PACIFIC JOURNAL OF MATHEMATICS
Vol. 150, No. 1, 1991

AUTOMORPHISMS OF CONGRUENCE FUNCTION FIELDS

M. RZEDOWSKI-CALDERÓN AND G. VILLA-SALVADOR

Let k be a finite field. For a function field K over k and $m \geq 3$, it is proven that there are infinitely many non-isomorphic function fields L such that L/K is a separable extension of degree m and $\mathrm{Aut}_k L = \{\mathrm{Id}\}$. It is also shown that for a finite group G, there are infinitely many non-isomorphic function fields L/k such that $\mathrm{Aut}_k L \cong G$. Finally, given any finite nilpotent group G such that $|G| > 1$ and $(|G|, |k| - 1) = 1$ and any function field K over k, there are infinitely many non-isomorphic function fields L over k with $\mathrm{Gal}(L/K) = \mathrm{Aut}_k L \cong G$.

1. Introduction. Let k be any field and K be an algebraic function field over k. Given a finite group G, does there exist a finite extension L/K, where the exact field of constants of L is k and whose full automorphism group, $\mathrm{Aut}_k L$, is isomorphic to G?

If k is an algebraically closed field, Madden and Valentini [**9**], proved that any finite group can be realized as the full group of automorphisms of an algebraic function field over k.

In [**13**] Stichtenoth, still under the assumption that k is algebraically closed, proved that if $E/k(x)$ is a finite separable extension with $[E : k(x)] > 1$, then, for any function field K/k of genus larger than one, there exist infinitely many separable extensions L/K such that $[L : K] = [E : k(x)]$ and $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong \mathrm{Aut}_{k(x)} E$. In particular, if the non-trivial finite group G is realizable as Galois group of an extension of the rational function field $k(x)$, then, for any function field K/k of genus larger than one, G is realizable as Galois group of an extension L/K and as the full group of automorphisms of L over k.

A congruence function field is a field of algebraic functions of one variable over a finite field of constants.

The main purpose of this paper is to prove that, under one ramification condition, Stichtenoth's result still holds when k is finite (Theorem 3). In this case, we have no restriction on the genus of K. We also prove the analogue, in congruence function fields, to the result of Madden and Valentini (Theorem 5). In §3 we obtain, as a

consequence of the results in §2, that if G is a finite nilpotent group such that $|G| > 1$ and $(|G|, |k| - 1) = 1$ and K is a function field over k, then there are infinitely many non-isomorphic Galois extensions L/K such that $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong G$.

Our approach is as follows: Given a congruence function field K over k and $m \geq 3$, infinitely many non-isomorphic function fields L of degree m over K are constructed whose exact field of constants is k and such that $\mathrm{Aut}_k L = \{\mathrm{Id}\}$. Theorem 2 achieves this.

From now on, k is a finite field of characteristic p and with q elements. If L is a field extension of K, $\mathrm{Aut}_K L$ denotes the group of automorphisms of L that fix K pointwise. In particular, if L/K is Galois, $\mathrm{Aut}_K L = \mathrm{Gal}(L/K)$. x, y, z denote transcendental elements over k; $K, E, F, T, L, \ldots$ are various function fields whose exact field of constants is k. For $x \in E$, $(x)_E$ is the principal divisor of x in E. If E/k is a function field, L/E denotes a separable finite extension where the exact field of constants of L and E is k and $D_{L/E}$ stands for the different of the extension. For a place P in a function field, $\deg(P)$ denotes the degree of the place. Finally, we write g_L for the genus of L.

2. Automorphism groups. As in the papers of Madden-Valentini [**9**] and Stichtenoth [**13**], here Castelnuovo's Inequality plays an important role:

THEOREM 1. *Let L, K, E be function fields with field of constants k and such that $L = KE$. Then*

$$g_L \leq [L : K]g_K + [L : E]g_E + ([L : K] - 1)([L : E] - 1).$$

Theorem 1 is an easy consequence of the Riemann-Hurwitz formula in the case that K and E contain a common transcendental element over k. In the case that K and E do not contain common nonconstants, the proof is not so easy (see [**12**]).

The following lemma is a direct consequence of Theorem 1 with $E = \sigma(K)$ ([**9**], [**13**]):

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

Given a congruence function field K and a positive integer m, we will construct extensions L/K such that the constant field of L

is k, $[L : K] = m$ and all the intermediate fields different from K have suitably large genus. Then, by Lemma 1, it will follow that any $\sigma \in \mathrm{Aut}_k L$ satisfies $\sigma(K) = K$. Also, we obtain these extensions satisfying one extra ramification condition that forces any $\sigma \in \mathrm{Aut}_k L$ to fix K pointwise.

DEFINITION. Let $E_0/k(x)$ be an extension of function fields and C be a real number. If an extension $E_1/k(y)$ satisfies:

(i) $[E_1 : k(y)] = [E_0 : k(x)]$,

(ii) $\mathrm{Aut}_{k(y)} E_1 \cong \mathrm{Aut}_{k(x)} E_0$,

(iii) if M_1 is any intermediate field, $k(y) \subsetneqq M_1 \subset E_1$, then $g_{M_1} \geq C$,

we say that $E_1/k(y)$ is a C-improvement of $E_0/k(x)$.

First we prove the analogue of Lemma 2 in [13].

LEMMA 2. *Let $E_0/k(x)$ be a function field extension. Then, for any real number C, there exists a C-improvement of $E_0/k(x)$.*

Proof. (See [9], [13].) Let $\tilde{E}_0$ be the normal closure of $E_0/k(x)$ and $n = [\tilde{E}_0 : k(x)]$.

Let us assume first that if M is any intermediate field, $k(x) \subsetneqq M \subset E_0$, we have $g_M \geq 1$. Choose any positive integer m such that $(m, pn) = 1$ and $m \geq C$. Let $y = x^{1/m}$. Then $k(y)/k(x)$ is a separable extension of degree m where the only ramified places are the zero and the pole divisors of x and are fully ramified. Let $E_1 = E_0(y)$. $E_1/k(y)$ is separable, $[E_1 : k(y)] = [E_0 : k(x)]$, the field of constants of E_1 is k ([7]) and $\mathrm{Aut}_{k(y)} E_1 \cong \mathrm{Aut}_{k(x)} E_0$. If M_1 is any intermediate field, $k(y) \subsetneqq M_1 \subset E_1$ and $M = M_1 \cap E_0$, then $M_1 = M(y)$. We have $k(x) \subsetneqq M \subset E_0$. Let $\wp$ be any place of M that lies above the zero or pole divisors of x. Since $(m, n) = 1$, $\wp$ is fully ramified in M_1/M. Thus, $\deg(D_{M_1/M}) \geq 2(m-1)$ and by the Hurwitz Genus Formula,

$$g_{M_1} = 1+[M : M_1](g_M-1)+\tfrac{1}{2}\deg(D_{M_1/M}) \geq 1+\tfrac{1}{2}(2(m-1)) = m \geq C.$$

It remains to prove that there exists a 1-improvement of $E_0/k(x)$.

Let m denote a natural number larger than one such that $(m, pn) = 1$ and again let $y = x^{1/m}$. Define $E_2 = E_0(y)$. As before, $E_2/k(y)$ satisfies (i) and (ii) of a 1-improvement of $E_0/k(x)$.

Let M_2 be such that $k(y) \subsetneqq M_2 \subset E_2$. Then $M = M_2 \cap E_0$ satisfies $k(x) \subsetneqq M \subset E_0$. Let $\wp_0$ and $\wp_\infty$ be the zero and the pole divisors of x in $k(x)$.

(a) Assume that at least one of $\wp_0$ and $\wp_\infty$ is not fully ramified in $M/k(x)$. Say that $\wp_0$ is not fully ramified. We have that in M, $\wp_0 = P_1^{e_1} \cdots P_h^{e_h}$. Then, either $h \geq 2$ or $\deg(P_1) \geq 2$. Thus, at least three places ramify fully in $M_1/M(P_1, P_2$ and a place of M that lies above $\wp_\infty)$ or at least two places ramify fully and one of them is of degree ≥ 2. By the Genus Formula, $g_{M_2} \geq 1/2$. Therefore $g_{M_2} \geq 1$.

(b) Observe that if $g_M \geq 1$, then $g_{M_2} \geq 1$.

(c) In the case that there exists M such that $k(x) \subsetneq M \subset E_0$, $g_M = 0$ and both $\wp_0$ and $\wp_\infty$ ramify fully in $M/k(x)$, we will require a further construction.

The extension $E_2/k(y)$ just obtained does satisfy that if $k(y) \subsetneq M_2 \subset E_2$ and $g_{M_2} = 0$, then $M_2 = k(y^{1/s})$ where $s = [M_2 : k(y)]$.

Therefore, the extension $E_2/k(y)$ is such that if $k(y) \subsetneq M_2 \subset E_2$ and $g_{M_2} = 0$, then the zero and pole divisors of y in $k(y)$ are fully ramified in $M_2/k(y)$.

Let d be any integer such that $d > 1$, $(d, np) = 1$ and large enough so we can choose two different places B_1 and B_2 in $k(x)$ of degree d.

$$\begin{array}{ccc} E_3 & \text{———} & E_4 \\ | & & | \\ M_3 & \text{———} & M_4 \\ | & & | \\ k(z) & \underset{d}{\text{———}} & k(x) \end{array}$$

Let $z \in k(x)$ be such that $(z)_{k(x)} = B_1 B_2^{-1}$. We construct an extension $E_3/k(z)$ satisfying (i) and (ii) of a 1-improvement of $E_0/k(x)$ and if M_3 is such that $k(z) \subsetneq M_3 \subset E_3$ and $g_{M_3} = 0$, then the zero and pole divisors, Q_0 and Q_∞, of z are fully ramified in $M_3/k(z)$.

We have $[k(x) : k(z)] = d$, Q_0 and Q_∞ are inert in $k(x)/k(z)$. We define $E_4 = E_3(x)$.

The extension $E_4/k(x)$ satisfies (i) and (ii) of a 1-improvement of $E_0/k(x)$. Let M_4 be any intermediate field $k(x) \subsetneq M_4 \subset E_4$. Then $M_3 = M_4 \cap E_3$ satisfies $k(z) \subsetneq M_3 \subset E_3$. If $g_{M_3} \geq 1$, then $g_{M_4} \geq 1$. If $g_{M_3} = 0$, then Q_0 and Q_∞ ramify fully in $M_3/k(z)$. Thus, B_1, B_2 ramify fully in $M_4/k(x)$. Again, by the Genus Formula,

$g_{M_4} \geq ([M_4 : k(x)] - 1)(d - 1) > 1$. The extension $E_4/k(x)$ is a 1-improvement of $E_0/k(x)$.

This completes the proof of Lemma 2.

REMARK. It follows from the proof of Lemma 2 that if $\wp_0$ ramifies and $\wp_\infty$ does not ramify in $E_0/k(x)$, then the same occurs in $E_1/k(y)$.

Next we have

LEMMA 3. *Let m be any integer, $m \geq 3$ and let x be any transcendental element over k. Then, there exists an extension $E/k(x)$ of degree m such that $\mathrm{Aut}_{k(x)} E = \{\mathrm{Id}\}$, the zero divisor of x ramifies in $E/k(x)$ and the pole divisor of x does not ramify in $E/k(x)$.*

Proof. (See [13].) Let $E = k(y)$, where $y^{m-1}(y - 1) = x$. Then $E/k(x)$ is separable of degree m. Since any automorphism of E over $k(x)$ fixes three places of degree one of E, $\mathrm{Aut}_{k(x)} E = \{\mathrm{Id}\}$. We observe that the zero and pole divisors of x ramify in E. It follows from $g_E = 0$ and the Hurwitz Genus Formula that there exists at most one place (which must be of degree one), besides the zero and pole divisors of x, that ramifies in $E/k(x)$. If $k \neq \mathbf{F}_2$, $\mathbf{F}_2$ the finite field with two elements, there is at least one place of degree one which is not ramified. If $k = \mathbf{F}_2$, there is wild ramification, thus the third place of degree one is not ramified. In any case, there is at least one place of degree one that ramifies and at least one place of degree one that does not ramify in $E/k(x)$. We may assume that the zero divisor of x is the one that ramifies and the pole divisor of x is the one that does not ramify.

This completes the proof of Lemma 3.

Now, we prove the analogue in congruence function fields to Satz 3 in [13].

THEOREM 2. *Let K be any function field over k and m be any integer, $m \geq 3$. Then there exist infinitely many non-isomorphic fields L such that L/K is separable of degree m, and $\mathrm{Aut}_k L = \{\mathrm{Id}\}$.*

Proof. Let $H = \mathrm{Aut}_k K$. We have that H is a finite group ([2], [11]) say of order n. Let F denote the subfield of K fixed by H.

Let A be a place of K of degree a, where $(a, mnp) = 1$. As a consequence of the Riemann Hypothesis, we have that the number of

places of degree t of K is $\frac{1}{t}q^t + O(q^{t/2})$ (see [3], page 41). We also have that the number of places of degree t of K that restrict to lower degree places of F is bounded by

$$\sum_{\substack{f|n \\ f>1}} \frac{n}{f} \cdot \left(\text{Number of places of degree } \frac{t}{f} \text{ of } F\right)$$

$$= \sum_{\substack{f|n \\ f>1}} \left(\frac{n}{f} \cdot \frac{f}{t} q^{t/f} + O(q^{t/2f})\right) \leq \frac{n}{t} q^{t/2} + O(q^{t/3}).$$

Therefore, there exists a positive integer t_0 such that for any $t \geq t_0$, there are places of degree t of K that restrict to places of F, also of degree t. Any of these places in F decomposes fully in K.

$$\begin{array}{ccc} E & \text{——} & L \\ {\scriptstyle m}\big| & & \big| \\ k(x) & \text{——} & K \\ & & \big|{\scriptstyle H} \\ & & F \end{array}$$

Choose a positive integer t such that $t \geq t_0$, $t > g_K + 1$ and $(t, mnp) = 1$. Let Q be a place of F of degree ta that is fully decomposed in K/F and denote by $B_1, \ldots, B_n$ the places of K that lie above Q.

Consider first the case $n \geq 2$. By the Riemann-Roch Theorem there exist $x \in K$ such that $(x)_K = B_1 A^r C B_2^{-s} B_3^{-1} \cdots B_n^{-1}$ where C is an integral divisor, $s \geq 2$ is such that $(mnp, n+s-2) = 1$ and $r = (n+s-4)t+1$. Since $\deg(C) = (t-1)a < ta = \deg(B_i)$, C is relatively prime to B_i, $i = 1, \ldots, n$. We have $[K : k(x)] = ta(n+s-2)$ and $(ta(n+s-2), n) = 1$. Hence $K = F(x)$.

Let $\wp_0$ and $\wp_\infty$ denote the zero and pole divisors of x in $k(x)$. Using Lemmas 3 and 2 we can construct an extension $E/k(x)$ such that $[E : k(x)] = m$, $\mathrm{Aut}_{k(x)} E = \{\mathrm{Id}\}$, for any intermediate field M, $k(x) \subsetneq M \subset E$, we have $g_M > m^2 + 2(g_K - 1)m + 1$, $\wp_0$ ramifies in $E/k(x)$ and $\wp_\infty$ does not ramify in $E/k(x)$.

Define $L = KE$. L/K is an extension of degree m. Let $\sigma \in \mathrm{Aut}_k L$. From Lemma 1 it follows that $\sigma(K) = K$. Now, since $\wp_0$ ramifies in $E/k(x)$ and B_1 is not ramified in $K/k(x)$, it follows

that B_1 ramifies in L/K. Since $\wp_\infty$ does not ramify in $E/k(x)$, $B_2, \ldots, B_n$, do not ramify in L/K. Hence $B_1^\sigma = B_1$. Thus, necessarily $\sigma = \mathrm{Id}$. Therefore $\mathrm{Aut}_k L = \{\mathrm{Id}\}$.

If $n = 1$, we have $\mathrm{Aut}_k K = \{\mathrm{Id}\}$ and the extension L is obtained as above.

Finally, we observe that since g_E can be chosen arbitrarily large, g_L can be arbitrarily large so there are infinitely many fields L with $[L : K] = m$ and $\mathrm{Aut}_k L = \{\mathrm{Id}\}$.

The proof of Theorem 2 is complete.

Partial analogues to Satz 1 and Satz 2 in [**13**] follow immediately from Lemma 2 and the proof of Theorem 2.

THEOREM 3. *Let $E_0/k(x)$ be an extension of function fields with $[E_0 : k(x)] > 1$. Let $\wp_0$ and $\wp_\infty$ denote the zero and pole divisors of x in $k(x)$, respectively. Then, if $\wp_0$ ramifies and $\wp_\infty$ does not ramify in $E_0/k(x)$, we have that for any function field K over k there exist infinitely many non-isomorphic extensions L/K such that $[L : K] = [E_0 : k(x)]$ and $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong \mathrm{Aut}_{k(x)} E_0$.*

THEOREM 4. *If G is a non-trivial finite group realizable as Galois group of an extension $E_0/k(x)$ with the ramification prescribed in Theorem 3, then for any function field K over k there exist infinitely many Galois extensions L/K such that $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong G$.*

We finish this section by proving the congruence function fields analogue to the result of Madden and Valentini [**9**].

THEOREM 5. *Let G be any finite group. Then, there exist infinitely many non-isomorphic function fields L/k such that $\mathrm{Aut}_k L \cong G$.*

Proof. Let l be a prime number such that $G \subset S_l$. Then, there is an extension $E_0/k(x)$ such that $\mathrm{Gal}(E_0/k(x)) \cong S_l$ ([**4**], [**6**], [**8**]). Let T denote the subfield of E_0 fixed by G. Then E_0/T is a Galois extension with Galois group isomorphic to G. Let d, d_1, d_2 be positive integers such that d is a prime number, $d \neq p$, $d_1 + d_2 = d$, $d_1 > d_2 \geq \max\{3, 2g_T - 2\}$ and large enough so we can choose two places B_1, B_2 in T that decompose fully in E_0, of degrees d_1, d_2 respectively. By the Riemann-Roch Theorem, there exists $y \in T$ whose pole divisor is $B_1 B_2$. Then, the extension $E_0/k(y)$ is not normal (see [**9**]). By Theorem 2, we can obtain an extension $K/k(y)$ of degree relatively prime to $[E_0 : k(y)]$ and $\mathrm{Aut}_k K = \{\mathrm{Id}\}$.

$$\begin{array}{ccc} E_1 & \text{——} & L \\ {\scriptstyle G}\big| & & \big|{\scriptstyle G} \\ T_1 & \text{——} & F \\ {\scriptstyle d}\big| & & \big| \\ k(y) & \text{——} & K \end{array}$$

Using Lemma 2, we can construct a C-improvement $E_1/k(y)$ of $E_0/k(y)$ such that there is an intermediate field T_1, $k(y) \subset T_1 \subset E_1$ with $\mathrm{Gal}(E_1/T_1) \cong G$, where $C = [E_1 : k(y)]^2 + 2(g_K - 1)[E_1 : k(y)] + 2$. Since the genus of K is smaller than the genus of any intermediate field of $E_1/k(y)$ other than $k(y)$, it follows that $K \cap E_1 = k(y)$.

Let $L = E_1K$ and $F = T_1K$. Then L/F is a Galois extension such that $\mathrm{Gal}(L/F) \cong G$ and by Lemma 1, $\mathrm{Aut}_k L = \mathrm{Aut}_K L$. Since L/K is not normal and $[F : K] = d$, a prime number, we must have F is the field fixed by $\mathrm{Aut}_k L$. Thus $\mathrm{Aut}_k L = \mathrm{Aut}_F L \cong G$.

The existence of infinitely many non-isomorphic such fields L follows from the fact that we can choose g_{E_1} arbitrarily large.

3. Nilpotent groups. We use the results obtained in §2 to prove the following theorem.

THEOREM 6. *Let G be a finite nilpotent group, $|G| > 1$ and $(|G|, q-1) = 1$. Then, for any function field K over k, there exist infinitely many non-isomorphic Galois extensions L/K such that* $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong G$.

Proof. We first prove the theorem for the case G is an l-group, where l is a prime number such that $(l, q-1) = 1$. Let $|G| = l^v$, $v \geq 1$. We will make the proof by induction on v.

For $v = 1$ we consider two cases:

(i) $l = p$: Let $x \in K$ be such that $([K : k(x)], p) = 1$. Let $E = k(x, y)$, where

$$\begin{array}{ccc} E & & \\ \big| & & y^p - y = \dfrac{1}{x}. \\ k(x) & \text{——} & K \end{array}$$

Then, $E/k(x)$ is a cyclic extension of degree p where $\wp_0$, the zero divisor of x in $k(x)$, is the only ramified place. By Theorem 4 we obtain infinitely many cyclic extensions L/K of degree p such that $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong G$.

(ii) $l \neq p$: Let $H, n, F, A, a, t_0, t, Q, B_1, \ldots, B_n, x, C, s, r$ as in the proof of Theorem 2, with $m = l$ in this case, $(x)_K = B_1 A^r C B_2^{-s} B_3^{-1} \cdots B_n^{-1}$. We have $K = F(x)$. We consider first the case $n \geq 2$.

Let $d \geq 1$ be such that

(a) $(d, l) = 1$;
(b) $\frac{1}{2}(l-1)(d-2) > l^2 + 2l(g_K - 1) + 1$;
(c) $l | q^d - 1$.

Such d exists. It suffices to take $d = u(l-1)$, $(u, l) = 1$ and u large enough.

Let α be a generator of the multiplicative group of the finite field of q^d elements. Then, the order of α is $q^d - 1$. Let P be the irreducible polynomial of α over k. P is of degree d.

Let $\Delta = k(x)(\Lambda_P)$ be the cyclotomic extension determined by P (see Hayes [5]). We have that P is fully ramified and $\wp_\infty$, the pole divisor of x in $k(x)$, is ramified with ramification index $q-1$ and decomposes in $(q^d-1)/(q-1)$ places in Δ. No other place is ramified in $\Delta/k(x)$. Let E be the unique subfield of Δ such that $[E : k(x)] = l$. Since $(l, q-1) = 1$, P is the only ramified place in $E/k(x)$ and $\wp_\infty$ decomposes into l factors. We have $g_E = \frac{1}{2}(l-1)(d-2)$. Let $\wp_0$ be the zero divisor of x in $k(x)$. It follows from the election of P that $x^f \equiv 1 \bmod P$ if and only if $q^d - 1 | f$. Therefore the minimal such f is $f = q^d - 1$. By Carlitz [1], Theorem 12, it follows that the degree of inertia of $\wp_0$ in $\Delta/k(x)$ is $q^d - 1$. Therefore, the degree of inertia of $\wp_0$ in $E/k(x)$ is l. Let $L = KE$. L/K

$$\begin{array}{ccc} E & \text{——} & L = KE \\ {\scriptstyle l}\,\big| & & \big|\,{\scriptstyle l} \\ k(x) & \text{——} & K \\ & & \big|\,{\scriptstyle H} \\ & & F \end{array}$$

is a cyclic extension of degree l. Let $\sigma \in \mathrm{Aut}_k L$. Since $g_L \geq g_E = \frac{1}{2}(l-1)(d-2) > l^2 + 2l(g_K - 1) + 1$, it follows from Lemma 1 that $\sigma(K) = K$. Now, $B_1^\sigma = B_i$, for some $i = 1, 2, \ldots, n$. Since $\wp_\infty$ decomposes in $E/k(x)$, it follows that B_i decomposes in L/K, $i = 2, \ldots, n$. Finally, since $\wp_0$ is inert in $E/k(x)$ and the degree of inertia of B_1 over $\wp_0$ is ta, and $(ta, l) = 1$, we have that B_1 is inert in L/K. Therefore, $B_1^\sigma = B_1$ and $\sigma|_K = \mathrm{Id}$. Thus $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong G$.

Finally, we observe that we have infinitely many such L because d can be chosen arbitrarily large.

If $n = 1$, we have $\mathrm{Aut}_k K = \{\mathrm{Id}\}$ and the extension L is obtained as above.

This finishes the case $v = 1$.

For $|G| = l^v$, let T be a subgroup of G of order l contained in the center of G. Let $\overline{G} = G/T$. We have $|\overline{G}| = l^{v-1}$. As induction hypothesis we have that there exist

$$\begin{array}{ccc} E & \text{———} & L = EK \\ | & & | \\ E_0 & \text{———} & L_0 = E_0K \\ | & & | \\ k(x) & \text{———} & K \end{array}$$

$x \in K$ and an extension $E_0/k(x)$ such that $([K : k(x)], l) = 1$, $E_0/k(x)$ and $L_0 = E_0K/K$ are Galois extensions with Galois group $\overline{G}$ and $\mathrm{Aut}_k L_0 = \mathrm{Aut}_K L_0 \cong \overline{G}$.

In [**10**], an extension E/E_0 is obtained such that $E/k(x)$ is a Galois extension with Galois group G and such that the number of ramified places in E/E_0 is arbitrarily large. We have $E \cap K = k(x)$. We choose the number of ramified places in E/E_0 so that $g_E > l^2 + 2l(g_{L_0} - 1) + 1$. Let $L = KE$. We have that L/K is a Galois extension with Galois group G. Now, let $\sigma \in \mathrm{Aut}_k L$. Since $g_L \geq g_E > l^2 + 2l(g_{L_0} - 1) + 1$, it follows from Lemma 1 that $\sigma(L_0) = L_0$. Therefore, $\sigma|_{L_0} \in \mathrm{Aut}_k L_0 = \mathrm{Aut}_K L_0$. Hence, $\sigma \in \mathrm{Aut}_K L$. L satisfies $\mathrm{Aut}_k L = \mathrm{Aut}_K L \cong G$.

This finishes the case G is an l-group.

For the general case, let G be a nilpotent group with $|G| > 1$, $(|G|, q-1) = 1$. We express G as the direct sum of its Sylow subgroups, $G \cong \bigoplus_{i=1}^{h} G_i$, $|G_i| = l_i^{\alpha_i}$, $l_1, \ldots, l_h$ the different primes dividing $|G|$. For $h = 1$, the theorem has been proved. For $h > 1$, we obtain, by induction, an extension L_1/K such that $\mathrm{Aut}_k L_1 = \mathrm{Aut}_K L_1 \cong G/G_h$. It follows from the case where G is an l-group and from [**10**], Lemma 1, that there exists a

$$\begin{array}{ccc} L_1 & & \\ | & & \\ K & \text{---} & L_2 \end{array}$$

Galois extension L_2/K with Galois group G_h such that $\mathrm{Aut}_k L_2 = \mathrm{Aut}_K L_2 \cong G_h$ and such that any intermediate field $K \subsetneqq M \subset L_2$ satisfies $g_M > l_h^{2\alpha_h} + 2l_h^{\alpha_h}(g_{L_1} - 1) + 1 \geq [M : K]^2 + 2[M : K](g_{L_1} - 1) + 1$.

We have $L_1 \cap L_2 = K$. Let $L = L_1 L_2$, L/K is a Galois extension with Galois group G. Let $\sigma \in \mathrm{Aut}_k L$. Since any intermediate field $L_1 \subsetneqq M_1 \subset L$ satisfies $g_{M_1} > [M_1 : L_1]^2 + 2[M_1 : L_1](g_{L_1} - 1) + 1$, we have $\sigma(L_1) = L_1$. Thus $\sigma|_{L_1} \in \mathrm{Aut}_k L_1 = \mathrm{Aut}_K L_1$. Hence $\sigma \in \mathrm{Aut}_k L = \mathrm{Aut}_K L \cong G$.

Finally, the existence of infinitely many such extensions L/K, follows from the fact that the genus of L can be chosen arbitrarily large.

References

[1] L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc., **43** (1938), 167–182.

[2] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, 1966.

[3] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, 1986.

[4] W.-D. Geyer, *Curves over finite fields are stable*, preprint.

[5] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc., **189** (1974), 77–91.

[6] ——, *The Galois group of* $x^n + x - t$, Duke Math. J., **40** (1973), 459–461.

[7] M. L. Madan, *Class groups of global fields*, J. Reine Angew. Math., **252** (1972), 171–177.

[8] M. L. Madan and D. J. Madden, *On the theory of congruence function fields*, Comm. Algebra, **8 (17)** (1980), 1687–1697.

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

[10] M. Rzedowski-Calderón, *Construction of global function fields with nilpotent automorphism groups*, to appear in Boletín de la Sociedad Matemática Mexicana.

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

[12] H. Stichtenoth, *Die Ungleichung von Castelnuovo*, J. Reine Angew. Math., **348** (1984), 197–202.
[13] ____, *Zur Realisierbarkeit endlicher Gruppen als Automorphismengruppen algebraischer Funktionenkörper*, Math. Z., **187** (1984), 221–225.

Received November 1, 1989 and in revised form April 27, 1990.

DEPARTAMENTO DE MATEMÁTICAS
CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I. P. N.
APARTADO POSTAL 14-740
07000 MÉXICO, D. F., MÉXICO