k^p[x]$.

Let $\sigma \in \underline{Aut_k}k(x)$ be defined by $\sigma(x) = x + a$. We choose an extension $\bar{\sigma}$ of σ, $\bar{\sigma} : E \to \overline{k(x)}$ such that $\bar{\sigma}|_{k(x)} = \sigma$. Let $E_1 = \bar{\sigma}(E)$.

Then $E_1/k(x)$ satisfies $[E : k(x)] = [E_1 : k(x)]$, $Aut_{k(x)}E \cong Aut_{k(x)}E_1$, the pole divisor de x ramifies in $E_1/k(x)$ and if P_f is a place of $k(x)$ either ramified or inseparable in $E_1/k(x)$ there exists $1 \leq i \leq n$ such that $f = \sigma(f_i) \notin k^p[x]$. □

Lemma 19. *Let $E/k(x)$ be a separable geometric extension such that the pole of x ramifies in $E/k(x)$. Then there exists a separable geometric extension $E_1/k(x)$ such that $[E : k(x)] = [E_1 : k(x)]$, $Aut_{k(x)}E \cong Aut_{k(x)}E_1$ and the pole of x is the only place of degree one of $k(x)$ either ramified or inseparable in $E_1/k(x)$.*

Proof. By Lemma 18 we can construct a geometric extension $E_2/k(x)$ such that $[E : k(x)] = [E_2 : k(x)]$, $Aut_{k(x)}E \cong Aut_{k(x)}E_2$, the pole divisor of x ramifies in $E_2/k(x)$ and if Q_f is either ramified or inseparable in $E_2/k(x)$ then $f \notin k^p[x]$.

$$\begin{array}{ccccc} k(y) & \text{——} & E_1 = E_2(y) & \text{——} & F(y) \\ | & & | & & | \\ k(x) & \text{————} & E_2 & \text{————} & F \end{array}$$

Let F be a normal closure of $E_2/k(x)$. Let $y^p = x$ and denote by R the various places of $k(y)$. Since $f(y^p)$ is irreducible (Lemma 16) we have that $R_{f(y^p)}|Q_{f(x)}$. Hence the places of $k(y)$ different from R_∞ which are either ramified or inseparable in $E_1/k(y)$, $E_1 = E_2(y)$, have degree larger than one.

$$\begin{array}{ccccc} N(y) & \text{——} & E_2(y) & \text{——} & FN(z) \\ | & & | & & | \\ N(x) & \text{——} & E_2N & \text{——} & FN \end{array}$$

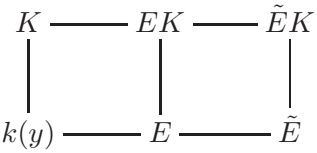
Let N denote the constant field of E_1. Since $[N : k]$ is separable $[E_2N : N(x)] = [E_2 : k(x)]$. Since $N(y)/N(x)$ is purely inseparable it follows that $[E_2(y) : N(y)] = [E_2N : N(x)]$. Hence $[E_2(y) : N(y)] = [E_2(y) : k(y)]$. Thus we have $N = k$. □

Lemma 20. *Let $E/k(x)$ be a separable geometric extension such that the pole divisor of x ramifies in $E/k(x)$. Let $C \in \mathbb{R}^+$. Then there is a geometric extension $E_1/k(y)$ satisfying:*
1) $[E : k(x)] = [E_1 : k(y)]$,
2) *the divisors in E_1 above the pole divisor of y are the only divisors in the different of $E_1/k(y)$ whose restriction to $k(y)$ are of degree one,*
3) *for each intermediate field, $k(y) \subset M \subseteq E_1$, we have that $g_M \geq C$.*

Proof. Let $E_2/k(x)$ be as in Lemma 19. Then the extension $E_1/k(y)$ can be defined by C-improvement of $E_2/k(x)$ with $y^m = x$ (see Lemma 8). □

Proposition 21. *Let $E/k(x)$ be a separable geometric extension. Let K/k be a function field with $g_K \geq 2$ and such that $\mathrm{Aut}_k K$ is infinite. Assume that the pole of x ramifies in $E/k(x)$. Then there exist infinitely many separable extensions L/K such that $[E : k(x)] = [L : K]$ and $Aut_{k(x)}E \cong Aut_K L = Aut_k L$.*

Proof. Let $E_1/k(y)$ be as in Lemma 20 with $C = 4n^2(g_K+1)^2+n(g_K-1)+1$, where $n = [E : k(x)]$. Let $\tilde{E}_1$ be the normal closure of $E_1/k(x)$ and $m = [\tilde{E}_1 : k(y)]$. We choose a prime number $q > m(2g_K + 4)$. Given $D_1, \ldots, D_{q-1} \in \mathbb{P}^1_K$ there exists $D \in \mathbb{P}^1_K$ such that if $\tau \in \mathrm{Aut}_k K$ and $\tau(\{D_1, \ldots, D_{q-1}, D\}) = \{D_1, \ldots, D_{q-1}, D\}$, we have $\tau = \mathrm{Id}$ (Lemma 13). From Riemann-Roch Theorem there exists $y \in K$ such that $N_y = D_1^q \cdots D_{q-1}^q D^{mp+q}$. Thus $([K : k(y)], mp) = 1$, hence $[EK : K] = n$. Lemma 6 implies that k is the full constant field of $L = EK$.



By Lemma 4 each $\sigma \in \mathrm{Aut}_k L$ satisfies $\sigma(K) = K$. Since the pole divisor of y is the only place of degree one ramified in $E/k(y)$, it follows that $\sigma|_K(\{D_1, \ldots, D_{q-1}, D\}) = \{D_1, \ldots, D_{q-1}, D\}$. Then Lemma 13 implies that $\sigma|_K = \mathrm{Id}$. □

5. Fields of Genus One

Let either X be a set of transcendental elements over $\mathbb{Q}$ or $X = \emptyset$. In the following k_0 denotes a finitely generated field over $\mathbb{Q}(X)$ and k is a field of characteristic zero.

Lemma 22. *Let $f_1, \ldots, f_s \in k_0[x]$. Let $a_1, \ldots, a_t$ be the roots of $f_1, \ldots, f_s$ and p be an odd prime number. Then, given n there exists $a \in k_0$ such that the irreducible polynomials in the decomposition of $f_i(x^{p^n} + a)$ over k_0 are of degree at least p^n.*

Proof. Let $v_1, \ldots, v_m$ be pairwise distinct valuations of k_0 which are unramified in $k_0(a_1, \ldots, a_t)$. We denote by $v_i^{\mathbb{I}}$ an extension of v_i. Let l be a prime number greater than $\max\{|v_i^{\mathbb{I}}(a_i)|, p\}$. There exists $a \in k_0$ such that $v_i(a) = -l$.

Hence $v_i^{\mathbb{l}}(a_i - a) = -l$. Now, if b_j is a root of $f_i(x^{p^n} + a)$ there exists a_{i_0} with $b_j^{p^n} + a = a_{i_0}$.

$$\begin{array}{ccc} & & k_0(b_i) \\ & & \Big| \, p^n \\ k_0 & \text{——} & k_0(a_i) \end{array}$$

Since $a_{i_0} - a \notin k_0(a_{i_0})^p$ we obtain that $[k_0(b_j) : k_0(a_{i_0})] = p^n$. Then each irreducible $g(x) \in k_0[x]$ that divides $f_i(x^{p^n} + a)$ has degree at least p^n. □

Lemma 23. *Let K/k be a function field and $\sigma \in \mathrm{Aut}_k K$ of order n. Suppose that $k^{\mathbb{l}}$, $k^{\mathbb{l}} \subseteq k \subseteq \bar{k}^{\mathbb{l}}$, is a field of definition of K. Let $\bar{\sigma} \in \mathrm{Aut}_{\bar{k}'} K\bar{k}^{\mathbb{l}}$ be the automorphism induced by σ. Then there exist a function field K_1/k_1 such that $K\bar{k}^{\mathbb{l}} = K_1\bar{k}^{\mathbb{l}}$ and $\bar{\sigma}(K_1) = K_1$ with $[k_1 : k^{\mathbb{l}}] \leq C(n, g_K)$, where $C(n, g_K) \in \mathbb{R}^+$ depends only on n and g_K.*

Proof. There exists $z \in K^\sigma$ such that $N_z = P^{2g_K+1}$. By Theorem 15 there exists a geometric extension $K^{\mathbb{l}}/k_1^{\mathbb{l}}(z)$ such that $K\bar{k}^{\mathbb{l}} = K^{\mathbb{l}}\bar{k}^{\mathbb{l}}$, where $[k_1^{\mathbb{l}} : k^{\mathbb{l}}] \leq n(2g_K + 1)$.

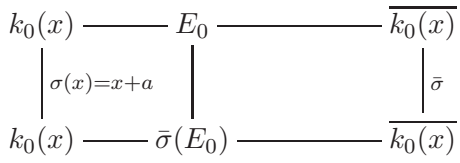
$$\begin{array}{ccccc} k(z) & \text{——} & K^\sigma & \text{——} & K \end{array} \qquad \begin{array}{ccc} \bar{k}^{\mathbb{l}}(z) & \text{————} & K\bar{k}^{\mathbb{l}} \\ \Big| \, \bar{k}' & & \Big| \, \bar{k}' \\ k_1^{\mathbb{l}}(z) & \text{————} & K^{\mathbb{l}} \end{array}$$

Let k_1 be the field of constants of the normal closure L of $K^{\mathbb{l}}/k_1^{\mathbb{l}}(z)$. Hence $[k_1 : k_1^{\mathbb{l}}] \leq n(2g_K + 1)!$. Define $K_1 = K^{\mathbb{l}}k_1$ and $C(n, g_K) = n(2g_K + 1)(n(2g_K + 1))!$. Since $\bar{\sigma}|_{k_1(z)} = \mathrm{Id}$ we have that $\bar{\sigma}(K_1)K_1 \subseteq K^{\mathbb{l}}\bar{k}^{\mathbb{l}} \cap L = K_1$. As $[K_1 : k_1(z)] = [\sigma(K_1) : k_1(z)]$ it follows that $\bar{\sigma}|_{K_1} \in \mathrm{Aut}_{k_1} K_1$. □

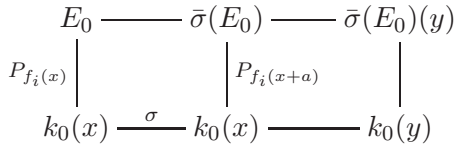
Lemma 24. *Let $E/k(x)$ be a separable geometric extension of function fields such that the infinite place of $k(x)$ is ramified. Suppose that there exists $E_0/k_0(x)$ such that $E = E_0k$. Let $C_0 \in \mathbb{R}^+$. Then there is a C-improvement $E_1/k_0(y)$ of $E_0/k_0(x)$ such that there are no places of degree less than or equal to C_0 of $k_0(y)$ other than the infinite place ramified in E_0.*

Proof. Let $\tilde{E}_0$ be the normal closure of $E_0/k_0(x)$. Let P_{f_i} be the places of $k_0(x)$ ramified in E_0. Let p be an odd prime number with $([\tilde{E}_0 : k_0(x)], p) = 1$.

From Lemma 22 there exists $a \in k_0$ such that $f_i(x^{p^n}+a)$ admits a decomposition over k_0 into irreducibles of degree at least p^n.



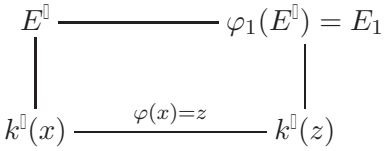
Consider the isomorphism $\sigma : k_0(x) \to k_0(x)$ given by $\sigma(x) = x + a$. We extended σ to an isomorphism $\bar{\sigma}$ of the algebraic closure $\overline{k_0(x)}$ of $k_0(x)$. Hence, the extension $\bar{\sigma}(E_0)/k_0(x)$ is geometric, of degree $[E_0 : k_0(x)]$, $\mathrm{Aut}_{k_0(x)}\, \sigma(E_0) \cong \mathrm{Aut}_{k_0(x)}\, E_0$ and such that the places of $k_0(x)$ ramified in $\bar{\sigma}(E_0)$ are $P_{f_i(x+a)}$.

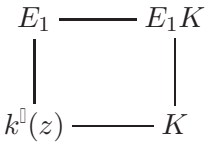


Choose an integer n such that $p^n > \max\{C_0, 2C + 1\}$. Let $y^{p^n} = x$ and $E_1 = \bar{\sigma}(E_0)(y)$. By Lemma 8 $E_1/k_0(y)$ satisfies the required conditions. □

Lemma 25. *Let $E/k(x)$ be an extension of function fields, where the pole divisor of x is ramified. Suppose that there exists $E^{\mathbb{k}}/k^{\mathbb{k}}(x)$ such that $E = E^{\mathbb{k}}k^{\mathbb{k}}$. Let K/k be a function field such that $x \in K$ and let $A \subseteq \mathbb{P}_K$ be an arbitrary finite subset. Then there exists an extension $E_1/k^{\mathbb{k}}(x)$ and an isomorphism $\varphi_1 : E^{\mathbb{k}} \to E_1$ such that the places of K that ramify in E_1K are elements of $(\mathbb{P}_K - A) \cup \{R \in \mathbb{P}_K | R | N_x\}$.*

Proof. Suppose that $P_\infty, P_{f_1}, \ldots, P_{f_t}$ are the places that ramify in $E^{\mathbb{k}}/k^{\mathbb{k}}(x)$. Let $P_{g_1}, \ldots, P_{g_s}$ be the restrictions to $k^{\mathbb{k}}(x)$ of the places in A. Let w be transcendental over $k^{\mathbb{k}}$. There exists $a \in k^{\mathbb{k}}$ such that $\{P_\infty, P_{f_i(w)}\} \cap \{P_\infty, P_{g_i(w-a)}\} = \{P_\infty\}$. Let $z = x + a$. We have that $N_x = N_z$ and the restrictions to $k^{\mathbb{k}}(z)$ of the places in A coincide with the places $P_{g_i(z-a)}$.





Define $\varphi : k^{\mathbb{k}}(x) \to k^{\mathbb{k}}(z)$ by $\varphi(x) = z$. Let φ_1 be an extension of φ to $E^{\mathbb{k}}$. Then the places that ramify in $E_1/k^{\mathbb{k}}(z)$ are $P_\infty, P_{f_i(z)}$, where $E_1 = \varphi_1(E^{\mathbb{k}})$. Thus

the places B of K that ramify in E_1K/K lie over the places $P_\infty, P_{f_i(z)}$. Since $\{P_\infty, P_{f_i(z)}\} \cap \{P_\infty, P_{g_i(z-a)}\} = \{P_\infty\}$ it follows that $B \in (\mathbb{P}_K - A) \cup \{R \in \mathbb{P}_K | R | N_x\}$. □

Definition 26. Let F/K be an extension of function fields over k. Denote by $R(F/K)$ the subgroup $\{\sigma|_K \,|\sigma \in \mathrm{Aut}_k\, F,\ \sigma(K) = K\}$ of $\mathrm{Aut}_k\, K$.

Let K/k be an elliptic function field with Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$. The substitution $x \to t^2x$, $y \to t^3y$, $t \in k^*$, leaves this equation in the same form, but the coefficients change $g_2 \to t^{-4}g_2$, $g_3 \to t^{-6}g_3$.

Lemma 27. *Let K/k be an elliptic function field. Then K is uniquely determined, up to the above substitution, by the generating Weierstrass equation. The invariant $j = 12^3 g_2^3/(g_2^3 - 27g_3^2)$ remains unchanged by such substitutions.*

Proof. See [4, p. 201]. □

Lemma 28. *Let K_1/k^*, K_2/k^* be elliptic function fields and $k^* \subseteq k \subseteq \bar{k}^*$. Suppose that $K_1k = K_2k$. Then there is l, $[l : k^*] \leq 6$, such that $K_1l = K_2l$.*

Proof. Let $y^2 = 4x^3 - g_2x - g_3$ and $y^{*2} = 4x^{*3} - g_2^*x^* - g_3^*$ be the Weierstrass equations associated to K_1 and K_2 respectively. Since $K_1k = K_2k$, from Lemma 27 there exists $t \in k^*$ such that $x^* = t^2x$ and $y^* = t^3y$. Moreover $g_2^* = t^{-4}g_2$ and $g_3^* = t^{-6}g_3$. We solve this equations in a suitable extension l/k^*. For $j \neq 0, 12^3$, $j = 12^3$, $j = 0$, respectively, the field l is obtained by adjoining a second, fourth or sixth root to k^*. Then $K_2 \subseteq K_1l$ and $K_1 \subseteq K_2l$ is proved similarly. □

Lemma 29. *Let K/k be an elliptic function field and $P \in \mathbb{P}_K^1$. The group $G_P = \{\sigma \in Aut_kK | \sigma(P) = P\}$ is cyclic of order 2,4 or 6. The translation automorphisms form a normal subgroup H of $\mathrm{Aut}_k\, K$ and $G_P \cong (Aut_kK)/H$.*

Proof. See [4, p. 195]. □

Lemma 30. *Let K/k be an elliptic function field and P be a place of degree one. Let L/K be a geometric extension. Suppose that P is the neutral element of the additive abelian group $\mathbb{P}_K^1$. If P is ramified in L/K and the other places of degree one that ramify in L/K have order greater than $2g_L + 1$, then $R(L/K)$ is embedded into G_P.*

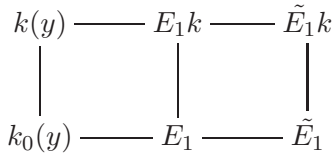
Proof. Let $\varphi : R(L/K) \to (Aut_kK)/H$ be the canonical homomorphism. Suppose that $\varphi(\sigma_1) = \varphi(\sigma_2)$. Then there exists $\tau_R \in H$ such that $\sigma_1\sigma_2^{-1} = \tau_R$. If R is different from P there are at least $|\langle R \rangle| > 2g_L + 1$ places that ramify in L/K. From the genus formula it follows that $R = P$. □

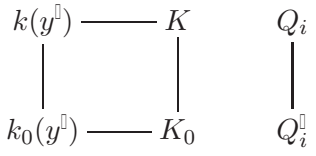
Proposition 31. *Let K/k be an elliptic function field with field of definition k_0, $k_0 \subseteq k \subset \bar{k_0}$. Let $E/k(x)$ be a separable geometric extension of degree m defined over k_0. Assume that the pole divisor of x is ramified in $E/k(x)$. Then there exist infinitely many separable geometric extensions L/K such that $[E : k(x)] = [L : K]$ and $Aut_{k(x)}E \cong Aut_K L = Aut_k L$.*

Proof. We have $g_K = 1$. Let $E_0/k_0(x)$ be a separable geometric extension such that $E = E_0 k$. Let $C = 4m^2(g_K + 1)^2 + m(g_K - 1) + 1 = 16m^2 + 1$, where $m = [E : k(x)]$. By Lemma 24 there exists a C-improvement $E_1/k_0(y)$ of $E_0/k_0(x)$ such that the infinite place of $k_0(y)$ is ramified in $E_1/k_0(y)$ and the other places of $k_0(y)$ ramified in $E_1/k_0(y)$ have degree greater than $C_0 = 6C(6,1)$ ($C(6,1)$ as in Lemma 23).

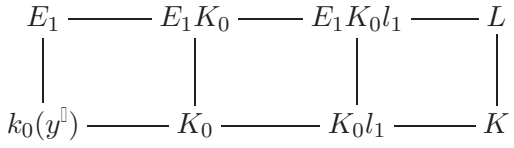
Let $\tilde{E_1}$ be the normal closure of $E_1/k_0(y)$ and $m_0 = [\tilde{E_1} : k_0(y)]$. Let P be the neutral element of the group $\mathbb{P}^1_K$ and p a large prime number such that $(m_0, p) = 1$. Define $A = \{R \in \mathbb{P}^1_K |\ |\langle R\rangle| \leq 2C_1 + 1\}$, where $C_1 = 1 + m(g_K - 1) + 4m(p^2 + m_0)(g_K + 1)(g_E + 1) = 1 + 8m(p^2 + m_0)(g_E + 1)$. Choose $T = \{Q_1, \ldots, Q_{p-1}\} \subset \mathbb{P}^1_K$ with $Q_1 = P$ and Q_i of order greater than $2C_1 + 1$, $2 \leq i \leq p - 1$.

There is an elliptic function field K_0/k_0 such that $K = K_0 k$. We may assume that K_0 has sufficiently many places of degree one. Hence, we may suppose that the places $Q_i^{[1]} = Q \cap K_0$ has degree one.





For a place $Q^{[1]}$ as in Lemma 13, $Q \notin A$, there exists $y^{[1]} \in K_0$ such that the pole divisor in K_0 is $N_{y'} = {Q_1^{[1]}}^p \cdots {Q_{p-1}^{[1]}}^p Q^{[1]m_0+p}$, where $Q^{[1]} = Q \cap K_0$. Hence $(m_0, [K_0 : k_0(y^{[1]})]) = 1$. Using an extension of the isomorphism $\varphi_0 : k_0(y) \to k_0(y^{[1]})$, $\varphi_0(y) = y^{[1]}$, to $\overline{k_0(y)}$ we may assume that E_1 is an extension of $k_0(y^{[1]})$ with the same properties as $E_1/k_0(y)$. By Lemma 25 we have that the places of K ramified in $E_1K = L$ are not elements of A. From Lemma 30 for each $\sigma \in \mathrm{Aut}_k\, L$ we have $|\langle \sigma|_K\rangle| \leq 6$.



Let $\sigma \in \mathrm{Aut}_k L$. There exists $l_1 = l_1(\sigma) \subseteq k$, $[l_1 : k_0] \leq 6C(6,1)$, such that $\sigma(K_0 l_1) = K_0 l_1$ (Lemmas 23, 28). Since the places of $k_0(y^{\square})$ that ramify in E_1 have degree greater than C_0 it follows that in $\sigma(L_1)L_1/K_0 l_1$ the ramified places of degree one of $K_0 l_1$ are $\{Q_i \cap K_0 l_1\} \cup \{Q \cap K_0 l_1\}$. Then Lemma 13 implies $\sigma|_K = \mathrm{Id}$. □

Proposition 32. *Let K/k be an elliptic function field and $E/k(x)$ be a finite separable geometric extension. Assume that the pole divisor of x is ramified in $E/k(x)$. Then there exist infinitely many separable geometric extensions L/K such that $[E : k(x)] = [L : K]$ and $Aut_{k(x)}E \cong Aut_K L = Aut_k L$.*

Proof. There exists $k_0^{\square}$ a finitely generated field over $\mathbb{Q}$ such that for both K/k and $E/k(x)$ the field $k_0^{\square}$ is field of definition. Let X be a transcendence basis of $k/k_0^{\square}$. Now we can apply Proposition 31 with $k_0 = k_0^{\square}(X)$. □

For function fields with infinite full automorphism group the following theorem is analogous to Theorem 1. We assume that if K/k is an elliptic function field then the characteristic of k is zero.

Theorem 33. *Let K/k be a function field either of genus at least two or elliptic such that $\mathrm{Aut}_k K$ is infinite. Let $E/k(x)$ be a finite separable geometric extension. Assume that the pole divisor of x is ramified in $E/k(x)$. Then there exist infinitely many separable geometric extensions L/K such that $[E : k(x)] = [L : K]$ and $Aut_{k(x)}E \cong Aut_K L = Aut_k L$.*

Proof. It follows from Proposition 21 and Proposition 32. □

References

[1] C. Alvarez-Garcia, G. Villa-Salvador, Groups of automorphisms of global function fields, *International Journal of Algebra*, **2**, No. 2 (2008), 65-78.

[2] C. Alvarez-Garcia, G. Villa-Salvador, Finite groups as Galois groups of function fields with infinite field of constants, *Journal of the Australian Mathematical Society*, **88** (2010), 301-312.

[3] G. Derome, Corps de définition et points rationnels, *Journal de Théorie des Nombres de Bordeaux*, **15** (2003), 45-55.

[4] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York and London (1966).

[5] M. Fried, M. Jarden, *Field Arithmetic*, Springer, Berlin New York (2005).

[6] H. Hammer, F. Herrlich, A remark on the moduli field of a curve, *Arch. Math.*, **81** (2003), 5-10.

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

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

[9] M. Rosenlicht, Automorphisms of function fields, *Trans. Amer. Math. Soc.*, **79**, (1955), 1-11

[10] M. Rzedowski-Calderón, G. Villa-Salvador, Automorphisms of congruence function fields, *Pacific Journal of Mathematics*, **150** (1991), 167-178.

[11] H. L. Schmid, Über die Automorphismen eines algebraischen Funktionenkörper von Primzahlcharacteristik. *J. Reine Angew. Math.*, **179** (1938), 5-15.

[12] R. C. Valentini, M. L. Madan, Automorphism groups of algebraic function fields. *Math. Z.*, **176** (1981), 39-52.

[13] G. Villa-Salvador, it Topics in the Theory of Algebraic Function Fields, Birkhaüser, Boston (2006).