Boletín de la Sociedad Matemática Mexicana Vol. 34, 1989

CONSTRUCTION OF GLOBAL FUNCTION FIELDS WITH NILPOTENT AUTOMORPHISM GROUPS*

By MARTHA RZEDOWSKI-CALDERON

1. Introduction

There is a close analogy between the fields of algebraic numbers and the fields K/k of algebraic functions of one variable. This analogy is most pronounced for the class of congruence function fields, i.e., when k, the field of constants, is a finite field. Together with algebraic number fields of finite degree, they form the class of global fields. Given a global field K and a finite group G, does there exists a Galois extension L/K such that $\mathrm{Gal}(L/K) \cong G$? This is the famous Inverse Problem of Galois Theory. Šafarevič [17] solved this problem for number fields when G is a solvable group. There is one important difference between the two classes of global fields. There is no unique subfield of the congruence function field which is the analogue of the field of rational numbers. In fact, there are infinitely many fields of rational functions contained in every function field K/k of one variable.

In this paper, we ask the following question which has no analogue for number fields: Given a finite field k with q elements, and a finite group G, does there exists a Galois extension L of the rational function field $k(x)$ such that G, $\mathrm{Gal}(L/k(x))$ and $\mathrm{Aut}(L/k)$, the group of all k-automorphisms of L, are all isomorphic? We answer this question in the affirmative if G is a nilpotent group such that $\mid G \mid > 1$ and $(\mid G \mid, q-1) = 1$. The Castelnuovo's Inequality is the most important ingredient in the proof. Our proofs also use techniques of Reichardt [15] and D'Mello-Madan[4].

We remark that the analogue of the Inverse Problem of Galois Theory is an unsolved problem even when k is algebraically closed and of characteristic p. If k is the field of complex numbers, Greenberg [6] showed that there exist extensions L/k such that $\mathrm{Gal}(L/k(x)) \cong G \cong \mathrm{Aut}(L/k)$. When k has characteristic $p > 0$, Madden and Valentini [13] showed that there exist L/k such that $\mathrm{Aut}(L/k) \cong G$. Finally, for fields of characteristic $p > 0$, algebraically closed k and solvable G, D'Mello and Madan [4] proved that there exist infinitely many extensions $L/k(x)$ such that $\mathrm{Aut}(L/k)$, $\mathrm{Gal}(L/k(x))$ and G are all isomorphic.

From now on, let k denote a finite field, $\mid k \mid = q = p^r$ for some prime number p. Let x be an indeterminate over k and denote $k(x)$ by K. Let G be a finite nilpotent group, $\mid G \mid > 1$ and $(\mid G \mid, q-1) = 1$.

Since our goal is to construct an extension L/K such that $\mathrm{Aut}(L/k) = \mathrm{Gal}(L/K) \cong G$ and $\mathrm{Aut}(K/k)$ is non-trivial, the condition $\mid G \mid > 1$ is clearly necessary.

---

* This is essentially part of the author's dissertation written at The Ohio State University. The author wishes to express her gratitude for the guidance provided by her thesis adviser, Professor Manohar L. Madan.

In §2 and §3 we consider, respectively, the cases that G is a p-group and G is an ℓ-group, ℓ a prime number, $\ell \neq p$. In these sections, to obtain the Galois extension, we follow closely the construction by induction that Reichardt [15] makes for number fields. Our condition $(\ell, q-1) = 1$ corresponds to his restriction $\ell \neq 2$. In §4 we utilize the results of §2 and §3 to prove the main result, that is, the case when G is nilpotent.

We will use the symbol □ to indicate the end of a proof.

2. G is a p-group

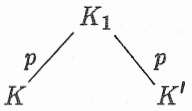
Assume $| G | = p^n$. Let $G_n = G$. For $\nu = n, n-1, \ldots, 1$, we obtain a subgroup H_ν of the center of G_ν, of order p and set $G_{\nu-1} = G_\nu / H_\nu$. We will construct fields $K_1 \subseteq \cdots \subseteq K_n = L$, so that $\mathrm{Gal}(K_\nu/K) \cong G_\nu$ and $\mathrm{Aut}(K_\nu/k) = \mathrm{Gal}(K_\nu/K)$.

The Case $\nu = 1$:

Let t_1 be a given natural number. Consider different primes $P_1, \ldots, P_{t_1}$ in K and let $f(x) = \frac{1}{P_1 \cdot \cdots \cdot P_{t_1}}$.

By Hasse [7, page 38], we have that $K_1 = K(y)$, where $y^p - y = f(x)$, is an extension of K of degree p and the primes $P_1, \ldots, P_{t_1}$ are precisely the primes of K that ramify in K_1. Thus $\mathrm{Gal}(K_1/K) \cong G_1$.

Let $\sigma \in \mathrm{Aut}(K_1/k)$. First we want to show $\sigma(K) = K$. Let $K' = \sigma(K)$. Assume



$K' \not\subseteq K$. Then $K_1 = KK'$.

We have genus of K = genus of K' = 0. Let g = genus of K_1. By the Riemann-Hurwitz Genus Formula, $g = p(0-1) + \frac{1}{2}\deg(D_{K_1/K}) + 1$, where $D_{K_1/K}$ denotes the different of K_1/K. Since there are t_1 primes of K ramifying in K_1, $\deg(D_{K_1/K}) \geq t_1 \cdot 2 \cdot (p-1)$ (see Hasse [7, page 42]).

Therefore

$$g \geq -p + t_1(p-1) + 1 = (p-1)(t_1 - 1). \tag{1}$$

On the other hand, by Castelnuovo's Inequality (see Madden-Valentini [13, page 163] and Eichler [5, page 281]),

$$g \leq p \cdot 0 + p \cdot 0 + (p-1)(p-1) = (p-1)^2. \tag{2}$$

From (1) and (2), $(p-1)(t_1-1) \leq (p-1)^2$, so $t_1 \leq p$. Thus, if we choose $t_1 > p$, we obtain a contradiction. Therefore, if $t_1 > p$, $\sigma(K) \subseteq K$. Since it is also true that $\sigma^{-1}(K) \subseteq K$, it follows $\sigma(K) = K$.

Now we show $\sigma|_K = \mathrm{id}_K$. To do this we use the following argument of Valentini-Madan [19, page 44].

First, we prove that there are infinitely many primes P of K such that $\tau(P) \neq P$ for all $\tau \in \mathrm{Aut}(K/k)$, $\tau \neq \mathrm{id}_K$. We have $\mathrm{Aut}(K/k)$ is finite. Let E be the field fixed by $\mathrm{Aut}(K/k)$. Then $\mathrm{Gal}(K/E) = \mathrm{Aut}(K/k)$. By Čebotarev's Density Theorem (see Jarden [10]), there are infinitely many primes Q of E that decompose fully in K. A prime P of K that lies above one of these Q satisfies $\tau(P) \neq P$ for all $\tau \in \mathrm{Aut}(K/k)$, $\tau \neq \mathrm{Id}_K$.

Let $S = \{P_1, \ldots, P_{t_1-1}\}$ be a set of $t_1 - 1$ primes of K. Let $M = \{\tau \in \mathrm{Aut}(K/k) \mid \tau \neq \mathrm{Id}_K \text{ and } | \tau(S) \cap S | \geq t_1 - 2\}$. Since $\mathrm{Aut}(K/k)$ is finite, M is finite. Thus, the set $\{P \mid P \text{ is prime in } K \text{ and } \tau(P) \in S \text{ for some } \tau \in M\}$ is also finite. Therefore, there exists a prime P_{t_1} in K such that $P_{t_1} \notin S$, $\tau(P_{t_1}) \neq P_{t_1}$ and $\tau(P_{t_1}) \notin S$ for all $\tau \in M$.

Let $i \in \{1, \ldots, t_1\}$. Then $\sigma(P_i) = P_j$ for some j because $P_1, \ldots, P_{t_1}$ are precisely the primes of K that ramify in K_1 and we have unique factorization in K_1.

If $\sigma|_K \neq \mathrm{Id}_K$, then $\sigma|_K \in M$. This contradicts our choice of P_{t_1}. Therefore $\sigma|_K = \mathrm{Id}_K$ as desired. We conclude $\sigma \in \mathrm{Gal}(K_1/K)$.

Thus, if $t_1 \geq p + 1$ and the Artin-Schreier extension K_1/K is defined as above, we have $\mathrm{Aut}(K_1/k) = \mathrm{Gal}(K_1/K)$ is a cyclic group of order p.

The Induction Step:

Assume $K\nu - 1$ constructed for $\nu \leq n$, with $\mathrm{Gal}(K_{\nu-1}/K) \cong G_{\nu-1}$ and $\mathrm{Aut}(K_{\nu-1}/k) = \mathrm{Gal}(K_{\nu-1}/K)$. We want to show that $K_{\nu-1}$ is contained in a field K_ν with Galois group isomorphic to G_ν such that $\mathrm{Aut}(K_\nu/k) = \mathrm{Gal}(K_\nu/K)$.

In order to handle this problem we refer first to Iwasawa [9]. Let K be a field and E/K a finite Galois extension. Let G be a finite group containing a normal subgroup H such that there is an isomorphic mapping φ from G/H onto $\mathrm{Gal}(E/K)$. The embedding problem $P(E/K, G/H, \varphi)$ has a solution (L, Ψ) if we can embed E in a finite Galois extension L of K so that the isomorphism Ψ from G onto $\mathrm{Gal}(L/K)$, maps H onto $\mathrm{Gal}(L/E)$ and induces, in a natural way, the given isomorphism φ from G/H onto $\mathrm{Gal}(E/K)$.

We state without proof the following Theorem of Iwasawa [9,Theorem 2'].

THEOREM 1. *Let K be a field of characteristic $p > 0$. In order that every embedding problem $P(E/K', G/H, \varphi)$ have a solution for an arbitrary finite separable extension K' of K and an arbitrary p-group H, it is necessary and sufficient that K have the following property:*

For any finite Galois extension E of K and for any integer $m \geq 1$, the additive group E^+ of E contains m elements $\alpha_1, \ldots \alpha_m$ such that the conjugates $\sigma(\alpha_i)$ of α_i, $i = 1, \ldots, m$, $\sigma \in Gal(E/K)$ are p-independent in E^+ modulo the subgroup $\mathcal{P}_p(E)$. (Here $\mathcal{P}_p(E) = \{a^p - a \mid a \in E\}$). □

To verify that in our situation the condition in Theorem 1 holds, we refer to Lemma 2(ii) of D'Mello-Madan [4]. To adapt their proof to our case, we only

have to argue that by Čebotarev's Density Theorem, there are infinitely many primes of K that decompose fully in E.

From the above remark it follows that there exists $K'_\nu/K_{\nu-1}$ such that $\mathrm{Gal}(K'_\nu/K) \cong G_\nu$.

Let t_ν be a given natural number. Let $P_1, \ldots, P_{t_\nu}$ be different primes of K that are unramified in K'_ν/K. As in case $\nu = 1$, construct $\Lambda = K(y)$, where $y^p - y = \frac{1}{P_1 \cdot \cdots \cdot P_{t_\nu}}$. $[\Lambda : K] = p$ and the primes $P_1, \ldots P_{t_\nu}$ ramify in Λ.

Let $< s >$ be the Galois group of Λ over K. Say $H_\nu =< h >$. We have the situation

$$G_\nu \left\{ \begin{array}{ccc} & K'_\nu & \text{——} & K'_\nu\Lambda \\ H_\nu & | & & | \\ & K_{\nu-1} & \text{——} & K_{\nu-1}\Lambda, \\ G_{\nu-1} & | & & | \\ & K & \text{——} & \Lambda \end{array} \right. \qquad \mathrm{Gal}(K'_\nu\Lambda/K) \cong G_\nu \times < s > .$$

Consider the subgroups $< (h^a, s) >$ for $0 \leq a < p$, of $G_\nu \times < s >$. We have $\frac{G_\nu \times < s >}{< (h^a, s) >} \cong G_\nu$ for $0 \leq a < p$, because:

(i) $< (h^a, s) >$ is normal in $(G_\nu \times < s >)$:

$(\gamma, s^t)^{-1}(h^a, s)^\nu(\gamma, s^t) = (\gamma^{-1}(h^a)^\nu\gamma, s^{-t}s^\nu s^t) = ((h^a)^\nu, s^\nu)$, since $H_\nu \subseteq$ center of G_ν. Actually $< (h^a, s) > \subseteq$ center of $(G_\nu \times < s >)$.

(ii) Let $\varphi_a : G_\nu \times < s > \rightarrow G_\nu$ be given by $\varphi_a((\gamma, s^t)) = \gamma h^{-ta}$. We have that φ_a is an epimorphism. Now $(\gamma, s^t) \in \ker \varphi_a \iff \gamma h^{-ta} = 1 \iff \gamma = h^{ta} \iff (\gamma, s^t) = (h^{at}, s^t) = (h^a, s)^t \in < (h^a, s) >$. Therefore, $\frac{G_\nu \times < s >}{< (h^a, s) >} \cong G_\nu$.

We claim that the primes $P_1, \ldots, Pt_\nu$ ramify in each of the subfields between $K_{\nu-1}$ and $K'_\nu\Lambda$, different from K'_ν. Let $\mathcal{P}_1$ be a prime of $K_{\nu-1}$ that lies above P_1. Let T be the inertia group of $\mathcal{P}_1$ for $K'_\nu\Lambda/K_{\nu-1}$. We have $\mid T \mid = p$. Thus the inertia field of $\mathcal{P}_1$ is K'_ν.

Choose any field between $K_{\nu-1}$ and $K'_\nu\Lambda$, different from $K_{\nu-1}\Lambda$ and K'_ν. Call it K_ν. $P_1, \ldots, P_{t_\nu}$ ramify in K_ν. We also have $\mathrm{Gal}(K_\nu/K) \cong G_\nu$.

To show that $\sigma(K_{\nu-1}) \subseteq K_{\nu-1}$ for any $\sigma \in \mathrm{Aut}(K_\nu/k)$ we use an argument that involves the Genus Formula and Castelnuovo's Inequality which is similar to that for the case $\nu = 1$. Here it is enough to require $t_\nu > \frac{pg_{\nu-1}+p^2-p}{p-1}$ where $g_{\nu-1}$ is the genus of $K_{\nu-1}$.

Analogously, $\sigma^{-1}(K_{\nu-1}) \subseteq K_{\nu-1}$, so $K_{\nu-1} \subseteq \sigma(K_{\nu-1})$. Thus $\sigma|_{K_{\nu-1}} \in \mathrm{Aut}(K_{\nu-1}/k)$. By induction hypothesis, $\sigma|_{K_{\nu-1}} \in \mathrm{Gal}(K_{\nu-1}/K)$ so $\sigma(x) = \sigma|_{K_{\nu-1}}(x) = x$. Then $\sigma \in \mathrm{Gal}(K_\nu/K)$. We conclude $\mathrm{Aut}(K_\nu/k) = \mathrm{Gal}(K_\nu/K)$.

Therefore, we have proved:

THEOREM 2. *Let p be a prime number, let G be a finite p-group,* $\mid G \mid > 1$, *and let k be a finite field of characteristic p. Then, if $K = k(x)$, there exists an extension L of K such that $G \cong Gal(L/K)$ and* $\mathrm{Aut}(L/k) = \mathrm{Gal}(L/K)$. □

3. G is an l-group

Here we have $|\ G\ | = l^n$, l a prime number different from p, $(l, q-1) = 1$ and $n \geq 1$.

As in the p-case, let $G_n = G$. For $\nu = n, n-1, \ldots, 1$ we obtain a subgroup H_ν of the center of G_ν, of order l and set $G_{\nu-1} = G_\nu / H_\nu$.

We will construct fields $K_1 \subseteq \cdots \subseteq K_n = L$ so that $\mathrm{Gal}(K_\nu/K) \cong G_\nu$ and $\mathrm{Aut}(K_\nu/k) = \mathrm{Gal}(K_\nu/K)$.

The Case $\nu = 1$:

We choose d such that $l^n \mid q^d - 1$ ($q^d = 1 \bmod l^n$, can choose d to be the order of q mod l^n or multiples of it).

Let P be a prime of K of degree d. In the notation of Hayes [8, pages 81 and 82], setting $M = P$ we get an abelian extension $K(\Lambda_M)/K$ of degree $\Phi(M) = q^d - 1$. In this extension the primes different from P and from P_∞ are unramified and P ramifies fully. For P_∞ the ramification index is $q-1$, the degree of inertia is 1 and $\frac{q^d-1}{q-1}$ primes of $K(\Lambda_M)$ lie above it.

Let F be the field fixed by the decomposition group of P_∞. F/K is an abelian extension, P is the only prime of K that ramifies in F. $[F : K] = \frac{q^d-1}{q-1}$, so $l \mid [F : K]$. Therefore, we get an extension Λ of degree l over K such that $K \subseteq \Lambda \subseteq F$. P is the only prime of K that ramifies in Λ.

Let t_1 be a given natural number. Choose $d_1, \ldots, d_{t_1}$ integers and $P_1, \ldots, P_{t_1}$, different primes of K such that P_i is of degree d_i and $q^{d_i} \equiv 1 \bmod l^n$. Let $\Lambda_1, \ldots, \Lambda_{t_1}$ be extensions of degree l of K obtained as Λ was obtained, with P_i ramifying in Λ_i and unramified in Λ_j (for $i \neq j$). To construct a field where all $P_1, \ldots, P_{t_1}$ ramify we use the following technique of Madan [12, step 2]. Consider the composite of $\Lambda_1, \ldots, \Lambda_{t_1}$ (inside an algebraic closure of K). Its Galois group is the direct product of the Galois groups of $\Lambda_1, \ldots \Lambda_{t_1}$. Let σ_i be a fixed generator of the Galois group of Λ_i/K. Let H be the group generated by $\sigma_1\sigma_2^{-1}, \ldots, \sigma_1\sigma_{t_1}^{-1}$. Let K_1 be the field fixed by H. The fixed field of $< \sigma_1 >$ is the inertia field of P_1. Clearly, $H \cap < \sigma_1 > = \{1\}$ and $< \sigma_1, H > = \mathrm{Gal}(\Lambda_1 \ldots \Lambda_{t_1}/K)$. It follows that K_1 is not contained in the inertia field of P_1 and $[K_1 : K] = l$. One sees that $P_1, \ldots, P_{t_1}$ are all ramified in K_1.

To prove that $\mathrm{Aut}(K_1/k) = \mathrm{Gal}(K_1/K)$ we argue similarly to the way we did in the case G is a p-group. Here it is enough to require $t_1 \geq 2l + 1$.

Following Reichardt [15, page 1] we will say that a prime of K is "fleissig" in L/K if the primes of L that lie above it have residue class degree equal to 1. We observe that each P_i in the above construction is fleissig in K_1/K.

The Induction Step:

Assume $K_{\nu-1}$ constructed for $\nu \leq n$ with $\mathrm{Gal}(K_{\nu-1}/K) \cong G_{\nu-1}$, $\mathrm{Aut}(K_{\nu-1}/k) = \mathrm{Gal}(K_{\nu-1}/K)$, and such that all primes of K that ramify in $K_{\nu-1}$ are fleissig and that if d is any of their degrees, $q^d \equiv 1 \bmod l^n$. We show that $K_{\nu-1}$ is contained in a field K_ν with Galois group isomorphic to

G_ν, $\mathrm{Aut}(K_\nu/k) = \mathrm{Gal}(K_\nu/K)$ and such that all primes of K that ramify in K_ν are fleissig and that if d is any of their degrees, $q^d \equiv 1 \bmod l^n$.

First we prove this when H_ν is a direct factor of G_ν.

Let $Q_1, \ldots, Q_N$ be the primes of K that ramify in $K_{\nu-1}$. The primes of $K_{\nu-1}$ that lie above $Q_1, \ldots, Q_N$ have residue class degree equal to one.

Let t_ν be a positive integer. By Reichardt [14], we can choose $P_1, \ldots P_{t_\nu}$ primes that decompose fully in $K_{\nu-1}(\sqrt[l]{Q_1}, \ldots, \sqrt[l]{Q_N})$ and such that if P_j is of degree d_j, $q^{d_j} \equiv 1 \bmod l^n$. For $i = 1, \ldots, N$ we have that since P_1 decomposes fully in $K(\sqrt[l]{Q_i})$, say $P_1 = \mathcal{P}_1 \ldots \mathcal{P}_\ell$, $\frac{\vartheta_{K(\sqrt[l]{Q_i})}}{\mathcal{P}_1} \cong \frac{F_q[x]}{P_1} \cong F_{q^{d_1}}$. Let $\alpha = \sqrt[l]{Q_i}$. Then $\alpha \in \vartheta_{K(\sqrt[l]{Q_i})}$. We have $\alpha^l \equiv Q_i \bmod \mathcal{P}_1$ so there exists $\beta \in F_q[x]$ such that $\beta^l \equiv Q_i \bmod P_1$. Thus

$$1 = \beta^{q^{d_1}-1} \equiv Q_i^{\frac{q^{d_1}-1}{l}} \bmod P_1. \tag{3}$$

Following Hayes [8], we construct a cyclic extension $K(\Lambda_{P_1})$ of K, $[K(\Lambda_{P_1}) : K] = q^{d_1} - 1$. As in case $\nu = 1$, obtain Λ_1, the subextension of $K(\Lambda_{P_1})$ of degree l over K. P_1 is the only prime of K that ramifies in Λ_1. It follows from (3) and Carlitz [1, Theorem 12] that the residue class degree of the primes in $\vartheta_{K(\Lambda_{P_1})}$ lying over Q_i is $\leq \frac{q^{d_1}-1}{l}$, thus Q_i is not inert in $K(\Lambda_{P_1})$. Since the extension $K(\Lambda_{P_1})/K$ is cyclic and Λ_1 is the unique subextension of degree l, we must have Q_i decomposes in Λ_1.

As it was done above with P_1, we construct extensions $\Lambda_1, \ldots, \Lambda_{t_\nu}$ of degree l of K where $Q_1, \ldots Q_N$ decompose fully and such that P_i is the only prime of K that ramifies in Λ_i. As it was done in case $\nu = 1$, we construct a field Δ such that $[\Delta : K] = l$, $P_1, \ldots, P_{t_\nu}$ ramify in Δ. We have $Q_1, \ldots, Q_N$ decompose in Δ.

$$\begin{array}{ccc} K_{\nu-1} & \text{——} & K_\nu \\ | & & | \\ K & \text{——} & \Delta \end{array}$$

Let $K_\nu = K_{\nu-1}\Delta$. Then $G_\nu \cong G_{\nu-1} \times H_\nu \cong \mathrm{Gal}(K_\nu/K)$. We have $Q_1, \ldots, Q_N$ and $P_1, \ldots P_{t_\nu}$ are precisely the primes of K that ramify in K_ν. Since P_i decomposes fully in $K_{\nu-1}$ and ramifies from $K_{\nu-1}$ to K_ν, we have P_i is fleissig in K_ν/K. Since Q_j decomposes in Δ/K and ramifies and is fleissig in $K_{\nu-1}/K$, we have Q_j is fleissig in K_ν/K. If d is any of their degrees, $q^d \equiv 1 \bmod l^n$.

To prove that $\mathrm{Aut}(K_\nu/k) = \mathrm{Gal}(K_\nu/K)$, we proceed as in the case G is a p-group (using the Genus Formula and Castelnuovo's Inequality). Here we require $t_\nu > \frac{2l}{l-1}(l + g_{\nu-1} - 1)$, where $g_{\nu-1}$ is the genus of $K_{\nu-1}$.

Then, the case when H_ν is a direct factor is completely proven.

Now we consider the case when H_ν is not a direct factor of G_ν. We proceed as in Reichardt [15] adjoining to $K_{\nu-1}$ and to K a primitive l-th root of unity ζ and proving that the crossed product of the extension by its Galois group splits. To do this we use that $l^n \mid q^d - 1$ and that our ramifying primes are fleissig. Then we obtain an extension K_ν/K that satisfies $\mathrm{Gal}(K_\nu/K) \cong G_\nu$.

We now have to make modifications so K_ν satisfies the conditions of the induction step and there are enough primes ramifying in the last step. (A) There might be primes of K that did not ramify in $K_{\nu-1}$ but ramify in K_ν.

Suppose P is a prime of K that ramifies in K_ν but not in $K_{\nu-1}$. Let $\mathcal{P}$ be a prime of K_ν that lies above P.

We have $\frac{\vartheta_{K_\nu,\mathcal{P}}}{\mathcal{P}} \cong \frac{\vartheta_{K_\nu}}{\mathcal{P}}$. Since there is tame ramification in the last step, $\vartheta_{K_\nu,\mathcal{P}}$ contains the l-th roots of 1. But $\frac{\vartheta_{K_\nu}}{\mathcal{P}}$ consists of the (q^d-1)-th roots of 1, where d is the degree of P, if P is not the infinite prime and 1 otherwise. Then $q^d - 1$ is divisible by l.

Now we again use Hayes [8] to construct an extension Λ of degree l over K, where P is the only prime of K that ramifies. We have P ramifies in $K_{\nu-1}\Lambda/K_{\nu-1}$ and also in $K_\nu/K_{\nu-1}$. Since the ramification of P in $K_\nu\Lambda/K_{\nu-1}$ is tame, the inertia group of P is cyclic, so P is not fully ramified in $K_\nu\Lambda/K_{\nu-1}$. Let K'_ν be the field fixed by the inertia group of P. We have $\mathrm{Gal}(K'_\nu/K) \cong \mathrm{Gal}(K_\nu/K) \cong G_\nu$. P does not ramify in $K'\nu/K\nu - 1$. Thus P does not ramify in K'_ν/K. By abuse of notation we denote K'_ν by K_ν.

In this fashion, one by one, we get rid of all the "bad" primes. We call again our final extension K_ν.

(B) There might be primes of K that were ramified in $K_{\nu-1}$ (and were fleissig) but are inert in the extension $K_\nu/K_{\nu-1}$, thus loosing their property of being fleissig.

Say $Q_1, \ldots, Q_N$ are the primes of K that ramify in $K_{\nu-1}$. Say $Q_1, \ldots, Q_h$ remain fleissig up to K_ν, but $Q_{h+1}, \ldots, Q_N$ become inert in the last step.

We have that $K_\nu(\eta, \sqrt[l]{Q_1}, \cdots, \sqrt[l]{Q_h}, \sqrt[l]{Q_N})$ is a proper extension of $K_\nu(\eta, \sqrt[l]{Q_1}, \cdots, \sqrt[l]{Q_h})$, where η is a primitive l^n-th root of unity. If it were not the case, by Kummer Theory, we would have that there exists Q_* such that Q_* is a product of powers of $Q_1, \ldots, Q_h, Q_N, \sqrt[l]{Q_*} \in K_\nu(\eta)$ and Q_* is not an l-th power in K. Since each automorphism of $K_\nu(\eta)$ over K_ν that is not the identity in $K(\eta)$ lies in the center of $\mathrm{Gal}(K_\nu(\eta)/K)$, we have that each automorphism of $K(\zeta, \sqrt[l]{Q_*})$ over $K(\sqrt[l]{Q_*})$ that is not the identity in $K(\zeta)$ must lie in the center of $\mathrm{Gal}(K(\zeta, \sqrt[l]{Q_*})/K)$. But this is not possible because we are assuming $(l, q-1) = 1$.

Choose a prime P of K of degree d that decomposes fully in $K_\nu(\eta, \sqrt[l]{Q_1}, \cdots, \sqrt[l]{Q_h})$ but becomes inert in the step $K_\nu(\eta, \sqrt[l]{Q_1}, \cdots, \sqrt[l]{Q_h})$ to $K_\nu(\eta, \sqrt[l]{Q_1}, \cdots, \sqrt[l]{Q_h}, \sqrt[l]{Q_N})$. Then $l^n \mid q^d - 1$ [3, page 147]. Once again, by Hayes [8], we construct Λ of degree l over K where P ramifies and $Q_1, \ldots, Q_h$ decompose. The polynomial $X^l - Q_N$ is irreducible in $K_\nu(\eta, \sqrt[l]{Q_1}, \cdots, \sqrt[l]{Q_h})$. Since P is inert in the last step, $X^l - Q_N$ is irreducible mod P.

Let α be in an algebraic closure of F_q be such that $\alpha^l \equiv Q_N \bmod P$ and $\alpha \notin F_{q^d}$. Let $q^d - 1 = sl^t$, $(s,l) = 1$, $t \geq 1$. We have $Q_N^{sl^t} = Q_N^{q^d-1} \equiv 1 \pmod{P}$. Assume $Q_N^{\frac{q^d-1}{l}} \equiv 1 \pmod{P}$, then $\alpha^{q^d-1} \equiv 1 \pmod{P}$, so $\alpha \in F_{q^d}$, a contradiction. Thus $Q_N^{sl^{t-1}} \not\equiv 1 \pmod{P}$. Thus the inertia degree is divisible by l^t. Then Q_N is inert in Λ/K. Therefore, Q_N is inert in $K_{\nu-1}\Lambda/K_{\nu-1}$ and Q_N is inert in $K_\nu/K_{\nu-1}$. Since $K_\nu\Lambda/K_{\nu-1}$ is not cyclic, Q_N is not fully inert in $K_\nu\Lambda/K_{\nu-1}$. Thus, if K'_ν is the field fixed by the decomposition group of Q_N, Q_N decomposes in $K'_\nu\Lambda/K_{\nu-1}$. We have $\mathrm{Gal}(K'_\nu/K) \cong \mathrm{Gal}(K_\nu/K) \cong G_\nu$. Since $Q_1, \ldots, Q_h$ were fleissig in K_ν/K and decompose in Λ/K, they are fleissig in $K_\nu\Lambda/K$, thus they are fleissig in K'_ν/K. The prime P decomposes fully in K_ν/K and ramifies in Λ/K so it is fleissig in K'_ν/K. In this manner we handle $Q_{h+1}, \ldots, Q_N$ and again we call our final extension K_ν.

(C) Let t_ν be a natural number. Choose $P_1, \ldots, P_{t_\nu}$ primes of K that decompose fully in $K_\nu(\eta, \sqrt[l]{Q_1}, \ldots, \sqrt[l]{Q_N})$ and if d is the degree of any of them, $l^n \mid q^d - 1$. As in (B), we obtain extensions $\Lambda_1, \ldots, \Lambda_{t_\nu}$ of degree l over K where $Q_1, \ldots, Q_N$ decompose and such that P_i ramifies in Λ_i. By Madan's merging technique [12] we obtain an extension Λ of degree l over K where $Q_1, \ldots, Q_N$ decompose and $P_1, \ldots, P_{t_\nu}$ ramify. Take any of the fields K'_ν between $K_{\nu-1}$ and $K_\nu\Lambda$, different from $K_{\nu-1}\Lambda$ and K_ν. We have $\mathrm{Gal}(K'_\nu/K) \cong \mathrm{Gal}(K_\nu/K)$. $P_1, \ldots, P_{t_\nu}$ ramify in $K'_\nu/K_{\nu-1}$. So they are fleissig in K'_ν/K. Again we call our new field K'_ν, K_ν.

To prove that $\mathrm{Aut}(K_\nu/k) = \mathrm{Gal}(K_\nu/K)$ we proceed as we did for case when H_ν is a direct factor. This concludes the case when H_ν is not direct factor of G_ν. Therefore, we have proved:

THEOREM 3. *Let k be a finite field with $q = p^r$ elements, where p is a prime, and let G be a finite l-group. We assume $l \neq p$, $(l, q-1) = 1$ and $|\, G \,| > 1$. Then, if $K = k(x)$, there exists an extension L of K such that $G \cong Gal(L/K)$ and* $\mathrm{Aut}(L/k) = \mathrm{Gal}(L/K)$. □

4. G is a Nilpotent Group

We state without proof the following

LEMMA 1. *Let E/F be a field extension of degree l^n and L a subextension of E of degree l over F. Let t_L be the number of primes of F that ramify in L. Assume $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = E$, where F_i/F_{i-1} is of degree l and at least t_0 primes of F_{i-1} ramify in F_i. Then $t_L \geq \frac{t_0}{l^{n-1}}$.* □

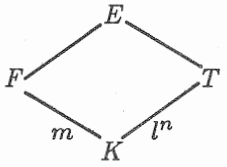
Next we prove:

LEMMA 2.

(a) *F is a Galois extension of K of genus g, degree m and let $G_F = \mathrm{Gal}(F/K) = \mathrm{Aut}(F/k)$,*

(b) *T is an extension of K of degree l^n and $G_T = \mathrm{Gal}(T/K)$,*

(c) $(m,l) = 1$. *T was constructed by l-steps, $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = T$, K_i/K_{i-1} is of degree l and at least t_0 primes of K_{i-1} ramify in K_i for $1 \leq i \leq n$, where $t_0 > 2l^{2n-1}(g + l^n - 1)$. These primes are unramified in F.*



Then $E = FT$ satisfies $\mathrm{Gal}(E/K) \cong G_F \times G_T$ *and* $\mathrm{Aut}(E/k) = \mathrm{Gal}(E/K)$.

Proof. We have $\mathrm{Gal}(E/K) \cong G_F \times G_T$ because $(m,l) = 1$.

Let $\sigma \in \mathrm{Aut}(E/k)$. Let us show $\sigma(F) \subseteq F$.

Assume $\sigma(F) \not\subseteq F$. Let $L = F\sigma(F)$. Then $F \subsetneq L$. Let $d = [L : F] = [L : \sigma(F)]$ and $g_L =$ genus of L. We have $g =$ genus of $\sigma(F)$.

By Lemma 1, there are at least $\frac{t_0}{l^{n-1}}$ primes of F that ramify in L. Using an argument that involves the Genus Formula and Castelnuovo's Inequality we obtain a contradiction.

Therefore, $\sigma(F) \subseteq F$. Analogously, $\sigma^{-1}(F) \subseteq F$. Thus $\sigma(F) = F$. Then $\sigma|_F \in \mathrm{Aut}(F/k)$, so $\sigma(x) = \sigma|_F(x) = x$. Hence $\sigma \in \mathrm{Gal}(E/K)$ as desired. □

Finally, we have

THEOREM 4. *Let G be a finite nilpotent group, $|\ G\ | > 1$ and let k be a finite field with q elements. We assume $(|\ G\ |, q-1) = 1$. Then, if $K = k(x)$, there exists an extension L of K such that $G \cong Gal(L/K)$ and* $\mathrm{Aut}(L/k) = \mathrm{Gal}(L/K)$.

Proof. We have G is the direct product of its Sylow subgroups:

$$G \cong G_{p^a} \times G_{l_1^{b_1}} \times \cdots \times G_{l_s^{b_s}}$$

where G_{p^a} is a p-group of order p^a with $a \geq 0$, $G_{l_i^{b_i}}$ is an l_i-group of order $l_i^{b_i}$ with $b_i > 0$, and $s \geq 0$.

We use Theorems 2 and 3 and Lemma 2 with $G_F = G_{p^a}$ and $G_T = G_{l_1^{b_1}}$. We observe from the proofs of Theorems 2 and 3 that we can take as many ramifying primes as necessary in order to satisfy condition (c) of Lemma 2. Next, we use Theorem 3 and Lemma 2 with $G_F = G_{p^a} \times G_{l_1^{b}}$ and $G_T = G_{l_2^{b_2}}$. We continue in this way until we finish with all Sylow subgroups of G. At the end, we obtain the required field extension. □

CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL IPN
MÉXICO, D.F. 07000 MÉXICO

REFERENCES

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

[2] C. CHEVALLEY, *Introduction to the theory of algebraic functions of one variable*. Amer. Math. Soc. Math. Surveys **6**, 1951.

[3] M. DEURING, *Lectures on the theory of algebraic functions of one variable*. Lecture Notes in Mathematics, Springer Verlag 414, 1973.
[4] J. D'MELLO AND M. MADAN, *Algebraic function fields with solvable automorphism group in characteristic p*. Comm. in Algebra **11**, (1983), 1187,1236.
[5] M. EICHLER, Introduction to the Theory of Algebraic Numbers and Functions. Academic Press, 1966.
[6] L. GREENBERG, *Maximal groups and signatures*. Ann. of Math. Studies **79** (1974), 207-226.
[7] H. HASSE, *Theorie der relativ-zyklischen algebraischen Functionen: Körper, insbesondere bei endlichen Konstantenkörper*. J. Reine angew. Math. **172** (1935), 37-54
[8] D. HAYES, *Explicit class field theory for rational function fields*. Trans. Amer .Math. Soc. **189** (1974), 77-91.
[9] K. IWASAWA, *On solvable extensions of algebraic number fields*. Ann. of Math. **58** (1953), 548,572.
[10] M. JARDEN, *The Čeboratev density theorem for function fields: An elementary approach*. Math. Ann.**261** (1982), 467,475.
[11] E. KANI, *On Castelnuovo's equivalence defect*. J. Reine angew. Math. **352** (1984), 24,70.
[12] M. MADAN, *On class numbers of algebraic number fields*. J. Number Theory **2** (1970), 116-119.
[13] D. MADDEN AND R. VALENTINI, *The group of automorphisms of algebraic function fields*. J. Reine angew. Math. **343**, (1983), 162-168.
[14] H. REICHARDT, *Der Primidivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper*. Math. Z. **40**,(1936), 713-719.
[15] ———, *Konstruktion von Zahlkörpern mit gegebener Galois-gruppe von Primzahlpotenzordnung*. J. Reine angew. Math. **177** (1937), 1-5.
[16] M. RZEDOWSKI-CALDERON, Galois Module Structure of Rings of Integers and Automorphism Groups of Congruence Fields. Dissertation. The Ohio State University, 1988
[17] I.R. ŠAFAREVIČ, *Construction of fields of algebraic numbers with given solvable Galois group*. Amer. Math. Soc. Transl. Series 2, **4** (1956), 185-237.
[18] A. SPEISER, *Zahlentheoretische Sätze aus der Gruppentheorie*. Math. Z. **5** (1919), 1-6.
[19] R. VALENTINI AND M. MADAN, *Automorphism groups of algebraic function fields*. Math. Z. **176** (1981), 39-52.