INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.

2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of "sectioning" the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again—beginning below the first row and continuing on until complete.

4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.
D'Mello, Joseph Gerard

CLASS GROUPS OF Z(L)-EXTENSIONS AND SOLVABLE AUTOMORPHISM GROUPS OF ALGEBRAIC FUNCTION FIELDS

The Ohio State University

Ph.D. 1983

University Microfilms International 300 N. Zeeb Road, Ann Arbor, MI 48106
CLASS GROUPS OF $\mathbb{Z}_p$-EXTENSIONS AND SOLVABLE AUTOMORPHISM
GROUPS OF ALGEBRAIC FUNCTION FIELDS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of The Ohio State University

By

Joseph Gerard D'Mello, B.Sc. (Hons.), M.Sc., M.A., M.S.

* * * * *

The Ohio State University

1982

Reading Committee: Approved By

Arno Cronheim

Koichiro Harada

James Leitzel

Manohar L. Madan

Manohar L. Madan

Adviser

Department of Mathematics
ACKNOWLEDGMENTS

Much gratitude is due my parents for all the love, understanding and encouragement I have received from them over the years. It is also a pleasure for me to take this opportunity to specially thank my adviser Professor Manohar Madan, not only for being very generous with his time but also for the important role he has played in my mathematical maturation, not to mention his friendly encouragement during all my years as a graduate student at Ohio State. To Professor Arnold Ross I owe a good measure of my interest in algebra and number theory; his stimulating Summer School which I was fortunate to have attended in 1973, helped me confirm my own suspicion that I had a predilection for algebra and number theory. I would like to thank Professor D.K. Ray-Chaudhuri for his helpfulness on several occasions and also for introducing me to combinatorics — a course he taught aroused in me a keen interest in matters combinatorial that has lingered in my mind ever since. Finally, I wish to express my appreciation to Professor A. Cronheim, Professor K. Harada and Professor James Leitzel for having made several suggestions that have improved the readability of this dissertation.
VITA

July 4, 1954. . . . . Born - Bagalkote, India
1974. . . . . . . . B.Sc. (Honors), Bangalore University, India
1976. . . . . . . . M.Sc., Bangalore University, India
1976-1977 . . . . Graduate Trainee, Department of Mathematics, State University of New York at Stony Brook
1977. . . . . . . . M.A., State University of New York at Stony Brook
1977-1978 . . . . University Fellow, Department of Mathematics, The Ohio State University
1978. . . . . . . . M.S., The Ohio State University
1978-1980 . . . . Teaching Associate, Department of Mathematics, The Ohio State University
1980-1981 . . . . Presidential Fellow, Department of Mathematics, The Ohio State University
1981-1982 . . . . Teaching Associate, Department of Mathematics, The Ohio State University

FIELDS OF STUDY

Major Field: Mathematics - Algebra, Analysis, Topology, Combinatorics, etc.

Minor Field: Computer Science - Programming Languages, Mathematical Foundations, Computer Organization, Data Structures, etc.
# TABLE OF CONTENTS

ACKNOWLEDGMENTS ............................................................... Page 11

VITA ...................................................................................................... iii

INTRODUCTION .................................................................................. 1

Chapter

I. CLASS GROUP RANK RELATIONS IN
ZZ/7-EXTENSIONS ................................................................. 5

§1. Number Fields ........................................................................... 5
§2. The Function Field Case ......................................................... 11
§3. Congruence Function Fields ................................................... 17

II. ALGEBRAIC FUNCTION FIELDS WITH SOLVABLE
AUTOMORPHISM GROUP IN CHARACTERISTIC p .................. 35

§1. Notation and some preliminary results ............................... 35
§2. Automorphism groups of prime order ............................... 47
§3. Imbedding problems and cohomology ................................. 51
§4. The main result ..................................................................... 65

BIBLIOGRAPHY .............................................................................. 85
INTRODUCTION

Let $F/K$ be a field of algebraic functions of one variable having an algebraically closed field $K$ as its field of constants. For a prime $\ell$, not necessarily different from the characteristic $p$ of $F$, let $E/K$ be a cyclic extension of degree $\ell$ of $F/K$. Deuring [4] proved that if $E/F$ is ramified,\[(1) \quad \lambda_E = \ell \lambda_F + (t - 8 - 1)(\ell - 1),\]
where $t$ is the number of ramified primes, $s = 0$ or 1 according as $\ell = p$ or not and $\lambda_E, \lambda_F$ denote the $\ell$-ranks of the group of divisor classes of degree zero of $E$ and $F$ respectively. For the unramified case, Šafarevič [19] proved this relation in the case $\ell = p$, where $\lambda_E, \lambda_F$ are the ranks of the Hasse-Witt matrices. Madan [13] gave a unified proof of (1), including the case $s = 1$, $t = 0$ which was covered neither by Deuring, Šafarevič nor any other author (see [13] for detailed references). Two facts are critical in this proof: "Tsen's theorem" and the divisibility of the null class group. The above proof is very much simplified if, in addition, one assumes a purely algebraic elementary theorem of Tate (see [24], page 97). In Chapter I, this idea is used to generalize the above theorem of Deuring and Šafarevič to $\mathbb{Z}_\ell$-extensions, i.e. when $K$ is an infinite $\ell$-extension of a finite field. For the ramified case, this generalization was done by Moriya [17] using Deuring's method and
class field theory. The method of this chapter also yields a proof of a recent result of Kida [11]. For an odd prime \( \ell \), let \( F \) be a \( \mathbb{Z}_\ell \)-extension of CM type and let \( E/F \) be a cyclic extension of degree \( \ell \). Using the standard notation for the Iwasawa invariants, it is known that \( \mu_F = 0 \) implies that \( \mu_E = 0 \). In this case, Kida [11] proved the following relation:

\[
\lambda_E^* = \ell \lambda_F^* + (\frac{\ell}{2} - 8)(\ell - 1),
\]

where \( t \) is the number of non-\( \ell \)-primes of \( E \) which are ramified over \( F \) and split over \( E^+ \); \( s = 1 \) or \( 0 \) according as \( F \) does or does not contain the \( \ell \)-th roots of unity. Iwasawa [10] and Sinnott [21] gave alternate proofs of Kida's theorem. The proof given here is simpler. As pointed out in [10] and [13], the above results are easily extended to the more general case of \( \ell \)-extensions of \( F \).

This proof is carried out in §1 of Chapter I. In §2 of this chapter, the function field case is discussed, but only briefly, because the proof is similar. In §3, \( K \) is an infinite \( \ell \)-extension of a finite field \( K_0 \); \( F/K_0 \) and \( E/K_0 \) are congruence function fields such that \( E/F \) is a cyclic extension of prime degree \( \ell \). Let \( E_\infty = EK \) and \( F_\infty = FK \). Then, assuming that \( \lambda_F = \lambda_{F_\infty} \), we give explicit bounds for the degree \( \ell^m \) of a constant extension \( E_m \) of \( E \) such that \( \lambda_{E_m} = \lambda_{E_\infty} \), in the ramified as well as in the unramified case.

In Chapter II, let \( K \) be an algebraically closed field and let \( F \) be a field of algebraic functions of one variable over \( K \). For
the case when $K$ is the field of complex numbers, it is a classical result of Poincaré and Klein that the group of $K$-automorphisms of $F$ is finite, provided that the genus of $F$ is at least two.

L. Greenberg [6] has shown that in this case any finite group $G$ is the full group of automorphisms of a suitable algebraic function field. The theorem of Poincaré and Klein was proved for fields of characteristic $p$ by H.L. Schmid [20]. Which finite groups occur as full groups of automorphisms for a given $K$? This is an open problem. In [23], Valentini and Madan showed the existence of infinitely many algebraic function fields which have a given finite abelian group as the full group of automorphisms for a given $K$. In this chapter, the main object is to extend this last result to the class of solvable groups. In §1 of Chapter II we introduce the notation and prove some preliminary results. In §2 we give a proof, which is simpler than that given in [23], for groups $G$ of prime order. §3 is closely related to a paper of Iwasawa [9] in which it is shown that every imbedding problem with solvable kernel has a solution (in the context of algebraic function fields with algebraically closed constant field). We show the existence of solutions with suitable arithmetical properties. The main result of the chapter is proved in §4. An inequality involving the genus of a function field and the genera and codegrees of two subfields of which it is a composite, plays a crucial role in the proof. This inequality, which in the classical case is due to Castelnuovo [2], is a consequence of the famous Castelnuovo-Severi inequality (see [5]). However, this inequality is not required to
establish the result for a supersolvable group $G$ (see Remark 3 at the end of Chapter II). The method of this chapter actually shows that the algebraic function fields $F/K$ with $\text{Aut}(F/K)$ isomorphic to a pre-assigned finite solvable group $G$, can in fact be so constructed that the fixed field of $\text{Aut}(F/K)$ is a rational subfield of $F$, i.e. a field of the form $K(x)$ with $x$ a (transcendental) element of $F$.

Chapters I and II can be read independently of each other. The symbol □ will be used to mark the end of a proof.
Suppose \( \ell \) is an odd prime. Let \( \mathbb{Q}_\infty \) be the unique \( \mathbb{Z}_\ell \)-extension of the rational number field \( \mathbb{Q} \) which is contained in the field of complex numbers. We then have

**Lemma 1.** If \( K \) is any \( \mathbb{Z}_\ell \)-field and \( p \) is a rational prime, then there are only finitely many places of \( K \) that lie above the place of \( \mathbb{Q} \) determined by \( p \).

**Proof:** Since \( K = k\mathbb{Q}_\infty \) for some finite extension \( k \) of \( \mathbb{Q} \), it suffices to prove the result for \( K = \mathbb{Q}_\infty \). Moreover, since \( \mathbb{Q}_\infty \) is contained in the field obtained from \( \mathbb{Q} \) by adjunction of all \( \ell^n \)-th roots of unity \( (n = 1, 2, 3, \ldots) \), which we shall denote by \( \mathbb{Q}_\infty \), it is enough to show that there are only finitely many places of \( \mathbb{Q}_\infty \) that lie above the place of \( \mathbb{Q} \) determined by \( p \).

Note that \( \mathbb{Q}_\infty = \bigcup_{n=1}^{\infty} \mathbb{Q}_n \), where \( \mathbb{Q}_n \) is obtained from \( \mathbb{Q} \) by adjunction of the \( \ell^n \)-th roots of unity. If \( p = \ell \), then \( p \) is fully ramified in \( \mathbb{Q}_n \); if \( p \neq \ell \), the theory of decomposition in cyclotomic extensions of \( \mathbb{Q} \) immediately shows that there is an \( s \geq 1 \) such that, in \( \mathbb{Q}_{s+1} \), \( p \) splits into as many primes as it does in \( \mathbb{Q}_s \), for all \( i \geq 0 \). This fact clearly completes the proof. \( \Box \)
Corollary. For any non-archimedean place $P$ of $K$, there is a subfield $K_1$ of $K$, $[K_1 : Q] < \infty$, such that $P$ is the unique extension of $P|K_1$ on $K$, $P|K_1$ being the restriction of $P$ on the subfield $K_1$. □

For a $\mathbb{Z}_l$-field $F = F_\infty$ we know that there is a finite extension $F_\infty$ of $Q$ such that $F_\infty Q = F_\infty$; and, for every positive integer $n$, there is a unique field $F_n$ between $F_\infty$ and $F_\infty$ such that $[F_n : F_\infty] = l^n$. Also $F_\infty = \bigcup_{n=0}^{\infty} F_n$, $F_{n+1} \supset F_n \forall n \geq 0$.

Let $E$ be a cyclic extension of $F$ of degree $l$. We can assume that there exists $E_\infty$ such that $[E_\infty : F_\infty] = l$, $E = E_\infty Q$; we also have similar subfields $E_n$ of $E$ such that $E_n \supset F_n \forall n \geq 0$.

Lemma 2. Let $E$ and $F$ be $\mathbb{Z}_l$-fields, $E$ cyclic over $F$ of degree $l$. Then there are no inert primes in $E/F$.

Proof: Let $P$ be a prime of $F$ that is unramified in $E$.

For this prime choose a subfield $F_n$ of $F$ corresponding to $K_1$ in the corollary to lemma 1. Let $P_n$ be the restriction of $P$ to $F_n$; $P_{n+1}$ the restriction of $P$ to $F_{n+1}$. Then, by a property of the Artin symbol (see [8], page 62), we have, since $P_{n+1}$ is inert over $F_n$,

$$
\left[\frac{F_{n+1}/F_{n+1}}{P_{n+1}}\right] = \left[\frac{E_n/F_n}{P_n}\right]^l = 1.
$$
Thus \( P_{n+1} \) must split completely in \( E_{n+1} \). Clearly, then, \( P \) must necessarily split completely in \( E \). □

**Lemma 3.** With \( E \) and \( F \) as in lemma 2, every \( \alpha \in F \) is a norm from \( E \).

**Proof:** Using the same notation as in lemma 2, given any \( \alpha \in F \), there is a positive integer \( n \) such that \( \alpha \in F_n \). By choosing \( n \) sufficiently large we can assume that

\[
(\alpha) = \prod_{i=1}^{r} P_{i,n}^{a_i} \prod_{i=1}^{r} P_{r,n}^{a_r}
\]

where the \( P_{i,n} \) (\( 1 \leq i \leq r \)) are primes of \( F_n \) and the ramified primes in \( E_n/F_n \) are inert in \( F_{\infty} \) as are also the \( P_{i,n} \) (\( 1 \leq i \leq r \)).

We recall that the norm residue symbol \( \left[ \frac{\alpha, E_n/F_n}{F_n} \right] \) can be non-trivial only if \( P_n \) is ramified or if \( P_n \) equals some \( P_{i,n} \).

Assuming, however, that \( P_n \) belongs to this finite set and that \( P_{n+1} \) is the prime of \( F_{n+1} \) lying above \( P_n \), we have, for the norm residue symbols,

\[
\left[ \frac{\alpha, E_{n+1}/F_{n+1}}{P_{n+1}} \right] = \left[ \frac{N_{F_{n+1}/F_n}(\alpha), E_n/F_n}{P_n} \right] = \left[ \frac{\alpha^\ell, E_n/F_n}{P_n} \right] = 1 .
\]

By Hasse's Norm Theorem, \( \alpha \) is thus a norm form \( E_{n+1} \), hence a norm from \( E \). □
Now suppose that \( E, F \) are fields of CM type. Let \( J \) denote complex conjugation and assume that \( E \) is a \( \mathbb{Z}_k \)-field, \( E \) cyclic of degree \( l \) over the \( \mathbb{Z}_k \)-field \( F \). The class group \( C_E \) of \( E \) can be written as

\[
C_E = C_E^+ \oplus C_E^- ,
\]

where

\[
C_E^\pm = \{ a \in C_E \mid J(a) = a^\pm 1 \} .
\]

We can then prove

**Lemma 4.** Let \( G \) be the Galois group of \( E \) over \( F \). Then the cohomology groups \( H^*(G, C_E^-) \) are all finite.

**Proof:** Let \( \mu_{C_E} \) denote the elements of \( C_E \) whose \( l \)-th power is trivial. The exact sequence

\[
1 \rightarrow \mu_{C_E} \rightarrow C_E \rightarrow C_E \rightarrow 1
\]

(where \( \mu \) denotes raising to the \( l \)-th power) obviously also yields the exact sequence

\[
1 \rightarrow \mu_{C_E^-} \rightarrow C_E^- \rightarrow C_E^- \rightarrow 1.
\]

In cohomology, the latter sequence yields

\[
\ldots \rightarrow H^i(G, \mu_{C_E^-}) \rightarrow H^i(G, C_E^-) \xrightarrow{\mu^*} H^i(G, C_E^-) \rightarrow \ldots .
\]

which is exact at each point. Since every element of \( H^i(G, C_E^-) \) has order dividing \( l \) and since \( H^i(G, \mu_{C_E^-}) \) is finite, it follows that \( H^i(G, C_E^-) \) is finite. \( \square \)
Let E and F be as in lemma 4. $I_E$ and $P_E$ denote, respectively, the ideals and principal ideals of E; $U_E$ and $W_E$, respectively, the units and roots of unity in E. The modules $P_E^\perp$, $I_E^\perp$ and $U_E^\perp$ are defined in exactly the same way as was $C_E^\perp$ earlier.

We then have the following exact sequences:

$$1 \rightarrow P_E^\perp \rightarrow I_E^\perp \rightarrow C_E^\perp \rightarrow 1,$$

$$1 \rightarrow U_E^\perp \rightarrow E^\perp \rightarrow P_E^\perp \rightarrow 1.$$

When dealing with a G-module, we shall write $h_0(G, \ )$ and $h_1(G, \ )$ for the orders of the cohomology groups $H^0(G, \ )$ and $H^1(G, \ )$ respectively.

Consider the second exact sequence. From lemma 3 and Hilbert's "Theorem 90" it follows that the Herbrand quotient

$$h(G, E^\perp) = \frac{h_0(G, E^\perp)}{h_1(G, E^\perp)} = \frac{h_0(E^\perp)}{h_1(E^\perp)} = 1,$$

and so, by a well known property of the Herbrand quotient, $h(P_E^\perp)h(U_E^\perp) = 1$. Now, it is a known fact that if the absolute value of all the conjugates of an algebraic integer is one, then it is a root of unity. Using this elementary result it follows that by definition $U_E^\perp = W_E$. Thus $h(P_E^\perp) = \frac{1}{h(W_E)}$. Again, it follows from the definition that $h_0(W_E) = 1$ and $h_1(W_E) = \ell^6$ (recall that $\delta = 1$ or 0 according as F does or does not contain the $\ell^{th}$ roots of unity). Thus $h(W_E) = \frac{1}{\ell^6}$ and, consequently, $h(P_E^\perp) = \ell^5$. 
The group $I_E^-$ is generated freely by the elements $\frac{v}{J(v)}$, where $v$ is ramified in $E/F$ and split in $E/E^+$. Thus, if $t$ is the number of non-$\ell$-primes of $E$ which are ramified over $F$ and split over $E^+$, it follows that

$$h_o(I_E^-) = \ell^t/2$$

and

$$h_l(I_E^-) = 1.$$ 

Hence $h(I_E^-) = \ell^t/2$ and the exactness of the first sequence above gives

$$(1.1) \quad h(C_E^-) = \ell(t/2) - 5.$$ 

We can now prove

**Theorem 1.** Let $\ell$ be an odd prime; $E,F$ $\mathbb{Z}_\ell$-fields of CM type with $E$ cyclic of degree $\ell$ over $F$. $t$ is the number of non-$\ell$-primes of $E$ which are ramified over $F$ and split over $E^+$. Then

$$\lambda_E^- = \ell \lambda_F^- + \left(\frac{t}{E} - 5\right)(\ell - 1).$$

**Proof:** By Tate's theorem (see [24], page 97), we have

$$\left(h(C_E^-)\right)^{\ell-1} = \left(\frac{(C_E^-: (C_E^-)^{\ell})}{(c_E^{c^-G} : (C_E^-)^{c^-G})}\right)^{\ell} \frac{(C_E^- : 1)}{(C_E^- : (C_E^-)^{\ell})}.$$
where, for a $G$-module $A$, $A^G$ denotes the $G$-invariant elements of $A$ and $\mathcal{A}$ the set of all elements of $A$ whose $\ell$th power is trivial. Using (1.1) and the fact that $c_E^-$ is $\ell$-divisible, we can rewrite the above equality as

$$\lambda_E^-=\ell\left(\frac{t}{2}-5\right)(\ell-1)\left[\frac{(\ell c_E^G:1)}{(c_E^G:(c_E^G)^{\ell})}\right]^\ell.$$  

The image of $c_F^-$ in $c_E^G$ under the conorm map is of finite index and the kernel of this map is finite too. Since the Herbrand quotient of a finite module is trivial, it follows that

$$\frac{(\ell c_E^G:1)}{(c_E^G:(c_E^G)^{\ell})} = \frac{(\ell c_F^G:1)}{(c_F^G:(c_F^G)^{\ell})} = \lambda_F^-,$$

since $c_F^-$ is also $\ell$-divisible. Hence, on equating the exponents of $\ell$, we obtain

$$\lambda_E^- = \left(\frac{t}{2}-5\right)(\ell-1) + \ell \lambda_F^-,$$

and this proves the theorem. □

### §2. The Function Field Case.

Let $K$ be an infinite $\ell$-extension of a finite field and let $F/K$ be a field of algebraic functions of one variable having $K$ as its field of constants. Let $E/K$ be a cyclic extension of $F/K$ of
prime degree \( \ell \). The corollary to lemma 1 carries over to this situation and so, by similar arguments, it follows that lemma 2 and lemma 3 are valid here too. We introduce the following notation:

\[
D_{E}(D_{oE}) -- \text{the group of divisors (of degree 0) of } E.
\]

\[
C_{E}(C_{oE}) -- \text{the group of divisor classes (of degree 0) of } E.
\]

\[
P_{E} -- \text{the group of principal divisors of } E.
\]

\[
C_{oE}^{(\ell)} -- \text{the } \ell \text{-part of } C_{oE}.
\]

\[
\ell^{C_{oE}} -- \text{the elements of } C_{oE} \text{ whose order divides } \ell.
\]

(Note: All modules mentioned below are, unless otherwise stated, to be looked upon as \( G \)-modules, \( G = \text{Gal}(E/F) \)).

We shall need an analogue of lemma 4, namely that the cohomology groups \( H^{1}(G, C_{oE}) \) are all finite. The proof is exactly the same as that of lemma 4 provided we can show that \( C_{oE} \) is \( \ell \)-divisible. This will be a consequence of the following lemma which is due to Moriya [17]. Since there is a minor gap in Moriya's proof, we present the lemma and its proof here.

**Lemma 5.** Let \( F_{1}, \overline{F}_{1} \) be subfields of \( F \) with finite constant fields such that \( \overline{F}_{1} \) is the constant extension of degree \( \ell \) over \( F_{1} \). Assume that \( C_{oF_{1}}^{(\ell)} \) and \( C_{\overline{F}_{1}}^{(\ell)} \) have the same number of direct factors, say \( s \), and that \( C_{oF_{1}}^{(\ell)} \) is of type \( (l_{1}^{a_{1}}, l_{2}^{a_{2}}, \ldots, l_{s}^{a_{s}}) \) with \( a_{i} \geq 2 \), \( 1 \leq i \leq s \). Then the group \( C_{\overline{F}_{1}}^{(\ell)} \) is of type
Proof: The divisor classes of $\mathbb{F}_1$ are injected into those of $\overline{\mathbb{F}}_1$. Let $C_1, C_2, \ldots, C_s$ be a basis for $C_{\mathbb{F}_1}$. These are then injected into classes $\overline{C}_1, \overline{C}_2, \ldots, \overline{C}_s$ of $\overline{\mathbb{F}}_1$. Assuming that $C_i$ has order $\ell^{a_i}$ ($1 \leq i \leq s$), then $\overline{C}_i$ also has order $\ell^{a_i}$. Let $\overline{C}_i^* = \overline{C}_i \ell^{-1}$, ($1 \leq i \leq s$). Then $N_{\mathbb{F}_1/\overline{\mathbb{F}}_1}(\overline{C}_i^*) = C_i^{\ell a_i} = 1$. It follows that there are divisor classes $\overline{A}_i$ (1 ≤ i ≤ s) of $\overline{\mathbb{F}}_1$ such that $\overline{C}_i^* = \overline{A}_i^{\ell^{-1}} \sigma$, where $\sigma$ is a generator of $\text{Gal}(\overline{\mathbb{F}}_1/\mathbb{F}_1)$. An easy argument (see Moriya [17]) shows that the $\overline{A}_i$ can be chosen to be of degree 0 and with the further properties that $\overline{A}_i \in H$, the subgroup of $C_{\overline{\mathbb{F}}_1}$ generated by $\overline{C}_1, \overline{C}_2, \ldots, \overline{C}_s$, and the $\overline{A}_i$ are $\ell$-independent modulo $H$, 1 ≤ i ≤ s.

Now consider the norm map $N: C_{\mathbb{F}_1}^{(\ell)} \to C_{\overline{\mathbb{F}}_1}^{(\ell)}$. Because $a_i \geq 2$ (1 ≤ i ≤ s), the number of elements of order $\ell^2$ in $C_{\mathbb{F}_1}^{(\ell)}$ is the same as the number of elements of order $\ell^2$ in $C_{\overline{\mathbb{F}}_1}^{(\ell)}$. It follows that no element of order $\ell^2$ (and hence no element of order exceeding $\ell^2$) is in the kernel of $N$. Thus the kernel consists precisely of the elements of order $\ell$. Hence $|C_{\mathbb{F}_1}^{(\ell)}| = \ell^s |C_{\overline{\mathbb{F}}_1}^{(\ell)}|$ (the norm map $N$ is surjective). Consequently, the elements
\( \bar{A}_1, \bar{A}_2, \ldots, \bar{A}_s, \bar{C}_1, \bar{C}_2, \ldots, \bar{C}_s \) generate all of \( C_{OF_1}^{(l)} \) and from this the result follows. \( \square \)

**Corollary.** \( C_{OF} \) (and similarly \( C_{OE} \)) is \( l \)-divisible.

**Proof:** Let \( c \in C_{OF} \). Then, in the sense of the corollary to lemma 1, \( c \) may be regarded as belonging to \( C_{OF_1} \) where \( F_1 \subseteq F \) has a finite constant field. Hence \( c \) has finite order \( n = n_0 l^e, \) \( (n_0, l) = 1 \). By making sufficiently many constant extensions of \( F_1 \) if necessary, we can assume that \( |lC_{OF_1}| = |lC_{OF}| \) (see Moriya [17]) and hence that \( F_1 \) meets the conditions of lemma 5. \( c \) can be written as a product of two divisor classes \( c_1 \) and \( c_2 \) whose orders are \( l^e \) and \( n_0 \) respectively. Lemma 5 shows that \( c_1 = b^l \) (since \( c_1 \) becomes an \( l \)-th power in \( F_1 \)). Choosing \( x \) such that \( lx = 1 \pmod{n_0} \), we see that \( c_2^lx = c_2 \) and so \( c = c_1 \cdot c_2 = b^l c_2^lx = (bc_2^x)^l \), which shows that \( c \) is an \( l \)-th power in \( C_{OF} \). \( \square \)

We remark that

(2.1) \( H^0(K) = 1 \), because \( K \) is an infinite \( l \)-extension of a finite field.

(2.2) \( H^1(E) = 1 \), by Hilbert's "Theorem 90".

(2.3) \( H^0(E) = 1 \), because every element of \( F \) is a norm from \( E \) (lemma 3).

(2.4) \( H^1(D_E) = 1 \), because \( D_E \) is generated as a free group by the prime divisors that are just permuted by \( G \).
(2.5) \( H'(\mathbb{Z}) = 1 \).

(2.6) \( H^0(D_E) = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \times \ldots \times \mathbb{Z}/\ell\mathbb{Z} \), \( t \) times, if \( t \) is the number of primes of \( F \) ramified in \( E \).

This follows from the definition and lemma 2.

The following are clearly exact sequences of \( G \)-modules:

(2.7) \hfill 1 \to K \to E \to P_E \to 1 \hfill \\
(2.8) \hfill 1 \to P_E \to D_E \to C_E \to 1 \hfill \\
(2.9) \hfill 1 \to C_{OE} \to C_E \xrightarrow{\text{DEGREE}} \mathbb{Z} \to 0 \hfill \\
(2.10) \hfill 1 \to \ell C_{OE} \to C_{OE} \xrightarrow{\ell} C_{OE} \to 1 \hfill \\

(the map \( \ell \) denotes raising to the \( \ell \)-th power).

Using (2.1), (2.2), (2.3), (2.4) and (2.5), the sequences (2.7), (2.8) and (2.9) yield in cohomology:

(2.7') \hfill 1 \to H^0(P_E) \to H'(K) \to H'(E) \to H'(P_E) \to 1 \hfill \\
(2.8') \hfill 1 \to H'(C_E) \to H^0(P_E) \xrightarrow{\alpha} H^0(D_E) \to H^0(C_E) \to 1 \hfill \\
(2.9') \hfill 0 \to H^0(C_{OE}) \to H^0(C_E) \xrightarrow{\beta} H^0(Z) \to H'(C_{OE}) \to H'(C_E) \to 0 \hfill \\

First suppose that \( E/F \) is unramified. Then \( H^0(D_E) = 1 \) and (2.7') and (2.8') force

(2.11) \hfill H^0(D_E) = H^0(C_E) = H^0(C_{OE}) = 1 \hfill \\
(2.12) \hfill H'(C_E) \cong H^0(P_E) \hfill \\

Also, (2.7') yields \( H^0(P_E) \cong H'(K) \). Thus

(2.13) \hfill H'(C_E) \cong H^0(P_E) \cong H'(K) \hfill .
Moreover, since $H^0(\mathbb{Z}) = \mathbb{Z}/\ell\mathbb{Z}$, (2.9') yields

$$h_1(C_{OE}) = \ell h_1(C_E) = \ell h_1(K)$$

$$= \ell \cdot \ell^\delta = \ell^{\delta+1}.$$ 

($\delta = 1$ or 0 according as $K$ does or does not contain the $\ell$-th roots of unity.) Since $h_0(C_{OE}) = 1$ (by (2.11)) it follows that

(2.14)

$$h(C_{OE}) = \ell^{1-\delta}.$$ 

Next, assume that $E/F$ is ramified and that $t > 0$ primes of $F$ are ramified in $E$. The map $\beta$ in (2.9') is onto because $F$, being an infinite $\ell$-extension of $F_0$, contains no primes of degree divisible by $\ell$ and hence $C_E$ contains an invariant class of degree one. Because every element of $F$ is a norm from $E$ and since the conorm map from $C_{OF}$ to $C_{OE}$ is injective, it follows that $\alpha$ in (2.8') is injective and $H'(C_E) = 1$. Thus (2.9') yields $H'(C_{OE}) = 1$.

Then (2.6) together with (2.8') and (2.9') imply that

$$h_0(C_E) = \frac{f^t}{h_0(P_E)}$$

and

$$h_0(C_{OE}) = \frac{f^{t-1}}{h_0(P_E)}$$

$$= \frac{\ell^{t-1}}{h_1(K)} \quad \text{(by the exactness of (2.7'))}$$

$$= \ell^{t-1-\delta}.$$ 

So $h(C_{OE}) = \ell^{t-1-\delta}$ and, together with (2.14), we have that for $E/F$ ramified or unramified,
We are now in a position to prove

**Theorem 2.** Let $\lambda_E$ and $\lambda_F$ denote the $l$-ranks of $C_{OE}$ and $C_{OF}$ respectively, $E/K$ being a Galois extension of $F/K$ of prime degree $l$, where $K$ is an infinite $l$-extension of a finite field. Then if $t > 0$ is the number of primes of $F$ that ramify in $E$,

$$\lambda_E = \lambda_F + (t - 8 - 1)(l - 1),$$

where $8 = 1$ or $0$ according as $K$ does or does not contain the $l$-th roots of unity.

**Proof:** If one uses (2.15), the proof is exactly the same as that of theorem 1, with $C_{gE}$ replaced by $C_{OE}$. □

§3. Congruence Function Fields.

Let $K$ be an infinite $l$-extension of a finite field $K_o$ and suppose that $F/K_o$, $E/K_o$ are congruence function fields such that $E/F$ is a Galois extension of prime degree $l$. Let $E_m = EK$ and $F_m = FK$. Assume that $\lambda_F = \lambda_{F_m}$. We shall obtain explicit bounds for the degree $l^m$ of a constant extension $E_m \subseteq E_m$ of $E$ such that $\lambda_{E_m} = \lambda_{E_m}$, in the ramified as well as in the unramified case.

The following two identities are easy to establish using the fact that $l(l - \eta)^{1-l}$ is a unit in $\mathbb{Z}[\eta]$, $\eta \neq 1$ denoting an
\( l \)-th root of unity.

(3.1) \( \ell = (1 - \sigma)^{l-1} f(\sigma) + (1 + \sigma + \ldots + \sigma^{l-1})g(\sigma) \)

(3.2) \( (1 - \sigma)^{l-1} = Ah(\sigma) + (1 + \sigma + \ldots + \sigma^{l-1}) \)

where \( \sigma \) is an indeterminate and \( f, g, h \) are polynomials with rational integral coefficients.

Now suppose that \( \text{Gal}(E/F) \) is generated by the automorphism \( \sigma \).

The spaces \( X_1, X_2, \ldots, X_{l-1} \) are defined as follows:

(3.3) \( X_i = \{ c \mid c \in \mathbb{C}_E, c(1-\sigma)^i = 1, c \in \ker(N) \} \)

where \( N : \mathbb{C}_E \to \mathbb{C}_E \) is the norm map, \( 1 \leq i \leq l - 1 \).

One verifies easily that

\[ X_1^{(1-\sigma)^{l-2}} \subseteq X_1^{(1-\sigma)^{l-3}} \subseteq \ldots \subseteq X_1^{1-\sigma} \subseteq X_1. \]

However, we claim that, in fact,

(3.4) \( N(X_{l\mathbb{C}_E}) \subseteq X_1^{(1-\sigma)^{l-2}} \subseteq X_1^{(1-\sigma)^{l-3}} \subseteq \ldots \subseteq X_1^{1-\sigma} \subseteq X_1. \)

To prove (3.4) we need only show that \( N(X_{l\mathbb{C}_E}) \subseteq X_1^{1-\sigma} \). So assume that \( c \in N(X_{l\mathbb{C}_E}) \). Then \( c = d^{1+\sigma+\ldots+\sigma^{l-1}}, d \in \mathbb{C}_{OE} \).

Using (3.2),

\[ c = d^{(1-\sigma)^{l-1}} - Ah(\sigma) \]

\[ = d^{(1-\sigma)^{l-1}} \quad \text{(since} \ d^l = 1 \text{)} \]
= (d^{1-\sigma})(1-\sigma)^{\ell-2}.

So we need only show that \( d^{1-\sigma} \in X_{\ell-1} \). But

\[
(d^{1-\sigma})(1-\sigma)^{\ell-1} = (d^{1-\sigma})\zeta_{\ell}(\sigma) + (1+\sigma+\ldots+\sigma^{\ell-1}) \quad \text{(by (3.2))}
\]

\[
= (d^{1-\sigma})(1+\sigma+\ldots+\sigma^{\ell-1})
\]

\[
= d^{1-\sigma} = 1,
\]

since \( \sigma^{\ell} \) is trivial.

This completes the proof of (3.4).

We now divide our discussion into two cases.

\section*{E/F unramified}

\textbf{Theorem 3}. If the extension \( E/F \) is unramified and \( \lambda_F = \lambda_{F_{\infty}} \), then,

if \( m = (\ell - 1)(\lambda_F - 5 - 1) + 2 \),

\[
\lambda_{E_m} = \lambda_{E_{\infty}} = \ell \lambda_{F_m} - (5 + 1)(\ell - 1),
\]

where \( 5 = 1 \) or \( 0 \) according as \( K \) does or does not contain the \( \ell \)-th roots of unity.

\textbf{Proof}: From the proof of lemma 5 it follows that if we make a constant extension of \( F \) of degree \( \ell^2 \) if necessary, we may assume that each of the cyclic direct factors of \( \zeta_{\ell} \) has order at least \( \ell^3 \).
Assume that this is indeed true of \( C^{(d)}_o E \) and that the \( \ell \)-rank of \( C_{oE} \) does not change in going from \( E \) to \( E_1 \), i.e. suppose that

\[
\ell\text{-rank of } C_{oE_1} = \ell\text{-rank of } C_{oE}.
\]

We claim that

\[
(3.5) \quad [X_1:1] = [\ell_{oE}^G:1] = \lambda_F.
\]

That \( X_1 = \ell_{oE}^G \) follows directly from the definition of \( X_1 \) by making use of (3.1) and (3.2). Consider the exact sequence

\[
1 \rightarrow N_1 \rightarrow C_{oF_1} \xrightarrow{\gamma} C'_{oF_1} \rightarrow 1,
\]

where \( \gamma \) is the conorm map from \( F_1 \) to \( E_1 \), \( N_1 \) is the kernel of \( \gamma \) and \( C'_{oF_1} = \gamma(C_{oF_1}) \). In cohomology, the above exact sequence yields

\[
1 \rightarrow N_1^\Gamma \rightarrow C_{oF_1}^\Gamma \rightarrow C'_{oF_1}^\Gamma \rightarrow H'(\Gamma,N_1) + H'(\Gamma,C_{oF_1}) \rightarrow 1,
\]

\(( \Gamma = \text{Gal}(F_1/F))\), which is exact at each point. For the null class group, the norm map is surjective for a constant extension; moreover, the Herbrand quotient for the finite \( \Gamma \)-module \( C_{oF_1} \) is trivial. It follows that \( |H'(\Gamma,C_{oF_1})| = |H^0(\Gamma,C_{oF_1})| = 1 \).

It is easily seen that \( [N_1:1] = \ell^5 \). Also, \( \Gamma \) operates trivially on \( N_1 \) because \( N_1 \subseteq C_{oF} \). So \( |H'(\Gamma,N_1)| = [N_1^\Gamma:1] \) and thus the exactness of the last sequence shows that \( |C_{oF_1}^\Gamma| = |C'_{oF_1}^\Gamma| \).
However, $|C_{\mathcal{O}_F}^{\Gamma}| = |C_{\mathcal{O}_F}|$. The number of ambiguous divisor classes of $E$ is given by

$$h_E = [C_{\mathcal{O}_E}^{\Gamma} : 1] = \frac{h_{\mathcal{F}} \overline{c}}{a}$$

(from [14] and the fact that the extension $E/F$ is unramified), where $h_\mathcal{F}$ is the class number of $F$, $a$ is the minimal positive degree in $E$ of a divisor of $F$ and $\overline{c}$ is the minimal positive degree of an invariant divisor class. By a theorem of F.K. Schmidt, $F$ has a divisor class of degree 1 and so $a = \ell$. Hence $h_E = \frac{h_{\mathcal{F}} \overline{c}}{\ell}$. Since $C_{\mathcal{O}_E}^{\Gamma} \supset C_{\mathcal{O}_F}^{\Gamma}$ and $|C_{\mathcal{O}_F}^{\Gamma}| = |C_{\mathcal{O}_F}^{\Gamma}| = |C_{\mathcal{O}_F}| = h_\mathcal{F}$, we must have $h_\mathcal{F} | h_E$ and so $\ell | \overline{c}$. Obviously, $\overline{c} \leq \ell$ and so $\overline{c} = \ell$, $h_\mathcal{F} = h_E$.

Consequently $C_{\mathcal{O}_E}^{\Gamma} = C_{\mathcal{O}_F}^{\Gamma}$. Since we have assumed that each of the cyclic factors of $C_{\mathcal{O}_F}^{(\ell)}$ has order at least $\ell^3$, it follows that $C_{\mathcal{O}_F}^{\Gamma}$ has the same $\ell$-rank as $C_{\mathcal{O}_F}$. Thus $\ell_\mathcal{F} = [C_{\mathcal{O}_E}^{\Gamma} : 1] = [X_1 : 1]$ and this proves (3.5).

We next assert that

(3.6) \[ H'(G, X_{\mathcal{O}_E}) \cong H'(G, C_{\mathcal{O}_E}) \]  

To prove (3.6), consider the exact sequence of $G$-modules

$$1 \rightarrow \mathcal{L}_{\mathcal{O}_E} \xrightarrow[\alpha]{} C_{\mathcal{O}_E} \xrightarrow[\text{norm}]{} C_{\mathcal{O}_E} + 1,$$

which yields
By our assumption on the \( \ell \)-ranks of \( C_{OE} \), \( C_{OE_1} \), the kernel of the norm map is \( \mathcal{L}_{C_{OE}} \) by lemma 5. It follows that the mapping \( i^* \) is surjective. Consequently \( j^* \) is injective. To prove (3.6) we thus need to show that \( j^* \) is surjective, i.e. that \((\text{norm})^*\) is the zero map.

Consider the inflation-restriction sequences

\[
1 \to H'(S/G, C_{OE_1}^\Gamma) \xrightarrow{\text{inf}} H'(S, C_{OE_1}) \xrightarrow{\text{res}} H'(\Gamma, C_{OE_1})
\]

\[
1 \to H'(S/G, C_{OE_1}^{G}) \xrightarrow{\text{inf}} H'(S, C_{OE_1}) \xrightarrow{\text{res}} H'(G, C_{OE_1})
\]

where \( S = \text{Gal}(E_1/F) \).

\( H^0(\Gamma, C_{OE_1}) \) is trivial and so \( H'(\Gamma, C_{OE_1}) \) is also trivial.

Hence the first inflation map is onto. Also, \( H'(S/G, C_{OE_1}^{G}) \) has the same order as \( H^0(S/G, C_{OE_1}^{G}) = H^0(\Gamma, C_{OE_1}^{G}) \). This last group is trivial by the argument used to show the surjectivity of \( i^* \); and thus the second restriction map is injective. Noting that \( C_{OE_1}^\Gamma = C_{OE} \) and that \( H'(G, C_{OE}) \) and \( H'(G, C_{OE_1}) \) both have the same order \( \ell^{k+1} \) (see [14]), inspection of the above two inflation-restriction sequences shows that the first inflation and second restriction are isomorphisms. Hence an element \( (c_1) \) of
$H'(G; C_{OE})$ is in fact also representable as $(c)$, where $c \in C_{OE}$.

So $(\text{norm}^*)^*(c_1) = (c^l) = (c)^l = 1$. Thus $(\text{norm}^*)^*$ is the zero map and so (3.6) holds.

Now consider the spaces $X_1, X_2, \ldots, X_{k-1}$ defined as in (3.3) but this time for $E_1$. Let $N: \ell^1_{C_{OE_1}} \to \ell^1_{C_{OE_1}}$ be the norm map. Since

$$[X_{k-1}:1] = [X_{k-1}:X_{k-2}] \ldots [X_2:X_1][X_1:1],$$

and since (3.5) is clearly valid in $E_1$ also, we can write

$$[X_{k-1}:1] = \lambda F_1(\sigma) \ell^{-2} \ldots [X_2^{-1}:1].$$

From (3.4) we know that

$$N(\ell^1_{C_{OE_1}}) \subseteq \lambda \sigma \ell^{-2} \subseteq \lambda \sigma \ell^{-3} \subseteq \ldots \subseteq X^{-1}_{2}. $$

We claim that the above containments are, in fact, equalities. This will be true if we can show that

$$N(\ell^1_{C_{OE_1}}) = X^{-1}_{2}. $$

Clearly, $X^{-1}_{2} \subseteq X_1 \cap \ell^1_{C_{OE_1}}$. Now suppose

$$y = z^1 - \sigma \in X_1 \cap \ell^1_{C_{OE_1}}, \ z \in \ell^1_{C_{OE_1}}. $$

Then $y^1 - \sigma = 1 = z(1 - \sigma)^2$ and so $z \in X_2$ and $y \in X^{-1}_{2}$. Hence $X^{-1}_{2} = X_1 \cap \ell^1_{C_{OE_1}}$. Now
\[ \frac{x_1^{1-\sigma}}{x_2^{1-\sigma}} = \frac{x_1}{x_1} \cap \mathcal{L}_{\mathcal{O}E_1}^{1-\sigma} = x_1^{1-\sigma} / \mathcal{L}_{\mathcal{O}E_1}^{1-\sigma} . \]

We contend that \( x_{\mathcal{L}-1} = x_1^{1-\sigma} \). Clearly, \( x_1^{1-\sigma} \subseteq x_{\mathcal{L}-1} \).

So suppose that \( x \in x_{\mathcal{L}-1} \). Then

\[ x^{1+\sigma+\ldots+\sigma^{\ell-1}} = 1 = x^{(1-\sigma)^{\ell-1}} . \]

The proof of lemma 5 shows that by our assumption on the \( \ell \)-ranks of \( \mathcal{O}_{\mathcal{E}}, \mathcal{O}_{\mathcal{E}_1} \), \( x \) is an \( \ell \)-th power in \( \mathcal{O}_{\mathcal{E}_1} \). Let \( x = y^\ell \), \( y \in \mathcal{O}_{\mathcal{E}_1} \). So

\[ x = y^{(1-\sigma)^{\ell-1} \Phi(\sigma) + (1+\sigma+\ldots+\sigma^{\ell-1}) \Phi(\sigma)} \quad \text{(using (3.1))} \]

\[ = x_1 \cdot x_2 , \]

where \( x_1 = y^{(1+\sigma+\ldots+\sigma^{\ell-1}) \Phi(\sigma)} \) and \( x_2 = y^{(1-\sigma)^{\ell-1} \Phi(\sigma)} \). But

\[ x_1^{1-\sigma} = y^{(1-\sigma^\ell) \Phi(\sigma)} = 1 , \]

\[ x_1^\ell = x^{(1+\sigma+\ldots+\sigma^{\ell-1}) \Phi(\sigma)} = 1 . \]

So \( x_1 \in x_1 \). Also, \( x_2 = y^{(1-\sigma)^{\ell-1} \Phi(\sigma)} \in \mathcal{O}_{\mathcal{E}_1}^{1-\sigma} \) and so, because of (3.6), \( x_2 \in \mathcal{O}_{\mathcal{E}_1}^{1-\sigma} \). Hence \( x_1/x_2^{1-\sigma} \cong x_{\mathcal{L}-1} / \mathcal{L}_{\mathcal{O}E_1}^{1-\sigma} \). Note that

\[ x_{\mathcal{L}-1} / \mathcal{L}_{\mathcal{O}E_1}^{1-\sigma} = H'(G, \mathcal{L}_{\mathcal{O}E_1}) \quad \text{and} \quad x_1/N(\mathcal{L}_{\mathcal{O}E_1}) = H^0(G, \mathcal{L}_{\mathcal{O}E_1}) . \]

Since \( |H'(G, \mathcal{L}_{\mathcal{O}E_1})| = |H^0(G, \mathcal{L}_{\mathcal{O}E_1})| \), it follows that \( x_2^{1-\sigma} = N(\mathcal{L}_{\mathcal{O}E_1}) \).
which is (3.8).

From (3.6) and the fact that \( |H'(0, C_{OE_1})| = \ell^{6+1} \) (see [14]) we see that \( |X_1/N(\ell C_{OE_1})| = \ell^{8+1} \) and so, from (3.5),

\[ |N(\ell C_{OE_1})| = \ell^{(8+1)} \]

Hence (3.7), (3.8) and the equation \([\ell C_{OE_1} : 1] = [X_1/1][N(\ell C_{OE_1}) : 1]\) yield \( \ell - 1 = \ell F - (8 + 1)(\ell - 1) \).

\[ \ell F = (8 + 1)(\ell - 1) \]

So \( \lambda_{E_1} = \ell - (8 + 1)(\ell - 1) = \lambda_{E_1} \) (theorem 2).

Hence the maximal \( \ell \)-rank has already been attained in \( E_1 \). This argument shows that if the maximal \( \ell \)-rank has not been reached, then it must increase by at least 1 in a constant extension of degree \( \ell \).

Hence the theorem follows by considering the value of \( \lambda_{E_1} - \lambda_{F_1} = \lambda_{E_1} - \lambda_F \) given by theorem 2, and the initial assumption on the structure of \( C_{OF}^{(\ell)} \). □

**E/F ramified**

Assume that \( \lambda_F = \lambda_{F_1} \) and that the extension \( E/F \) is ramified.

Let \( t \) be the number of primes of \( F \) that are ramified in \( E \).

**Lemma 6.** If the degrees of the primes of \( F \) which ramify in \( E \) are all relatively prime to \( \ell \), and if \( X_1 \) is defined as in (3.3) for the field \( E_1 \), then
\[ [x_1 : 1] = [\mathcal{O}_{\mathcal{E}_1}^G : 1] = \lambda_F + t - 8 - 1 \]

**Proof:** We first show that every class in \( \mathcal{O}_{\mathcal{E}_1}^G \) contains an invariant divisor. For this, we consider the two exact sequences

1. \( 1 \rightarrow K_1 \rightarrow \mathcal{E}_1 \rightarrow P_{\mathcal{E}_1} \rightarrow 1 \)

2. \( 1 \rightarrow P_{\mathcal{E}_1} \rightarrow \mathcal{O}_{\mathcal{E}_1} \rightarrow \mathcal{E}_1 \rightarrow 1 \)

(\( K_1 \) is the constant field of \( \mathcal{E}_1 \)). The first exact sequence yields

\[ 1 = H^1(\mathcal{E}_1) \rightarrow H^1(P_{\mathcal{E}_1}) \rightarrow \overline{H^0(K_1)} \rightarrow \mathcal{E}_1 \rightarrow \ldots \]

If \( K \) (and hence \( K_1 \)) does not contain the \( \ell \)-th roots of unity, \( |\overline{H^0(K_1)}| = 1 \). If \( K \) contains the \( \ell \)-th roots of unity, it follows from Hasse's norm theorem that a generator of \( K_1 \) is a norm from \( \mathcal{E}_1 \) iff the degrees of the ramified primes are all divisible by \( \ell \).

However, the hypothesis of the lemma requires that the degrees of such primes be relatively prime to \( \ell \). So a generator of \( K_1 \) cannot be a norm from \( \mathcal{E}_1 \). It follows that, whether or not \( K \) contains the \( \ell \)-th roots of unity, the map \( i^* \) is injective, whence \( H^1(P_{\mathcal{E}_1}) \) is trivial.

The second exact sequence yields

\[ 1 \rightarrow \mathcal{E}_1^G \rightarrow \mathcal{O}_{\mathcal{E}_1}^G \rightarrow \mathcal{E}_1^G \rightarrow H^1(P_{\mathcal{E}_1}) = 1 \]

which shows that every element of \( \mathcal{O}_{\mathcal{E}_1}^G \) contains an invariant divisor.
Now Deuring's counting argument in [4] as modified by Moriya [17] is applicable. We repeat it here briefly for the sake of completeness.

Suppose that \( P_1, P_2, \ldots, P_t \) are the primes of \( F \) that ramify in \( E \) and let \( \overline{P}_i \) \((1 \leq i \leq t)\) be the prime of \( E \) lying above \( P_i \). We shall use this same notation for ramified primes in \( E_1/F_1 \). This is harmless since the \( P_i, (\overline{P}_i) \) are inert in \( F_1(E_1) \). Given an element \( x_1 \in \mathcal{O}_E \), we have shown that there is a divisor \( \overline{C} \) in \( x_1 \) such that \( \overline{C} \cdot \sigma^{-1} = 1 \). Hence we can obviously write \( \overline{C} \) in the form \( \prod_{i=1}^{t} \overline{P}_i^{v_i} \), where \( 0 \leq v_i < t \) \((i=1,2,\ldots,t)\) and \( C \) is a divisor of \( F_1 \). It follows that \( x_1 = \prod_{i=1}^{t} \overline{P}_i^{v_i} \mathcal{O}_E \), where \( \overline{P}_i \) is the divisor class of \( E \) containing \( \overline{P}_i \) \((1 \leq i \leq t)\) and \( \mathcal{O}_E \) is the divisor class of \( E \) containing \( C \). Denoting by \( \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_t \) the divisor classes of \( F_1 \) containing \( P_1, P_2, \ldots, P_t \) respectively, and by \( \mathcal{C} \) the divisor class of \( F_1 \) containing \( C \), we obtain

\[
1 = N(x_1) = \prod_{i=1}^{t} N(\overline{P}_i)^{v_i} N(\mathcal{C}) = \prod_{i=1}^{t} \overline{P}_i^{v_i} \mathcal{C}^t.
\]

\((N \) is the norm map from \( E_1 \) to \( F_1 \).) Let \( d_i \) be the degree of \( P_i \) \((1 \leq i \leq t)\). Then the previous equation shows that

\[
\sum_{i=1}^{t} v_i d_i \text{ must be divisible by } t.
\]

Conversely, suppose \( v_1, v_2, \ldots, v_t \) are integers such that \( \sum_{i=1}^{t} v_i d_i \equiv 0 \pmod{t} \); say \( \sum_{i=1}^{t} v_i d_i = ts \). By a theorem of F.K. Schmidt, \( F \) possesses a divisor class, say \( \mathcal{C}_1 \),
whose degree is \(-s\). Then the divisor class \((\prod_{i=1}^{t} p_i v_i)c_1^t\) of \(F\)
is of degree 0 and so, by lemma 5, it becomes an \(\ell\)-th power in \(F_1\).
That is to say, there is a divisor class \(c_0\) in \(F_1\) such that
\[
\prod_{i=1}^{t} p_i v_i c_0^t = 1.\]
Let \(\mathcal{C}_0\) be the divisor class of \(E_1\) containing \(c_0\). Then
\[
((\prod_{i=1}^{t} p_i v_i)\mathcal{C}_0)^{1-s} = 1 \quad \text{and} \quad \mathcal{N}(\prod_{i=1}^{t} p_i v_i \mathcal{C}_0) = 1.
\]

Hence every vector \(V = (v_1, v_2, \ldots, v_t)\) such that
\[
v_1^d_1 + v_2^d_2 + \ldots + v_t^d_t \equiv 0 \pmod{\ell}
\]
determines an element of \(X_1\) in the above manner and conversely. Let \(A_V\) denote all the elements of \(X_1\) determined by \(V\) in this way. Clearly, then, if \(x_1, x_2 \in A_V\) we must have \(x_1 x_2^{-1} = d_0\), where \(d_0\) is a divisor class of \(F_1\). Also, because \(\mathcal{N}(x_1 x_2^{-1}) = d_0^\ell\), \(d_0 \in \ell \mathcal{C}_{OF_1}\)
runs through all elements of \(\ell \mathcal{C}_{OF_1}\), \(x_1 d_0\) (where \(x_1\) is a fixed element of \(A_V\)) runs through all elements of \(A_V\). Thus
\[
|A_V| = \ell \cdot 1 = \ell^\lambda_F.
\]

Since any two elements of \(A_V\) differ by an element of \(\ell \mathcal{C}_{OF_1}\)
(and conversely) it follows that \(A_V\) and \(A_{V'}\) are either identical
or disjoint, \(V_1\) and \(V_2\) being vectors "orthogonal" to
\((d_1, d_2, \ldots, d_t)\). Note that the vectors "orthogonal" to \((d_1, d_2, \ldots, d_t)\)
form a vector space over $GF(\ell)$ of dimension \((t - 1)\), since the \(d_i\) are prime to \(\ell\). Let us say that two such vectors \(V_1\) and \(V_2\) are equivalent iff \(A_{V_1} = A_{V_2}\). It is clear from the construction of the \(A_V\) that \(A_{V_1} = A_{V_2}\) iff \(A_{V_1} - V_2\) contains the principal class. It is easy to see that there are precisely \(\ell^6\) distinct \(V\)'s for which \(A_V\) contains the principal class. Since the number of \(V\)'s is \(\ell^{t-1}\) and each \(A_V\) is of size \(\ell^F\), it follows that the total number of distinct classes in \(X_1 = \bigcup A_V\) is precisely \(\frac{\ell^F \cdot \ell^{t-1}}{\ell^6}\).

\[\lambda_F + \ell - 8 - 1\]

We now refine our notation. We shall write \(X_{1,j}\) for the spaces \(X_1\) defined as in (3.3), but with the field \(E\) replaced by \(E_j\), the constant extension of \(E\) of degree \(\ell^j\). Hence the equality in the statement of lemma 6 can be written as \([X_{1,1}:1] = \ell^F + \ell - 8 - 1\).

With this notation we can then state

**Lemma 7.** With the same hypothesis as in lemma 6,

\[
\begin{align*}
X_{1,2\ell - 2} &= X_{2,2\ell - 2} = X_{3,2\ell - 2} = \ldots = X_{t-1,2\ell - 2} \\
\end{align*}
\]

and hence, from lemma 6, \([X_{\ell-1,2\ell - 2}] = \ell^{(\lambda_F + \ell - 8 - 1)(\ell - 1)}\).
Proof: Obviously, since

\[[X^{l-1,2l-2}:1] = [X^{l-1,2l-2}:X^{l-2,2l-2}] \cdots [X^{2,2l-2}:X^{1,2l-2}][X^{1,2l-2}:1]\]

\[(1-\sigma)^{l-2} \cdot 1-\sigma \]

\[[X^{l-1,2l-2}:1] \cdots [X^{2,2l-2}:1][X^{1,2l-2}:1] \cdot \]

the lemma will be proved completely if we can show that

\[1-\sigma \cdot (1-\sigma)^{l-2} = X^{1,2l-2} = X^{2,2l-2} = \cdots = X^{l-1,2l-2}.\]

To establish this we will need to justify the

Claim: If \( j \geq 0 \) is an integer and \( c \in X^{l-1,j} \), then \( c = b^{1-\sigma} \), \( N(b) = 1 \), where \( b \) is in \( C_{E_{j+2}} \) and \( N \) is the norm map from \( E_{j+2} \) to \( F_{j+2} \).

In order to prove the claim, suppose indeed that \( c \in X^{l-1,j} \). Then \( N(c) = 1 \) (here \( N \) is norm from \( E_{j} \) to \( F_{j} \)). Choose a divisor \( A \in c \) which is relatively prime to the conductor of \( E_{j}/F_{j} \). Since \( N(c) \) is principal there is an \( \alpha \in F_{j} \) such that \( N(A) = (\alpha) \). We assert that there is a \( \beta \in E_{j+1} \) such that \( \alpha = N(\beta) \). By Hasse's norm theorem, this will follow if we can show that in the extension \( E_{j+1}/F_{j+1} \), \( \alpha \) is a local norm everywhere (i.e. for all primes). This follows as in lemma 3 if one notes that for the inert primes, the exponent in the principal divisor \( (\alpha) \) is a multiple of \( l \). Then \( N(A(\beta)^{-1}) = 1 \) and so, by Hilbert's "Theorem 90" for
divisors, \( A(\beta)^{-1} = D^{1-\sigma} \quad (D \in C_{E_{j+1}}) \). However, since a prime of \( F_{j+1} \) of degree relatively prime to \( \ell \) is ramified in \( E_{j+1} \), an elementary argument shows that \( d \) can be chosen to be of degree 0. This shows that \( c = d^{1-\sigma}, \quad D \in d, \) where \( d \in C_{E_{j+1}} \). Then \( N_{E_{j+1}/F_{j+1}}(d) \) is an \( \ell \)-th power in \( C_{F_{j+2}} \), say \( N_{E_{j+1}/F_{j+1}}(d) = g^\ell \). Setting \( b = \frac{d}{g} \) we then have \( c = d^{1-\sigma} = b^{1-\sigma} \) and \( N_{E_{j+2}/F_{j+2}}(b) = 1 \), since \( N_{E_{j+1}/F_{j+1}}(d) = g^\ell \). Hence our claim is justified.

Now, we know that

\[(3.9) \quad x_{1,j} \subseteq x_{2,j} \subseteq \cdots \subseteq x_{l-1,j} \]

for all integers \( j \geq 0 \); and that

\[(3.10) \quad x_{i,j}^{(1-\sigma)^{i-1}} \subseteq x_{i,j} \]

for all integers \( j \geq 0 \) and for \( i = 1, 2, \ldots, l-1 \).

Suppose \( c \in x_{1,0} \). Then, by our claim, \( c = b^{1-\sigma} \), \( N(b) = 1 \), \( b \in C_{E_2} \).

Thus \( b \in x_{2,2} \) and (3.10) shows that \( x_{1,0} = x_{1,2} = x_{2,2}^{1-\sigma} \); and so it clearly follows that \( x_{2,j}^{1-\sigma} = x_{2,2}^{1-\sigma} \) for all \( j \geq 2 \). Then exactly the same argument shows that \( x_{3,j}^{(1-\sigma)^2} = x_{2,4}^{1-\sigma} \) and that

\( x_{3,j}^{(1-\sigma)^2} = x_{3,4}^{(1-\sigma)^2} \) for all \( j \geq 4 \). Continuing in this manner we
finally obtain

\[ X_{1,2l-2} = X_{2,2l-2} = \cdots = X_{l-1,2l-2} = x^{(1-c)\ell - 2} \]

which completes the proof of lemma 7. \( \square \)

Theorem 4. Suppose that the primes \( P_1, P_2, \ldots, P_s \) of \( F \) ramifying in \( E \) have degrees given by

\[ d_i = \deg(P_i) = d_i^{a_i}, \]

\( \ell \) prime to \( d_i \). Then if \( m = (2\ell - 2) + \max(a_1, a_2, \ldots, a_s) \) and

\[ t = \sum_{i=1}^{s} a_i, \]

we have \( \lambda_E^m = \lambda_{E_m} = \lambda_F + (t - s - 1)(\ell - 1) \), where \( s = 1 \) or 0, according as \( K \) does or does not contain the \( \ell \)-th roots of unity.

Proof: Let \( m_1 = \max(a_1, a_2, \ldots, a_s) \). From lemma 7 and the fact that in a constant extension of \( F \) of degree \( m_1 \) there are \( t \) primes of degrees prime to \( \ell \) ramifying in \( E_{m_1} \), it follows that in \( E_m \) we have

\[ |X_{\ell - 1, m}| = \ell^{(\lambda_F^m + t - s - 1)(\ell - 1)}. \]

Consider the norm map \( N: \mathcal{O}_{E_m} / \mathcal{O}_{E_m}^\times \to \mathcal{O}_{E_m} / \mathcal{O}_{E_m}^\times \). The kernel of this map is precisely \( X_{\ell - 1, m} \). Hence

\[ \mathcal{O}_{E_m} / X_{\ell - 1, m} \cong N(\mathcal{O}_{E_m}). \]
We intend to show that \( |N(\mathcal{C}^E_{m})| = \lambda_F \). For this to be true, it is enough to show that every element of \( \mathcal{C}^E_m \) is a norm from \( \mathcal{C}^E_{m_1} \), where \( m_1 = \max(a_1, a_2, \ldots, a_s) \). So let \( c \) be an element of \( \mathcal{C}^E_{m_1} \). From the claim stated in lemma 7 (and observing that \( \mathcal{C}^E_{m_1} \subset \mathcal{C}^E_{m} \)) we can conclude that \( c = d(1 - \sigma)^{l-1} \).

\[ N_{E_m/F_m}(d) = 1 \] for some \( d \in C_{E_m} \). But, using (3.2), this means that

\[
\begin{align*}
    c &= d^{\ell h(\sigma)} + (1 + \sigma + \ldots + \sigma^{\ell-1}) \\
    &= [d^{h(\sigma)}]^{\ell} \\
    &= x^{\ell}, \text{ where } x = d^{h(\sigma)}.
\end{align*}
\]

So \( N(x) = 1 \). However, from lemma 5, we know that in \( F_{m_1} + 1 \) we have \( c = s^{\ell} = N(s) \). Hence \( N(s/x) = c \) and \( (s/x)^{\ell} = s^{\ell}/x^{\ell} = c/c = 1 \).

Hence every element of \( \mathcal{C}^E_{m_1} \) is a norm from \( \mathcal{C}^E_m \) and so

\[ |N(\mathcal{C}^E_m)| = \lambda_F. \]

Finally,

\[
\begin{align*}
    \lambda_{m} &= \left[ \mathcal{C}^E_{m} : 1 \right] = \left[ \mathcal{C}^E_{m_1} : 1 \right] |N(\mathcal{C}^E_m)| \\
    &= (\lambda_F + \ell - 1)(\ell - 1) \cdot \lambda_F,
\end{align*}
\]
which yields

\[ \lambda_{E_{m}} = 2\lambda_{F} + (t - 8 - 1)(\ell - 1) \]

\[ = 2\lambda_{F} + (t - 8 - 1)(\ell - 1) \]

The maximal \(\ell\)-rank has thus been attained already in \(E_{m}\). \(\square\)
§1. Notation and some preliminary results.

In this chapter, \( K \) will always denote an algebraically closed field; and algebraic function fields will always be assumed to have algebraically closed constant field. We will use the notation \( F/K \) for an algebraic function field with constant field \( K \). For a prime \( P \) of an algebraic function field, the symbol \( V_p \) will be used to denote the normalized valuation that \( P \) induces on the function field. This symbol \( V_p \) will also be allowed to have divisors as arguments, in which case the integer returned is just the exponent to which the prime \( P \) occurs in the particular divisor. The symbol * , when placed above the symbol for a field, indicates that we are considering the multiplicative group of nonzero elements of that field.

If \( F \) is a function field over \( K \) and \( x \in F \), we shall write \( (x)_F \) for the divisor of \( x \) in \( F \). If there is no danger of confusion arising, we shall just write \( (x) \). Similarly, \( (dx)_F \), or just \( (dx) \), will denote the exact differential determined by \( x \). For a divisor \( A \) of \( F \), \( L(A) \) denotes the set of all elements \( x \) of \( F \) for which \( (x)_F \cdot A^{-1} \) is an integral divisor. \( d(A) \) stands for the degree of \( A \); \( g_F \) for the genus of \( F \). If \( L \) is an extension of \( F \) of finite degree and \( A \) is a divisor of \( F \), we write \( \text{Con}_{F/L}(A) \).
for the divisor determined by $A$ in the group of divisors of $L$.

$D_{L/F}$ denotes the different of $L$ over $F$.

Whenever we write a divisor $A$ in the form $\frac{B}{C}$, it is to be understood that $B$ and $C$ are integral and prime to each other.

Finally, if $L_1$ and $L_2$ are two fields such that $L_2 \supseteq L_1$, we write $\text{Aut}(L_2/L_1)$ for the group of all automorphisms of $L_2$ that are trivial on $L_1$. If $L_2$ is Galois over $L_1$ we may write $\text{Gal}(L_2/L_1)$ instead of $\text{Aut}(L_2/L_1)$. Also, $[L_2:L_1]$ denotes the degree of $L_2$ over $L_1$ and, if this degree is finite, $\text{Tr}_{L_2/L_1}$ denotes the usual trace function from $L_2$ to $L_1$. For a finite set $S$, $|S|$ denotes the cardinality of $S$ and for $n$ a prime power, $GF(n)$ denotes a finite field with $n$ elements.

In this section we prove some preliminary lemmas, some of them interesting results by themselves. The main aim of the section is to investigate the nature of the ramification in an extension $L_2/K$ of prime degree of an algebraic function field $L_1/K$, which will ensure that any automorphism of $L_2$ over $K$ restricts to an automorphism of $L_1$ over $K$. These results will be utilized in §3 and §4.

**Definition 1.** A function $f$ of a function field $F$ will be called a \textit{minimal pole function} of a prime $P$ of $F$, if $(f) = \frac{B}{P^\lambda}$, where $\lambda$ is the least pole number of $P$. A set $S$ of primes of $F$ is said to \textit{saturate} $F$ if $F$ can be generated over $K$ by minimal pole functions of primes in $S$. 
Lemma 1. Let \( F \) be an algebraic function field over \( K \) and let \( I \) be an infinite set of primes of \( F \). Then there is a finite subset of \( I \) that saturates \( F \).

Proof: Choose any prime \( P_1 \in I \) and let \( f_{P_1} \) be a minimal pole function for \( P_1 \). If \( \{P_1\} \) does not saturate \( F \), then, since \( f_{P_1} \notin K \), it follows that \( [F:K(f_{P_1})] \) is finite and exceeds 1.

Since \( f_{P_1} \) is a minimal pole function for \( P_1 \), it follows that \( f_{P_1} \) is not a \( p \)-th power in \( F \) and, consequently, \( f_{P_1} \) is a separating element of \( F \) (see [5], page 146). Hence, since only finitely many primes of \( F \) can ramify over \( K(f_{P_1}) \), there is a prime \( P_2 \in I \) such that \( P_2 \) does not ramify over \( K(f_{P_1}) \). \( K \) being algebraically closed, \( P_2 \) cannot be inert over \( K(f_{P_1}) \). So there must be a prime \( P_2' \neq P_2 \) of \( F \) such that \( P_2' \cap K(f_{P_1}) = P_2 \cap K(f_{P_1}) \). Thus any minimal pole function \( f_{P_2} \) of \( P_2 \) cannot be in \( K(f_{P_1}) \) and so \([F:K(f_{P_1}, f_{P_2})] < [F:K(f_{P_1})] \) is also finite. If \( \{P_1, P_2\} \) does not saturate \( F \), it is clear that we can repeat the above process and that the process cannot continue indefinitely. \( \Box \)

Definition 2. (i) Given a field \( L \), a subgroup \( H \) of \( L^\times \) and an integer \( n \neq 0 \), we shall say that \( \ell_1, \ell_2, \ldots, \ell_r \in L \) are
n-independent modulo H if \( \ell_1^{n_1} \ell_2^{n_2} \ldots \ell_r^{n_r} \in H \) implies that 
\( a_i = 0 \mod n \) for \( 1 \leq i \leq r \).

(i) Let \( n>0 \) be an integer, \( L \) a field and \( k \) a subset of \( L \) with \( 0 \in k \). Define \( P_n(L) = \{ \ell^n - \ell \mid \ell \in L \} \). We shall say that the elements \( \ell_1, \ell_2, \ldots, \ell_r \in L \) are \( k \)-independent modulo \( P_n(L) \) if 
\[ \sum_{i=1}^{r} k_i \ell_i \in P_n(L) \ (k_i \in k) \] implies that \( k_i = 0 \) for \( 1 \leq i \leq r \).

Lemma 2. (i) Let \( L_1 \subset L_2 \) be algebraic function fields over \( K \) and assume that \( L_2/L_1 \) is a non-trivial finite Galois extension. Let \( \ell \) be any integer such that \( |\ell| \geq 2 \). Then for any integer \( m \geq 1 \), the multiplicative group \( L_2^* \) of \( L_2 \) contains \( m \) elements \( \alpha_1, \alpha_2, \ldots, \alpha_m \), such that the elements of \( \{ \sigma(\alpha_1) \mid 1 \leq i \leq m ; \sigma \in \text{Gal}(L_2/L_1) \} \) are \( \ell \)-independent modulo \( (L_2^*)^\ell \).

(ii) Let \( L_2/L_1 \) be as in (i) above and let \( \ell \geq 2 \) be an integer. Then for any integer \( m \geq 1 \), the additive group of \( L_2 \) contains \( m \) elements \( \alpha_1, \alpha_2, \ldots, \alpha_m \), such that the elements of \( \{ \sigma(\alpha_1) \mid 1 \leq i \leq m ; \sigma \in \text{Gal}(L_2/L_1) \} \) are \( \ell \)-independent modulo \( P_{\ell}(L_2) \).

Proof: (i) It is well known that since \( L_2/L_1 \) is Galois, all but finitely many primes of \( L_1 \) decompose fully in \( L_2 \). Let \( P_1, P_2, \ldots, P_m \) be primes of \( L_1 \) which decompose fully in \( L_2 \) and choose primes \( \overline{P}_1, \overline{P}_2, \ldots, \overline{P}_m \) in \( L_2 \) such that \( \overline{P}_i \) lies above \( P_i \) (\( 1 \leq i \leq m \)). The approximation theorem allows us to choose \( \alpha_1, \alpha_2, \ldots, \alpha_m \) in \( L_2 \) such that
\[
\begin{align*}
V_{\overline{P}_i}(\alpha_i) &= 1 \quad (1 \leq i \leq m) \\
V_{\overline{P}_i}(\alpha_j) &= 0 \quad (1 \leq i, j \leq m ; i \neq j) \\
V_{Q}(\alpha_i) &= 0 \quad \text{if } Q \text{ is a prime}
\end{align*}
\]

of \( L_2 \) which is conjugate (over \( L_1 \)) but not equal to any of
\( \overline{P}_1, \overline{P}_2, \ldots, \overline{P}_m \) \( (1 \leq i \leq m) \). One easily checks that the \( \alpha_i \)
\( (1 \leq i \leq m) \) have the required property. \( \square \)

(ii) Let the \( P_i \) and \( \overline{P}_i \) \( (1 \leq i \leq m) \) be as in (i) above and
let \( \lambda > 0 \) be an integer such that \( \ell \nmid \lambda \). Again, choose
\( \alpha_1, \alpha_2, \ldots, \alpha_m \) in \( L_2 \) such that
\[
\begin{align*}
V_{\overline{P}_i}(\alpha_i) &= -\lambda \quad (1 \leq i \leq m) \\
V_{\overline{P}_i}(\alpha_j) &= 0 \quad (1 \leq i, j \leq m ; i \neq j) \\
V_{Q}(\alpha_i) &= 0 , \quad \text{where } Q \text{ are the}
\end{align*}
\]

same primes described in (i); \( 1 \leq i \leq m \).

Now suppose that
\[
\sum_{i=1}^{m} c_{\sigma,i} \sigma(\alpha_i) = \ell_2^l - \ell_2 \text{ , where}
\sigma \in \text{Gal}(L_2/L_1)
\]
\( \ell_2 \in L_2 \) and \( c_{\sigma,i} \in K \). If some \( c_{\sigma,i} \) is nonzero, noting that
if follows that \( V_{\sigma} (\overline{F_1}) (\sum \sigma_i \sigma(\alpha_i)) = -\lambda \). Hence

\[ V_{\sigma} (\overline{F_1}) (l_2^L - l_2) = -\lambda. \]

Consequently \( V_{\sigma} (\overline{F_1}) (l_2) < 0 \) (or else \( V_{\sigma} (\overline{F_1}) (l_2^L - l_2) \) would be at least 0). So \( V_{\sigma} (\overline{F_1}) (l_2^L - l_2) = -\lambda \), whence \( \lambda \) is divisible by \( l \), a contradiction.

Thus \( c_{\sigma, i} = 0 \) for all \( \sigma \in \text{Gal}(L_2/L_1) \) and \( 1 \leq i \leq m \). \( \square \)

Theorem 1. Let \( L_1 \subseteq L_2 \) be algebraic function fields over \( K \), \( \text{char } (K) = p > 0 \), with \( L_2/L_1 \) a nontrivial solvable Galois extension and let \( G = \text{Gal}(L_2/L_1) \) have order \( n \). Let \( P \) be a prime of \( L_1 \) that ramifies fully in \( L_2 \) and suppose \( \overline{F} \) is the (unique) prime of \( L_2 \) lying above \( P \). Then if \( \lambda \) is the least pole number of \( P \) and more than \( n \lambda \) primes of \( L_1 \) ramify fully in \( L_2 \), \( n \lambda \) is the least pole number of \( \overline{F} \). Moreover, if \( G \) is nilpotent and \( n = mp^s \), \( (m,p) = 1 \), the same result holds even if we assume that only more than \( m \lambda \) primes of \( L_1 \) ramify fully in \( L_2 \); and if \( m = 1 \) we need just two or more primes to ramify fully in order that the same conclusion be correct.
Proof: Suppose first that $\bar{L}$ is a Galois extension of $L_1$ of degree $\ell$, a prime. Two cases arise.

**Case 1:** $\ell = p$. Let $\bar{P}$ be a prime of $\bar{L}$ that is ramified over $L_1$ and let $P$ be the prime of $L_1$ lying below $\bar{P}$. Further assume that $\bar{P}$ is not the only prime of $\bar{L}$ ramifying over $L_1$ and that $\lambda$ is the least pole number of $P$. We will show that $\lambda p$ is the least pole number of $\bar{P}$. If this were not so, there would be a least integer $\mu < \lambda p$ for which $L(\bar{P}^{-\mu})$ is of dimension exceeding one. Thus $L(\bar{P}^{-\mu}) = \langle 1, z \rangle$, the $K$-subspace of $\bar{L}$ generated by 1 and $z$. Clearly, $z \notin L_1$ or else $v_P(z) = -\frac{\mu}{p} > -\frac{\lambda p}{p} = -\lambda$, contradicting the fact that $\lambda$ is the least pole number of $P$. Let $\sigma$ be a generator of $\text{Gal}(\bar{L}/L_1)$. Then since $\sigma(\bar{P}) = \bar{P}$, we see that $\sigma$ maps $L(\bar{P}^{-\mu})$ onto itself. Consequently,

$$\sigma(z) = az + b \quad (a, b \in K)$$

$$\sigma^2(z) = \sigma(az + b) = a^2z + ab + b, \text{ etc.}$$

Since $\sigma^p(z) = z$, it follows that $a^p = 1$. So $a = 1$, $\sigma(z) = z + b$ and since $z \notin L_1$ we have $b \neq 0$. Then

$$\sigma\left(\frac{z}{b}\right) = \frac{z + b}{b} = \frac{z}{b} + 1.$$

Since more than one prime of $L_1$ ramifies in $\bar{L}$, let $Q \neq P$ be a prime of $L_1$ ramifying in $\bar{L}$. We can thus find a $y \in \bar{L}$ such that $\bar{L} = L_1(y)$, $y^p - y = \beta \in L_1$ and $e = v_Q(\beta)$ is negative and prime to $p$. (See [7]). Also, by multiplying $y$ by an element of the prime
field if necessary, we can assume that

$$\sigma(y) = y + 1$$

Hence $$\sigma(y - \frac{z}{b}) = y - \frac{z}{b}$$ and so $$y - \frac{z}{b} \in L_1$$. But $$v_{Q}(\frac{z}{b}) \geq 0$$ since $$z \in L(\overline{F}^{-\mu})$$ and $$\overline{F} \neq \overline{Q}$$, the prime of $$\overline{L}$$ lying above $$Q$$. Also $$p = v_{Q}(\beta) = v_{Q}(y^p - y) = pv_{Q}(y)$$, since $$e < 0$$. Thus $$v_{Q}(y) = e$$.

Hence $$v_{Q}(y - \frac{z}{b}) = e$$ which is impossible since $$y - \frac{z}{b} \in L_1$$ and $$p \nmid e$$. This completes the proof of case 1.

**Case 2:** $$l \neq p$$. Again, let $$\overline{P}$$ be a prime of $$\overline{L}$$ that is ramified over $$L_1$$ but now let us assume that more than $$\lambda$$ primes of $$L_1$$ ramify in $$\overline{L}$$, $$\lambda$$ the least pole number of $$P$$, the prime of $$L_1$$ lying below $$\overline{P}$$. As in case 1, let $$\mu$$ be the least integer $$< \lambda$$ such that $$L(\overline{F}^{-\mu}) = \langle 1, z \rangle$$. If there is no such $$\mu$$ then there is nothing to prove; i.e. $$\lambda$$ will be the least pole number of $$\overline{P}$$. Clearly, $$z \notin L_1$$. With $$\sigma$$ as in case 1 we again have

$$\sigma(z) = az + b, \ a, b \in K; a \neq 0$$

Suppose $$b \neq 0$$. Then $$a \neq 1$$ or else $$z = \sigma'(z) = z + b \ell \neq z$$, a contradiction. Then $$\sigma(\frac{b}{a - 1} + z) = \frac{b}{a - 1} + az + b = a(\frac{b}{a - 1} + z)$$.

If $$b = 0$$, then $$\sigma(z) = az$$. Thus, whether or not $$b = 0$$, there is always a non-constant element $$z_1$$ in $$L(\overline{F}^{-\mu})$$ such that $$\sigma(z_1) = az_1$$. This implies that $$\sigma(z_1) = \alpha z_1 = z_1$$ and thus $$a$$ is an $$\ell$$th root of unity. On the other hand $$\overline{L} = L_1(y)$$ with $$y^\ell = \beta \in L_1$$; and $$\sigma(y) = \zeta y$$ with $$\zeta$$ a primitive $$\ell$$th root of unity. Let $$a = \zeta^i$$,
0 < i ≤ ℓ - 1. Then \( \sigma(\frac{z_i}{y^i}) = \frac{z_i}{y} \) and so \( \frac{z_i}{y} \in L_1 \). Now \( (z_i)_{L_1} = A_{\overline{F}_i} \) and so \( d(A) = \mu < \lambda \ell \). It follows that the divisor of \( z_1 \) in \( \overline{L} \) can involve at most \( \mu + 1 \leq \lambda \ell \) distinct primes. However, (see [7]), since at least \( \lambda \ell + 1 \) primes of \( L_1 \) ramify in \( \overline{L} \), it follows that the divisor of \( y \) in \( \overline{L} \) contains at least \( \lambda \ell + 1 \) distinct primes occurring to exponent prime to \( I \) and these primes are all fully ramified over \( L_1 \). Since \( 0 < i \leq \ell - 1 \), the same is true of the divisor \( (y^{-1})_{L_1} \) in \( \overline{L} \).

Consequently the divisor of \( z_1 y^{-1} \) in \( \overline{L} \) must contain at least one prime occurring to exponent prime to \( \ell \) and which is ramified over \( L_1 \). This is clearly impossible because \( z_1 y^{-1} \in L_1 \). So the proof of case 2 is complete.

Now let \( L_1 \) and \( L_2 \) be as in the statement of the lemma. Since \( G \) is solvable, it has a composition series:

\[
G = N_1 \supset N_2 \supset N_3 \supset \ldots \supset N_k = \{e\},
\]

where \( N_{i+1} \) is normal in \( N_i \) and \( |N_i/N_{i+1}| \) is a prime, \( 1 \leq i \leq k - 1 \). We shall refer to \( k \) as the length of the composition series. Since \( G \) is non-trivial, \( k \geq 2 \). If \( k = 2 \) the result is a consequence of cases 1 and 2 above. Assume that the result has been proved for all solvable groups which have a composition series of length \( < k \) and at least two. Let \( F_{N_2} \) be the fixed field of \( N_2 \) and let \( \mathbb{F} \) be the prime of \( F_{N_2} \) lying below \( \overline{F} \). Let
The document contains a proof of a theorem regarding the normal closure of a field extension. The proof involves the use of the Galois group and the properties of primes ramifying in the extension. The text is a continuation of the previous passage, discussing the least pole number and the composition series of the Galois group.

The theorem states that if $F_{N_2}$ is normal over $L_1$ of prime degree $\ell$, then for any prime $\lambda$, the number of primes of $L_1$ ramifying fully in $L_2$ is at least $\ell \lambda + 1$. This leads to the conclusion that the least pole number of $F_{N_2}$ is the least pole number of $\overline{F}$.

The proof then considers the case where $G$ is nilpotent and $|G| = n = mp^s$, with $(m,p) = 1$. It involves writing $G$ as the direct product of its $p$-Sylow subgroup $S_p$ and another group, say $G_1 \subset G$. Let $F_{S_p}$ be the fixed field of $S_p$ and let $\overline{F}$ be the prime of $F_{S_p}$ lying below $F$. If more than $m \lambda$ primes of $L_1$ ramify fully in $L_2$, then more than $m \lambda$ primes of $L_1$ ramify fully in $F_{S_p}$. Since $F_{S_p}/L_1$ is a nilpotent, hence solvable, extension of degree $m$, it follows from above that $\overline{F}$ has $m \lambda$ as its least pole number. Since $m \lambda \geq 1$ it follows also that at least $m \lambda + 1 \geq 2$ primes of $F_{S_p}$ ramify fully in $L_2$; thus from case 1 above and the fact that we can reach $L_2$ from $F_{S_p}$ by a series of normal extensions of degree $p$, it follows that $p^s(m \lambda) = n \lambda$ is the least pole number.
pole number of $\mathbb{F}$. If $m = 1$, then $G = S_p$ and from the last part of the previous sentence it follows that the conclusion in the lemma is true even if we assume that just two or more primes ramify fully.

**Lemma 3.** Let $L_1$ and $L_2$ be algebraic function fields over $K$ with $L_2 \supset L_1$ and $L_2 / L_1$ a non-trivial solvable Galois extension of degree $n$. Let $S$ be a set of primes of $L_1$ that saturates $L_1$ and assume that $|S| \geq (g_{L_1} + 1)n + 1$. Also suppose every prime of $S$ ramifies fully in $L_2$ and that every prime of $L_2$ that is not fully ramified over $L_1$ has a gap sequence distinct from that of all primes $\bar{Q}$ of $L_2$ for which the prime of $L_1$ lying below $\bar{Q}$ is in $S$. Then every automorphism of $L_2$ over $K$ maps $L_1$ onto itself.

**Proof:** Let $S_1$ be the set of all primes of $L_1$ that ramify fully in $L_2$. Then $S_1 \supset S$ and so $|S_1| \geq |S|$. Since every prime of $L_1$ has exactly $g_{L_1}$ gap numbers between 1 and $2g_{L_1} - 1$ (both numbers inclusive) it follows that no prime of $L_1$ can have least pole number exceeding $g_{L_1} + 1$. Thus the number of primes in $L_1$ that ramify in $L_2$ measures up to the requirements of theorem 1 (for every prime of $L_1$ that ramifies in $L_2$). Let $S_2$ consist of those primes of $L_2$ whose gap sequence equals the gap sequence of some prime of $S = \{Q \mid \bar{Q} \text{ lies above a prime of } S\}$. Also let $S_1$ be the set of all primes of $L_2$ lying above primes in $S_1$ and let $S_2$ be the set of all primes of $L_1$ lying below primes of $S_2$. 
By the definition of $S_2$, we have $S \subseteq \overline{S}_2$ and the conditions of our lemma imply $S_2 \subseteq S_1$; so $S_1 \supseteq \overline{S}_2 \supseteq S$. Let $\overline{P} \in \overline{S}_2$ and let $\sigma$ be any automorphism of $L_2$ over $K$. Then $\sigma(\overline{P})$ has the same gap sequence as $\overline{P}$ and hence $\sigma(\overline{P}) \in \overline{S}_2$. That is, $\sigma(S_2) = \overline{S}_2$.

For each prime $P \in S_2$, let $z_p$ be a minimal pole function for $P$. Suppose $\nu_p(z_p) = -\lambda_p$. Then from theorem 1 we know that

$$L(\overline{P}^{-\lambda_p}) = \langle 1, z_p \rangle, \quad \overline{P} \text{ lying above } P.$$ 

Then $\sigma(L(\overline{P}^{-\lambda_p})) = L(\sigma(\overline{P})^{-\lambda_p})$ and this space is again of dimension two. But $\sigma(\overline{P}) \in \overline{S}_2$ since $\sigma(S_2) = \overline{S}_2$. Let $\sigma(P)$ be the prime of $L_1$ lying below $\sigma(\overline{P})$. Then the only way that $L(\sigma(\overline{P})^{-\lambda_p})$ can have dimension two is that it equal $\langle 1, z_{\sigma(P)} \rangle$. Hence $\sigma(z_p) = a_p + b_p z_{\sigma(P)} (a_p, b_p \in K)$. Since $S \subseteq S_2$, $S_2$ also saturates $L_1$ and so

$$\sigma(L_1) = \sigma(K(\langle z_p \mid P \in S_2 \rangle))$$

$$= K(\langle \sigma(z_p) \mid P \in S_2 \rangle)$$

$$= K(\langle a_p + b_p z_{\sigma(P)} \mid P \in S_2 \rangle)$$

$$= L_1, \text{ since } \sigma(P) \in S_2 \text{ whenever } P \text{ does.} \quad \Box$$

**Lemma 4.** Let $F$ be an algebraic function field over $K$ and let $P_1, P_2, \ldots, P_r$ be distinct primes of $F$; $m_1, m_2, \ldots, m_r$ arbitrary integers. Then in any divisor class of $F$ whose degree is at least $2g_F + \sum_{i=1}^{r} m_i$, there is a divisor $A$ such that $V_p(A) = m_i$. 
1 ≤ i ≤ r, and \( V_q(A) ≥ 0 \) if \( Q \notin \{ P_1, P_2, \ldots, P_r \} \).

**Proof:** Let \( D = \prod_{i=1}^{r} P_i^{m_i} \) and \( D_i = DP_i \), \( 1 ≤ i ≤ r \). Let \( C \) be an arbitrary divisor of the divisor class in question. Then
\[
d(CD^{-1}) ≥ 2g_F \quad \text{and} \quad d(\langle D_i \rangle^{-1}) \geq 2g_F - 1.
\]
It follows from the Riemann-Roch theorem that \( L(C^{-1}D_i) \) is a proper subspace of \( L(C^{-1}D) \). Now \( K \) is algebraically closed and hence infinite; so by a well known elementary result it follows that \( \bigcup_{i=1}^{r} L(C^{-1}D_i) \neq L(C^{-1}D) \). Let \( f \) belong to
\[
L(C^{-1}D) - \bigcup_{i=1}^{r} L(C^{-1}D_i)
\]
Then the divisor \( A = (f)_F \) \( C \) is in the same divisor class as \( C \) and an easy verification shows that \( A \) has the desired properties. \( \square \)

§2. Automorphism groups of prime order.

We now prove a theorem which will later help us get started when we use induction on \( |G| \), \( G \) a solvable group, to prove that every solvable group can be realized as the group of automorphisms of a suitable function field over \( K \).

**Theorem 2.** Let \( H \) be a group of prime order \( \ell \). Then, for \( x \) a transcendental over \( K \), there is a Galois extension \( F_H \) of \( K(x) \) of degree \( \ell \) such that \( \text{Gal}(F_H/K(x)) = \text{Aut}(F_H/K) \); i.e. every automorphism of \( F_H \) over \( K \) fixes \( x \).
Proof: We first show that given any integer \( n \geq 5 \), there is always a set \( T \) of primes of \( K(x) \) with \( n = |T| \) and the property that the only automorphism of \( K(x) \) that permutes \( T \) is the identity. The method is the one given in [23]. Choose any set \( T' = \{P_1, P_2, \ldots, P_{n-1}\} \) of \( n - 1 \) primes of \( K(x) \). Let \( Z \) be the automorphism group of \( K(x)/K \) and let \( L = \{\sigma \in Z \mid \sigma(T') \cap T' \geq n - 2\} \).

Since any automorphism of \( K(x) \) is determined by its action on any three primes, \( L \) is a finite set. For \( \sigma \in L \), let

\[
W_\sigma = \{P \notin T' \mid \sigma(P) = P \text{ or } \sigma(P) \in T'\}.
\]

Any non-identity automorphism of \( K(x) \) fixes at most two primes and for any \( \sigma \in L \) there is at most one prime \( P \notin T' \) for which \( \sigma(P) \in T' \). So \( W_\sigma \) contains at most three primes. Hence we can choose \( P_n \notin U W_\sigma \ (\sigma \in L , \sigma \neq 1) \).

Set \( T = T' \cup \{P_n\} \).

Now if \( \sigma \in Z \) with \( \sigma(T) = T \), we must have \( \sigma \in L \). However, by our choice of \( P_n \) the identity is the only element in \( L \) which maps \( P_n \) onto an element of \( T \). Therefore the identity is the only automorphism of \( K(x)/K \) which maps \( T \) onto itself.

Now suppose \( n \geq 5 \) and assume that a set \( T \) has been chosen as above. For \( 1 \leq i \leq n \), let \( x - a_i \) be a prime element for \( P_i, a_i \in K \). (\( 1/x \) if \( P_i \) is the infinite prime of \( K(x) \)). Let \( |T| = n \).
Now it is clear from the manner in which $T$ was constructed that we can ensure that: If $\ell \neq p$, then $T$ does not contain the infinite prime of $K(x)$ and $|T| = \ell(\ell+2) = n$. If $\ell = p$, then $T$ contains the infinite prime $P_\infty$ of $K(x)$.

Consider the extension $F_H = K(x,y)$ of $K(x)$ given by

$$y^\ell = \prod_{P_i \in T} (x - a_i) \quad \text{if} \quad \ell \neq p$$

and by

$$y^\ell - y = \prod_{P_i \in T} \frac{x^{\lambda}}{\prod_{P_i \neq P_\infty}} \quad \text{if} \quad \ell = p$$

where $\lambda$ is chosen so that $\lambda - |T| + 1$ is prime to $\ell$ and is larger than $n - 1 + \frac{p(\ell+1)}{p-1}$.

In either case it follows (see [7]) that the primes in $K(x)$ that ramify in $K(x,y)$ are precisely those in $T$. Let $F_i$ denote the (unique) prime of $F_H$ lying above $P_i$.

If $\ell \neq p$ we have (see [1]) that

$$\frac{(dx)_{F_H}}{(y)_{F_H}} = \left(\text{Con}_K(x)/F_H P_\infty^\ell\right)^{t-2} \left(\prod_{P_i \in T} \frac{x}{P_i} \right)^{t-2}$$

So if $P$ is any unramified prime (over $K(x)$) of $F_H$ and if $x - a$ is a prime element of $P \cap K(x)$, assuming that $P \cap K(x) \neq P_\infty$, then for $0 \leq \lambda \leq \ell$ the differential $\frac{(x-a)^\lambda}{y}$ is holomorphic, the exponent of $P$ in it is $\lambda$ and the exponent of the infinite primes (i.e. those lying above $P_\infty$) is $\ell - \lambda$. Thus every prime of $F_H$ that is unramified over $K(x)$ has $1,2,\ldots,\ell$ as gap numbers.
If $\ell = p$ we have (see [1])

$$
(dx)_{F_H} = \frac{1}{(p^2)^{2p}} \prod_{P_i \in T, P_i \neq P_{\infty}} (P_i)^2 (p-1) (P_{\infty})^{(\lambda - n + 1)(p-1)}.
$$

Making use of the inequality $\lambda > n - 1 + \frac{p(\ell + 1)}{p-1}$ we can verify easily as before that if $x - a$ is a prime element for $P \cap K(x)$, $P$ unramified over $k(x)$, then for $0 \leq \lambda < \ell - 1$ the differential $(x-a)^\lambda(dx)$ is holomorphic and contains $P$ to exponent $\lambda$.

Thus, whether or not $\ell = p$, we see that the numbers $1, 2, \ldots, \ell$ are all gap numbers of all primes of $F_H$ unramified over $K(x)$.

However, $\ell$ is obviously a pole number for all the $P_i$, $1 \leq i \leq n$. Consequently, if $\sigma$ is any automorphism of $F_H$ over $K$, $\sigma$ must map the $P_i$ ($1 \leq i \leq n$) onto themselves.

Consequently, $\sigma\left(\frac{P_i^{\ell}}{P_j^{\ell}}\right) = \left(\frac{P_i}{P_j}\right)^{\ell}$ where $1 \leq i \neq j \leq n$. Noting that $\frac{x-a_1}{x-a_2}$ has divisor $\frac{P_i^{\ell}}{P_j^{\ell}}$ in $F_H$, we see that $\sigma\left(\frac{x-a_1}{x-a_2}\right) = \sigma\left(\frac{x-a_1}{x-a_j}\right)$ for some $c \in K$. Since $a_1 \neq a_2$ and $a_1 \neq a_j$, $K(x) = K\left(\frac{x-a_1}{x-a_2}\right) = K\left(c \cdot \frac{x-a_1}{x-a_j}\right)$; it follows that $\sigma$ maps $K(x)$ onto itself, i.e. $\sigma$ is an automorphism when restricted to $K(x)$. This restriction maps the elements of $T$ onto themselves and so, by our construction of $T$, this means that $\sigma$ is the identity on $K(x)$. 
§3. Imbedding problems and cohomology.

3.1 Imbedding problems. Let \( k \) be a field and let \( k' \) be a finite Galois extension of \( k \). Let \( G \) be a finite group (not necessarily solvable) which contains a normal subgroup \( N \) such that there is an isomorphic mapping \( \varphi \) from \( G/N \) onto the Galois group \( \text{Gal}(k'/k) \). We shall say that the problem \( P(k'/k,G/N,\varphi) \) "has a solution \((L,\psi)\)" if we can imbed \( k' \) in a finite Galois extension \( L \) of \( k \) so that there is an isomorphism \( \psi \) from \( G \) onto the Galois group \( \text{Gal}(L/k) \), which maps \( N \) onto the Galois group \( \text{Gal}(L/k') \) and induces, in a natural way, the given isomorphism \( \varphi \) from \( G/N \) onto \( \text{Gal}(k'/k) \). We are using here the terminology of Iwasawa [9].

This section deals with imbedding problems \( P(F_1/K(x),G/N,\varphi) \), where \( x \) is a transcendental over the algebraically closed field \( K \), \( G \) is a solvable group and \( N \) an elementary abelian normal subgroup of \( G \). We seek solutions \((L,\psi)\) with \( L/F_1 \) having suitable ramification. In the next section, we use this ramification behavior and the results of §1 to show that \( L \) can be chosen so that not only is \( \text{Gal}(L/K(x)) \) isomorphic to \( G \), but \( \text{Aut}(L/K) \) is also isomorphic to \( G \); that is, every automorphism of \( L \) over \( K \) fixes \( x \), and hence every such automorphism necessarily belongs to \( \text{Gal}(L/K(x)) \).

From now on \( N \) will always denote an elementary abelian group. Suppose \( N \) is an elementary abelian \( t \)-subgroup of a group \( G \), \( N \)
normal in \( G \). \( \Gamma \) will always denote the group \( G/N \). \( \Gamma \) operates on \( N \) by the action

\[
\sigma(u) = s u s^{-1} \quad \text{where} \quad \sigma \in \Gamma, \; u \in N \; \text{and}
\]

\( s \) is an element of \( G \) belonging to the coset \( \sigma \). Clearly,

\[
(\sigma \tau)(u) = \sigma(\tau(u)).
\]

Let \( |N| = \ell^r \), \( \ell \) prime. We choose a basis \( u_1, u_2, \ldots, u_r \) of \( N \). Then

\[
\sigma(u_j) = \prod_{i=1}^{r} a_{ij}(\sigma) u_i, \; 1 \leq j \leq r,
\]

where the integers \( a_{ij}(\sigma) \) are uniquely determined modulo \( \ell \). Thus \( \sigma \) induces a representation

\[
(3.1.1) \quad \bar{\alpha}(\sigma) = (\bar{a}_{ij}(\sigma))
\]

of \( \Gamma \) in the prime field \( GF(\ell) \) with \( \ell \) elements; here the \( \bar{a}_{ij}(\sigma) \) are just the residue classes of \( a_{ij} \) modulo \( \ell \). We are assuming that the field \( K \) is algebraically closed. Hence it contains the \( \ell \)th roots of unity for every integer \( \ell \). In this context we can interpret the results in [9] as follows: (whenever it is used, \( x \) always denotes an arbitrarily fixed transcendental over \( K \).

### 3.2 The case \( \ell \neq p \).

Let \( P(F_1/K(x), G/N, \varphi) \) be an embedding problem with \( N \) an elementary abelian normal \( \ell \)-subgroup of \( G \), \( \ell \neq p \). Then there is a group \( G' \) which also has an elementary abelian normal \( \ell \)-subgroup \( N' \), and a problem \( P(F_1/K(x), G'/N', \varphi') \) such that
(i) \( G'/N' \) is isomorphic to \( G/N \). Let \( \Gamma' = G'/N' \cong \Gamma \).

(ii) There is a suitable basis of \( N' \) relative to which the representation \( \overline{A}'(\sigma') \) as defined in (3.1.1) is in fact obtainable from an integer representation \( \overline{B}'(\sigma') \) when the components of the latter are reduced modulo \( \ell \).

(iii) If the problem \( P(F_1/K(x),G'/N',\varphi') \) has a solution \( (L',\psi') \), then there is a subfield \( L \supseteq F_1 \) of \( L' \) which is Galois over \( K(x) \) and which, together with a suitable mapping \( \psi \), gives a solution \( (L,\psi) \) of the problem \( P(F_1/K(x),G/N,\varphi) \).

(In fact the above is true even if \( \ell = p \), but we shall not even need to consider \( P(F_1/K(x),G'/N',\varphi') \) when \( \ell = p \).)

We shall refer to \( P(F_1/K(x),G'/N',\varphi') \) as the equivalent reduced problem corresponding to \( P(F_1/K(x),G/N,\varphi) \).

Let \( |N'| = \ell^{r'} \) and let \( V_{F_1} \) denote the direct product of \( r' \) copies of the multiplicative group \( F_1^* \) of \( F_1 \). For any \( \sigma' \) in \( \Gamma' \) and \( \xi' = (\xi'_1,\xi'_2,\ldots,\xi'_r) \) in \( V_{F_1} \), we define \( \sigma'(\xi') \) to be the element of \( V_{F_1} \) whose \( i \)th component is \( \prod_{j=1}^{r'} \sigma'(\xi'_j) b_{ij}(\sigma') \), where \( (b_{ij}(\sigma')) = \overline{B}'(\sigma') \) is the matrix mentioned in (ii) above. Of course, \( \sigma'(\xi'_j) \) denotes the image of \( \xi'_j \) under the automorphism \( \varphi'(\sigma') \) in \( \text{Gal}(F_1/K(x)) \).

Thus

\[
(3.2.1) \quad \sigma'(\xi') = (\ldots, \prod_{j=1}^{r'} \sigma'(\xi'_j) b_{ij}(\sigma'), \ldots)
\]

\( \text{ith} \) spot.
Let \( u_1', u_2', \ldots, u_{r'}' \) be a basis for \( N' \) (\( N' \) as in (11) above) and \( \chi_1, \chi_2, \ldots, \chi_{r'} \) be a basis for the character group of \( N' \) dual to this basis for \( N' \). Thus \( \chi_1(u_1') = \zeta, \chi_j(u_j') = 1 \) (\( i \neq j \)) for \( 1 \leq i, j \leq r' \), where \( \zeta \) is an arbitrarily fixed primitive \( \ell \)-th root of unity in \( K \).

Then for any \( u' \in N' \) we set \( \chi(u') = (\chi_1(u'), \ldots, \chi_{r'}(u')) \).

We take a system of representatives \( x_{\sigma'} \) of \( \Gamma' = G'/N' \) in \( G' \) and put

\[
\begin{align*}
\chi_{\sigma', \tau'} &= u_{\sigma', \tau' \chi_{\sigma', \tau'}} ; \quad \sigma', \tau' \in \Gamma', u_{\sigma', \tau'} \in N'.
\end{align*}
\]

One can verify that the 2-cochain \( \chi_{\sigma', \tau'} \) is in fact a 2-cocycle (see [9]). We can now formulate the following lemma 6 of [9]:

**Lemma 5.** In order that the problem \( P(F_{1}/K(x), G'/N', \varphi') \) have a solution \( (L', \varphi') \), it is necessary and sufficient that the 2-cocycle \( \chi_{\sigma', \tau'} \) be the coboundary of a 1-cochain \( \gamma_{\sigma'} \) of \( \Gamma' \) in \( V_{F_{1}} \) and that the 1-cochain \( \gamma_{\sigma'}^{L'} \) be the coboundary of a 0-cochain \( \alpha' = (\alpha_1', \ldots, \alpha_{r'}') \) such that the \( \alpha_i' \) \( (1 \leq i \leq r') \) are \( L \)-independent modulo \( (F_{1})^{L'} \). (Under these conditions, \( L' \) is in fact realizable as the field obtained from \( F_{1} \) by adjoining to it the \( L \)-th roots of \( \alpha_1', \ldots, \alpha_{r'}' \).) Thus we shall say that \( \alpha' \) "generates" \( L' \) over \( F_{1} \).
Now, in the above context, we can prove

Lemma 6. Let $\beta' = (\beta'_1, \beta'_2, \ldots, \beta'_r) \in V_{F_1}$. Then the element $\theta(\beta')$ of $V_{F_1}$ whose $i$th component is $\prod_{\sigma' \in \Gamma'} (\prod_{j=1}^{r'} \sigma'(\beta'_j))^{b'_{ij}(\sigma')}$ is a 0-cocycle.

Proof: We need to show that $\tau'(\theta(\beta')) = \theta(\beta')$ for every $\tau' \in \Gamma'$. Let $\theta(\beta') = (\delta'_1, \delta'_2, \ldots, \delta'_r)$. Then 3.2.1 yields that the $i$th component of $\tau'(\theta(\beta'))$ is $\prod_{j=1}^{r'} (\tau'(\delta'_j))^{b'_{ij}(\tau')}$, which by the definition of $\theta(\beta')$, is equal to

\[
\prod_{j=1}^{r'} \left( \tau' \left( \prod_{\sigma' \in \Gamma'} (\prod_{k=1}^{r'} (\tau'(\sigma'))^{b'_{jk}(\sigma')})^{b'_{ij}(\tau')} \right) \right)
\]

\[
= \prod_{j=1}^{r'} \left\{ \prod_{\sigma' \in \Gamma'} (\tau'(\sigma'))^{b'_{jk}(\sigma')} \right\}^{b'_{ij}(\tau')}
\]

\[
= \prod_{\sigma' \in \Gamma'} \left( \prod_{k=1}^{r'} ((\tau'(\sigma'))^{b'_{jk}(\sigma')})^{b'_{ik}(\tau')} \right)
\]

\[
= \prod_{\sigma' \in \Gamma'} \left( (\tau'(\sigma'))^{b'_{ik}(\tau')} \right) = b'_{i1},
\]

since $b'(\tau'(\sigma')) = \overline{b}'(\tau')\overline{b}'(\sigma')$ and $\tau'(\sigma')$ ranges over $\Gamma'$ as $\sigma'$ does. $\square$
**Definition 3.** Let $F$ be an algebraic function field over $K$ and $L$ a finite Galois extension of $F$. A set $T$ of primes of $L$ is called **non-conjugate** over $F$ if each prime of $T$ is unramified over $F$ and no two distinct primes of $T$ are conjugate over $F$. A collection $T_1, T_2, \ldots, T_h$ of sets of primes of $L$ is said to be **totally disjoint** over $F$ if

1. $T_i \cap T_j$ is empty for $i \neq j$ ($1 \leq i, j \leq h$).
2. $\bigcup_{i=1}^{h} T_i$ is non-conjugate over $F$.

**Lemma 7.** In the preceding cohomological context, let $\alpha' = (\alpha'_1, \alpha'_2, \ldots, \alpha'_{r'})$ be an arbitrary $0$-cochain (i.e. $\alpha' \in V_{F_1}$) of $\Gamma'$ in $V_{F_1}$. Let $S = \{P_1, P_2, \ldots, P_n\}$ be a set of primes of $F_1$ such that $S$ is non-conjugate over $K(x)$. Let $\mathbf{C} = (C_{ij})$ be any integer matrix of size $r' \times n$. Then, if $\theta$ is the map of lemma 6, there exists a $0$-cochain $\beta' = (\beta'_1, \ldots, \beta'_{r'})$ of $\Gamma'$ in $V_{F_1}$ such that

$$V_{F_1}(\alpha'_i \cdot \delta'_i) = C_{ij} \pmod{\ell}; \quad 1 \leq j \leq n, \quad 1 \leq i \leq r',$$

where $\theta(\beta') = (\delta'_1, \delta'_2, \ldots, \delta'_{r'})$. Moreover, $\beta'$ can be so chosen as to ensure that the $r'$ components of $\alpha' \cdot \theta(\beta')$ are $\ell$-independent modulo $(F_1^*)^\ell$.

**Proof:** Let $S'$ be a set of primes of $F_1$ that is totally disjoint from $S$ (hence $S'$ is also non-conjugate over $F_1$) and...
such that \( |S'| = r' \). Let \( C' = (c'_{ij}) \) be the matrix of size 
\( r' \times (n + r') \) whose first \( n \) columns are those of \( C \) and whose last 
\( r' \) columns are those of the \( r' \times r' \) identity matrix. Thus

\[
C' = \begin{bmatrix}
c_{11} & c_{12} & \cdots & c_{1n} & 1 & 0 & 0 & \cdots & 0 \\
c_{21} & c_{22} & \cdots & c_{2n} & 0 & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
c_{r'1} & c_{r'2} & \cdots & c_{r'n} & 0 & 0 & 0 & \cdots & 1
\end{bmatrix}.
\]

Let us write \( S' = \{p_{n+1}, p_{n+2}, \ldots, p_{n+r'}\} \) and define the 
\( r' \times (n + r') \) matrix \( D' = (d'_{ij}) \) by \( d'_{ij} = v_{p_j}(\alpha'_{i}) \).

Using the approximation theorem for valuations, choose the 
elements \( \beta'_{i} \) \((1 \leq i \leq r')\) as follows:

(3.2.3) \[ v_{p_j}(\beta'_{i}) = c'_{ij} - d'_{ij} ; \quad 1 \leq j \leq n + r' , \quad 1 \leq i \leq r' \]

(3.2.4) \[ v_{Q}(\beta'_{i}) = 0 \] \((1 \leq i \leq r')\) if \( Q \) is conjugate but 
not equal to an element of \( S U S' \).

(Here the congruences are modulo \( \mathfrak{A} \).)

Now suppose \( p_j \in S U S' \). Let us calculate \( v_{p_j}(\delta'_{i}) \). This

is equal to
\[ V_{p_j} \left( \sigma' \in \Gamma' \right) = V_{p_j} \left( \prod_{k=1}^{r'} \beta_k^{b_{ik}(0^i)} \right) \]

\[ = V_{p_j} \left\{ \left( \prod_{k=1}^{r'} \beta_k^{b_{ik}(e')} \right) \prod_{\sigma' \in \Gamma' - \{e'\}} \left( \prod_{k=1}^{r'} \sigma' \beta_k^{b_{ik}(\sigma')} \right) \right\} \]

(where \( e' \) is the identity element of \( \Gamma' \))

\[ = V_{p_j} \left( \prod_{k=1}^{r'} \beta_k^{b_{ik}(e')} \right) (\text{mod } \ell), \text{ since} \]

\[ V_{p_j} \left( \sigma' \beta_k^{i} \right) = V^{(\sigma')^{-1}(p_j)} \left( \beta_k^i \right) = 0 \left( \text{mod } \ell \right) \text{ if } \sigma' \]

is not the identity (by (3.2.4)).

However, note that \( b_{ik}^{i}(e') = \overline{B}_i^{i}(e') \) is an integer matrix which when reduced modulo \( \ell \) gives the matrix \( \overline{A}_i^{i}(e') \) (see (3.1.1)) with entries in \( GF(\ell) \). But \( \overline{A}_i^{i}(e') \) is the trivial matrix. Hence \( b_{ik}^{i}(e') = 1 \left( \text{mod } \ell \right) \) if \( i = k \) and \( b_{ik}^{i}(e') = 0 \left( \text{mod } \ell \right) \) if \( i \neq k \).

Hence we now have \( V_{p_j} (\delta_i^{i}) = V_{p_j} \left( \prod_{k=1}^{r'} \beta_k^{b_{ik}(e')} \right) = V_{p_j} (\beta_i^i) = C_{ij} - d_{ij} \left( \text{mod } \ell \right), \) by (3.2.3). Hence \( V_{p_j} (\alpha_i^i \cdot \delta_i^i) = V_{p_j} (\alpha_i^i) + V_{p_j} (\delta_i^i) = d_{ij} + C_{ij} - d_{ij} \left( \text{mod } \ell \right) = C_{ij} \left( \text{mod } \ell \right). \) But note that \( C_{ij} = C_{ij} \) if \( 1 \leq j \leq n \). Hence if \( 1 \leq j \leq n \) and \( 1 \leq i \leq r' \), we have \( V_{p_j} (\alpha_i^i \cdot \delta_i^i) = C_{ij} \left( \text{mod } \ell \right) \) which is part of what we wanted to prove.
All that is left to establish is the statement about \( \ell \)-independence. That is, we need to show that \( \alpha_{1}^{\delta_{1}} \alpha_{2}^{\delta_{2}} \cdots \alpha_{r}^{\delta_{r}} \) are \( \ell \)-independent modulo \( (F_{\ell})^{*} \). Indeed, suppose
\[
\prod_{i=1}^{r'} (\alpha_{i}^{\delta_{i}})^{a_{i}^{i}} \in (F_{\ell})^{*}. \]
Then for \( 1 \leq j \leq r' \) we have
\[
\ell \mid V_{p_{n+j}} \left( \prod_{i=1}^{r'} (\alpha_{i}^{\delta_{i}})^{a_{i}^{i}} \right) = \sum_{i=1}^{r'} a_{i}^{i} V_{p_{n+j}} (\alpha_{i}^{\delta_{i}}),
\]
and so \( \ell \)-independence is ensured. \( \square \)

3.3 The case \( \ell = p \). We now return to the problem
\[ P(F_{\ell}/K(x),G/N,\varphi), \]
where \( N \) is an elementary abelian normal \( p \)-subgroup of \( G \), \( p = \text{characteristic of } K \). As in 3.1, we obtain the representation of \( \Gamma = G/N \) in the prime field \( GF(p) \). This representation is given by \( \overline{A}(\sigma) \) as in 3.1.1. However, since \( \text{char}(K) = p \) we may consider \( \overline{A}(\sigma) \) as a representation of \( \Gamma \) in the field \( K(x) \). This obviates any further reduction which was done in the \( \ell \neq p \) case; i.e., we do not need to consider the equivalent reduced problem
\[ P(F_{\ell}/K(x),G'/N',\varphi'), \]
Instead, we simply set \( B(\sigma) = \overline{A}(\sigma) \) and denote by \( V_{F_{\ell}} \) the direct sum of \( r \) copies of the additive group of \( F_{\ell} \). Then we define an action of \( \Gamma \) on \( V_{F_{\ell}} \) by
\[
(3.3.1) \quad \sigma(\xi) = (\ldots, \sum_{j=1}^{r} \text{b}_{ij} (\sigma) \sigma(\xi_{j}), \ldots),
\]
where \( \text{b}_{ij} \) is the \( i \)th spot.
where \( \xi = (\xi_1, \xi_2, \ldots, \xi_r) \) and \( (b_{ij}(\sigma)) = B(\sigma) \).

We then take additive characters \( \chi_1, \chi_2, \ldots, \chi_r \) of \( N \) whose values are in the prime field of \( K(x) \) and are such that

\[
\chi_i(u_j) = \begin{cases} 
0 & \text{if } i \neq j \\
1 & \text{if } i = j
\end{cases}
\]

(of course, \( u_1, u_2, \ldots, u_r \) is a basis for \( N \) relative to which we have the given representation \( \overline{A}(\sigma) \)). For \( u \in N \), let \( \chi(u) = (\chi_1(u), \ldots, \chi_r(u)) \) and for a factor set \( u_{\sigma, \tau} \) of the extension \( G \) over \( N \) (as in 3.2) we define as in 3.2.2

\[
\chi_{\sigma, \tau} = \chi(u_{\sigma, \tau})
\] (3.3.2)

Again one verifies that the 2-cochain \( \chi_{\sigma, \tau} \) is a 2-cocycle of \( \Gamma \) in \( V_{F_1} \) and we can state

**Lemma 5**. In order that the problem \( P(F_1/K(x), G/N, \psi) \) have a solution \( (L, \psi) \) it is necessary and sufficient that the 2-cocycle \( \chi_{\sigma, \tau} \) be the coboundary of a 1-cochain \( \gamma_\sigma \) and that the 1-cochain \( \gamma_\sigma^P - \gamma_\sigma \) is the coboundary of a 0-cochain \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r) \) such that the \( \alpha_i (1 \leq i \leq r) \) are \( GF(p) \)-independent modulo \( P_p(F_1) \).

(\( GF(p) \) is being considered as the prime field of \( K(x) \).) Under these conditions \( L \) is in fact realizable as the field obtained from \( F_1 \) by adjoining to it \( \overline{\beta}_1, \overline{\beta}_2, \ldots, \overline{\beta}_r \) where \( \overline{\beta}_1^P - \overline{\beta}_i = \alpha_i (1 \leq i \leq r) \).
(Thus we shall say that \( \alpha \) "generates" \( L \) over \( F_1 \).)

**Proof**: See 1.9 of [9]. \( \square \)
In the above context we have

**Lemma 6'.** Let \( \beta = (\beta_1, \beta_2, \ldots, \beta_r) \in V_{F_1} \). Then the element \( \theta(\beta) \) of 
\( V_{F_1} \) whose \( i^{th} \) component is

\[
\sum_{\sigma \in \Gamma} \left( \sum_{j=1}^{r} b_{ij}(\sigma) \sigma(\beta_j) \right)
\]

is a 0-cocycle.

**Proof:** Similar to that of lemma 6. \( \square \)

**Lemma 7'.** In the cohomological context of 3.3, let \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r) \)
be an arbitrary 0-cochain and let \( S = \{P_1, P_2, \ldots, P_n, P_{n+r+1}, \ldots, P_{n+r+m}\} \)
be a set of primes of \( F_1 \) of size \( n + m \) (the choice of this somewhat
unusual notation will become clear in the proof) and let \( S \) be non-
conjugate over \( K(x) \). Let \( C = (c_{ij}) \) be an \( r \times (n + m) \) matrix

\[
\begin{pmatrix}
c_{11} & c_{12} & \cdots & c_{1n} & c_{1n+r+1} & c_{1n+r+2} & \cdots & c_{1n+r+m} \\
c_{21} & c_{22} & \cdots & c_{2n} & c_{2n+r+1} & c_{2n+r+2} & \cdots & c_{2n+r+m} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
c_{r1} & c_{r2} & \cdots & c_{rn} & c_{rn+r+1} & c_{rn+r+2} & \cdots & c_{rn+r+m}
\end{pmatrix}
\]

with integer entries such that

\[
c_{ij} < \min \left(0, V_{F_1}(\alpha_i) \right) \text{ for } 1 \leq i \leq r; 1 \leq j \leq n.
\]

Then, if \( \theta \) is the mapping of lemma 6', there exists a 0-cochain
\( \beta = (\beta_1, \beta_2, \ldots, \beta_r) \) of \( \Gamma \) in \( V_{F_1} \) for which
\[ v_p(\alpha_1 + \delta_1) = c_{ij} \quad (1 \leq j \leq n \text{ and } 1 \leq i \leq r) \]

\[ v_p(\alpha_1 + \delta_1) \geq \min (0, c_{ij}, v_p(\alpha_1)) \]

\[ (1 \leq i \leq r \text{ and } n + r + 1 \leq j \leq n + r + m) \]

where \( \theta(\beta) = (\delta_1, \delta_2, \ldots, \delta_r) \). Moreover \( \beta \) can be so chosen as to ensure that the \( r \) components of \( \alpha + \theta(\beta) \) are \( \text{GF}(p) \)-independent modulo \( p_\beta(F_1) \).

**Proof:** We proceed as in lemma 7, augmenting \( S \) by a set \( S' \) totally disjoint from it, \( |S'| = r \). Let \( S' = \{P_{n+1}, P_{n+2}, \ldots, P_{n+r}\} \). Again, we augment the matrix \( C \) to a matrix \( C' \) of dimension \( r \times (n + r + m) \) where

\[
(c'_{ij}) = C' =
\begin{pmatrix}
    c_{11} & c_{12} & \cdots & c_{1n} & \lambda & \lambda & \cdots & \lambda & c_{1n+r+1} & \cdots & c_{1n+r+m} \\
    c_{21} & c_{22} & \cdots & c_{2n} & \lambda & \lambda & \cdots & \lambda & c_{2n+r+1} & \cdots & c_{2n+r+m} \\
    \vdots & & & & & & & & & \vdots \\
    c'_{r1} & c'_{r2} & \cdots & c'_{rn} & \lambda & \lambda & \cdots & \lambda & c'_{rn+r+1} & \cdots & c'_{rn+r+m}
\end{pmatrix}
\]

where \( \lambda \) is an integer, \( p \nmid \lambda \); and \( \lambda < v_p(\alpha_1) \), \( 1 \leq j \leq r \text{ and } 1 \leq i \leq r \). In other words \( c'_{ij} < v_p(\alpha_1) \)

\[ (1 \leq i \leq r \text{ and } 1 \leq j \leq n + r) \]

Now the approximation theorem for valuations can be used to choose \( \beta_1, \beta_2, \ldots, \beta_r \) so that:
(3.3.3) \( V_{P_j}(\beta_i) = c_{ij}^d \) (\( 1 \leq j \leq n + r \) and \( 1 \leq i \leq r \))

(3.3.4) \( V_{P_j}(\beta_i) \geq c_{ij}^d \) (\( n + r + 1 \leq j \leq n + r + m \) and \( 1 \leq i \leq r \))

(3.3.5) \( V_Q(\beta_i) \geq 0 \), \( 1 \leq i \leq r \) if \( Q \) is conjugate but not equal to an element of \( S \cup S' \).

Then, if \( P_j \in S \cup S' \), we have

\[
V_{P_j}(\alpha_i + \delta_i) = V_{P_j}(\alpha_i + \sum_{\sigma \in \Gamma} \sum_{k=1}^{r} b_{ik}(\sigma) \sigma(\beta_k))
\]

\[
= V_{P_j}(\alpha_i + \sum_{k=1}^{r} b_{ik}(e) \beta_k + \sum_{\sigma \in \Gamma - \{e\}} \sum_{k=1}^{r} b_{ik}(\sigma) \sigma(\beta_k))
\]

(where \( e \) is the identity of \( \Gamma \); so \( b_{ik}(e) \) is the identity matrix)

\[
= V_{P_j}(\alpha_i + \beta_i + \sum_{\sigma \in \Gamma - \{e\}} \sum_{k=1}^{r} b_{ik}(\sigma) \sigma(\beta_k))
\]

Now let \( 1 \leq j \leq n + r \) and \( 1 \leq i \leq r \).

We then have \( V_{P_j}(\alpha_i) > c_{ij}^d = V_{P_j}(\beta_i) \) and for \( \sigma \neq e \) and \( 1 \leq k \leq r \) we have

(3.3.6) \( V_{P_j}(\sigma(\beta_k)) = V_{\sigma^{-1}(P_j)}(\beta_k) \geq 0 \) by (3.3.5).
Hence, since \( c_{ij} < 0 \), it follows that \( V_{p_j}(\alpha_i + \delta_i) = c'_{ij} \) (1 \( \leq i \leq r \); 1 \( \leq j \leq n + r \)).

In particular,

\[
V_{p_j}(\alpha_i + \delta_i) = c'_{ij} = c_{ij} \quad (1 \leq i \leq r; \ 1 \leq j \leq n) .
\]

Next, let \( n + r + 1 \leq j \leq n + r + m \) and 1 \( \leq i \leq r \). Then, since 3.3.6 still holds, it is clear that \( V_{p_j}(\alpha_i + \delta_i) \geq \min \)

\[
(0, V_{p_j}(\alpha_i + \beta_i)) \geq \min (0, \min (V_{p_j}(\alpha_i), V_{p_j}(\beta_i)))
\]

\[= \min (0, V_{p_j}(\alpha_i), V_{p_j}(\beta_i))
\]

\[\geq \min (0, V_{p_j}(\alpha_i), c'_{ij}) \text{ by 3.3.4}
\]

\[= \min (0, V_{p_j}(\alpha_i), c_{ij}) \text{ since } c'_{ij} = c_{ij},
\]

which is what we want to show.

To prove the statement about GF(p)-independence, assume that

\[
\sum_{i=1}^{r} k_i(\alpha_i + \delta_i) \in F_p(F_1), \ k_i \in K \ (1 \leq i \leq r).
\]

Then \( \sum_{i=1}^{r} k_i(\alpha_i + \delta_i) = \ell^{p} - \ell_1 \) where \( \ell_1 \in F_1 \). If some \( k_i \) is non-zero, then

\[
V_{p_{n+1}}(k_i(\alpha_i + \delta_i)) = V_{p_{n+1}}(\alpha_i + \delta_i) = c'_{i,n+1} = \lambda.
\]
But $V_{p_{n+1}}(k_j(\alpha_j + \delta_j)) \geq V_{p_{n+1}}(\alpha_j + \delta_j) = c'_j$, $n+1 = \lambda > k$. For

$j \neq 1$. Hence $V_{p_{n+1}}(\sum_{i=1}^{r} k_i(\alpha_i + \delta_i)) = \lambda = V_{p_{n+1}}(k_1^p - k_1) = p V_{p_{n+1}}(k_1) \text{ since } \lambda < 0$. So $p | k$, a contradiction. Hence

$k_i = 0, 1 \leq i \leq r$ and so $\alpha_1 + \delta_1, \alpha_2 + \delta_2, \ldots, \alpha_r + \delta_r$ are

K-independent modulo $GF(p)$-independent modulo

$\mathfrak{p}_p(F_1)$. \hfill \Box$

\section{The main result.}

In this section we go about the task of proving that any solvable
group $G$ can be realized as the group of automorphisms of a suitable
algebraic function field over $K$. Of course, by "automorphism" we
mean an automorphism that fixes $K$. The proof is accomplished in
steps. Assuming that for a transcendental $x$ over $K$, and a proper
normal elementary abelian subgroup $N$ of $G$, we have a Galois exten­
sion $F_1$ of $K(x)$ such that $Gal(F_1/K(x)) = Aut(F_1/K) = G/N$ (and
that this isomorphism is given by $\varphi$), we endeavor to find solutions
$(F, \psi)$ of $P(F_1/K(x), G/N, \varphi)$ such that every automorphism of $F$ over
$K$ restricts to an automorphism of $F_1$. This would, of course, ensure
that $Aut(F/K) = Gal(F/K(x)) = G$. From the results of $\S 3$, we shall see
that solutions of $P(F_1/K(x), G/N, \varphi)$ do exist which have suitable
ramification over $F_1$. It is precisely the nature of this ramification
which will enable us to show that every automorphism of $F$ over $K$
restricts to an automorphism of $F_1$. Lemma 3 plays a crucial role in
the argument.

In fact, if \( G \) is solvable with \(|G| = n\) we prove the following for \( n \geq 1\): \( P(n) \). If \( n = 1\), i.e. if \( G \) is trivial, there is an algebraic function field over \( K \) whose automorphism group is \( G \). If \( n > 1\), \( x \) transcendental over \( K \), there is a Galois extension \( F \) of \( K(x) \) depending on \( G \) such that \( \text{Gal}(F/K(x)) = \text{Aut}(F/K) \cong G \).

\( P(1) \) is a result of Cronheim [3] which states that the algebraic function field \( F = K(x,y) \) with \( y^q + y^{q-1} = x^{hq}(x+1) \) has no non-trivial automorphisms if \( q \geq 3 \) is a power of \( p \), \( h \geq q \) and \((h,q-1) = 1\). We prove \( P(n), \ n \geq 2 \) by induction on \( n \). P(2) is true because of theorem 2. So assume that \( P(2), P(3), \ldots, P(n-1) \) have been proved and let \( G \) be of order \( n \). Since \( G \) is solvable any minimal normal subgroup \( N \) of \( G \) is elementary abelian (see [18], page 112). If \( G = N \), then \( G \) is of prime order and we are done, once again by theorem 2. So assume \( G \neq N \). Then \( G/N \) is solvable, \(|G/N| > 2\) and \(|G/N| < |G| = n\). By our induction hypothesis there is a Galois extension \( F_1 \) of \( K(x) \) such that \( \text{Gal}(F_1/K(x)) = \text{Aut}(F_1/K) \cong G/N \). Let the isomorphism between \( \text{Gal}(F_1/K(x)) \) and \( G/N \) be given by \( \varphi \).

We now consider the problem \( P(F_1/K(x), G/N, \varphi) \). We need to distinguish two cases:

4.1 The case \( q \neq p \). Let \( P(F_1/K(x), G'/N', \varphi') \) be the equivalent reduced problem corresponding to \( P(F_1/K(x), G/N, \varphi) \) (see 3.2). Since we are assuming that the field \( K \) is algebraically closed, it follows from a result of Tsen [22] and from theorem 2 of Iwasawa [9] that the
following condition is sufficient for the existence of a solution to $P(F_1/K(x), G'/N', \varphi')$:

For any finite Galois extension $F$ of $K(x)$ and for any integer $m \geq 1$, the multiplicative group $F^*$ of $F$ contains $m$ elements $\alpha_1, \alpha_2, \ldots, \alpha_m$ such that the conjugates $\sigma(\alpha_i)$ of $\alpha_i$, $i = 1, 2, \ldots, m$, $\sigma \in \text{Gal}(F/K(x))$, are $L$-independent modulo $(F^*)^L$.

That this condition is met by $K(x)$ is a direct consequence of lemma 2 (i). Thus our problem $P(F_1/K(x), G'/N', \varphi')$ has a solution, say $(L', \psi')$ and, by property (iii) of $P(F_1/K(x), G'/N', \varphi')$ mentioned in 3.2, there is a subfield $L \supset F_1$ of $L'$ which, together with a suitable mapping $\psi$, provides a solution to $P(F_1/K(x), G/N, \varphi')$. We shall say that $L$ is a solution of $P(F_1/K(x), G/N, \varphi')$ associated with $L'$.

Noting that $|N'| = \ell^{r'}$ we now prove

**Lemma 8.** Let $T$ be any finite set of primes of $F_1$ unramified over $K(x)$ and let $S_1, S_2, \ldots, S_r'$ be a totally disjoint collection (over $K(x)$) of finite sets of primes of $F_1$ such that no prime of $T$ is equal or conjugate to any of the primes in $\bigcup_{i=1}^{r'} S_i$. Then the problem $P(F_1/K(x), G/N, \varphi)$ has a solution $(L_1, \psi_1)$ with the following properties: For any subfield $\bar{L}$ of $L_1$ such that $\bar{L} \supset F_1$ and $[\bar{L} : F_1] = \ell$ we have

(i) no prime of $T$ ramifies in $\bar{L}$.
(ii) for at least one \( i, \ 1 \leq i \leq r' \), every prime of \( S_i \) ramifies in \( L \).

**Proof:** It is clear that (i) is equivalent to the statement that no prime of \( T \) ramifies in \( L_1 \). So without loss in generality, we can assume that \( T \) is a non-conjugate set over \( K(x) \). For, if two primes of \( F_1 \) are conjugate over \( K(x) \) the normality of \( L_1 \) over \( K(x) \) ensures that one cannot ramify in \( L_1 \) without the other also ramifying.

So let \( T \) be non-conjugate. Then the collection \( T, S_1, S_2, \ldots, S_r \) is totally disjoint over \( K(x) \). We know that the equivalent reduced problem \( P(F_1/K(x), G'/N', \varphi') \) has a solution \( (L', \psi') \) by the discussion preceding this lemma. According to lemma 5 we have a \( 1 \)-cochain \( \gamma' \) and a \( 0 \)-cochain \( \alpha' \) satisfying the conditions stated therein. Then, according to lemma 7, we can find a \( 0 \)-cochain \( \beta' \) such that \( \theta(\beta') \) is a \( 0 \)-cocycle and such that, if \( \theta(\beta') = (\delta_1', \ldots, \delta_r') \), the components of \( \alpha' \cdot \delta_i' \) are \( 1 \)-independent modulo \((F_1^*)\) and the following holds:

For each \( i \), \( 1 \leq i \leq r' \), the primes of \( S_i \) all occur in \( \alpha_i' \delta_i' \) to exponent prime to \( \ell \) whereas they occur in \( \alpha_j' \delta_j' \) to exponent divisible by \( \ell \). Also \( \psi_p(\alpha_i' \delta_i') \) is divisible by \( \ell \) for \( 1 \leq i \leq r' \), \( P \in T \).

Since \( \theta(\beta') \) is a \( 0 \)-cocycle it follows that \( \alpha' \cdot \theta(\beta') \) has the same coboundary as \( \alpha' \) and thus \( \alpha' \cdot \theta(\beta') \) meets all the conditions of lemma 5 that were satisfied by \( \alpha' \). Thus, according
to lemma 5 again, $\alpha' \cdot \theta(\beta')$ "generates" a solution $(L_1', \psi_1')$ of $P(F_1/K(x), G'/N', \varphi')$. Let $(L_1, \psi_1)$ be a solution of $P(F_1/K(x), G/N, \varphi)$ associated with $L_1'$.

Now let $L \supseteq F_1$ be any subfield of $L_1$ (and hence of $L_1'$) such that $[L : F_1] = \ell$. We know from Kummer theory that $L = F_1(y)$ where $y^t = \prod_{i=1}^{r'} (\alpha_1^i \beta_1^i)^{t_1^i}$ where for $1 \leq i \leq r'$ we have $0 \leq t_1^i \leq \ell - 1$ and at least one of the $t_1^i$ is non-zero. For this $i$, every prime of $S_{1^-}$ occurs in the divisor of $y^t$ to exponent prime to $\ell$ and hence (see [7]) ramifies in $L$. Moreover, every prime of $T$ occurs in this divisor to exponent divisible by $\ell$ and so does not ramify in $L$. □

We can now prove the main result of 4.1.

**Theorem 3.** The problem $P(F_1/K(x), G/N, \varphi)$ has a solution $(F, \psi)$ such that $\text{Aut}(F/K) = G$.

**Proof:** Since $G = \text{Gal}(F/K(x)) \subseteq \text{Aut}(F/K)$ for any solution $(F, \psi)$, we need only show that every automorphism of $F$ over $K$ fixes $x$. However, since $\text{Aut}(F_1/K) = \text{Gal}(F_1/K(x))$ it follows that every automorphism of $F_1$ over $K$ fixes $x$. Hence we need only establish the existence of a solution $(F, \psi)$ such that every automorphism of $F$ over $K$ maps $F_1$ onto itself.

Let $P(F_1/K(x), G'/N', \varphi')$ be the equivalent reduced problem corresponding to $P(F_1/K(x), G/N, \varphi)$; let $|N'| = \ell^{r'}$, $|N| = \ell^r$.

Denote by $P_1, P_2, \ldots, P_s$ the primes of $F_1$ that ramify over $K(x)$ and let them occur to exponent $e_1, e_2, \ldots, e_s$, respectively, in
Let \( P_\infty \) denote the infinite prime of \( K(x) \).

Choosing \( I \) to be an infinite set of non-conjugate primes of \( F_1 \), it is clear from Lemma 1 that we can choose \( r' \) totally disjoint sets \( S'_1, S'_2, \ldots, S'_r \) (all contained in \( I \)) and such that:

\[
S'_i \text{ saturates } F_1 \quad (1 \leq i \leq r')
\]

Each \( S'_i \) is finite and \(|S'_i| \geq (g_{F_1} + 1)\ell + 1 \quad (1 \leq i \leq r')\).

Let \( \bar{t} \) be the maximum of the least pole numbers of primes of \( \bigcup_{i=1}^{r'} S'_i \).

Then we again find sets \( \bar{S}_1, \bar{S}_2, \ldots, \bar{S}_r \), each of which is finite, such that the collection \( \bar{S}_i \quad (1 \leq i \leq r') \) is totally disjoint and:

\[
\bar{S}_i = S'_i \quad (1 \leq i \leq r')
\]

\[
|\bar{S}_1| \geq \max \left\{ (2g_{F_1} + \bar{t} - 1 + 2 \frac{n}{\ell}), \frac{2g_{F_1} \ell(2\ell^{R-1} - 1) + 2(\ell^r - 1)^2 + 2\ell}{\ell - 1} \right\}
\]

where \( n = |G| \) and \( 1 \leq i \leq r' \).

We now divide the argument into two cases depending on whether \( r = 1 \) or \( r \geq 2 \). In the latter case we will have to invoke the inequality of Castelnuovo-Severi; but if \( r = 1 \) we can avoid using this inequality.

**Case (i):** \( r = 1 \). Lemma 8 assures us that there is a solution \((F_1, \psi)\) to the problem \( P(F_1/K(x), G/N, \varphi) \) such that all the primes in at least one of the sets \( \bar{S}_i \quad (1 \leq i \leq r') \) ramify in \( F \). For this \( i \), let \( \bar{S}_i = S \) and \( S'_i = S' \).
Let $F = F_1(y)$ with $y^\ell = \alpha \in F_1$ and let $S_1$ be the set of all primes of $F_1$ that ramify in $F$. Since some of the $p_1, p_2, \ldots, p_s$ could ramify in $F$ we can assume without loss in generality that $p_1', p_2', \ldots, p_s'$ do not ramify in $F$ whereas $p_{s+1}', \ldots, p_s$ do. We then have, see [7],

$$(\alpha)_{F_1} = \left( \prod_{Q \in S_1} q^Q \right) A_{1}^\ell,$$

involves no primes of $S_1$ and $q^Q (Q \in S_1)$ are integers prime to $\ell$.

Let $h_Q = \ell d_Q + r_Q$ where $0 < r_Q \leq \ell - 1$. Now use the approximation theorem to find a function $z \in F_1$ such that

$$(z)_{F_1} = \left( \prod_{Q \in S_1} q^Q \right) A_{2}^\ell,$$

involves no primes of $S_1$. Then

$$(z^\ell \alpha)_{F_1} = (z^\ell y^\ell)_{F_1} = ((zy)_{F_1})^\ell = \left( \prod_{Q \in S_1} q^Q \right) (A_{1} A_{2})^\ell = \frac{\left( \prod_{Q \in S_1} q^Q \right) A^\ell}{B^\ell},$$

say, where $AB$ involves no primes of $S_1$ and for $Q \in S_1$, $0 < r_Q \leq \ell - 1$.

Now let $P$ be any prime of $F_1$. Since the degree of $(z^\ell \alpha)_{F_1}$ is zero we must have

$$\ell d(B) = \ell d(A) + \sum_{Q \in S_1} r_Q \geq \ell d(A) + |S_1| \geq \ell d(A) + |S|.$$
Hence \( d(B) \geq d(A) + \frac{|S|}{\ell} \geq d(A) + 2e_{F_1} + \ell - 1 + \frac{2n}{\ell} \). Let \( \mu \) be an integer such that \( \mu \leq \ell - 1 \) (\( \mu \) could be negative). Noting that \( d(\text{Con}_K(x)/F_1\omega) = \frac{n}{\ell} \), we see from lemma 4 that there is a function \( f_{\mu,P} \) in \( F_1 \) such that \( (f_{\mu,P})_{F_1} B(A(\text{Con}_K(x)/F_1\omega)^2)^{-1} = P^{\mu} C_{\mu,P} \), where \( C_{\mu,P} \) is integral and prime to \( P \). Hence \( (f_{\mu,P})_{F_1} BA^{-1} = P^{\mu}(\text{Con}_K(x)/F_1\omega)^2 C_{\mu,P} \), \( C_{\mu,P} \) integral and prime to \( P \).

We now adopt the following convention: If \( Q \) is any prime of \( F_1 \) ramifying in \( F \) we write \( \mathcal{Q} \) for the unique prime of \( F \) lying above \( Q \). If \( A \) is any divisor of \( F_1 \) involving only primes unramified in \( F \), we write \( \mathcal{A} \) for the conorm of \( A \) in \( F \), i.e. \( \mathcal{A} = (\text{Con}_{F_1/F} A) \).

Let \( S_1 = S_1 - \{P_{s'} + 1, \ldots, P_s\} \). We clearly have

\[
\mathcal{D}_{F/K}(x) = \mathcal{C}_{1}^{e_1} \mathcal{C}_{2}^{e_2} \cdots \mathcal{C}_{s'}^{e_{s'}+1} \cdots \mathcal{C}_{s}^{e_{s'}} (\prod_{Q \in S_1} Q)^{\ell - 1},
\]

where

\[
e_{s'} + 1 = le_{s'} + i + \ell - 1 \quad (1 \leq i \leq s - s').
\]

Also

\[
(zy)_F = \left( \prod_{Q \in S_1} \mathcal{C}_Q^{r_Q} \right) \left( \prod_{Q \in S_1 - S_1'} \mathcal{C}_Q^{r_Q} \right)^{\mathcal{A}}, \quad 0 \leq r_Q \leq \ell - 1.
\]
Since \((dx)_F = (\text{Con}_{K(x)/F^\infty})^{-2} D_{F/K}\) we see that \((z^{-1}y^{-1}dx)_F = \frac{\mathcal{P}_{x_1} \cdots \mathcal{P}_{x_1}^{e_{s_1}} \mathcal{P}_{s_1}^{e_{s_1}+1} \cdots \mathcal{P}_{s_1}^{e_{s_1}''}}{(\pi_{Q \in S_1} Q^{\ell - 1 - q}) (\text{Con}_{K(x)/F^\infty})^{-2} \mathcal{P}_x} ,

where \(e_{s_1}' + 1 = e_{s_1}' + 1 - r_{s_1} > 0\). Hence we may write

\[(z^{-1}y^{-1}dx)_F = R \frac{\mathcal{P}_{x_1} \cdots \mathcal{P}_{x_1}^{e_{s_1}} (\text{Con}_{K(x)/F^\infty})^{-2} \mathcal{P}_x}{\mathcal{P}_x} ,
\]

where \(R\) is an integral divisor involving \(\mathcal{P}_{s_1}^{e_{s_1}}\) and the primes \(Q, Q \in S_1\).

Now let \(\mathcal{P}\) be a prime of \(F\) unramified over \(F^\infty\) and let \(P\) be the prime of \(F_1\) lying below \(\mathcal{P}\). Suppose \(\mu \leq \ell - 1\) is an integer. We saw that there is a function \(f_{\mu, P}\) in \(F_1\) such that

\[(f_{\mu, P})^{F_1}_{F_1} = P_1^{e_1} \cdots P_{s_1}^{e_{s_1}} (\text{Con}_{K(x)/F^\infty})^2 \cdot C_{\mu, P}, \text{ where } C_{\mu, P} \text{ is an integral divisor of } F_1 \text{ that is prime to } P .
\]

Hence \((f_{\mu, P})^{F_1}_{F_1} = P_1^{e_1} \cdots P_{s_1}^{e_{s_1}} (\text{Con}_{K(x)/F^\infty})^2 \cdot C_{\mu, P}, \text{ where } C_{\mu, P} \text{ is an integral divisor of } F \text{ which is prime to } \mathcal{P} .
\]

Thus \((f_{\mu, P} z^{-1}y^{-1}dx)_F = R \frac{\mathcal{P}_{x_1} \cdots \mathcal{P}_{x_1}^{e_{s_1}} \mathcal{P}_{s_1}^{e_{s_1}'} (\text{Con}_{F_1/F^\infty C_{\mu, P}})}{\mathcal{P}_x} , \quad \text{where} \quad R \frac{\mathcal{P}_{x_1} \cdots \mathcal{P}_{x_1}^{e_{s_1}} \mathcal{P}_{s_1}^{e_{s_1}'} (\text{Con}_{F_1/F^\infty C_{\mu, P}})}{\mathcal{P}_x} \text{ is integral. If } P \notin \{P_1, P_2, \ldots , P_{s_1}\} \text{ and } 0 \leq \mu \leq \ell - 1 \text{ it follows that the above differential is holomorphic and contains } \mathcal{P} \text{ to precisely the exponent } \mu .\)
If $P = P_1$, $1 \leq i \leq s'$, and $0 \leq \mu \leq \bar{t} - 1$ the differential $(f_\mu - e_\mu P z^{-1} y^{-1} dx)_F$ is also holomorphic and contains $\bar{P}$ to precisely the exponent $\mu$.

Hence if $\bar{P}$ is any prime of $F$ that is not ramified over $F_1$, the numbers $1, 2, \ldots, \bar{t}$ are gap numbers of $\bar{P}$.

Also note that $|S'| \geq (e_{F_1} + 1)\ell + 1$, that every prime of $S' \subseteq S \subseteq S_1$ ramifies in $F$ and that if $Q \in S'$ then the least pole number of $Q$ is $\leq \bar{t}$; and hence, for some $t \leq \bar{t}$, $\bar{t}$ is a pole number of $\bar{Q}$. Hence $\bar{Q}$ has a gap sequence distinct from that of any prime $\bar{P}$ of $F$ which is unramified over $F_1$. We can now invoke lemma 3 (note that $S'$ saturates $F_1$) to conclude that any automorphism of $F$ over $K$ maps $F_1$ onto itself.

Case (ii): $r \geq 2$. From lemma 8 we know that there is a solution $(F, \psi)$ to the problem $P(F_1/K(x), G/N, \varphi)$ such that for any subfield $\bar{L}$ of $F$ containing $F_1$, $[\bar{L}:F_1] = \ell$, all the primes in at least one of the $S_i$ ($1 \leq i \leq r'$) ramify in $\bar{L}$. Let $\sigma$ be any automorphism of $F$ over $K$. We want to show that $\sigma(F_1) = F_1$. If this were not true, the composite $F_1 \sigma(F_1)$ of $F_1$ and $\sigma(F_1)$ (in $F$) would properly contain $F_1$, and so there would be a subfield $\bar{L}$ of $F$ containing $F_1$ such that $\bar{L} \subseteq F_1 \sigma(F_1)$ and $[\bar{L}:F_1] = \ell$. Let $[F_1 \sigma(F_1):F_1] = d_1$ and let $[F_1 \sigma(F_1):\sigma(F_1)] = d_2$. Then since $[F:F_1] = \ell^\Gamma$ we must have $d_1 \leq \ell^\Gamma$ and $d_2 \leq \ell^\Gamma$. Moreover, it is obvious that the genera of $F_1$ and $\sigma(F_1)$ are the same, i.e. $e_{F_1} = e_{\sigma(F_1)}$. From the inequality of Castelnuovo-Severi (see [15], page 69)
we have \( g_{F_1} \sigma(F_1) \leq d_1 g_{F_1} + d_2 g_{\sigma(F_1)} + (d_1 - 1)(d_2 - 1) \) =

\[ d_1 g_{F_1} + d_2 g_{F_1} + (d_1 - 1)(d_2 - 1) \leq 2k^r g_{F_1} + (k^r - 1)^2. \]

Since \( \overline{L} \subset F_1 \sigma(F_1) \), we thus have

\[ (4.1.2) \quad g_{\overline{L}} \leq g_{F_1} \sigma(F_1) \leq 2k^r g_{F_1} + (k^r - 1)^2. \]

However, from the genus formula we have \( 2g_{\overline{L}} - 2 = k(2g_{F_1} - 2) + t_0(k - 1) \) where \( t_0 \) is the number of primes of \( F_1 \) that ramify in \( \overline{L} \). So, because at least one of the \( S_i \) is such that all primes in it ramify in \( \overline{L} \), it follows that \( t_0 \geq \min_{1 \leq i < r, 1 \leq j \leq r,} |S_j| \geq \frac{2g_{F_1} - l(2k^r - 1 - 1) + 2(k^r - 1)^2 + 2l}{k - 1} \). Using this inequality in the genus formula above yields, on simplification, \( g_{\overline{L}} \geq 1 + \frac{2g_{F_1} k^r + (k^r - 1)^2}{k - 1} \), which contradicts \((4.1.2)\) above. Hence \( g(F_1) = F_1 \) and our proof is complete. \( \square \)

Remark 1. In the proof of theorem 3 we saw that we could obtain solutions \( F \) of \( P(F_1/K(x), G/N, \varphi) \) in which the number of primes ramifying over \( F_1 \) could be made as large as desired. In other words the solution fields can be made to have arbitrarily large genus. In particular, the number of solution fields \( F \) obtainable by the construction method of theorem 3 is infinite. Also, from lemmas 1 and 8 and an inspection of the proof of theorem 3, we see that the solutions in theorem 3 can be constructed so as to force any preassigned finite
set $T$ of primes of $F_1$ unramified over $K(x)$ to also not ramify in the solution field.

4.2 The case $k = p$. We remarked in 3.3 that we did not need to consider the equivalent reduced problem $P(F_1/K(x), G'/N', \varphi')$ in this case but could work directly with the problem $P(F_1/K(x), G/N, \varphi)$ itself. Referring to section 1.9 (theorem 2') of Iwasawa [9], we see that in order that the problem $P(F_1/K(x), G/N, \varphi)$ have a solution it is sufficient that the following condition be met:

For any finite Galois extension $F$ of $K(x)$ and for any integer $m \geq 1$, the additive group of $F$ contains $m$ elements $\alpha_1, \alpha_2, \ldots, \alpha_m$ such that the conjugates $\sigma(\alpha_1)$ of $\alpha_1$, $i = 1, 2, \ldots, m$, $\sigma \in \text{Gal}(F/K(x))$, are $GF(p)$-independent modulo $P_p(F)$. (Here $GF(p)$ is the prime field of $K$.) That this condition is met by $K(x)$ is a direct consequence of lemma 2 (ii). Hence we can always assume that the problem $P(F_1/K(x), G/N, \varphi)$ has a solution.

We now prove an analogue of lemma 8.

Lemma 8'. There is a finite set $X$ of primes of $F_1$ such that, if $S_1$ is a non-conjugate set of primes of $F_1$, $T$ a set of primes of $F_1$ no element of which is equal or conjugate to an element of $S_1$, and no prime of $X$ is equal or conjugate to a prime in $S_1 \cup T$, then the problem $P(F_1/K(x), G/N, \varphi)$ has a solution $(L_1, \psi_1)$ with the following properties:

(i) No prime of $T$ ramifies in $L_1$. 

(ii) Every prime in $S_1$ is fully ramified in $L_1$.

Proof: Again, as in lemma 8, we can assume that $T$ is non-conjugate. We know that the problem $F(F_1/K(x), G/N, \varphi)$ has a solution, say $(L_1', \psi_1')$. According to lemma 5' we have a 1-cochain $\gamma_\sigma$ and a 0-cochain $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r)$ satisfying the conditions stated therein.

Let $X$ consist of all primes of $F_1$ which occur in the divisor of any one of the $\alpha_i$ ($1 \leq i \leq r$) to a negative exponent. $X$ is obviously finite. For this $X$, let $S_1$ and $T$ be as in the lemma. Let $S_1 = \{P_1, P_2, \ldots, P_n\}$ and $T = \{P_{n+r+1}, \ldots, P_{n+r+m}\}$ where $m = |T|$. Choose integers $\lambda_1 < \lambda_2 < \ldots < \lambda_r < 0$ which are all relatively prime to $p$. Let $C = (C_{ij})$ be the $r \times (n + m)$ matrix defined by

$$ C_{ij} = \begin{cases} 0 & \text{if } j > n, \\ \lambda_i & \text{if } 1 \leq j \leq n, \quad 1 \leq i \leq r \end{cases} $$

By our choice of $X$ we have

$$ C_{ij} < \min \left(0, V_{P_j}(\alpha_i) \right) \text{ for } 1 \leq i \leq r; \quad 1 \leq j \leq n,$$

since $C_{ij}$ is negative and $V_{P_j}(\alpha_i) \geq 0$ if $1 \leq j \leq n$. So $\alpha$, $S_1$ and $C$ meet the requirements of lemma 7'. Choose $\beta$ as in lemma 7' relative to our choice of $\alpha$, $S_1$ and $C$. Since $\theta(\beta) = (\delta_1, \delta_2, \ldots, \delta_r)$ is a 0-cocycle it follows that $\alpha + \theta(\beta)$ has the same coboundary as $\alpha$ and thus $\alpha + \theta(\beta)$ meets all the requirements of lemma 5' that were met by $\alpha$. Thus, according to lemma 5'
again, \( \alpha + \Theta(\beta) \) "generates" a solution \((L_1, \xi_1)\) of \( P(F_1/K(x), G/H, \varphi) \).

Now suppose that \( 1 \leq j \leq n \). From lemma 7' we have

\[ V_{P_j}(\alpha_i + \xi_1) = c_{ij} = \lambda_i \quad \text{while if } n + r + 1 \leq j \leq n + r + m \text{ we have} \]

\[ (\ref{4.2.1}) \quad V_{P_j}(\alpha_i + \xi_1) \geq \min (0, c_{ij}, V_{P_j}(\alpha_i)) = \min (0, V_{P_j}(\alpha_i)) = 0 \]

since \( V_{P_j}(\alpha_i) \geq 0 \).

By lemma 5', \( L_1 = F_1(y_1, y_2, \ldots, y_r) \) where \( y_i^r - y_i = \alpha_i + \xi_1 \), \( 1 \leq i \leq r \).

For each \( j \), \( 1 \leq j \leq n \), since \( V_{P_j}(\alpha_i + \xi_1) = \lambda_i < 0 \) and \( p \nmid \lambda_i \), and since \( \lambda_i \neq \lambda_j \) for \( i \neq j \), it follows that, in the terminology of Maus [16], the fields \( F_1(y_i) \), \( 1 \leq i \leq r \), are pairwise arithmetically disjoining over \( F_1 \) for \( P_j \) (see [16], satz 3.9).

From the definition of the upper ramification numbers and from satz 3.8 of [16], one easily sees that the decomposition group (over \( F_1 \)) of a prime of \( L_1 \) lying above any given \( P_j \) is isomorphic to the product of the decomposition groups (over \( F_1 \)) of the primes \( P_{i,j} \) \( (1 \leq i \leq r) \), where the prime \( P_{i,j} \) is the (unique) prime of \( F_1(y_i) \) that lies above \( P_j \). Since each of the latter decomposition groups is of order \( p \) the former is of order \( p^{r} \). So each \( P_j \) ramifies fully in \( L_1 \). Thus every prime of \( S_1 \) is fully ramified in \( L_1 \).

Also, for any prime \( Q \in T \), we have from 4.2.1,

\[ V_Q(\alpha_i + \xi_1) \geq 0 \quad \text{and so } Q \text{ does} \]
not ramify in $F_1(y_i), 1 \leq i \leq r$. Hence $Q$ cannot ramify in the composite of all the $F_1(y_i), 1 \leq i \leq r$, which is just $L_1 = F_1(y_1, y_2, \ldots, y_r)$.

\[\square\]

Theorem 3'. The problem $P(F_1/K(x), G/N, \varphi)$ has a solution $(F, \psi)$ such that $\text{Aut}(F/K) = G$.

**Proof:** As in theorem 3, we need only establish the existence of a solution $(F, \psi)$ such that every automorphism of $F$ over $K$ maps $F_1$ onto itself.

Let $P_1, P_2, \ldots, P_s; e_1, e_2, \ldots, e_s$, be as in the proof of theorem 3. Let $X$ be the finite set of primes of $F_1$ mentioned in lemma 8' and choose an infinite non-conjugate (over $K(x)$) set $I$ of primes of $F_1$ such that no prime in $I$ is equal or conjugate to any prime in $X$. Let $S' \subset I$ be a finite set that saturates $F_1$ and is such that

$$|S'| \geq (g_{F_1} + 1) p^r + 1.$$  

[Note: Actually it suffices, for the purposes of the following proof, that $|S'| \geq 2$. The reason is that in the statement of lemma 3 we can replace $|S| \geq (g_{L_1} + 1)n + 1$ by $|S| \geq 2$ if $n$ is a power of $p$, a fact that is easily seen to be true in the light of theorem 1 and from an inspection of the proof of lemma 3.]

Let $\tilde{t}$ be the largest pole number of the primes in $S'$. Next, choose a finite $S \subset I$ such that $S \supset S'$ and
Then lemma 8' assures us that there is a solution \((F, \dagger)\) to the problem \(P(F_1/K(x), G/N, \varphi)\) such that all the primes in \(S\) ramify fully in \(F\).

Let \(\overline{F}\) be any subfield of \(F\) such that \(F_1 \subseteq \overline{F}\) and \([\overline{F}:F_1] = p\). Then since \(\overline{F}\) is clearly Galois over \(F_1\) we have \(\overline{F} = F_1(y)\) with \(y^p - y = \alpha \in F_1\). Since every prime in \(S\) ramifies fully in \(F\) it follows that every prime in \(S\) also ramifies fully in \(\overline{F}\).

Again, as in the proof of theorem 3, suppose \(P_{s', P_2, \ldots, P_s}\) do not ramify in \(\overline{F}\) whereas \(P_{s+1, \ldots, P_2}\) do. Let \(\overline{S}\) be the set of all primes of \(F_1\) that ramify in \(F\). So \(S \subseteq \overline{S}\).

From [7] we know that we can write \((\alpha)_{F_1} = \frac{B_1}{(\prod_{Q \in \overline{S}} Q^{h_Q})A_1}\), where \(h_Q\) are all positive and \(A_1\) and \(B_1\) involve no primes of \(\overline{S}\).

By the approximation theorem there exists a function \(z \in F_1\) such that

\[(z)_{F_1} = \left(\prod_{Q \in \overline{S}} Q^{h_Q^{-1}}\right)B_2, \text{ where } B_2\]

involves no primes of \(\overline{S}\). It follows that

\[(\alpha z)_{F_1} = \frac{B}{(\prod_{Q \in \overline{S}} Q)A}, \text{ where } A \text{ and } B\]

involve no primes of \(\overline{S}\).
Thus \( d(B) = d(A) + |\overline{s}_1| \geq d(A) + |s| \geq 2s_{F_1} + \frac{p^{r_1} - 1 + \frac{2n}{p^{r_2}}}{p^{r_1}} \).

Then, as in the proof of case (i) of theorem 3, given any prime \( P \) of \( F_1 \) and an integer \( \mu \leq p^{r_1} - 1 \), there is a function \( f_{\mu, P} \) in \( F_1 \) such that \( (f_{\mu, P})_{F_1} B^A = p^\mu (C_{K(x)/F_1})^2 C_{\mu, P} \) where \( C_{\mu, P} \) is integral and prime to \( P \).

Using the same convention as in the proof of case (i) of theorem 3, we have (see [7]) \( \frac{D}{F/K(x)} = \prod_{1 \leq i \leq s'}^s \left( \prod_{Q \in S'_1} Q^{(h^1_Q + 1)(p - 1)} \right) \), where \( h^1_Q \) is a positive integer not exceeding \( h_Q \), \( \overline{s}_1 = s_1 - \{P_1, \ldots, P_s\} \) and \( e^1_{s'_i + i} = pe^s_{s'_i + i} + r_i \) (\( r_i \) a positive integer depending on \( i \)). At any rate \( e^1_{s'_i + i} \geq p^\mu (1 \leq i \leq s - s') \). Also \( (h^1_Q + 1)(p - 1) \geq 2(p - 1) = 2p - 2 \geq p \).

So we can write

\[
\frac{D}{F/K(x)} = \prod_{1 \leq i \leq s'}^s \left( \prod_{Q \in S'_1} Q^{(r^1_{s'_i + i})} \right) \left( \prod_{Q \in S'_1} Q^{p} \right) \overline{R}^P \text{,}
\]

where \( \overline{R} \) is an integral divisor involving only primes that are ramified over \( F_1 \). Since \( \frac{(dx)}{F} = (C_{K(x)/F})^{2} \frac{D}{F/K(x)} \) (note that \( F \) is separable over \( K(x) \) although, perhaps, not normal over \( K(x) \)) and
since

\[
(\text{Con}_{F_1/F} \left( \prod_{Q \in \mathcal{S}_1} Q \right))^{-1} = \left( \prod_{Q \in \mathcal{S}_1} \tilde{Q} \right)^{-P} \text{ it follows that}
\]

\[
(\alpha z dx)_{\tilde{F}} = R \prod_{\tilde{F}_{a_1}^{e_1}} \ldots \prod_{\tilde{F}_{a_s}^{e_s}} (\text{Con}_{K(x)/F_{\infty}})^{-2} \frac{F}{K},
\]

\( R \) being an integral divisor involving primes of \( \tilde{F} \) that are ramified over \( F_1 \). This last equation corresponds to 4.1.1 in the proof of case (i) of theorem 3. Exactly the same reasoning as was used there now shows that any prime of \( \tilde{F} \) which is unramified over \( F_1 \) has the integers \( 1, 2, \ldots, p^{\mathcal{R}_t} \) as gap numbers. From this it follows that every prime of \( F \) which is not fully ramified over \( F_1 \) also has \( 1, 2, \ldots, p^{\mathcal{R}_t} \) as gap numbers. For, if \( \hat{P} \) is such a prime, the decomposition field of \( \hat{P} \) (over \( F_1 \)) properly contains \( F_1 \) and so must contain a subfield \( \tilde{F} \) of \( F \) such that \( \tilde{F} \supset F_1 \) and \( [\tilde{F}:F_1] = p \). Let \( \bar{F} \) be the prime of \( F \) lying below \( \hat{P} \). Since \( \bar{F} \) is unramified over \( F_1 \) we know from above that \( 1, 2, \ldots, p^{\mathcal{R}_t} \) are all gap numbers of \( \bar{F} \). The fact that \( 1, 2, \ldots, p^{\mathcal{R}_t} \) are gap numbers of \( \hat{P} \) now follows from the following general assertion:

If \( L_1 \subset L_2 \) are algebraic function fields over \( K \) and \( P_1 \) is a prime of \( L_1 \) lying below a prime \( P_2 \) of \( L_2 \), then, if the extension \( L_2/L_1 \) is Galois and an integer \( \lambda \) is a gap number of \( P_1 \), \( \lambda \) is also a gap number of \( P_2 \).
For, let \( L \) be the decomposition field of \( P_2 \) (over \( L_1 \)) and let \( P \) be the prime of \( L \) lying below \( P_2 \). Since \( P \) is unramified over \( L_1 \) and \( P_1 \) has \( \lambda \) as a gap number, it follows that \( \lambda \) is a gap number of \( P \) (see [23], lemma 4). If \( \lambda \) were not a gap number of \( P_2 \), there would exist \( \chi \in L_2 \) such that \( (\chi)_{L_2} = \frac{A}{P_2^\lambda} \). Since \( P_2 \) is fully ramified over \( L \), \( N_{L_2/L}(\chi) \) has \( P_2^\lambda \) as its pole divisor, a contradiction.

Now note that \(|S'| \geq (g^F_1 + 1)p^F + 1\), \( S' \) saturates \( F_1 \) and, since every prime of \( S' \subset S \) ramifies fully in \( F \), \( p^F t_Q \) is a pole number of any prime \( Q \) of \( F \) that lies above a prime \( Q \) of \( S' \), for some \( t_Q \leq \overline{t} \). Hence we have shown that every prime of \( F \) that is not fully ramified over \( F_1 \) has a gap sequence distinct from that of all primes of \( F \) that lie above primes in \( S' \). Then lemma 3 immediately yields that every automorphism of \( F \) over \( K \) maps \( F_1 \) onto itself. \( \square \)

Remark 2. The construction of theorem 3' can be made to yield solutions \( F \) in which the number of primes ramifying over \( F_1 \) is arbitrarily large. Hence the solution fields can have arbitrarily large genus. This fact, together with remark 1, allows us to state that for a given solvable group \( G \) there are infinitely many algebraic function fields \( F \) over \( K \) such that \( \text{Aut}(F/K) = G \). Note, however, that unlike the construction in theorem 3, the construction in theorem
3' does not ensure that a preassigned finite set $T$ of primes of $F_1$ which are unramified over $K(x)$ can be made to remain unramified in $F$. However, this can be ensured provided we know that every element of $T$ is not equal or conjugate to any prime in a certain finite set $X$ of primes of $F_1$.

Remark 3. Since the proof of case (i) of theorem 3 and that of theorem 3' do not invoke the inequality of Castelnuovo-Severi, it follows that this inequality is not needed to establish the result for groups $G$ which have the following property:

There exist distinct subgroups $G = N_0, N_1, N_2, \ldots, N_k = \{1\}$ of $G$ which are all normal in $G$, $N_i \supset N_{i+1}$ $(0 \leq i \leq k-1)$ and such that $N_i/N_{i+1}$ is either of prime order $\ell \neq p$ or is an elementary abelian $p$-group. Every supersolvable group clearly has this property.


