ON THE INVARIANTS OF SOME $\mathbb{Z}_\ell$-EXTENSIONS

Thesis By

John Roll Bloom

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

California Institute of Technology
Pasadena, California

1977

ACKNOWLEDGEMENTS

I would like to thank my wife Janet, and my parents for the love and support they have given me.

I became interested in this topic through my advisor, Dr. Kisilevsky. I appreciate the help he gave me, and the opportunity I had to work with him.

I received financial support from a Ford Foundation Fellowship, and through various fellowships and assistantships granted by the California Institute of Technology.

ABSTRACT

Let k be a number field, ℓ a prime, $k \subset k_1 \subset k_2 \subset \ldots \subset K$, and $k \subset m_1 \subset m_2 \subset \ldots \subset M$ two $\mathbb{Z}_\ell$-extensions of k. The structure of the galois group of a certain extension of MK is studied, and it is shown how, in some cases, the ℓ-parts of the class groups of the intermediate fields $m_i k_j$ can be obtained from this group.

This galois group is a module over $\mathbb{Z}_\ell[[S,T]]$, the power series ring in two variables over the ℓ-adic integers, but the structure theory of such modules is not well developed. The main results come from studying the structure of this group as a $\mathbb{Z}_\ell[[S]]$ or $\mathbb{Z}_\ell[[T]]$ module. Necessary and sufficient conditions are given for this group to be a Noetherian module over $\mathbb{Z}_\ell[[T]]$, and thus it has a well known structure. Sufficient conditions are given for the module to be a torsion module.

The structure of this group is then used to obtain information on the Iwasawa invariants μ and λ of the $\mathbb{Z}_\ell$-extensions Km_i/m_i and Mk_j/k_j. In suitable situations it is shown that $\mu(K/k)=0$ implies that $\mu(Km_i/m_i)=0$ for all i, and $\lambda(Km_i/m_i)=r\ell^i + \sum_{j=0}^{i} c_j\varphi(\ell^j)$, with $c_j=0$ for all $j>n_0$ and it is shown that r=0 iff the above module is torsion.

In certain situations, this group is also used to study the invariants of all $\mathbb{Z}_\ell$-extensions of k contained in MK. With suitable hypotheses, it is shown that at most one $\mathbb{Z}_\ell$-extension has $\mu \neq 0$.

Some examples are computed.

TABLE OF CONTENTS

I. INTRODUCTION

Let k be an algebraic number field and ℓ a fixed rational prime. We shall be concerned with a certain type of extension of k, called a Γ-extension, or a $\mathbb{Z}_\ell$-extension. Let $\mathbb{Z}_\ell$ denote the ring of ℓ-adic integers, and $\mathbb{Z}_\ell^+$ the ℓ-adic integers considered as an additive group. Let K be a field containing k (not necessarily a finite extension of the rationals, Q), then we say that K/k is a $\mathbb{Z}_\ell$-extension if K/k is normal and $g(K/k)\cong\mathbb{Z}_\ell^+$, where $g(K/k)$ denotes the galois group of the extension K/k.

Let $\Gamma=g(K/k)$. Γ has as subgroups of finite index $\Gamma_n=\ell^n\Gamma$, $n=0,1,\ldots$. Let k_n denote the fixed field of Γ_n. Then $k=k_0\subset k_1\subset\ldots\subset k_n\subset\ldots\subset K$. The k_n are the only subfields of K containing k, and $K=\bigcup_{n=1}^{\infty} k_n$. It can be shown that k_n/k is cyclic of order ℓ^n. The field k_n is called the n-th layer of the $\mathbb{Z}_\ell$-extension K/k.

An example of a $\mathbb{Z}_\ell$-extension is constructed in the following fashion. Let ζ_n denote a primitive (ℓ^{n+1})-st root of unity. Let $k_n=Q(\zeta_n)$, $K=\bigcup_{n=1}^{\infty}k_n$. Then $g(k_n/k_0)\cong\mathbb{Z}/\ell^n\mathbb{Z}$, and $g(K/k_0)\cong\varprojlim \mathbb{Z}/\ell^n\mathbb{Z}\cong\mathbb{Z}_\ell$. If $\ell=2$ we take k_1 instead of k_0 as the base field. For ℓ odd, K/k_0 is a $\mathbb{Z}_\ell$-extension, and furthermore K is normal over Q. Then $g(K/Q)$ contains a unique element of order $\ell-1$, and $g(K/Q)\cong\mathbb{Z}_\ell\oplus\Delta$, with $|\Delta|=\ell-1$. Let $\mathbb{P}$ be the subfield of K fixed by Δ. $\mathbb{P}/Q$ is a $\mathbb{Z}_\ell$-extension of Q, in fact the only $\mathbb{Z}_\ell$-extension of Q. For $\ell=2$, we take

$\mathbb{P}$ to be the subfield of K fixed by complex conjugation. For any number field k, the extension $k\mathbb{P}/k$ is a $\mathbb{Z}_\ell$-extension, called the basic, or cyclotomic, $\mathbb{Z}_\ell$-extension of k.

An algebraic number field always has at least one $\mathbb{Z}_\ell$-extension, the cyclotomic one. For a number field k, let M denote the composite of all $\mathbb{Z}_\ell$-extensions of k. Then $g(M/k)\cong\mathbb{Z}_\ell^a$ for some integer a. If k has $2r_2$ distinct complex imbeddings into the complex numbers then $1+r_2\leq a\leq[k:Q]$ [7, p.253]. The conjecture that $a=1+r_2$ is equivalent to Leopoldt's conjecture on the nonvanishing of the ℓ-adic regulator.

For any algebraic extension of Q, F, let $\overline{F}$ denote the maximal abelian unramified ℓ-extension of F (i.e., $\overline{F}/F$ is unramified and $g(\overline{F}/F)$ is a profinite ℓ-group. In general, a normal extension L/F is unramified, if for each valuation v of L, the inertial group,

$$T_v=\{\sigma\in g(L/F)\mid v(\sigma(\alpha)-\alpha)>0\,\forall\alpha\in L\}$$

is trivial). Let $A_F=g(\overline{F}/F)$. For F a number field, $\overline{F}$ is a subfield of the Hilbert class field of F and $A_F\cong$ the Sylow ℓ-subgroup of C_F, the class group of F.

For the $\mathbb{Z}_\ell$-extension K/k, $k\subset k_1\subset\ldots\subset k_n\subset\ldots\subset K$, the groups A_{k_n} are related in an interesting way. Define e_n by $\ell^{e_n}=|A_{k_n}|$.

<u>THEOREM</u> (Iwasawa). There exist integers μ, λ, and ν such that $e_n=\mu\ell^n+\lambda n+\nu\ \forall n\geq n_0$ for some integer $n_0=n_0(K/k)$, with $\mu,\lambda\geq 0$.

The integers $\mu=\mu$ (K/k) and $\lambda=\lambda$ (K/k) are called the (Iwasawa) invariants for the $\mathbb{Z}_\ell$- extension K/k.

A natural question would be, for a $\mathbb{Z}_\ell$-extension K/k, how does one determine the invariants μ, λ and the integers ν and n_0. The main interest has been in the invariants μ and λ, and although methods for the determining μ and λ are not known in general, there are results for certain special cases. For the cyclotomic $\mathbb{Z}_\ell$-extension of the field of ℓ-th roots of unity, the invariants can be computed via the ℓ-adic L-series (modulo Vandiver's conjecture), with the connection based upon a theorem of Stickelberger. Greenberg [3] has some results on the basic extensions of totally real fields. A number field which is not totally real has infinitely many $\mathbb{Z}_\ell$-extensions, and the question is still open for the non-cyclotomic extensions. In fact, the set of $\mathbb{Z}_\ell$-extensions of a number field has not been canonically indexed, so it is difficult to work with a specific non-cyclotomic $\mathbb{Z}_\ell$-extension. Carroll and Kisilevsky [2] have, in certain situations, characterized a set of $\mathbb{Z}_\ell$-extensions of k, which are independent, and together with the cyclotomic $\mathbb{Z}_\ell$-extension, generate the composite of all $\mathbb{Z}_\ell$-extensions. These independent $\mathbb{Z}_\ell$-extensions are the unique $\mathbb{Z}_\ell$-extensions normal over Q. For this case, certain congruence relations in the invariants were found, and a functional equation was given for a certain characteristic polynomial. (The polynomial uniquely determines the invariants μ and λ.)

This thesis investigates the situation where a $\mathbb{Z}_\ell$-extension is described in terms of one or more "known" $\mathbb{Z}_\ell$-extensions. The first situation investigated is the composition of a $\mathbb{Z}_\ell$-extension K/k with a field of F to obtain a $\mathbb{Z}_\ell$-extension KF/F. (c.f., Iwasawa [6]). The same situation is considered where F runs through the various finite layers of a $\mathbb{Z}_\ell$-extension M/k.

II. FURTHER DEFINITIONS AND NOTATIONS

Let K/k be a $\mathbb{Z}_\ell$-extension. Let $\overline{K}$ be the maximal abelian unramified ℓ-extension of K. Let

$$G = g(\overline{K}/k), \quad X = A_K = g(\overline{K}/K).$$

Then X is a normal subgroup of G, and $G/X \cong \Gamma = g(K/k) \cong \mathbb{Z}_\ell$. Thus Γ acts on X by conjugation, and $\mathbb{Z}_\ell$ also acts naturally on X, with the action of $a \in \mathbb{Z}_\ell$ given by $x \mapsto x^a = \lim_{a_n \to a} x^{a_n}$. (This limit exists since X is a profinite ℓ-group.) Both these actions are continuous.

These actions allow us to consider X as a module over the group ring $\mathbb{Z}_\ell[\Gamma]$. X can also be considered as a module over the ring of (formal) power series in one variable, $\mathbb{Z}_\ell[[T]]$. This action is obtained by picking a topological generator γ_0 of Γ (i.e., $<\gamma_0>$ is dense in Γ), and defining the action of T on X by $\gamma_0 x = (1+T)x$ for all $x \in X$. Since $\mathbb{Z}_\ell[(1+T)]$ is dense in $\mathbb{Z}_\ell[[T]]$, this defines a unique action of $\mathbb{Z}_\ell[[T]]$ on X. c.f., [7]. From now on, we will let Λ_T denote $\mathbb{Z}_\ell[[T]]$.

In general any compact profinite ℓ-group on which Γ acts continuously admits a continuous action by Λ_T. c.f.[7]

A few elements of Λ_T are defined for future use.

<u>DEFINITION</u>. $\omega_n(T) = (1+T)^{\ell^n} - 1$, $n \geq 0$.

$\nu_{n,m}(T) = \omega_m(T)/\omega_n(T)$, $m \geq n \geq 0$.

DEFINITION. Given two Λ_T modules X and Y, a homomorphism $f: X \to Y$ is a pseudo-isomorphism if the kernel and co-kernel are finite. We say X is pseudo-isomorphic to Y if there exists a pseudo-isomorphism $f: X \to Y$ and write $X \underset{p}{\cong} Y$.

Pseudo-isomorphism is not, in general, an equivalence relation. That is, we can have $X \underset{p}{\cong} Y$ but $Y \underset{p}{\ncong} X$. Pseudo-isomorphism is, however, transitive. Also, if X and Y are Noetherian torsion Λ_T modules, then $X \underset{p}{\cong} Y$ implies $Y \underset{p}{\cong} X$.

Let $e_0, e_1, \ldots, e_s$ be non-negative integers and $p_1, \ldots, p_s$ be prime ideals of height one in Λ_T. Each p_i is either (ℓ), the ideal generated by ℓ, or $(f_i(T))$, the ideal generated by a distinguished irreducible polynomial in $Z_\ell[T]$. (A polynomial f(T) is distinguished if, $f(T) = T^d + \ell g(T)$, $d>0$, $d>\deg g(T)$.) Define the module,

$$E(e_0 ; p_1^{e_1}, \ldots, p_s^{e_s}) = \Lambda_T^{e_0} \oplus \Lambda_T/p_1^{e_1} \oplus \cdots \oplus \Lambda_T/p_s^{e_s}.$$

Such a module is called an elementary Λ_T module. Every Noetherian Λ_T module is pseudo-isomorphic to a unique elementary module E_X. If $X \underset{p}{\cong} Y$, then $E_X = E_Y$. Also, X is a Noetherian torsion Λ_T module if and only if the associated elementary module $E(e_0 ; p_1^{e_1}, \ldots, p_s^{e_s})$ has $e_0 = 0$.

For a $\mathbb{Z}_\ell$-extension of a number field, K/k, the module $X = A_K$ is always a Noetherian torsion Λ_T module.

If we write,

$$X \underset{p}{\cong} E = \bigoplus_{i=1}^{m} \Lambda_T/(f_i(T))^{q_i} \bigoplus_{i=1}^{n} \Lambda_T/(\ell)^{\mu_i} ,$$

then the invariants $\mu(K/k)$, $\lambda(K/k)$ are as follows:
$\mu = \sum_{i=1}^{n} \mu_i$. $\lambda = \sum_{i=1}^{m} q_i \deg f_i$.

The above description of μ and λ also allows us to characterize them in the following way. Let $V = X \otimes_{\mathbb{Z}_\ell} Q_\ell$. V is a vector space over Q_ℓ, and $\dim_{Q_\ell} V = \lambda$. Let D denote the kernel of the map,

$$X \xrightarrow{\ell} X.$$
$$x \mapsto \ell x$$

Then $\mu = 0$ if and only if D is finite.

At this point we also wish to mention the following fact, a consequence of ramification theory. If F is an abelian extension of a number field k with $g(F/k) \cong \mathbb{Z}_\ell^a = \mathbb{Z}_\ell \oplus \ldots \oplus \mathbb{Z}_\ell$, then F/k is unramified outside primes above ℓ. The case F/k a $\mathbb{Z}_\ell$-extension is of particular interest.

III. COMPOSITION WITH A FINITE EXTENSION

Let k be a number field, K/k a $\mathbb{Z}_\ell$-extension, and F/k a cyclic extension of degree ℓ^r, $k = F_0 \subset F_1 \subset \dots \subset F_r = F$, with $[F_i:k] = \ell^i$. Assume furthermore that $F \cap K = k$.

Since $g(KF_i/k) = g(KF_i/F_i) \oplus g(KF_i/K) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}/\ell^i\mathbb{Z}$, KF_i/F_i is a $\mathbb{Z}_\ell$-extension for $i = 0, \dots, r$. We will obtain certain relations among the λ-invariants of the various extensions KF_i/F_i. For the relationship of the μ-variants, see [6].

Let $X_i = g(\overline{KF_i}/KF_i)$. Then $\lambda(KF_i/F_i) = \dim_{\mathbb{Q}_\ell}(X_i \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$.

Let $g(KF/K) = \langle\sigma\rangle$. $\sigma^{\ell^r} = 1$.

<u>LEMMA</u> 3.1.

$$\dim_{\mathbb{Q}_\ell}(X_i \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) = \dim_{\mathbb{Q}_\ell}(X_r/(\sigma^{\ell^i}-1)X_r \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$$

If each prime of k which ramifies in F/k is finitely decomposed in K/k, then $X_i \underset{p}{\cong} X_r/(\sigma^{\ell^i}-1)X_r$.

To simplify the formulas, we will let $D(X) = \dim_{\mathbb{Q}_\ell}(X \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$ for any Λ_T module X. The first statement of the lemma now reads $D(X_i) = D(X_r/(\sigma^{\ell^i}-1)X_r)$.

<u>PROOF OF LEMMA</u>. We construct the following fields. Let $E_i = KF\,\overline{KF_i}$. Let $G_i = g(\overline{KF}/KF_i)$, and let G_i' be the commutator subgroup of G_i. Let M_i be the fixed field of G_i'. The field M_i is the maximal subextension of $\overline{KF}/KF_i$ which is abelian over KF_i. The following relationship holds

among these fields:

$$KF \subseteq E_i \subseteq M_i \subseteq \overline{KF}.$$

This provides us with an exact sequence.

$$0 \to g(M_i/E_i) \to g(M_i/KF) \to g(E_i/KF) \to 0.$$

If we form the tensor product of each element of the sequence with Q_ℓ, and take the dimension of the resulting vector space, we get,

$$D(g(M_i/KF)) = D(g(M_i/E_i)) + D(g(E_i/KF)).$$

Since $D(X_r) = D(g(\overline{KF}/KF))$ is finite, each term in the above equation is finite. The first part of the lemma will be done if we show $D(X_i) = D(g(E_i/KF))$, $D(g(M_i/KF)) = D(X_r/(\sigma^{\ell^i}-1)X_r)$, and $D(g(M_i/E_i)) = 0$.

First, $g(E_i/KF) \cong g(\overline{KF}_i/KF \cap \overline{KF_i})$. We also have

$$0 \to g(\overline{KF}_i/KF \cap \overline{KF_i}) \to g(\overline{KF}_i/KF_i) \to g(KF \cap \overline{KF_i}/KF_i) \to 0.$$

Since the last term in this exact sequence is finite, we can actually conclude that $g(E_i/KF) \underset{p}{\cong} X_i$, so the relationship $D(X_i) = D(g(E_i/KF))$ is proven.

To prove the second relationship we argue as follows. By the definition of M_i, $g(M_i/KF_i) \cong G_i/G_i'$, and therefore $g(M_i/KF) \cong X_r/(G_i' \cap X_r)$. We can take σ^{ℓ^i} as a generator of $g(KF/KF_i)$. Let $a = \overline{\sigma^{\ell^i}}$ denote a lifting of σ^{ℓ^i} to G_i. Since X_r and a generate G_i, and X_r is an abelian group, one sees that $G_i' = \langle a\,x\,a^{-1}\,x^{-1} \mid x \in X_r \rangle = (\sigma^{\ell^i}-1)X_r$.

Thus we have $g(M_i/KF) \cong X_r/(\sigma^{\ell^i}-1)X_r$, and therefore $D(g(M_i/KF)) = D(X_r/(\sigma^{\ell^i}-1)X_r)$.

Finally, we show that $D(g(M_i/E_i)) = 0$. Since $g(M_i/E_i) \subseteq g(M_i/\overline{KF_i})$, it suffices to show that $D(g(M_i/\overline{KF_i})) = 0$.

Let $\{W_j\}$ be the set of valuations of KF_i which ramify in M_i/KF_i. Let $\{T_j\}$ be the set of inertial group for the W_j in $M_i/\overline{KF_i}$. Since $KF_i \subseteq \overline{KF_i} \subseteq M_i$, and KF_i is the maximal unramified subextension of M_i/KF_i, $g(M_i/\overline{KF_i})$ is precisely the group generated by the T_j. $T_j|_{KF}$ is the inertial group for W_j in KF/KF_i. Let $t_j \in T_j$. Then $t_j^{\ell^{r-i}}|_{KF}$ is the identity so $t_j^{\ell^{r-i}} \in T_j \cap g(M_i/KF)$. Now M_i/KF is unramified, so $T_j \cap g(M_i/KF) = 1$. Thus $t_j^{\ell^{r-i}} = 1$, and therefore, $g(M_i/\overline{KF_i})^{\ell^{r-i}} = 1$, and $g(M_i/\overline{KF_i}) \otimes_{\mathbb{Z}_\ell} Q_\ell = 0$.

This completes the proof of the first statement of the lemma.

The second statement now follows quickly. We have already shown that,

$$g(E_i/KF) \underset{p}{\cong} X_i, \text{ and } g(M_i/KF) \cong X_r/(\sigma^{\ell^i}-1)X_r.$$

We also have the exact sequence,

$$0 \to g(M_i/E_i) \to g(M_i/KF) \to g(E_i/KF) \to 0.$$

We will be done if we show $g(M_i/E_i)$ is finite. We actually show that $g(M_i/\overline{KF_i})$ is finite.

It was shown above that $g(M_i/\overline{KF_i})$ is the group generated by the inertia groups $\{T_j\}$, and each T_j is finite. Let ν_j be the restriction of W_j to F_i. Since W_j ramifies in KF/KF_i, ν_j must ramify in F/F_i. Since F/F_i is a finite extension of an algebraic number field, there are only finitely many ramified primes. The hypothesis that each prime ramifying in F/k is finitely decomposed in K/k implies that there are only finitely many extensions of ν_j to KF_i. Thus $\{T_j\}$ is finite, and $g(M_i/\overline{KF_i})$ is finite. □

This lemma can now be used to relate the λ-invariants for the various $\mathbb{Z}_\ell$-extensions KF_i/F_i.

<u>THEOREM 1</u>. $\lambda(KF_i/F_i) \equiv \lambda(KF_{i-1}/F_{i-1}) \pmod{\varphi(\ell^i))}$, hence for $j \le i$ $\lambda(KF_i/F_i) \equiv \lambda(KF_j/F_j) \pmod{\varphi(\ell^{j+1})}$.

<u>PROOF</u>. The characterization of $\lambda(KF_i/F_i)$ in section II is that $\lambda(KF_i/F_i) = D(X_i)$. The above lemma shows that $D(X_i) = D(X_r/(\sigma^{\ell^i}-1)X_r)$.

Let V be the Q_ℓ vector space $X_r \otimes_{Z_\ell} Q_\ell$. The map $(\sigma^{\ell^j}-1)$ is a linear map on V. Let V_j denote the null space of $(\sigma^{\ell^j}-1)$. We have $V_0 \subseteq V_1 \subseteq \ldots \subseteq V_r = V$.

Now,

$\lambda(KF_i/F_i) = D(X_r/(\sigma^{\ell^i}-1)X_r) = \dim_{Q_\ell}(X_r \otimes_{Z_\ell} Q_\ell) - \dim_{Q_\ell}$ $((\sigma^{\ell^i}-1)X_r \otimes_{\mathbb{Z}_\ell} Q_\ell) = \dim_{Q_\ell} V - \dim_{Q_\ell} (\sigma^{\ell^i}-1)V = \dim_{Q_\ell} V_i$.

Therefore, we have,

$$\lambda(KF_i/F_i) - \lambda(KF_{i-1}/F_{i-1}) = \dim_{Q_\ell} V_i - \dim_{Q_\ell} V_{i-1} =$$

$$\dim_{Q_\ell} (\sigma^{\ell^{i-1}}-1)V_i$$

Let $W_i = (\sigma^{\ell^{i-1}}-1)V_i$. We are done if we show $\varphi(\ell^i) \mid \dim_{Q_\ell} W_i$. If $W_i = 0$, we are done. Assume $W_i \neq 0$. Let $\Phi(t) = t^{\ell^i}-1/t^{\ell^{i-1}}-1$. $\Phi(t)$ is an irreducible polynomial in $Q_\ell[t]$. Since $W_i \neq 0$, but $\Phi(\sigma)W_i = 0$, $\Phi(t)$ is the minimal polynomial for σ on W_i. Therefore, $P(t)$, the characteristic polynomial for σ on W_i, is a power of $\Phi(t)$. $P(t) = (\Phi(t))^s$. Thus $\dim_{Q_\ell} W_i = \deg P(t) = s \deg \Phi(t) = s\varphi(\ell^i)$. □

IV. COMPOSITION WITH A $\mathbb{Z}_\ell$-EXTENSION

Let $k=k_0\subset k_1\subset\ldots\subset k$, and $k=m_0\subset m_1\subset\ldots\subset M$ be two disjoint $\mathbb{Z}_\ell$-extensions of k. The invariants of the $\mathbb{Z}_\ell$-extension Mk_i/k_i can be related to the invariants of the $\mathbb{Z}_\ell$-extension M/k by Theorem 1, but in this case, stronger results hold. We therefore study these extensions. Since not every number field has two disjoint $\mathbb{Z}_\ell$-extensions, it is necessary to assume that k has at least one complex imbedding.

For the remainder of this thesis, let k be a number field with at least one complex imbedding.

Let $k_{\mathbb{Z}_\ell}$ be the composite of all $\mathbb{Z}_\ell$-extensions of k. Then $G=g(k_{\mathbb{Z}_\ell}/k)\cong \mathbb{Z}_\ell^a$, with $a\geq 2$. It is possible to pick $H\subseteq G$ with $G/H\cong\mathbb{Z}_\ell\oplus\mathbb{Z}_\ell$, and if N is the fixed field of H, $g(N/k)\cong\mathbb{Z}_\ell\oplus\mathbb{Z}_\ell$. One can pick Γ_1 and Γ_2 contained in g(N/k) such that $\Gamma_1\cong\Gamma_2\cong\mathbb{Z}_\ell$, and $g(N/k) = \Gamma_1\oplus\Gamma_2$.

Let K be the fixed field of Γ_1, and M the fixed field of Γ_2. Then K/k and M/k are disjoint $\mathbb{Z}_\ell$-extensions of k, and N=MK.

Let $\overline{N}$ be the maximal abelian unramified ℓ-extension of N, and $X_N=g(\overline{N}/N)$. We will show that X_N is a module over $\mathbb{Z}_\ell[[S,T]]$ in a natural way.

Let σ be a topological generator of Γ_1, and let τ be a topological generator of Γ_2. Since $g(M/k)\cong\Gamma_1$, with the isomorphism given by restriction, g(M/k) is topologically generated by the restriction of σ to M, which we also call σ. Similarly, $g(K/k)$ is generated by τ.

Let N_n denote the subfield of N fixed by $<\sigma^{\ell^n}, \tau^{\ell^n}>$, the closed subgroup generated by σ^{ℓ^n} and τ^{ℓ^n}. Then $N_0=k$, and $N=\bigcup_{n=1}^{\infty} N_n$. Since $\overline{N} = \bigcup_{n=1}^{\infty} \overline{N}_n$ (c.f.[10]), $g(\overline{N}/N) = \varprojlim g(\overline{N_n}/N_n)$. Each $g(\overline{N}_n/N_n)$ is a finite ℓ-group, and therefore X_N is a profinite ℓ-group.

Let $G = g(\overline{N}/k)$. Since $G/X_N \cong \Gamma_1 \oplus \Gamma_2$, $\Gamma_1 \oplus \Gamma_2$ acts on X_N by conjugation, and thus one obtains a continuous action of $\mathbb{Z}_\ell[\Gamma_1 \oplus \Gamma_2]$ on X_N. It is not hard to show that the correspondence $1+T \leftrightarrow \tau$, $1+S \leftrightarrow \sigma$, provides a continuous action of $\mathbb{Z}_\ell[[S,T]]$ on X_N. (c.f.[4]).

THEOREM (Greenberg). X_N is a Noetherian torsion $\mathbb{Z}_\ell[[S,T]]$ module.

The structure of $\mathbb{Z}_\ell[[S,T]]$ modules is not as well classified as the structure of $\mathbb{Z}_\ell[[S]]$ modules. The ℓ-part of the class group of the intermediate fields $k_i m_j$ ($k_i \subset K$, $m_j \subset M$) is connected with the $\mathbb{Z}_\ell[[S,T]]$ structure of X_N. The following proposition describes the connection in the particular case where N/k has a unique totally ramified prime.

PROPOSITION. If N/k has a unique totally ramified prime, then,

$$g(\overline{k_i m_j}/k_i m_j) \cong X_N/<\omega_i(T)X_N,\ \omega_j(S)X_N>.$$

PROOF. Let i and j be fixed. Let E denote the largest subfield of $\bar{N}$ which is abelian over $k_i m_j$. Then $N \subseteq E \subseteq \bar{N}$. We will show that $g(\overline{k_i m_j}/k_i m_j) \cong g(E/N)$, and that $g(E/N) \cong X_N/<\omega_i(T)X_N, \omega_j(S)X_N>$.

Let $G = g(\bar{N}/k_i m_j)$. Then E is the fixed field of G'. We will show that $G' = <\omega_i(T)X_N, \omega_j(S)X_N>$.

Let $\mathfrak{p}$ denote the prime of $k_i m_j$ which is totally ramified in $N/k_i m_j$, and let T_v be the inertial group in $\bar{N}/k_i m_j$, for a valuation v of $\bar{N}$ which extends the valuation induced by $\mathfrak{p}$.

Since $\bar{N}/N$ is unramified, $T_v \cap X_N = 0$. Since $T_v X_N/X_N$ is the inertial group for $\mathfrak{p}$ in N/M, $T_v X_N = G$. We have $G/X_N \cong T_v$, and T_v acts on X_N by conjugation, so G is a semidirect product of X_N by T_v.

Thus $G' = <txt^{-1}x^{-1} \mid t \in T_v, x \in X_N> = <X_N^{t-1} \mid t \in T_v>$. We can also identify T_v with $g(N/k_i m_j)$. If,

$$t = (\tau^{\ell^i})^a (\sigma^{\ell^j})^b,$$

then,

$$t-1 = (\tau^{\ell^i})^a((\sigma^{\ell^j})^b - 1) + (\tau^{\ell^i})^a - 1,$$

so,

$$X_N^{t-1} \subseteq (\sigma^{\ell^j} - 1)X_N + (\tau^{\ell^i} - 1)X_N = <\omega_i(T)X_N. \omega_j(S)X_N>.$$

Also $\omega_j(T)X_N = X_N^{\tau^{\ell^i}-1} \subseteq G'$, and $\omega_j(S)X_N = X_N^{\sigma^{\ell^j}-1} \subseteq G'$, so $G' = <\omega_i(T)X_N, \omega_j(S)X_N>$.

Thus, $N \subseteq E \subseteq \overline{N}$, with $G' = g(\overline{N}/E) \subseteq g(\overline{N}/N) = X_N$. Therefore, $g(E/N) \cong X_N/G' = X_N/<\omega_i(T)X_N, \omega_j(S)X_N>$.

Let $\mathfrak{p}$ be the prime of k_im_j which ramifies in N/k_im_j, and let $T_{\mathfrak{p}}$ be the inertia group for $\mathfrak{p}$ in E/k_im_j. Since $T_{\mathfrak{p}}$ projects onto $g(N/k_im_j)$ and is disjoint from $g(E/N)$, we have $g(E/k_im_j) \cong g(E/N) \oplus T_{\mathfrak{p}}$.

Since $\overline{k_im_j} \subseteq E$ and the fixed field of $T_{\mathfrak{p}}$ is contained in $\overline{k_im_j}$, we have $E = N\,\overline{k_im_j}$. Therefore, $g(E/N) \cong g(\overline{k_im_j}/k_im_j)$, and we are done. □

We now return to the study of X_N.

Since the structure of $\mathbb{Z}_\ell[[S,T]]$ modules is not well known, we notice that the action of $\mathbb{Z}_\ell[[S,T]]$ on X_N provides an action of $\mathbb{Z}_\ell[[S]]$ and $\mathbb{Z}_\ell[[T]]$ on X_N, and study the structure of X_N as a module over these rings.

<u>THEOREM</u> 2. If ℓ is finitely decomposed in M, then X_N is a Noetherian $\mathbb{Z}_\ell[[T]]$ module if and only if $\mu(M/k) = 0$. Similarly, if ℓ is finitely decomposed in K, then X_N is a Noetherian $\mathbb{Z}_\ell[[S]]$ module if and only if $\mu(K/k) = 0$.

<u>PROOF</u>. We will prove the first statement. The second follows from a change in notation.

The module X_N is a Noetherian $\mathbb{Z}_\ell[[T]]$ module if and only if $X_N/(T,\ell)X_N$ is finite. The module $X_N/(T,\ell)X_N$ is finite if and only if X_N/TX_N has a finite rank.

Let $E \subseteq \overline{N}$ be the fixed field of TX_N. Then $H = g(E/N) \cong X_N/TX_N$. Since TX_N is the commutator subgroup of $g(\overline{N}/M)$, $G = g(E/M)$ is abelian. Therefore we can form the factor group G/H, and $G/H \cong g(N/M) \cong \mathbb{Z}_\ell$. Thus X_N is Noetherian if and only if G has finite rank.

Let I denote the subgroup of G generated by the inertia groups of all valuations of M. Since only valuations above ℓ can have non-trivial inertia groups, and we have assumed there are only finitely many valuations above ℓ, I has finite rank. Hence G has finite rank if and only if G/I has finite rank.

Let L be the fixed field of I. Then L is the maximal abelian unramified extension of M contained in $\overline{N}$. Since $\overline{M} \subseteq \overline{N}$, $L=\overline{M}$. Therefore $G/I \cong g(\overline{M}/M)$. Finally, X_N is Noetherian if and only if $g(\overline{M}/M)$ has a finite rank, which occurs if and only if $\mu(M/k) = 0$. □

Recall that $k = k_0 \subset k_1 \subset \ldots \subset k$, and $k = m_0 \subset m_1 \subset \ldots \subset M$ are two disjoint $\mathbb{Z}_\ell$-extensions of k, and N = MK. For each $i \geq 0$, let $F_i = k_i M$. Then F_i/k_i is a $\mathbb{Z}_\ell$-extension and we now study these extensions.

Let $X_i = g(\overline{F_i}/F_i)$. The structure of the class group of $k_i m_n$, the n-th layer of F_i/k_i, is determined by the structure of X_i as a Λ_S module. That structure is not easily determined in the general case. We will find information about the invariants of F_i/k_i from the Λ_T structure of X_i.

Recall that $X_N = g(\bar{N}/N)$.

<u>THEOREM 3</u>. If N/M is unramified, then,

$$X_i \cong X_N/\omega_i(T)X_N \oplus \mathbb{Z}_\ell.$$

<u>PROOF</u>. If N/M is unramified, then $N \subseteq \overline{F_i} \subseteq \bar{N}$, and $\overline{F_i}$ is the maximal abelian extension of F_i contained in $\bar{N}$. Let $G_i = g(\bar{N}/F_i)$. Then $X_i = g(\overline{F_i}/F_i) \cong G_i/G_i'$. Since G_i is a semidirect product of X_N by $g(N/F_i) = \langle\tau^{\ell^i}\rangle \cong \mathbb{Z}_\ell$, we have $G_i' = (\tau^{\ell^i}-1)X_N = \omega_i(T)X_N$. Therefore X_i is a semi-direct product of $X_N/\omega_i(T)X_N$ with $g(N/F_i) \cong \mathbb{Z}_\ell$. But since X_i is abelian, the product must actually be a direct product. $\square$

<u>COROLLARY</u>. If $\mu(M/k) = 0$ and N/M is unramified, then $\mu(F_i/k_i) = 0$ and $\lambda(F_i/k_i) = r\ell^i + \sum_{n=0}^{i} c_n\varphi(\ell^n)$. The numbers r and c_n are non-negative integers, and $c_n = 0$ $\forall n \geq n_0$, for some integer n_0. The integer r is zero if and only if X_N is a torsion Λ_T module.

<u>PROOF</u>. If $\mu(M/k) = 0$, then X_N is a Noetherian Λ_T module, by Theorem 2. Therefore X_N is pseudo-isomorphic to some elementary module E, and $X_N/\omega_i(T)X_N \underset{p}{\cong} E/\omega_i(T)E$. Thus we have $X_i \underset{p}{\cong} E/\omega_i(T)E \oplus \mathbb{Z}_\ell$.

If,

$$E = \Lambda_T^r \bigoplus_{j=i}^{m} \Lambda_T/(f_j(T))^{n_j} \bigoplus_{g=1}^{h} \Lambda_T/(\ell^{n_g}),$$

then,

$$X_i \underset{p}{\cong} (\Lambda_T/(\omega_i(T)))^r \bigoplus_{j=1}^{m} \Lambda_T/(\omega_i(T),(f_j(T))^{n_j})$$

$$\bigoplus_{g=1}^{h} \Lambda_T/(\omega_i(T),\ell^{n_g}) \oplus \mathbb{Z}_\ell.$$

The module $\Lambda_T/(\omega_i(T),\ell^{n_h})$ is a finite for each i, n_h. The module $\Lambda_T/(\omega_i(T),(f_j(T)^{n_j}))$ is either finite, if $f_j(T) \nmid \omega_i(T)$, or is pseudo-isomorphic to $\Lambda_T/\nu_{n-1,n}(T)$ for some $n \subseteq i$, if $f_j(T) = \nu_{n-1,n}(T)$. Define $\nu_{-1,0}(T) = T$.

Let c_n be the number of $f_j(T)$ equal to $\nu_{n-1,n}(T)$. Then $c_n = 0$ $\forall n \geq n_0$, and $X_i \underset{p}{\cong} (\Lambda_T/(\omega_i(T))^r \bigoplus_{n=0}^{i} (\Lambda_T/\nu_{n-1,n}(T))^{c_n} \oplus \mathbb{Z}_\ell$. Since the module on the right has no elements annihilated by ℓ, X_i has only finitely many elements annilated by ℓ, hence $\mu(F_i/k_i) = 0$. We also have,

$$\lambda(F_i/k_i) = \dim_{\mathbb{Q}_\ell}(X_i \otimes_{\mathbb{Z}_\ell} \mathbb{Q}) = r\ell^i + \sum_{n=0}^{i} c_n \varphi(\ell^n) + 1.$$

This can be made into appropriate form by change of c_0. □

<u>Remark</u>: If $\lambda(M/k) = 1$, then $r = 0$, thus $\lambda(F_i/k_i)$ is bounded.

<u>THEOREM 4</u>. If N/M is ramified at some valuation, and unramified at all but a finite number of valuations, then there are integers n_0 and n_1, and Λ_T submodules $Y_i \subseteq X_N$

such that $\forall i \geq n_0, X_i \cong X_N/Y_i$, and $\forall i < n_0$, $X_i \underset{p}{\cong} X_N/Y_i$. Furthermore, $\forall i \geq n_1$, $Y_i = \nu_{n_1,i}(T)Y_{n_1}$.

Remark: A more exact description of n_0, n_1, and the Y_i is given in the proof.

Remark: Both the statement and proof of this theorem are essentially the same as in the case of a Z_ℓ-extension of a number field, and closely follow Serre [10].

PROOF. Recall that $\overline{F_i}$ is the maximal abelian unramified ℓ-extension of F_i. The extension $N\overline{F_i}/N$ is unramified, so $N\overline{F_i} \subseteq \overline{N}$, and therefore $\overline{F_i} \subseteq \overline{N}$. Let $G_i = g(\overline{N}/F_i)$, and $H_i = g(\overline{N}/\overline{F_i})$. Then,

$$X_i = g(\overline{F_i}/F_i) \cong G_i/H_i.$$

The theorem will follow from a description of the H_i.

Since G_i/H_i is abelian, $G_i' \subseteq H_i$. As above, $G_i' = \omega_i(T)X_N$. Let L_i denote the fixed field of G_i'. We have $F_i \subseteq \overline{F_i} \subseteq L_i \subseteq \overline{N}$. The extension L_i/F_i is abelian, and $\overline{F_i}$ is the maximal unramified subextension.

Let $v_0, \ldots, v_r$ denote the valuations of N which ramify in N/M, and $I_0, \ldots, I_r$ the corresponding inertia groups. Define b_j by $I_j = \ell^{b_j}\Gamma_2$, and let $n_0 = \min b_j$, $n_1 = \max b_j$. If necessary, relabel the v_i so that $b_0 = n_0$.

Pick valuations $w_0, \ldots, w_r$ of $\overline{N}$ which extend $v_0, \ldots, v_r$. Let I_j' denote the inertia group for w_j in $\overline{N}/M$.

Then $I_j' \cong \mathbb{Z}_\ell$. Pick $\sigma_0, \ldots, \sigma_r$ topological generators for $I_0', \ldots, I_r'$ such that $\sigma_j|_N = \tau^{\ell^{b_j}}$.

We have $F_i \subseteq N \subseteq L_i$, with L_i/N unramified, so each valuation which ramifies in L_i/F_i ramifies in N/F_i. We conclude that $\overline{F_i}$ is the subfield of L_i fixed by,

$$<I_0', \ldots, I_r'> \cap g(L_i/F_i).$$

Thus we have,

$$H_i = <\omega_i(T)X_N, \bigsqcup_{j=0}^{r} I_j' \cap G_i>.$$

Let $t_{ij} = \max(0, i-b_j)$. Then $I_j' \cap G_i = <\sigma_j^{\ell^{t_{ij}}}>$.

Let $a_{ij} = \sigma_j^{\ell^{t_{ij}}} \sigma_0^{-\ell^{b_j - b_0 + t_{ij}}}$. Since $a_{ij}|_N$ is the identity, $a_{ij} \in X_N$. We have $<I_j' \cap G_i, I_0' \cap G_i> = <I_0' \cap G_i, a_{ij}>$.

Therefore,

$$H_i = <\omega_i(T)X_N, a_{i1}, \ldots a_{ir}, I_0' \cap G_i>.$$

The groups X_N and $I_0' \cap G_i$ are disjoint, and for $i \geq n_0$, $X_N(I_0' \cap G_i) = G_i$. Since $G_i/X_N \cong I_0 \cap G_i \cong I_0' \cap G_i$, we have $I_0' \cap G_i$ acting on X_N by conjugation. Therefore G_i is a semidirect product of X_N by $I_0' \cap G_i$, and we have,

$$G_i/H_i = G_i/<\omega_i(T)X_N, a_{i1}, \ldots, a_{ir}, I_0' \cap G_i> \cong X_N/<\omega_i(T)X_N, a_{i1}, \ldots, a_{ir}>.$$

Let $Y_i = \langle \omega_i(T)X_N, a_{i1}, \ldots, a_{ir} \rangle$. We have shown that for $i \geq n_0$, $X_i \cong X_N/Y_i$.

For $i<n_0$, we have $F_i \subseteq F_{n_0} \subseteq \overline{F_i} \subseteq L_i$. In this case we have $g(\overline{F_i}/F_{n_0}) \cong G_{n_0}/\langle Y_i, I_0' \rangle \cong X_N/Y_i$. Since $g(F_{n_0}/F_i)$ is finite, $g(\overline{F_i}/F_{n_0}) \underset{p}{\cong} g(\overline{F_i}/F_i) = X_i$. Therefore, we have, for $i<n_0$, $X_i \underset{p}{\cong} X_N/Y_i$.

It remains to show that for $i \geq n_1$, $Y_i = \nu_{n_1,i}(T)Y_{n_1}$.

Since $Y_i = \langle \omega_i(T)X_N, a_{i1}, \ldots, a_{ir} \rangle$, and $\omega_i(T) = \nu_{n_1,i}(T)\omega_{n_1}(T)$, it suffices to show that,

$a_{ij} = \nu_{n_1,i}(T)a_{n_1j}$. For $j = 0, \ldots, r$, let $\gamma_j = \sigma_j^{\ell^{n_1-b_j}}$.

Then by the definition of a_{n_1j},

$$\gamma_j = a_{n_1j}\,\gamma_0$$

and therefore,

$$\gamma_j^{\ell^{i-n_1}} = (a_{n_1j}\,\gamma_0)^{\ell^{i-n_1}}$$

$$= a_{n_1j}\,\gamma_0\, a_{n_1j}\,\gamma_0^{-1}\,\gamma_0^2\, a_{n_1j} \cdots \gamma_0^{\ell^{i-n_1}-1}\, a_{n_1j}\,\gamma_0^{-(\ell^{i-n_1}-1)}\,\gamma_0^{\ell^{i-n_1}}$$

$$= a_{n_1j}^{1+\gamma_0+\gamma_0^2+\cdots+\gamma_0^{\ell^{i-n_1}-1}}\,\gamma_0^{\ell^{i-n_1}}.$$

Now, $a_{ij} = \gamma_j^{\ell^{i-n_1}}\,\gamma_0^{-\ell^{i-n_1}}$

so, $$a_{ij} = a_{n_1 j}^{1+\gamma_0+\gamma_0^2+\dots+\gamma_0^{\ell^{i-n_1-1}}}.$$

Since $\gamma_0|_N = \tau^{\ell^{n_1}}$, we have,

$$a_{ij} = a_{n_1 j}^{1+\tau^{\ell^{n_1}}+\tau^{2\ell^{n_1}}+\dots+\tau^{(\ell^{i-n_1}-1)\ell^{n_1}}} = \nu_{n_1,j}(T)a_{n_1 j}. \square$$

<u>COROLLARY 1</u>. If in addition to the hypotheses of Theorem 4, $\mu(F_{n_1}/k_{n_1}) = 0$, then for all $i \geq n_1+1$, $\mu(F_i/k_i) = 0$ and

$$\lambda(F_i/k_i) = r(\ell^i - \ell^{n_1}) + \sum_{n=n_1+1}^{i} c_n\, \varphi(\ell^n) + c,$$

for non-negative integers r, c, and c_n, with $c_n = 0$ $\forall n \geq n_2$ for some integer n_2.

<u>PROOF</u>. Theorem 4 states that $X_i \cong X_N/Y_i$. From the isomorphism for $i \geq n_1+1$

$$X_N/Y_{n_1} \cong \frac{X_N/Y_i}{Y_{n_1}/Y_i},$$

we obtain the exact sequence,

$$1) \quad 0 \to Y_{n_1}/Y_i \to X_i \to X_{n_1} \to 0.$$

If ${}_{\ell}A = \{a \in A \mid \ell a = 0\}$, then $\mu(F_i/k_i) = 0$ if and only if ${}_{\ell}X_i$ is finite. Applying the snake lemma to the exact sequence 1), we obtain the exact sequence,

$$0 \longrightarrow {}_{\ell}(Y_{n_1}/Y_i) \longrightarrow {}_{\ell}X_i \longrightarrow {}_{\ell}X_{n_1} .$$

Since ${}_{\ell}X_{n_1}$ is finite, we can show that $\mu(F_i/k_i) = 0$ by showing that ${}_{\ell}(Y_{n_1}/Y_i)$ is finite.

Since $\mu(F_{n_1}/k_{n_1}) = 0$, $\mu(M/k) = 0$, and by Theorem 2, X_N is a Noetherian Λ_T module. The submodule Y_{n_1} is also a Noetherian Λ_T module.

Proceeding as in the unramified case, we have,

$$Y_{n_1} \underset{p}{\cong} E = \Lambda_T^r \bigoplus_{j=1}^{m} \Lambda_T/(f_j(T))^{n_j} \bigoplus_{g=1}^{h} \Lambda_T/(\ell^{n_g})$$

and therefore,

$$2) \quad Y_{n_1}/Y_i = Y_{n_1}/\nu_{n_1,i}(T)Y_{n_1} \underset{p}{\cong} \left(\Lambda_T/\ \nu_{n_i,i}(T)\right)^r \bigoplus_{n=n_1+1}^{i} (\Lambda_T/\nu_{n-1,n}(T))^{c_n},$$

where c_n is the number of $f_j(T) = \nu_{n-1,n}(T)$. Thus ${}_{\ell}(Y_{n_1}/Y_i)$ is finite.

Now $\lambda(F_i/k_i) = \dim_{Q_\ell}(X_i \otimes_{\mathbb{Z}_\ell} Q_\ell)$. From 1), we have that for $i \geq n_1+1$

$$3) \quad \lambda(F_i/k_i) = \dim_{Q_\ell}(Y_{n_1}/Y_i \otimes_{\mathbb{Z}_\ell} Q_\ell) + \dim_{Q_\ell}(X_{n_1} \otimes_{\mathbb{Z}_\ell} Q_\ell).$$

We obtain from 2),

$$\dim_{Q_\ell}(Y_{n_1}/Y_i \otimes_{\mathbb{Z}_\ell} Q_\ell) = r(\ell^i - \ell^{n_1} + \sum_{n=n_1+1}^{i} c_n \varphi(\ell^n), \text{ with}$$

$c_n = 0 \ \forall_n \geq n_2$. Inserting this in 3), we are done. □

COROLLARY 2. If N/M has only finitely many ramified primes, and each prime which ramifies is totally ramified, and $\mu(M/k) = 0$, then for all i,

$$\lambda(F_i/k_i) = r\ell^i + \sum_{n=0}^{i} c_n \varphi(\ell^n)$$

with $c_n = 0$ for all $n \geq n_2$.

If, in addition, $\lambda(M/k) = 0$, then $r = 0$, so $\lambda(F_i/k_i)$ is bounded.

PROOF. The first part follows as in the previous corollary, since $n_0 = n_1 = 0$, and $X_i \cong X_N/\omega_n(T)X_N$.

If $\lambda(M/k) = 0$, then $0 = r\ell^0 + c_0$, so $r = c_0 = 0$.

Remark: If $r = 0$, then X_N is a torsion $Z_\ell[[T]]$ module, and therefore $d = \dim_{Q_\ell}(X_N \otimes_{\mathbb{Z}_\ell} Q_\ell)$ is finite. It follows that for any $\mathbb{Z}_\ell$-extension L/E, with $L \subseteq N$ and L having only finitely many valuations above ℓ, $\lambda(L/E) \leq d+1$ because X_L is essentially a factor module of $X_N \oplus \mathbb{Z}_\ell$.

V. OTHER $\mathbb{Z}_\ell$-EXTENSIONS CONTAINED IN N

We study here an extension N/k, as above, with $g(N/k) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$. Since for any $a, b, \in \mathbb{Z}_\ell$, such that ℓ does not divide both a and b, $\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell / \langle (a,b) \rangle \cong \mathbb{Z}_\ell$, the extension N/k contains infinitely many $\mathbb{Z}_\ell$-extensions.

For the next few results we look first at the situation where N/M has a unique ramified prime which is totally ramified, and later at the special case where N/k has a unique totally ramified prime. The examples in Section VI show that the second situation occurs infinitely often, and therefore the first does as well.

Recall that N = MK, with $k=k_0 \subset k_1 \subset \ldots \subset K$, and $k=m_0 \subset m_1 \subset \ldots \subset M$ two disjoint $\mathbb{Z}_\ell$-extensions, and $F_i = k_i M$.

<u>PROPOSITION 1</u>. If N/M has a unique totally ramified prime, then $X_i \doteq g(\overline{F_i}/F_i) \cong X_N/\omega_i(T)X_N$.

<u>PROOF</u>. This follows from the proof of Theorem 4, with $n_0 = n_1 = 0$ and $Y_i = \omega_i(T)X_N$.

We also use the following lemma [9 pg. 155], which is corollary of Nakayama's lemma.

We quote Nakayama's lemma for reference. [9].

Nakayama's Lemma. Let R be a ring, and E an R module. If I is an ideal of R contained in every maximal ideal, and IE=E, then I=0.

LEMMA. Let $\mathcal{O}$ be a local ring and $\mathfrak{m}$ its maximal ideal. Let E be a finitely generated $\mathcal{O}$ module, and F a submodule. If $E=F+\mathfrak{m}E$, then $E=F$.

PROOF. We have,

$$E = F+\mathfrak{m}E = F+\mathfrak{m}(F+\mathfrak{m}E) = F+\mathfrak{m}^2E.$$

By induction $E = F+\mathfrak{m}^nE$ for all n, and hence $E - F \subseteq \mathfrak{m}^nE$ for all n. Let $D = \bigcap_{n=1}^{\infty}\mathfrak{m}^nE$. $\mathfrak{m}D = D$, hence $D = 0$ by Nakayama's Lemma, so $E = F$. □

We now combine these two results.

THEOREM 5. If N/M has a unique totally ramified prime and $g(\overline{M}/M)$ is a cyclic $\mathbb{Z}_\ell$ module (i.e., $\mathbb{Z}/\ell^n\mathbb{Z}$ or $\mathbb{Z}_\ell$), then $X_N = \Lambda_T r$ for some $r \in g(\overline{N}/N)$. Thus $X_N \cong \Lambda_T/I$, where I is the ideal $\{h(T) \in \Lambda_T \mid h(T)r = 0\}$.

PROOF. Let $r' \in g(\overline{M}/M)$ generate $g(\overline{M}/M)$. By Proposition 1, $X_N/TX_N \cong g(\overline{M}/M)$, and the isomorphism is given by restriction. Let r be an element of $X_N = g(\overline{N}/N)$ such that $r|\overline{M} = r'$. Then $X_N = \mathbb{Z}_\ell r+TX_N \subseteq \Lambda_T r+\mathfrak{m}X_N$, where $\mathfrak{m} = (T,\ell)$ is the maximal ideal of the local ring Λ_T. Applying the lemma we see that $X_N = \Lambda_T r$. □

This characterization of X_N allows us to represent the action of Λ_S on X_N in terms of the Λ_T structure of X_N.

With the hypotheses of Theorem 5, we have $X_N = \Lambda_T r$. Since $Sr \epsilon X_N$, there is a power series $f(T) \epsilon \Lambda_T$ such that $SR = f(T)r$. The power series $f(T)$ is unique mod I. Thus $g(S)r = g(f(T))r$ and $g(S)X_N = g(f(T))X_N$.

In order for $g(f(T))$ to be well defined, and for future calculations, we show that $f(T)$ is in (T,ℓ), the maximal ideal of Λ_T.

If $f(T) \notin (T,\ell)$, then $f(T)$ is a unit in Λ_T and $f(T)X_N = X_N$. Thus $SX_N = X_N$, and if $X_M = g(\overline{M}/M)$, we have $SX_M = X_M$, since X_M is a factor module of X_N. But X_M is a Noetherian Λ_S module, and S is contained in the maximal ideal of Λ_S, so we can apply Nakayama's lemma to conclude $X_M = 0$. We have $X_M = X_N/TX_{N_1}$ so $X_N = TX_N$, hence $X_N = 0$. If $X_N = 0$, we may assume $f(T) \epsilon (T,\ell)$.

Recall that N = MK, with τ generating $g(N/M)$ and σ generating $g(N/K)$. There is a 1-1 correspondence between $\mathbb{Z}_\ell$-extensions of k contained in N and subgroups $H \subseteq g(N/k)$ such that $g(N/k)/H \cong \mathbb{Z}_\ell$. Such subgroups H are all of the form $<\tau^a\sigma^b>$ where ℓ does not divide both a and b. Let $L_{a,b}$ denote the subfield of N fixed by $<\tau^a\sigma^b>$. Then $\{L_{a,b} \mid a,b\epsilon\mathbb{Z}_\ell,\ \ell|a \Rightarrow \ell\nmid b\}$ is the set of all $\mathbb{Z}_\ell$-extensions of k contained in N. If $\ell \nmid a$, then a is a unit in $\mathbb{Z}_\ell$, so $<\tau^a\sigma^b> = <(\tau^a\sigma^b)^{a^{-1}}> = <\tau\sigma^{ba^{-1}}>$. Thus we can actually describe the set of $\mathbb{Z}_\ell$-extensions of k contained in N as $\{L_{1,b}, L_{a,1} \mid a,b\epsilon\mathbb{Z}_\ell,\ \ell|a\}$. Notice that $M = L_{1,0}$, and $K = L_{0,1}$.

Assume for the rest of this section that N/k has a unique totally ramified prime, and $g(\overline{M}/M)$ is a cyclic $\mathbb{Z}_\ell$ module. From Theorem 5, there is an $r \in X_N$ such that $X_N = \Lambda_T r \cong \Lambda_T/I$. Pick $f(T) \in \Lambda_T$ such that $Sr = f(T)r$. For $g(T) \in \Lambda_T$, with $g(T) \equiv 1 \pmod{m}$, and $a \in \mathbb{Z}_\ell$, define $(g(T))^a = \lim_{a_n \to a} (g(T))^{a_n}$.

THEOREM 6. With the above hypotheses and notation,

$$g(\overline{L_{a,b}}/L_{a,b}) \cong \Lambda_T/(I, (1+T)^a(1+f(T))^b-1).$$

PROOF. Since $N/L_{a,b}$ has a unique totally ramified prime, the field $\overline{NL_{a,b}}$ is the maximal subextension of $\overline{N}$ abelian over $L_{a,b}$. Since $g(N/L_{a,b}) = \langle \tau^a\sigma^b \rangle$, the subfield of $\overline{N}$ fixed by $(\tau^a\sigma^b-1)X_N$ is precisely $\overline{NL_{a,b}}$.

Thus we have,

$$g(\overline{L_{a,b}}/L_{a,b}) \cong g(\overline{NL_{a,b}}/N) \cong X_N/(\tau^a\sigma^b-1)X_N \cong X_N/((1+T)^a(1+f(T))^b-1)X_N$$

$$\cong \frac{\Lambda_T/I}{((1+T)^a(1+f(T)^b-1)(\Lambda_T/I)} \cong \Lambda_T/(I, (1+T)^a(1+f(T))^b-1). \qquad \square$$

For $L_{a,b} \neq L_{1,0}$, $\tau|_{L_{a,b}}$ generates a subgroup of finite index in $g(L_{a,b}/k)$, so it is precisely this Λ_T structure in which we are interested. In fact, for $k \subseteq L_n \subseteq L_{a,1}$, with $[L_n : k] = \ell^n$, we have,

$$g(\overline{L_n}/L_n) \cong \Lambda'_T/(I, (1+T)(1+f(T))^b-1, \omega_n(T)).$$

We cannot completely describe the invariants of $L_{a,b}/k$ without knowing I and f(T), but we can determine that $\mu(L_{a,b}/k) \neq 0$ for at most one of the $L_{a,b}$.

Greenberg [4] has shown that $\mu(L_{a,b}/k)$ is bounded in this situation, by entirely different methods. The result of this thesis assumes a stronger hypothesis, and is more explicit in its result.

We first prove the following results.

LEMMA. With the above hypotheses and notation, if $\ell \nmid ((1+T)^a(1+f(T))^b-1)$, then $\mu(L_{a,b}/k) = 0$.

PROOF. Assume $\mu(L_{a,b}/k) \neq 0$. Then if $Y = g(\overline{L_{a,b}}/L_{a,b})$, $Y/\ell Y$ is infinite. By Theorem 6 we have $Y \cong \Lambda_T/J$, where $J = (I, (1+T)^a(1+f(T))^b-1)$. We have the isomorphism,

$$Y/\ell Y \cong \frac{\Lambda_T/(\ell)}{(\ell, J)/(\ell)} .$$

Since $\Lambda_T/(\ell)$ has no infinite proper quotients, we must have $J \subseteq (\ell)$, and therefore $\ell \mid (1+T)^a(1+f(T))^b-1$. □

PROPOSITION 2. Assume that N/k has a unique totally ramified prime and $g(\overline{M}/M)$ is a cyclic $\mathbb{Z}_\ell$-module. If $\mu(K/k) \neq 0$, then $\mu(L_{a,b}/k) = 0$ for all other $L_{a,b}$.

PROOF. Since $K = L_{0,1}$, and $\mu(K/k) \neq 0$, the lemma implies that $\ell \mid (1+T)^0(1+f(T))-1 = f(T)$. For any $a,b \in \mathbb{Z}_\ell$, $(1+T)^a(1+f(T))^b-1 \equiv (1+T)^a-1 \pmod{(\ell)}$. If c is a unit in $\mathbb{Z}_\ell$, then $L_{a,b} = L_{ac,bc}$. Thus we may assume that a is an integer. For $a \neq 0$, $\ell \nmid (1+T)^a-1$, and therefore $\ell \nmid (1+T)^a(1+f(T))^b-1$. By the lemma, again, we have $\mu(L_{a,b}/k) = 0$ for $L_{a,b} \neq L_{0,1}$. □

PROPOSITION 3. Assume that N/k has a unique totally ramified prime and $g(\bar{M}/M)$ is a cyclic $\mathbb{Z}_\ell$-module. If $\mu(K/k) = 0$, and $L_{a,b} \cap M \neq k$, then $\mu(L_{a,b}/k) = 0$.

PROOF. Since $L_{a,b} \cap M \neq k$, we have $\ell \mid b$. Therefore $\ell \nmid a$, and we may assume $a = 1$. It suffices to show that $\ell \nmid (1+T)(1+f(T))^b-1$.

We will show that,

$$(1+T)(1+f(T))^b-1 \equiv T \qquad (\mathrm{mod}\ (\ell, T^\ell)).$$

It suffices to show that,

$$(1+f(T))^b \equiv 1 \qquad (\mathrm{mod}\ (\ell, T^\ell)).$$

We have,

$$(1+f(T))^b = (1+f(T))^{\ell c} = ((1+f(T))^c)^\ell = (1+g(T))^\ell$$

for some $g(T) \in (T, \ell)$.

Now,

$$\begin{aligned} (1+g(T))^\ell &\equiv 1+g(T)^\ell && (\mathrm{mod}\ \ell) \\ &\equiv 1 && (\mathrm{mod}\ (\ell, T^\ell)) \end{aligned}$$

and we are done. □

Combining these results we have the following theorem.

<u>THEOREM 7.</u> If N/k has a unique totally ramified prime, and $g(\bar{M}/M)$ is a cyclic $\mathbb{Z}_\ell$ module then there is at most one $\mathbb{Z}_\ell$-extension $L_{a,b}/k$, $L_{a,b} \subseteq N$, such that $\mu(L_{a,b}/k) \neq 0$.

<u>PROOF</u>. If $\mu(L_{a,b}/k) = 0$ for all $L_{a,b}$, then we are done. Assume $\mu(L_{a_0,b_0}/k) \neq 0$. If $\mu(K/k) \neq 0$, then Proposition 2 shows that $\mu(L_{a,b}/k) = 0$ for all other $L_{a,b}$.

Thus we may assume that $\mu(K/k) = 0$. By Proposition 3, L_{a_0,b_0} is disjoint from M. We may take $K_0 = L_{a_0,b_0}$, and since $M \cap K_0 = k$ and $N = MK_0$, we may apply Proposition 2 and conclude that $\mu(L_{a,b}/k) = 0$ for all other $L_{a,b}$.

<u>Remark</u>: (Suggested by Richard Foote.) If N and k were normal over Q, and $\mu(L/k) \neq 0$ for some $\mathbb{Z}_\ell$-extension of k contained in N, then any field L' conjugate to L would be a $\mathbb{Z}_\ell$-extension of k contained in N, with $\mu(L'/k) \neq 0$. If the hypotheses of Theorem 7 hold, we must have $L = L'$, so L is normal over Q. This places severe restrictions on L, and in most cases restricts it to a single extension.

If $\mu(L_{a,b}/k) = 0$ for all $L_{a,b}$, we will show that $\lambda(L_{a,b}/k)$ is bounded. This has been shown in a similar, more general setting by Greenberg [4].

PROPOSITION 4. If N/k has a unique totally ramified prime, $g(\bar{k}/k)$ is cyclic, and $\mu(L_{a,b}/k)=0$ for all $L_{a,b}$, then $\lambda(L_{a,b}/k)$ is bounded.

PROOF. We will assume λ unbounded, and construct a $\mathbb{Z}_\ell$-extension $L_{a,b}/k$ with nonzero μ invariant.

Given a field F, $k \subseteq F \subseteq N$, let $E(F)=\{L_{a,b} \mid F \subseteq L_{a,b}\}$. If F/k is not cyclic, $E(F)=\emptyset$. Notice that each field F, with F/k finite, $F \subseteq N$, has only $\ell+1$ extensions of degree ℓ, $F_0,\ldots,F_\ell$, with $F_i \subseteq N$. Also $E(F) = \bigcup_{i=0}^{\ell} E(F_i)$.

Let $F_0=k$. We will pick F_n with $[F_1:k]=\ell^n$, in the following manner. Pick F_1 with $[F_1:k]=\ell^n$, and λ unbounded in $E(F_1)$. This can be done since λ is unbounded in $E(F_0)$ and E(F) is the finite union of $E(F_{1,i})$ for the extensions $F_{1,i}$ of F of degree ℓ.

Pick F_n containing F_{n-1} with $[F_n:F_{n-1}]=\ell$, and λ unbounded in $E(F_n)$. We now show that there is a $\mathbb{Z}_\ell$-extension $L_{a,b}$, with $F_n \subseteq L_{a,b}$ for all n, thus $L_{a,b}=\bigcup_{n=1}^{\infty} F_n$.

We may assume $F_1 \cap M=k$. Thus $F_1 \subseteq L_{a_1,1}$ for at least one a_1. Pick such an a_1. Pick a_n so that $F_n \subseteq L_{a_n,1}$. Since the n-th layer of $L_{a,1}$ is the subfield of N fixed by $\langle \tau^a\sigma, \tau^{\ell^n} \rangle$, we see that the n-th layer is uniquely determined by the congruence class of a mod ℓ^n.

Thus we have for $i<j$, $a_i \equiv a_j \pmod{\ell^i}$. Let $a=\lim a_n$. Then $a \equiv a_n \pmod{\ell^n}$, and $F_n \subseteq L_{a,1}$.

One may see this in another way. The field F_n is the fixed field of $\langle \tau^{a_1}\sigma, \tau^{\ell^n} \rangle = \langle \tau^a\sigma, \tau^{\ell^n} \rangle$. Thus the union of the F_n is the fixed field of $\bigcap_{n=1}^{\infty} \langle \tau^a\sigma, \tau^{\ell^n} \rangle = \langle \tau^a\sigma \rangle$, so $\bigcup_{n=1}^{\infty} F_n = L_{a,1}$.

In order to show that $\mu(L_{a,1})\neq 0$, we use the following lemma.

LEMMA. If $k=F_0\subset F_1\subset\ldots\subset F_\infty$ is a Z_ℓ-extension with a unique totally ramified prime, $\mu(F_\infty/k)=0$, $\lambda(F_\infty/k)\neq 0$, and $g(\overline{k}/k)$ is cyclic, then rank $g(\overline{E_n}/E_n) = \min(\ell^n, \lambda(F_\infty/k))$.

PROOF. Let $X = g(\overline{F_\infty}/F_\infty)$. Let γ be a topological generator for $g(F_\infty/k)$, and make X into a Λ_T module by the action $1+T \longleftrightarrow \gamma$. Since F_∞/k has a unique totally ramified prime, $g(\overline{F_n}/F_n) \cong X/\omega_n(T)X$.

Since $g(\overline{k}/k) = X/TX$ is cyclic, $X \cong \Lambda_T/I$.

Since $\mu=0$, $\lambda\neq 0$, $I=(f(T))$, $\deg f(T)=\lambda$.

Thus if $G=g(\overline{F_n}/F_n)$, $G \cong \Lambda_T/(f(T), \omega_n(T))$, and $G/\ell G \cong \Lambda_T/(f(T), \omega_n(T), \ell) = \Lambda_T/(T^\lambda, T^{\ell^n}, \ell) \cong (\mathbb{Z}/\ell\mathbb{Z})^m$ with $m = \min(\lambda, \ell^n)$. □

Returning to the proof of the proposition, each F_n is contained in a $\mathbb{Z}_\ell$-extension L which satisfies the hypotheses of the lemma, and $\lambda(L/k)>\ell^n$.

Therefore, rank $g(\overline{F_n}/F_n) = \ell^n$, so $|g(\overline{F_n}/F_n)| \geq \ell^{\ell^n}$, so $\mu(L_{a,1}/k) \neq 0$. □

If $\mu(K/k) \neq 0$, then there are certain restrictions on the possible values of $\lambda(L_{a,b}/k)$, given by the following proposition.

PROPOSITION 5. If N/k has a unique totally ramified prime, $g(\overline{M}/M)$ is a cyclic $\mathbb{Z}_\ell$ module, and $\mu(K/k)\neq 0$, then $\lambda(L_{a,b,}/k)$ is either 0 or $[L_{a,b} \cap K:k]$.

PROOF. We can take $L_{a,b} = L_{\ell^n,b'}$, where $\ell^n = [L_{a,b} \cap K:k]$. We have $g(\overline{L_{a,b}}/L_{a,b}) \cong \Lambda_T/(I,(1+T)^{\ell^n}(1+f(T))^b-1)$ by Theorem 6. Since $\mu(K/k) \neq 0$, $\ell \mid f(T)$, so,

$$(1+T)^{\ell^n}(1+f(T))^b-1 \equiv T^{\ell^n} \pmod{\ell}$$

We also have $(1+T)^{\ell^n}(1+f(T))^b-1 = h(T)\,u(T)$ for some distinguished polynomial $h(T)$, and unit power series $u(T)$, by the Weierstrass preparation theorem. If $d=\deg h(T)$, then T^d is the smallest power of T with coefficient not divisible by ℓ in the power series,

$$\sum_{n=0}^{\infty} a_n T^n = (1+T)^{\ell^n}(1+f(T))^b-1.$$

Thus $d = \ell^n$.

Therefore $g(\overline{L_{a,b}}/L_{a,b})$ is a factor module of $\Lambda_T/h(T)$, with degree $h(T) = \ell^n$. Thus $\lambda(L_{a,b}/k) \le \ell^n$. If $\ell^n = 1$, we are done.

If $\lambda(L_{a,b}/k) \neq 0$, then $\Lambda_T/(I,h(T))$ is not finite, and $\Lambda_T/(I,h(T)) = \Lambda_T/p(T)$, with $p(T) \mid h(T)$ and $p(T) \mid I$. If $1 \le$ degree $p(T) < \ell^n$, then we argue as follows.

If, $K \subseteq L_n \subseteq L_{a,b}$, with $[L_n:k] = \ell^n$, then $L_n = k_n = L_{a,b} \cap K$, so rank $g(\overline{L_n}/L_n) = \ell^n$. But rank $g(\overline{L_n}/L_n) \le$ degree $p(T) < \ell^n$, a contradiction. Therefore $p(T)=h(T)$, and $\lambda(L_{a,b}/k) = \ell^n$. □

VI SOME EXAMPLES

Let ℓ be an odd prime, ζ a primitive ℓ-th root of unity, and $k=Q(\zeta)$. Let M be the cyclotomic $\mathbb{Z}_\ell$-extension of k. The extension M/k has a unique totally ramified prime.

If ℓ is a regular prime, i.e., $\ell\nmid h_k$, then any $\mathbb{Z}_\ell$-extension K/k has a unique totally ramified prime, and $\mu=\lambda=\gamma=n_0=0$. (c.f.[5]). In fact, if N is the composite of two $\mathbb{Z}_\ell$-extensions of such a field k, and $X_n=g(\bar{N}/N)$, then $X_n/(T,S)X_n \cong g(\bar{k}/k)=0$, whence $X_n=0$ by our corollary to Nakayama's lemma. Thus, every number field $k_i m_j$ contained in N has class number prime to ℓ, and every $\mathbb{Z}_\ell$-extension $L_{a,b}$ has zero invariants.

Let ℓ be such that $k=Q(\zeta)$ has class number exactly divisible by ℓ. Assume furthermore that $g(\bar{M}/M) \cong \mathbb{Z}_\ell$, where M is the cyclotomic Z_ℓ-extension of k. This occurs for $\ell=$ 37, 59, 67, and for all primes $\ell<30{,}000$ where $\ell \| h_k$. (See[8]).

<u>LEMMA.</u> (Suggested by David Dummit) If ℓ is such a prime, M/k the cyclotomic $\mathbb{Z}_\ell$extension, K/k a disjoint $\mathbb{Z}_\ell$-extension, and N=MK, then N/k has a unique totally ramified prime iff $\bar{k}$ is not contained in N.

<u>PROOF</u>. The field k has a unique prime $\mathfrak{p}$ over ℓ. Let v be a valuation of N extending the valuation of k

induced by $\mathfrak{p}$. Let T denote the inertia group for v in N/k. Since N/k is abelian, T does not depend upon the choice of v. Let E denote the fixed field of T. The extension E/k is unramified at $\mathfrak{p}$, and since only primes above ℓ can ramify in N/k, E/k is unramified.

If $\bar{k} \not\subseteq N$, then E=k, and $\mathfrak{p}$ is totally ramified in N/k. Thus N/k has a unique totally ramified prime.

If $\bar{k} \subseteq N$, then $\mathfrak{p}$ is not totally ramified in N/k. In fact, since $\mathfrak{p}$ is principal in k, splits in $\bar{k}/k$, so N does not even have a unique prime over $\mathfrak{p}$. □

Since k has $\ell+1/2$ independent Z_ℓ-extensions, there are many Z_ℓ-extensions K/k such that $\bar{k} \not\subseteq MK$. Let K be such a Z_ℓ-extension.

Thus we have the situation of Theorems 5 - 7, and can conclude from the results of that section that:

1. The μ invariant is nonzero for at most one Z_ℓ-extension of k contained in N. (Theorem 7)
2. If μ is nonzero for one such Z_ℓ-extension, then $\ell+1$ extensions of k of degree ℓ and contained in N must have the following structure. One extension has class group $(Z/\ell Z)^\ell$, and the other ℓ have class group $Z/\ell Z$ or $Z/\ell^2 Z$. One can see this as follows.

Since ℓ is not regular, $g(\bar{M}/M)$ is not finite [5]. We have shown that $g(M/M) \cong X_N/TX_N \cong \Lambda_T/(I,T)$. Thus $T \mid I$.

Now $g(\overline{k}/k) \cong \Lambda_T/(I,T,f(T)) \cong \mathbb{Z}_\ell/(f(0))$, so $f(0)=\ell u$, with u a unit in $\mathbb{Z}_\ell$. We may assume that $\mu(K/k) \neq 0$. Then, $g(\overline{k_1}/k_1) \cong \Lambda_T/(I, f(T), (1+T)^\ell - 1)$. Since $\ell \mid f(T)$, we have $f(T)=\ell u(T)$, with $u(T)$ a unit power series, and since $\mu(K/k) \neq 0$, $\ell \mid I$. Thus $g(\overline{k_1}/k_1) \cong \Lambda_T/(\ell, T^\ell) \cong (\mathbb{Z}/\ell\mathbb{Z})^\ell$. We also have,

$$g(\overline{m_1}/m_1) \cong \Lambda_T/(I,T,(1+f(T))^\ell - 1) \cong \mathbb{Z}_\ell/(1+f(0))^\ell - 1 \cong \mathbb{Z}_\ell/\ell^2$$
$$\cong \mathbb{Z}/\ell^2\mathbb{Z}.$$

Each other extension of k of degree ℓ is contained in some $L_{a,1}$, with $g(\overline{L_{a,1}}/L_{a,1}) \cong \Lambda_T/(I,(1+T)^a(1+f(T)-1)$. Since $f(T)=\ell u(T)$, $(1+T)^a(a+f(T))-1$ evaluated at $T = 0$ is ℓ times a unit. We have already shown (Proposition 5) that, $(1+T)^a(1+f(T))-1 = (T-c)u_a(T)$, where $u_a(T)$ is a unit power series, and $\ell \mid c$. We may now conclude that $\ell^2 \nmid c$. We now have $g(\overline{L_{a,b}}/L_{a,b}) \cong \Lambda_T/(I,T-c)$, and the ℓ-part of the class group of the first layer is a factor module of,

$$\Lambda_T/(T-c,(1+T)^\ell - 1) \cong \mathbb{Z}_\ell/(1+c)^\ell - 1 \cong \mathbb{Z}/\ell^2\mathbb{Z}.$$

If the structure mentioned in 2 of the class groups of the degree ℓ extensions of k did not exist, then one could conclude that μ would be zero for all $\mathbb{Z}_\ell$-extensions of k contained in N.

We now present a few examples for which the invariants can be computed. The theory of $\mathbb{Z}_\ell$-extensions of complex quadratic k is more developed than for arbitrary k, and portions of these examples have been computed.

by other authors. See, for example, Carroll and Kisilevsky [1].

In these examples k will be a complex quadratic number field, $k=\sqrt{-d}$. Let N be the composite of all $\mathbb{Z}_\ell$-extensions of k. Then $g(N/k) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$. Let M/k be the cyclotomic $\mathbb{Z}_\ell$-extension of k.

If ℓ is odd, or if $\ell=2$ and all quadratic extensions of k contained in N are normal over Q (it suffices that d have a prime factor congruent to ± 3 mod 8.), then there is a unique $\mathbb{Z}_\ell$-extension K/k which is normal over Q, and MK=N. See [1] for a proof of this fact.

If ℓ ramifies or remains prime in k/Q, and the class number of k is prime to ℓ, then $g(\bar{N}/N)=0$, and $\mu=\lambda=v=n_0=0$ for every $\mathbb{Z}_\ell$-extension of k.

<u>Example 1</u>. Let $\ell=2$ and $k=Q\sqrt{-p}$, where p is a prime, $p \equiv 5 \pmod 8$. Then $2 \mid h_k$, $4 \nmid h_k$.

If F is a quadratic extension of k contained in N, then F/Q is normal, since $p \equiv -3 \pmod 8$. Since k is complex, we have $g(F/Q) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, so $F=k\sqrt{d}$, $d \in \mathbb{Z}$. Because F/k is unramified outside 2, the only possible choices for F are $k(\sqrt{2})$, $k(\sqrt{-2})$, $k(\sqrt{-1})$, and each of these fields is contained in N.

Now $k(\sqrt{-1})/k$ is unramified and cyclic, and $4 \nmid h_k$. Therefore $k(\sqrt{-1})$ has class number prime to 2. Since $\mathfrak{p}_2$, the prime above z in k is not principal in k, $\mathfrak{p}_2$ remains prime in the extension $k(\sqrt{-1})/k$. Thus $N/k(\sqrt{-1})$ has a unique totally ramified prime over 2, and since the class number of $k(\sqrt{-1})$ is prime to 2, $g(\overline{N}/N)=0$.

Thus $\mu=\lambda=0$ for every $\mathbb{Z}_2$-extension of k. For $k\subseteq F\subseteq N$, we have $g(\overline{F}/F)=0$ if $k(\sqrt{-1})\subseteq F$, and $g(\overline{F}/F)\cong \mathbb{Z}/2\mathbb{Z}$ if $k(\sqrt{-1})\not\subseteq F$.

Example 2. Let $\ell=2$, $p\equiv 5 \pmod 8$ and $k=Q\sqrt{-2p}$. Again $2|h_k$, $4\nmid h_k$. The quadratic extensions of k contained in N are again $k(\sqrt{2})$, $k(\sqrt{-2})$, and $k(\sqrt{-1})$. Here $\overline{k} = k(\sqrt{-2})$, and the class number of $\overline{k}$ is prime to 2. Thus $N/k(\sqrt{-2})$ has a unique totally ramified prime and $g(\overline{N}/N)=0$. We have $\mu=\lambda=0$ for every $\mathbb{Z}_2$-extension of k. For $k\subseteq F\subseteq N$, $g(\overline{F}/F)=0$ if $\sqrt{-2}\in F$, and $g(\overline{F}/F)\cong \mathbb{Z}/2\mathbb{Z}$ if $\sqrt{-2}\notin F$.

Example 3. Let $\ell=2$, $p\equiv 3 \pmod 8$, and $k = \sqrt{-2p}$. Then $2|h_k$, $4\nmid h_k$, and $k(\sqrt{2})$, $k(\sqrt{-2})$, $k(\sqrt{-1})$ are the quadratic subextensions of k contained in N. We have $\overline{k} = k(\sqrt{2})$ and $\mathfrak{p}_2$ remains prime in $\overline{k}/k$. Again, $g(\overline{N}/N)=0$, and $\mu=\lambda=0$ for every $\mathbb{Z}_2$-extension of k. If $k\subseteq F\subseteq N$, we have $g(\overline{F}/F)=0$ if $\sqrt{2}\in F$, and $g(\overline{F}/F)\cong \mathbb{Z}/2\mathbb{Z}$ if $\sqrt{2}\notin F$.

Example 4. Let $\ell=2$, $p\equiv 7 \pmod 8$, and $k = Q\sqrt{-p}$. Assume furthermore that 8 does not divide the class number of $Q\sqrt{-2p}$. These conditions occur for p = 7,23,71, and for infinitely many other p.

The class number of k is prime to 2, and 2 splits in k/Q. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ denote the primes above 2 in k.

Let M be the cyclotomic $\mathbb{Z}_2$-extension of k. We have $k\subseteq k(\sqrt{2})\subseteq M$, and $\mathfrak{p}_1$, $\mathfrak{p}_2$ ramify in $k(\sqrt{2})/k$, so $\mathfrak{p}_1$ and $\mathfrak{p}_2$ ramify totally in M.

For $k\subseteq m_n\subseteq M$ with $[m_n:k]=2^n$, let $G = g(m_n/k)$. Genus theory implies that $|C_{m_n}^G|$ is either $2^n h_k$ or $2^{n-1}h_k$. Let F_n be the maximal unramified 2-extension of m_n which is abelian over k. Then $[F_n:m_n]$ is either 2^n or 2^{n-1}. Let $F = \bigcup_{n=1}^{\infty} F_n$. Then F/k is abelian, $k\subseteq M\subseteq F$, and F/M is not finite.

Let $G = g(F/k)$, $X = g(F/M)$ and let T_i be the inertia group for $\mathfrak{p}_i$ in F/k (i = 1,2). Let K_i denote the fixed field of T_i.

Since F/M is unramified, $T_i \cap X=0$ for i = 1,2. The fixed field of XT_i is contained in M and unramified at $\mathfrak{p}_i$, and is therefore equal to k. Thus $XT_i=G$, and $G \cong X\oplus T_i$. Therefore,

$$T_i \cong G/X \cong g(M/k) \cong \mathbb{Z}_2.$$

The fixed field of T_1T_2 is unramified over k, thus $T_1T_2 = G$. We also have $X\cong G/T_i \cong T_2/T_1\cap T_2$. Therefore X is isomorphic to a factor of $\mathbb{Z}_2$. But X is an infinite pro-2 group, so $X \cong \mathbb{Z}_2$, and $T_1\cap T_2=0$. Thus F is the composite of all $\mathbb{Z}_2$-extensions of k. The fields K_1 and K_2 are disjoint $\mathbb{Z}_2$-extensions of k and $F = K_1K_2$.

Let k_i denote the first layer of K_i. Then k_1, k_2, and $k(\sqrt{2})$ are the quadratic extensions of k contained in F.

We claim that the ramification index of $\mathfrak{p}_i$ in k_1k_2/k is 2. Since $k/(\sqrt{2})$ k_1k_2, and $\mathfrak{p}_i$ ramifies in $k(\sqrt{2})/k$, it is at least 2. Since $\mathfrak{p}_i$ does not ramify in k_i/k, it is at most 2.

Thus $k_1k_2/k(\sqrt{2})$ is unramified at 2, therefore unramified. One can easily show that $k(\sqrt{2})/Q(\sqrt{-2p})$ is unramified. Thus $k_1k_2/Q(\sqrt{-2p})$ is unramified.

The field k_1k_2 is normal over Q, hence normal over $Q(\sqrt{-2p})$. Since $[k_1k_2:Q(\sqrt{-2p})]=4$, $k_1k_2/Q(\sqrt{-2p})$ is an abelian unramified extension. We have $k_1k_2 \subset \overline{Q(\sqrt{2p})}$, whence $k_1k_2 = \overline{Q(\sqrt{-2p})}$. Using the fact that $g(\overline{Q(\sqrt{-2p})}/Q(\sqrt{-2p}))$ is cyclic, and that the prime above 2 in $Q(\sqrt{-2p})$ is not principal, we conclude that primes above 2 do not split in $k_1k_2/k(\sqrt{2})$. Therefore $\mathfrak{p}_1$ does not split in k_1/k, and thus does not split in K_1/k. Similarly, $\mathfrak{p}_2$ does not split in K_2/k.

Thus K_i/k has a unique totally ramified prime. Since $g(\overline{k}/k)=0$, $g(\overline{K_i}/K_i)=0$. The extension F/K_i also has a unique totally ramified prime, therefore $g(\overline{F}/F)=0$. Since F does not have an abelian unramified 2-extension, $F = \overline{M}$.

We can now describe the invariants of any $\mathbb{Z}_2$-extension, L, of k. If $L = K_1$ or $L = K_2$, then $\mu=\lambda=0$. Otherwise $\mu=0$, $\lambda=1$, $g(\overline{L}/L) \cong \mathbb{Z}_2$.

For $k \subseteq F \subseteq N$, $[F:Q]<\infty$, we have $g(\overline{F}/F)=0$ if $F \subseteq K_1$, and if $F \not\subseteq K_1$, $g(\overline{F}/F) \simeq \mathbb{Z}/2^n\mathbb{Z}$, where $2^n = [F:F \cap K_2]$.

REFERENCES

1. Carroll, J.E., and H. Kisilevsky, "Initial Layers of $\mathbb{Z}_\ell$-extensions of Complex Quadratic Fields," Compositio Mathematica 32 (1976), 157-168.

2. Carroll, J.E., and H. Kisilevsky, "On Iwasawa's λ-Invariant for Certain $\mathbb{Z}_\ell$-extensions," to appear.

3. Greenberg, R., "On the Iwasawa Invariants of Totally Real Number Fields," American Journal of Mathematics 98 (1976), 263-284.

4. Greenberg, R., "The Iwasawa Invariants of Γ-extensions of a Fixed Number Field," American Journal of Mathematics 95 (1973), 204-214.

5. Iwasawa, K., "On the Theory of Cyclotomic Fields," Annals of Mathematics 70 (1959), 530-561.

6. Iwasawa, K., "On the μ-invariants of $\mathbb{Z}_\ell$-extensions," Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1973, 1-11.

7. Iwasawa, K., "On $\mathbb{Z}_\ell$-extensions of Algebraic Number Fields," Annals of Mathematics 98 (1973) 246-326.

8. Johnson, W., "Irregular Primes and Cyclotomic Invariants," Mathematics of Computation 29 (1975), 113-120.

9. Lang, S., Algebra, Addison-Wesley, 1971.

10. Serre, J.-P., "Classes des Corps Cyclotomiques," Seminaire Bourbaki, Expose 174 (1958-59).