INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the original text directly from the copy submitted. Thus, some dissertation copies are in typewriter face, while others may be from a computer printer.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyrighted material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each oversize page is available as one exposure on a standard 35 mm slide or as a 17" × 23" black and white photographic print for an additional charge.

Photographs included in the original manuscript have been reproduced xerographically in this copy. 35 mm slides or 6" × 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
$\mathbb{Z}_p$-extensions of global fields and semisimple differentials

Villa-Salvador, Gabriel Daniel, Ph.D.

The Ohio State University, 1988
Z\textsubscript{p}-EXTENSIONS OF GLOBAL FIELDS
AND
SEMISIMPLE DIFFERENTIALS

DISSERTATION

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

By

Gabriel Daniel Villa Salvador, B.Sc., M.Sc.

\* \* \* \* \*

The Ohio State University

1988

Reading Committee

Robert Gold
Warren Sinnott
Manohar L.Madan

Approved By

Manohar L. Madan
Advisor
Department of Mathematics
ACKNOWLEDGMENTS

I am very grateful to my adviser Professor Manohar L. Madan for all his time and all his ideas which generously shared with me. Without them, his continued help and encouragement, none of this work would have been possible. It is a pleasure for me to say that Professor Madan not only has played the most important role in my mathematical maturation during these years at Ohio State, but also has been a wonderful friend.

I wish to express my appreciation to Professor Robert Gold and Professor Warren Sinnott for reading the original manuscript of this dissertation.
February 2, 1955 ............ Born - México Distrito Federal, México

1976...................... B.Sc., Escuela Superior de Física y Matemáticas
del Instituto Politécnico Nacional, México

1978...................... M.Sc., Centro de Investigaciones y Estudios
Avanzados del Instituto Politécnico Nacional,
México

1984-1988 ............... Teaching Assistantship, Department of Mathematics,
The Ohio State University

FIELDS OF STUDY

Major Field: Mathematics - Algebraic Number Theory
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>ii</td>
</tr>
<tr>
<td>VITA</td>
<td>iii</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td><strong>CHAPTER</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I. Zp-EXTENSIONS AND SEMISIMPLE DIFFERENTIALS</strong></td>
<td></td>
</tr>
<tr>
<td>§1. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>§2. Function Fields</td>
<td>4</td>
</tr>
<tr>
<td>§3. Number Fields</td>
<td>12</td>
</tr>
<tr>
<td><strong>II. AN ANALOGUE OF A CONJECTURE OF GROSS</strong></td>
<td>33</td>
</tr>
<tr>
<td>§1. Introduction</td>
<td>33</td>
</tr>
<tr>
<td>§2. Geometric Extensions</td>
<td>34</td>
</tr>
<tr>
<td>§3. Constant Extensions</td>
<td>49</td>
</tr>
<tr>
<td>§4. Examples</td>
<td>50</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>53</td>
</tr>
</tbody>
</table>
INTRODUCTION

A global field is a finite extension of the field of rational numbers or a finite extension of the field of rational functions of one variable over a finite field of constants. A $\mathbb{Z}_p$-extension of a global field is a Galois extension such that the Galois group is isomorphic to the additive group of $\mathbb{Z}_p$ the ring of $p$-adic integers. The field $\mathbb{Q}$ of rational numbers has a unique $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$. A $\mathbb{Z}_p$-extension of number fields is said to be basic or cyclotomic if it is obtained by forming the composite with $\mathbb{Q}_\infty$ of a finite extension of $\mathbb{Q}$. It is an important conjecture of Iwasawa that the $p$-part of the class group of a basic $\mathbb{Z}_p$-extension is divisible. In this dissertation the $\mathbb{Z}_p$-extensions of number fields considered will be always cyclotomic and we shall assume the truth of Iwasawa's conjecture. A $\mathbb{Z}_p$-extension of number fields is said to be of CM-type if it is obtained by forming the composite with a finite extension of $\mathbb{Q}$ which is totally imaginary and it is a quadratic extension of a totally real field. For $\mathbb{Z}_p$-extensions of CM type the minus part and the plus part of the $p$-class group are defined in a natural way. In Chapter I, we consider a finite Galois $p$-extension $E/F$ of basic extensions of CM type. We obtain an exact sequence which determines uniquely (Theorem 5) the structure of the minus $p$-part of the elementary abelian $p$-subgroup of the class group of $E$ as $F_p[G]$-module, where $G = \text{Gal}(E/F)$ and $F_p$ is the field with $p$ elements. In some special cases, the structure is determined explicitly. In the case that $E/F$ is unramified, we also determine explicitly the structure of the minus $p$-part of the class group of $E$ as $\mathbb{Z}_p[G]$-module. In Chapter I, we also study the differentials of a field of algebraic functions of one variable over an algebraically closed field of constants $k$. If $E/F$ is a finite Galois extension of such fields, $\text{Gal}(E/F)$ operates in a natural way on the space of holomorphic differentials of $E$ giving it the structure of a $k[G]$-module. In the classical case, when $k$ is the field of complex numbers, the structure was determined completely by Chevalley and Weil [2]. We are
interested in the case when $k$ has characteristic $p$. We study the submodule of holomorphic differentials which is generated by differentials invariant under the Cartier operator. If $E/F$ is a finite $p$-extension, Nakajima [27] obtained two exact sequences which determined implicitly the structure of this submodule of semisimple differentials as $k[G]$-module. In many cases, e.g. if there is a fully ramified prime, we determine the structure explicitly. Heller's operator [13, 14] plays a critical role in our study.

In Chapter II we are concerned with a problem in the theory of global fields of characteristic $p$ which is analogous to a conjecture of Gross in Iwasawa Theory. $\mathbb{Z}_p$-extensions $K_\infty/K_0$ of congruence function fields $K_0$ of characteristic $p \neq 2$ involving no new constants are considered such that the set $S$ of ramified primes is finite and these primes are fully ramified. Is the set of $S$-classes invariant under $\text{Gal}(K_\infty/K_0)$ finite? Gross' conjecture asserts that a similar question has an affirmative answer for the class of cyclotomic $\mathbb{Z}_p$-extensions of CM-type if $S$ is the set of $p$-primes and the classes considered are minus $S$-classes. Using a formula of Witt for the norm residue symbol in cyclic $p$-extensions of local fields of characteristic $p$, a necessary and sufficient condition for the validity of the analogue of Gross' conjecture is given for a class of extensions $K_\infty/K_0$. It is shown by examples that the analogue of Gross' conjecture is not always true.

The above remarks will be elaborated in the introductions to the two chapters and more references to the relevant literature will be provided.
CHAPTER I

Z_p-EXTENSIONS AND SEMISIMPLE DIFFERENTIALS

§1. Introduction.

Let $F/k$ be a field of algebraic functions of one variable, $k$ algebraically closed. The holomorphic differentials $\Omega_F(0)$ form a vector space over $k$ of dimension $g_F$, the genus of $F$. If $E/k$ is a Galois extension of $F/k$, $G = \text{Gal}(E/F)$ operates in a natural way on $\Omega_E(0)$. In the classical case, when $k$ is the field of complex numbers, the structure of $\Omega_E(0)$ as a $k[G]$-module was completely determined by Chevalley and Weil [2]. For fields of finite characteristic $p$, the problem has been solved if the extension $E/F$ is tamely ramified [5, 20, 26, 28, 37, 39, 40]. If the extension is wildly ramified, the structure of $\Omega_E(0)$ has been determined only in the case when $E/F$ is a cyclic $p$-extension [39].

In this chapter, we are primarily interested in the case when $E/F$ is a wildly ramified $p$-extension. In this case, in a recent paper [27], Nakajima has obtained two exact sequences which determine implicitly the structure of the $k[G]$-module $\Omega_E^S(0)$ of semisimple holomorphic differentials, that is, the submodule generated by holomorphic differentials which are invariant under the Cartier operator. Assuming that at least one prime ramifies fully, we determine explicitly the structure of the $k[G]$-module $\Omega_E^S(0)$. This is the main result (Theorem 1) of § 2. The holomorphic differentials which are invariant under the Cartier operator, $\Omega_{E,F_p}^S(0)$, form a $F_p[G]$-module which is canonically isomorphic to the $F_p[G]$-module of divisor classes formed by classes of order dividing $p$, $F_p$ denoting the field with $p$ elements. Theorem 1 enables us to determine the structure of this module. If $E/F$ is unramified, we use Heller's loop-operation [13, 14] and some ideas of Nakajima [26] to determine the structure of $\Omega_{E,F_p}^S(0)$.
§ 3 is devoted to number fields. For an odd prime $p$, we consider a Galois $p$-extension $E/F$ such that $E$, $F$ are basic $\mathbb{Z}_p$-extensions of CM-type. We obtain an exact sequence (Theorem 5) which determines uniquely the structure of $pC_E$, the minus part of the $p$-elementary abelian class group of $E$ as $F_p[G]$-module (we assume Iwasawa's conjecture that the $\mu$-invariant vanishes for basic $\mathbb{Z}_p$-extensions). In two special cases, Theorem 5 enables us to determine the structure of $pC_E$ explicitly, firstly if the extension is ramified and $F$ does not contain the $p$-th roots of unity (Theorem 6) and secondly if there is one fully ramified prime (Theorem 7). Theorem 8 deals with the unramified case.

Finally, Theorem 9 is on integral representations. Let $\mathbb{Z}_p$, $\mathbb{Q}_p$ denote the ring of $p$-adic integers and the field of $p$-adic numbers respectively. In [15], Iwasawa determines the structure of $C_E(p)$, the minus $p$-part of the class group of $E$ as a $\mathbb{Q}_p[G]$-module, we determine explicitly its structure as $\mathbb{Z}_p[G]$-module in the unramified case. This is the analogue of a Theorem of Valentini [38] in the function field case. Using Theorem 9 we give alternative proof of Theorem 8.

§2. Function Fields.

Let $k$ be an algebraically closed field, $\text{char } k > 0$. Let $E/k$ be a finite Galois $p$-extension of $F/k$, where $E$, $F$, are algebraic function fields of one variable over $k$, say $[E:F] = p^n$, $n \geq 1$. We assume that there exists at least one fully ramified prime in this extension. Let $\{P_1, P_2, \ldots, P_r\}$ be the primes in $F$ which ramify in $E/F$ and let $P_r$ be fully ramified. We choose $\{Q_1, Q_2, \ldots, Q_r\}$ primes in $E$ dividing $P_j$, $1 \leq i \leq r$, with $p^{e_i}$ the ramification degree of $P_j$, $1 \leq i \leq r$. Note that $e_i = n$.

Consider $G_i = \{\sigma \in G \mid Q_i^\sigma = Q_i\} = \text{Dec } (Q_i)$, the decomposition group of $Q_i$ ($G = \text{Gal}(E/F)$). We have $|G_i| = p^{e_i}$, $|G/G_i| = p^{n-e_i}$, $1 \leq i \leq r$. In particular, $G_r = G$, $G/G_r = \{1\}$.

We have the following $k[G]$-exact sequence [27]:

\[
\begin{align*}
0 \longrightarrow \Omega_E^8(0) \longrightarrow k[G]^\tau_F \longrightarrow \ker \Phi \longrightarrow 0,
\end{align*}
\]

where: $\tau_F$ = The Hasse - Witt invariant of $F$, $\Phi = \bigoplus_{i=1}^r \Phi_i$, $\Phi_i : k[G/G_i] \longrightarrow k$. 

\[ \Phi_i \left( \sum_{\sigma \in G/G_i} a_\sigma \sigma \right) = \sum_{\sigma \in G/G_i} a_\sigma \] (\( \oplus \) denotes direct sum).

Note that \( k[G/G_t] = k \) as \( k[G] \)-modules with \( k \) considered as trivial \( k[G] \)-module.

We consider the following map: \( \phi : \oplus\limits_{i=1}^{r-1} k[G/G_i] \rightarrow \ker \Phi \),

\[ \phi (\xi_1, \xi_2, \ldots, \xi_{r-1}) = (\xi_1, \xi_2, \ldots, \xi_{r-1}, -\Phi_1(\xi_1) - \Phi_2(\xi_2) - \cdots - \Phi_{r-1}(\xi_{r-1})). \]

Then, \( \phi \) is 1 to 1, \( k[G] \)-homomorphism and since \( \dim_k \left( \oplus\limits_{i=1}^{r-1} k[G/G_i] \right) = \)

\[ \dim_k \left( \ker \Phi \right) = \sum_{i=1}^{r-1} \frac{|G|}{|G_i|}, \phi \text{ is } k[G]-\text{isomorphism}. \]

Hence, (1) becomes

\[
\begin{array}{c}
0 \longrightarrow \Omega^0 \longrightarrow k[G]^{\mathbb{Z}_{-1} \mathbb{Z}} \longrightarrow \oplus\limits_{i=1}^{r-1} k[G/G_i] \longrightarrow 0
\end{array}
\]

Let \( \Omega \) be the loop-space operation defined in [13], that is: for a \( k[G] \)-module \( M \), choose \( X \) any \( k[G] \)-projective module such that there exists a \( k[G] \)-epimorphism \( \zeta : X \longrightarrow M \). Write \( N = \ker \zeta = N^{(0)} + N^{(1)} \), where \( N^{(1)} \) is \( k[G] \)-projective and \( N^{(0)} \) contains no projective direct summand. Then the loop-space operation is defined by:

\( \Omega M = N^{(0)} \). The module \( N^{(0)} \) is determined uniquely up to isomorphism.

In general we have \( \Omega \left( \oplus\limits_{i \in I} M_i \right) = \oplus\limits_{i \in I} \Omega M_i \). So in particular

\[
\begin{array}{c}
\Omega \left( \oplus\limits_{i=1}^{r-1} k[G/G_i] \right) = \oplus\limits_{i=1}^{r-1} \Omega \left( k[G/G_i] \right)
\end{array}
\]

We define \( A_i = \Omega(k[G/G_i]), 1 \leq i \leq r - 1 \). Now for any subgroup \( H \neq \{1\} \) of \( G \), we consider \( k[G/H] \) as a \( k[G] \)-module. We write \( G = x_1 H \cup \cdots \cup x_r H \), where the symbol \( \cup \) means disjoint union and \( t = [G : H] \).

Let \( \gamma \) be the map: \( \gamma : k[G] \longrightarrow k[G/H] \), given by

\[ \gamma \left( \sum_{\sigma \in G} a_\sigma \sigma \right) = \sum_{i=1}^{t} \left( \sum_{\sigma \in \tilde{x}_i} a_\sigma \right) \tilde{x}_i, \text{ where } \tilde{x}_i = x_i H. \]
Then $\gamma$ is $k[G]$-epimorphism. So we have the following $k[G]$-exact sequence:

$$0 \longrightarrow \ker \gamma \longrightarrow k[G] \longrightarrow k[G/H] \longrightarrow 0.$$  

We have $\dim_k (\ker \gamma) = \dim_k (k[G]) - \dim_k (k[G/H]) < \dim_k (k[G]).$

From this follows $\Omega(k[G/H]) = \ker \gamma$, since $G$ is a $p$-group and $\text{char } k = p$.

In particular, we have:

(4) $A_i = \Omega(k[G/G_i]) = \left\{ \sum_{\sigma \in G} a_{\sigma} \sigma \in k[G] \mid \sum_{\sigma \in G} a_{\sigma} = 0, 1 \leq j \leq t_i \right\},$

where $G = \beta_{1,1} G_1 \cup \beta_{2,1} G_1 \cup \ldots \cup \beta_{t_i,1} G_1$, $\beta_{j,i} = \beta_{j,i} G_i, 1 \leq i \leq r - 1$.

Observe that $\dim_k A_i = \dim_k (k[G]) - t_i = |G| - p^n - p^{n-e_i}$.

From (2) we obtain

(5) $\Omega^s_E(0) = k[G]^u \oplus \sum_{i=1}^{r-1} (k[G/G_i]) - k[G]^u \oplus (\oplus A_i)^u, \text{ for some } u.$

Now by the Deuring - Šafarevič formula [23], we have

$$\dim_k \Omega^s_E(0) = \tau_E = |G| \cdot \left\{ \tau_F - 1 + \sum_{i=1}^{r} (1 - p^{e_i}) \right\} + 1 =$$

$$|G| \cdot \tau_F - |G| + \sum_{i=1}^{r} (|G| - \frac{|G|}{|G_i|}) + 1.$$

From (5), we have:

$$\dim_k \Omega^s_E(0) = u \cdot |G| + \sum_{i=1}^{r-1} \dim_k A_i = u \cdot |G| + \sum_{i=1}^{r-1} (|G| - \frac{|G|}{|G_i|}).$$

Therefore:

$$|G| \cdot \tau_F - |G| + \frac{|G|}{|G_F|} + 1 = u \cdot |G| \text{ or } u = \tau_F, \text{ because } \frac{|G|}{|G_F|} = 1.$$

We can now state:
THEOREM 1.

With the notation as above, we have:

\[ \Omega^s_E(0) = k[G]^{TF} \oplus (\oplus A_i) \] as \( k[G] \)-modules, and \( A_i \) is the indecomposable \( k[G] \)-module given by (4).

PROOF.

It remains to prove that \( A_i \) is indecomposable.

If \( H \) is any subgroup of \( G \),

\[ (k[G/H])^G = \{ a \sum_{\sigma \in G/H} a \in k \} \]

where \( M^G = \{ m^\sigma = m \text{ for all } \sigma \in G \} \), \( M \) any \( k[G] \)-module.

So \( \dim_k (k[G/H])^G = 1 \). If \( k[G/H] = M \oplus N \) then \( (k[G/H])^G = M^G \oplus N^G \) and since \( G \) is a \( p \)-group, \( \dim_k M^G \geq 1 \), \( \dim_k N^G \geq 1 \) this contradicts (6). Therefore \( k[G/H] \) is an indecomposable \( k[G] \)-module.

From ([13], Proposition 1), it follows that \( \Omega(k[G/H]) \) is indecomposable. Therefore, \( A_i \) is \( k[G] \)-indecomposable.

\[ \sqrt{ } \]

If \( pC_{0E} \) denotes the subgroup of \( C_E \), the class group of \( E \), consisting of the elements of order dividing \( p \), then we have

PROPOSITION 1.

\[ pC_{0E} = \Omega^s_{E,F_p} \] (0) as \( F_p[G] \)-modules.

PROOF.

Let \( \theta : pC_{0E} \longrightarrow \Omega^s_{E,F_p} \) (0) be given as follows:
If \( d \in pC_0E \), choose a divisor \( D \) in the class \( d \), then \( D^p \) is principal, \( C^p=(f) \). Define \( \theta(d)=\frac{df}{f} \). This is an isomorphism of abelian groups ([34], Proposition 10), and \( \theta \) is \( F_p[G] \)-homomorphism, hence we have Proposition 1.

Let \( S \) be any finite set of prime divisors of \( F \). Following [27] we define

\[
\Omega^S_{F,S,F_p}(0) = \bigcup_{l=1}^{\infty} \Omega^S_{F,F_p}(-l[S]),
\]

where

\[
\Omega^S_{F,F_p}(-l[S]) = \{ \omega \mid \omega \text{ differential in } F, C(\omega) = \omega \text{ and } \text{div}(\omega) \geq -l[S] \},
\]

\( [S] = \sum_{P \in S} P, \) \( \text{div}(\omega) = \text{divisor of } \omega \) and \( C \) denotes the Cartier operator.

Observe that \( \Omega^S_{F,S,F_p}(0) = \{ \text{semisimple differentials with poles in } S \} \).

Now we have

**Proposition 2.**

(i) \( \Omega^S_{F,S,F_p} = \Omega^S_{F,F_p}(-[S]) \).

(ii) \( \dim_{F_p} \Omega^S_{F,F_p}(-[S]) = \tau_F - 1 + |S|, \) if \( S \neq \emptyset \).

\( (\tau_F = \text{the Hasse-Witt invariant of } F) \).

**Proof.**

(i) [27], Proposition 1, page 561 or [35], Lemma 2.5, page 174.

(ii) From [27] we have \( \dim_k \Omega^S_F(-[S]) = \tau_F - 1 + |S| \), and on the other hand:

\[
\Omega^S_F(-[S]) = k(\{ \omega \in \Omega^S_F \mid C(\omega) = \omega \}) =
\]

\{linear space over \( k \) generated by \( \omega \) with \( C(\omega) = \omega \}.

Hence \( \dim_k \Omega^S_F(-[S]) = \dim_{F_p} \Omega^S_{F,F_p}(-[S]) = \tau_F - 1 + |S| \).

The following two Lemmas are straightforward
LEMMA 1.


♦

LEMMA 2.

\[ \Omega_{E,F_p}^S(-[\Pi^{-1}(S)]) \otimes_{F_p} k = \Omega_{E}^S(-[\Pi^{-1}(S)]) \] as \( k[G] \)-modules where
\[ \Pi^{-1}(S) = \{Q \mid Q \text{ prime in } E \text{ such that } Q \mid P, \text{ for } P \in S \} \].

♦

LEMMA 3.

If \( M \otimes_{F_p} k = N \otimes_{F_p} k \) as \( k[G] \)-modules, then \( M = N \) as \( F_p[G] \)-modules.

PROOF.

[26], Lemma 2, page 5.

♦

PROPOSITION 3.

Let \( S_0 = \{ P \text{ prime divisor in } F \mid P \text{ is ramified in } E/F \} \) and let \( S \supseteq S_0 \) with \( S \neq \emptyset \). Then we have \[ \Omega_{E,F_p}^S(-[\Pi^{-1}(S)]) = F_p[G]^{5F^{-1}+|S|} \].

PROOF.

By Lemma 1, \[ F_p[G]^{5F^{-1}+|S|} \otimes_{F_p} k = k[G]^{5F^{-1}+|S|} \].

By Lemma 2, \[ \Omega_{E,F_p}^S(-[\Pi^{-1}(S)]) \otimes_{F_p} k = \Omega_{E}^S(-[\Pi^{-1}(S)]) \].

Now, when \( S \neq \emptyset \), \( \Omega_{E}^S(-[\Pi^{-1}(S)]) \) is a \( k[G] \)-free module [27, Theorem 1, page 561], so \( \Omega_{E}^S(-[\Pi^{-1}(S)]) = k[G]^{5F^{-1}+|S|} \).

Hence by Lemma 3, \[ \Omega_{E,F_p}^S(-[\Pi^{-1}(S)]) = F_p[G]^{5F^{-1}+|S|} \].
Now we define $B_i = \Omega (F_{p[G/G_i]})$, with $\Omega$ = loop-space operation.

Then $B_i = \left\{ \sum_{\sigma \in G} a_{\sigma} \sigma \mid \sum_{\sigma \in B_{j,i}} a_{\sigma} = 0, 1 \leq j \leq t_i \right\}$, and $\dim_{F_p} B_i = p^{n - p^{n-e_i}}, 1 \leq i \leq r$. Also $B_i$ is indecomposable $F_p[G]$-module.

**LEMMA 4.**

$B_i \otimes_{F_p} k = A_i$ as $k[G]$-modules.

So, if we have that at least one prime ramifies fully, then

**THEOREM 2.**

$\Omega^S_{E,F_p}(0) = F_p[G]^T F \oplus \bigoplus_{i=1}^{r-1} B_i$.

**PROOF.**

We have that $\Omega^S_{E,F_p}(0) \otimes_{F_p} k = \Omega^S_E(0)$ as $k[G]$-modules (the proof is similar to that in Lemma 2). Therefore by (4), Lemmas 1 and 4, we obtain

$\Omega^S_{E,F_p}(0) \otimes_{F_p} k = \Omega^S_E(0) = k[G]^T F \oplus \left( \bigoplus_{i=1}^{r-1} A_i \right) \cong \left( F_p[G]^T F \oplus \left( \bigoplus_{i=1}^{r-1} B_i \right) \right) \otimes_{F_p} k$

as $k[G]$-modules. Therefore, Lemma 3 gives us Theorem 2.

Finally, we study the unramified case.

**THEOREM 3.**

Let $E/F$ be unramified, $G = \text{Gal}(E/F)$ a $p$-group and let $d$ be the minimum number of generators of $G$, then $d \leq \tau_F$ and $\Omega^S_{E,F_p}(0) = \Omega^2 F_p \oplus F_p[G]^T F^{-d}$, where $\Omega$ = loop-operation, and $\Omega^2 F_p$ is an indecomposable $F_p[G]$-module.
The following proof is similar to that of Proposition 13 in [26].

In [27], Theorem 2 (ii), Nakajima obtained the following exact sequence of $k[G]$-modules:

\begin{equation}
0 \rightarrow \Omega^5_E(0) \rightarrow k[G]^F \rightarrow I_G \rightarrow 0
\end{equation}

where $I_G = \left\{ \sum_{\sigma \in G} a_{\sigma} \in k[G] \mid \sum_{\sigma \in G} a_{\sigma} = 0 \right\}$.

Following [26], we have:

\[d = \dim_k \left( I_G / I_G^2 \right), \theta : k[G] \rightarrow k, \theta \left( \sum_{\sigma \in G} a_{\sigma} \sigma \right) = \sum_{\sigma \in G} a_{\sigma}, \theta \text{ is a $k[G]$-epimorphism and ker } \theta = I_G \text{ which has no projective direct summands, that is the sequence:}\]

\[0 \rightarrow I_G \rightarrow k[G] \rightarrow k \rightarrow 0\]

is exact and $\Omega k \cong I_G$.

There exists a $k[G]$-epimorphism $\mu : k[G]^d \rightarrow I_G$, and since $d$ is minimal, ker $\mu$ does not contain any projective summand. Thus

\[0 \rightarrow \ker \mu \rightarrow k[G]^d \rightarrow I_G \rightarrow 0\]

is exact, $\Omega I_G = \ker \mu = \Omega^2 k$ indecomposable, and $\dim_k (\ker \mu) = \dim_k k[G]^d - \dim_k I_G = d \cdot |G| - (|G| - 1) = |G| \cdot (d - 1) + 1$.

From (7) we obtain $\Omega^8_E(0) = (k[G])^t \oplus \Omega I_G = (k[G])^t \oplus \Omega^2 k$ with $t \geq 0$. Therefore, $\dim_k \Omega^8_E(0) = \tau_E = 1 + |G| \cdot (\tau_F - 1) = \dim_k \left( (k[G])^t \oplus \Omega^2 k \right) = t \cdot |G| + 1 + |G| \cdot (d - 1)$.

Hence $t + d - 1 = \tau_F - 1$ and $t = \tau_F - d \geq 0$.

Now, it can be easily proved that $\Omega^2 k = \Omega^2 F_p \otimes_{F_p} k$. Also

$\Omega^8_E(0) = (k[G])^t \oplus \Omega^2 k \text{ ([26])}$.
Therefore, using Lemma 2 and these remarks, we have

$$\Omega^S_{E,F_p}(0) \otimes_{F_p} k = \Omega^S_E(0) = (k[G])^{\tau F-d} \oplus \Omega^2 k = (\Omega^2 F_p \oplus (F_p[G])^{\tau F-d}) \otimes_{F_p} k$$

as $k[G]$-modules. Thus, by Lemma 3, $\Omega^S_{E,F_p}(0) = \Omega^2 F_p \oplus (F_p[G])^{\tau F-d}$

We finish this section by stating analogous of Theorems 2 and 3 for $pC_{0E}$.

**THEOREM 4.**

Let $E/F$ be as above.

(i) If $E/F$ is unramified, then $d \leq \tau_F$, $pC_{0E} = \Omega^2 F_p \oplus (F_p[G])^{\tau F-d}$ as $F_p[G]$-modules, $\Omega^2 F_p$ is indecomposable and $\dim_{F_p} \Omega^2 F_p = 1 + |G| \cdot (d - 1)$.

(ii) If $E/F$ is ramified and there is at least one fully ramified prime, then

$$pC_{0E} = F_p[G]^{\tau F} \oplus \left( \bigoplus_{i=1}^{r-1} B_i \right)$$

as $F_p[G]$-modules, where

$$B_i = \left\{ \sum_{\sigma \in G} a_{ij} \sigma \mid \sum_{\sigma \in G} a_{ij} = 0, 1 \leq j \leq t_i \right\}$$

is indecomposable.

§3. Number Fields.

In this section we consider, for a prime number $p$, a basic cyclotomic $\mathbb{Z}_p$-field $F$.

If $\zeta_{pn}$ denotes a primitive $p^n$-th root of 1, $Q_{n-1}$ the unique subfield of $\mathbb{Q}(\zeta_{pn})$ such that

$$[Q_{n-1} : \mathbb{Q}] = p^{n-1}, n \geq 1,$$

then $F = F_\infty = F_0 Q_\infty$ with $F_0$ a finite extension of $\mathbb{Q}$, $Q_\infty = \bigcup_{n=1}^{\infty} Q_n$. If $F_0 \cap Q_\infty = Q_0$, then we define $F_n = F_0 Q_{a+n}$, and $F_0 \subset F_1 \subset \ldots \subset F_n \subset \ldots \subset F_\infty = F = \bigcup_{n=1}^{\infty} F_n$, $[F_n : F_0] = p^n$, $\text{Gal}(F_n/F_0) = \mathbb{Z}/p^n \mathbb{Z}$, the cyclic group with $p^n$ elements. We have the following diagram:
Let $E$ be a finite Galois $p$-extension of $F$. Then there exists a finite extension of $Q$, say $E_0$, such that $\text{Gal}(E_0/F_0) = \text{Gal}(E/F) = G$. Also we have $\text{Gal}(E_n/F_n) = G$ for all $n$, and $\text{Gal}(E/E_0) \cong \varprojlim_n \text{Gal}(E_n/E_0) \cong \varprojlim_n \left(\mathbb{Z}/p^n\mathbb{Z}\right) \cong \mathbb{Z}_p$ and $\text{Gal}(F/F_0) \cong \mathbb{Z}_p$.

Henceforward, we will assume $p$ to be odd, and $E$, $F$ fields of CM type. Also we assume $\mu_E = \mu_F = 0$, $\mu$ the $\mu$-invariant of Iwasawa.

Let $W_n(P) = \{\xi \in \mathbb{C} \mid \xi^{p^n} = 1\}$, $W(p) = \bigcup_{n=1}^{\infty} W_n(p)$ and $C_E$, $C_F$ be the class groups of $E$ and $F$ respectively. Also we denote by $W$ the roots of 1 in $\mathbb{C}$, the field of the complex numbers.

Let $\{P_1, \ldots, P_k\}$ be a finite set of different primes in $F$, and $M = \prod_{i=1}^{k} P_i^{\delta_i}$, $\delta_i > 0$.

Now we define

$I_M = \{\text{ideals of } F \text{ relative prime to } M\}$.
$P_M = \{(\alpha) \mid \alpha \in F^*, \ alpha \equiv 1 \mod M\}$.
$T_M = \{(\alpha) \mid \alpha \in F^* \text{ and } (\alpha) \text{ is relative prime to } M\} \supseteq P_M$.
$C_M = I_M/P_M$ (ray class group).
$I_F = \{\text{ideals of } F\}$ = ideal group of $F$.
$P_F = \{(\alpha) \mid \alpha \in F^*\} \supseteq I_F$.
$C_F = I_F/P_F$ = class group of $F$.
$F_M^* = \{\alpha \in F^* \mid (\alpha) \in T_M = I_M \cap P_F\} = \{\alpha \in F^* \mid ((\alpha), M) = 1\}$.
$F_M^{*1} = \{\alpha \in F_M^* \mid \alpha \equiv 1 \mod M\}$.
$\mathfrak{d}_F$ = ring of integers of $F$.
$U_F$ = units of $\mathfrak{d}_F$. 
PROPOSITION 4.

(i) If $M = \prod_{i=1}^{k} M_i$, with $(M_i, M_j) = 1$ for $i \neq j$, then $F_M^*/F_{M_1}^* = \prod_{i=1}^{k} (F_{M_i}^*/F_{M_1}^*)$.

(ii) $I_M^*/T_M^* = C_F^*$.

(iii) $1 \rightarrow T_M^*/P_M \rightarrow C_M \rightarrow C_F \rightarrow 1$ is an exact sequence of abelian groups.

(iv) $F_M^*/(F_{M_1}^* U_F) = T_M^*/P_M$.

(v) $\mu : C_M^*(p) \rightarrow C_F^*(p)$ is onto, where $A(p)$ denotes the $p$-torsion of the abelian group $A$.

PROOF.

(i), (ii): [19], pages 111, 112.

(iii): Follows from (ii).

(iv): $\psi : F_M^* \rightarrow T_M^*$, $\psi (\alpha) = (\alpha)$ is onto and $\psi^{-1}(P_M^*) = F_{M_1}^* U_F$.

(v): Follows from the fact that $\mu : C_M \rightarrow C_F$ is onto and that $C_M$, $C_F$ are torsion groups.

We denote $A^+ = \{ x \in A \mid x^J = x \}$, $A^- = \{ x \in A \mid x^J = x^{-1} \}$, where $A$ is an arbitrary abelian group, $J = \text{complex conjugation}$, and $J$ acts on $A$.

PROPOSITION 5.

Consider $M = \prod_{i=1}^{r} P_i$, $P_i \neq P_j$, for $i \neq j$, $P_i$ prime ideal in $F$ such that $P_i|_Q \neq p$, $1 \leq i \leq r$, that is, no $P_i$ is a $p$-prime.

Let $pC_M^* = \{ c \in C_M \mid c^p = 1 \}$. Then $\mu : pC_M^- \rightarrow pC_F^*$ is onto when $P_i$ is ramified in $E/F$, $1 \leq i \leq r$.

PROOF.
First we assume that $F \supset W(p)$. So in this case we have $\partial F \supset W(p)$ and $(\partial F/P_i)^* \supset W(p)$.

Let $\Lambda$ be an ideal such $\Lambda \in \mathfrak{p}_F$. By the Approximation Theorem ([19], page 109) we may assume that $(\Lambda, M) = 1$ and $\Lambda^p = (f), f \in F^*$.

Since $C_M^\ast(p) \rightarrow C_F^\ast$ is onto, when we consider $\Lambda$ as an element of $C_M^\ast$, we have that order $(\Lambda) = p^n$ some $n$. In other words $\Lambda^{p^n} = (g)$ and $g \equiv 1 \mod M$.

Hence $\Lambda^{p^n} = (\Lambda^p)^{p^{n-1}} = (f)^{p^{n-1}} = (f_1 \cdots f_r)^{p^{n-1}}$, so there exists a unit in $U_F^\ast = W_F = W \cap F$ such that $g = u \cdot f^{p^{n-1}}$.

We have $W_F = W_F(p) \times W_1$ where $W_1 = \left( \prod_{q \text{ prime, } q \nmid p} W_F(q) \right)$, so $u = a \cdot b, a \in W(p), b \in W_1$. Since $F \supset W(p)$, if $a^{pn+1} = 1$, we can choose a $p^{n+m}$-th root of 1, say $c$, such that $c^{p^{n-1}} = a$. On the other hand, since $W_1$ has no $p$-torsion, $W_1^{p^{n-1}} = W_1$, so we can choose $d \in W_1$ with $c^{p^{n-1}} = b$. Therefore, $u = a \cdot b = (c \cdot d)^{p^{n-1}}$. Let $v = c \cdot d$.

$\Lambda^p = (f) = (v \cdot f)$ and $(v \cdot f)^{p^{n-1}} = g \equiv 1 \mod P_i, 1 \leq i \leq r$. Hence $v \cdot f$ is a $p$-power root of 1 in $\partial F/P_i$ and since $W(p) \subset \partial F/P_i$, it follows that there exists $h_i$ such that $h_i^{p^n} \equiv v \cdot f \mod P_i, 1 \leq i \leq r$. Again by the Approximation Theorem, there exists $h$ with $h \equiv h_i \mod P_i, 1 \leq i \leq r$, so $h^{p^n} \equiv h_i^{p^n} \equiv v \cdot f \mod P_i, 1 \leq i \leq r$ (note that $(h, M) = 1$). Then in $C_F$ we have $\Lambda = (h^{-1})\Lambda$ and $(h^{-1})\Lambda)^P = (h^{-p} \cdot f), h^{-p} \cdot f \equiv f \cdot r^{1} \equiv 1 \mod P_i, 1 \leq i \leq r$, so $h^{-p} \cdot f \equiv 1 \mod M$ and $\mu : pC_M^\ast \rightarrow pC_F^\ast$ is onto.

Now we assume that $W(p)$ is not contained in $F$. In this case we have $W_F(p) = \{1\}$, so $W_F = \left( \prod_{q \text{ prime, } q \nmid p} W_F(q) \right)$. With the same notation as above, we still have $v^{p^{n-1}} = u, v \in W_F$. So again $(v \cdot f)^{p^{n-1}} = g \equiv 1 \mod P_i, 1 \leq i \leq r$, and $v \cdot f$ is a $p$-power root of 1 in $\partial F/P_i$. Now since we are dealing with primes which ramify, $p^\infty \left| (\partial F/P_i^*) \right|$, ([15], page 268). Therefore $W(p) \subset \partial F/P_i$ and $(v \cdot f)^{p^{n-1}} \equiv 1 \mod P_i$. The rest of the proof is the same as in the first case.
LEMMA 5.

If $M$ is as in Proposition 5, $W(p) \cap F_M^* = \{1\}$.

PROOF.

If $W_F(p) = \{1\}$, the Lemma is trivial, so we assume that $W(p)$ is contained in $F$. Let $\xi \in W(p) \cap F_M^*$, then $\xi^{p^n} = 1$ for some $n$, $\xi \equiv 1 \mod M$.

Then $(\xi - 1) \cdot (\xi^{p^n-1} + \ldots + \xi + 1) = (\xi^{p^n} - 1) = 0$, so if we had $\xi \neq 1$, $\xi^{p^n-1} + \ldots + \xi + 1 = 0$. But $\xi \equiv 1 \mod M$ implies $\xi^{p^n-1} + \ldots + \xi + 1 \equiv p^n \mod M$, that is, $p^n \equiv 0 \mod M$ which contradicts that $M = \mathbb{P} \mid g \neq p^i, 1 \leq i \leq r$. Therefore $\xi = 1$.

REMARC 1.

i) Since we are assuming $\mu_F = \mu_E = 0$ (so $\mu_F = \mu_E = 0$), $C_F^*(p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_F}$, $\lambda_F$ denoting Iwasawa's $\lambda$-invariant ([15], page 272). Therefore $pC_F^- = F_p^{\lambda_F}$ and $\dim_{F_p} pC_F^- = \lambda_F$.

ii) We have that $\{P/P^j = P^{1-j} | P$ is a prime ideal in $F\}$ generates $I_F$. Also $J$ acts on $C_M$ iff $M^j = M$, so we will assume henceforth that $M^j = M$.

iii) If $0 \rightarrow A \xrightarrow{\sigma} B \xrightarrow{\delta} C \rightarrow 0$ is any exact sequence of abelian groups, where $J$ acts on $A, B, C$, $\sigma \circ J = J \circ \sigma$, $\delta \circ J = J \circ \delta$, then the sequence

$0 \rightarrow A' \xrightarrow{\sigma} B' \xrightarrow{\delta} .C \rightarrow 0$

is exact where $C' = \{\delta(b) | b \in B, and there exists a \in A with b^{1+j} = a^{1+j}\}$. Also $C'$ is contained in $C^-$ and $C'/C$ is a 2-group, so $(C'/C)(p) = \{1\}$. In particular, if $C$ is a torsion group, $C^-(p) = C(p)$.
Now we study the structure of $T_\text{M}/P_\text{M}$.

First we have the exact sequence

$$1 \longrightarrow P_\text{M} \longrightarrow T_\text{M} \longrightarrow T_\text{M}/P_\text{M} \longrightarrow 1$$

from which we obtain

$$1 \longrightarrow P_\text{M}^- \longrightarrow T_\text{M}^\circ \longrightarrow (T_\text{M}/P_\text{M})^- \longrightarrow 1$$

and $(T_\text{M}/P_\text{M})(p) = (T_\text{M}^-/P_\text{M}^\circ)(p)$.

Now from Proposition 4 (iii), we have the exact sequence:

$$1 \longrightarrow T_\text{M}/P_\text{M} \longrightarrow C_\text{M} \longrightarrow C_\text{F} \longrightarrow 1$$

and since all these groups are torsion groups, we have that

$$(8) \quad 1 \longrightarrow (T_\text{M}/P_\text{M})^-(p) \longrightarrow C_\text{M}^-(p) \longrightarrow C_\text{F}(p) = C_\text{F}^-(p) \longrightarrow 1$$

is exact.

Also

$$T_\text{M}/P_\text{M} = \frac{F_\text{M}^*}{(F_\text{M}^* \cdot U_\text{F})} = \frac{(F_\text{M}^*/F_\text{M}^*_{1})}{(F_\text{M}^1 \cdot U_\text{F})/F_\text{M}^1},$$

hence

$$(T_\text{M}/P_\text{M})^- = \frac{(F_\text{M}^*/F_\text{M}^*_{1})^-}{((F_\text{M}^1 \cdot U_\text{F})/F_\text{M}^1)^-},$$

and since all these groups are torsion groups we obtain

$$(T_\text{M}/P_\text{M})(p) = (T_\text{M}/P_\text{M})^- (p) =$$
\[
\frac{(F_M^*/F_{M1}^*)^+(p)}{(F_{M1}^* U_F^*/F_{M1}^*)^-(p)} = \frac{(F_M^*/F_{M1}^*)^-(p)}{(F_{M1}^* U_F^*/F_{M1}^*)^+(p)} = \frac{(F_{M}^*/F_{M1}^*)^-(p)}{(F_{M1}^* U_F^*/F_{M1}^*)^+(p)} = \frac{(F_{M}^*/F_{M1}^*)^+(p)}{(F_{M1}^* U_F^*/F_{M1}^*)^-(p)}
\]

(by Lemma 5).

From now on we consider \( M = D \cdot D^j = \prod_{i=1}^{r} (P_i \cdot P_i^j) \) with \( D = \prod_{i=1}^{r} P_i \) and \( P_i \) a non p-prime, \( 1 \leq i \leq r \), \( P_i \) ramified in \( E/F \).

We write \( M = \prod_{i=1}^{2r} Q_i \) with \( Q_{2i-1} = P_i \), \( Q_{2i} = P_i^j \), \( 1 \leq i \leq r \).

Then \( F_M^*/F_{M1}^* = \prod_{i=1}^{2r} F_{Q_i}^* / F_{Q_i^1}^* = \prod_{i=1}^{2r} L_j^* \), where \( L_j \) is an algebraic extension of a finite field.

Since \( Q_j \) is ramified in \( E \), \( E \) is a \( p \)-extension of \( F \), therefore \( p^\infty \mid \mid L_j^* \), \( 1 \leq i \leq 2r \) ([15], page 268). Therefore \( L_j \supseteq W(p) \), and then \( L_j(p) = W(p), \) \( 1 \leq i \leq 2r \).

So \( (F_M^*/F_{M1}^*)^+(p) = \prod_{i=1}^{2r} \left( \frac{F_{Q_i}^*}{F_{Q_i^1}^*} \right)^+(p) = \prod_{i=1}^{2r} L_j^*(p) = \prod_{i=1}^{2r} W(p) = W(p)^{2r} \).

Let us see how \( J \) acts on \( \prod_{i=1}^{2r} L_j^* \). If \( \alpha \in F_M^* \) then \( ((\alpha), Q_j) = 1 \), hence \( ((\alpha^J), Q_j^1) = 1 \). The isomorphism:

\[
F_M^*/F_{M1}^* \xrightarrow{\sigma} \prod_{i=1}^{2r} \left( \frac{F_{Q_i}^*}{F_{Q_i^1}^*} \right)
\]

is given by
\[
\alpha_{F^*_{M1}} \longrightarrow (\alpha_{F^*_1}, \alpha_{F^*_2}, \ldots, \alpha_{F^*_ {2r}}, \alpha_{F^*_ {2r-1}}).
\]

So we define : \( (\beta_1, \beta_2, \ldots, \beta_{2r-1}, \beta_{2r})^I = (\beta_1^I, \beta_2^I, \ldots, \beta_{2r-1}^I, \beta_{2r}^I) \), with
\[
\beta_i = \beta_i F^*_i, \quad 1 \leq i \leq 2r.
\]

We have \( \sigma^{-1}(\beta_1, \beta_2, \ldots, \beta_{2r-1}, \beta_{2r})^I = (\sigma^{-1}(\beta_1, \beta_2, \ldots, \beta_{2r-1}, \beta_{2r}))^I \), hence

the action of \( J \) on \( \prod_{i=1}^{2r} L^*_i(p) = \prod_{i=1}^{2r} W(p) \) is given by :

\[
(\xi_1, \xi_2, \ldots, \xi_{2r-1}, \xi_{2r})^J = (\xi_1^I, \xi_1^I, \ldots, \xi_{2r-1}^I, \xi_{2r}^I).
\]

Since \( \xi_j \in W(p) \), \( \xi_j = 1 \), therefore

\[
(\xi_1, \xi_2, \ldots, \xi_{2r-1}, \xi_{2r})^I = (\xi_2^I, \xi_1^I, \ldots, \xi_{2r-1}^I) \)

and

\[
(\xi_1, \xi_2, \ldots, \xi_{2r-1}, \xi_{2r})^I \in (F^*_M/F^*_M^I)^{-1}(p) \Leftrightarrow
(\xi_1, \xi_2, \ldots, \xi_{2r-1}, \xi_{2r})^I \Leftrightarrow
(\xi_2^I, \xi_1^I, \ldots, \xi_{2r-1}^I) = (\xi_1^I, \xi_2^I, \ldots, \xi_{2r-1}^I) \Leftrightarrow
\xi_{2i-1} = \xi_{2i}, \quad 1 \leq i \leq r \Leftrightarrow \xi_{2i-1} = \xi_{2i}, \quad 1 \leq i \leq r.
\]

Finally, \( (F^*_M/F^*_M^I(p))^I = \prod_{i=1}^{r} W(p) \) and \( (T_{M/\mathbb{F}_M})^-(p) = \frac{i-1}{W_F(p)} = W(p)^{r-\delta_F} \),

where we define \( \delta_F = 1 \) if \( W(p) \subset \mathbb{F} \), and 0 otherwise.

By (8) and Proposition 5 we have the exact sequence:

\[
1 \longrightarrow F_p^{r-\delta_F} \longrightarrow (p(W(p)))^{r-\delta_F} \longrightarrow \mathbb{C}_p^- \longrightarrow \mathbb{C}_F^- \longrightarrow 1.
\]

Define \( \lambda_{M}^- = \dim_{\mathbb{F}_p} \mathbb{C}_M^- \) and we have \( \lambda_{F}^- = \dim_{\mathbb{F}_p} \mathbb{C}_F^- \), therefore we have

**Proposition 6.**

\[
\lambda_{M}^- = \lambda_{F}^- + r - \delta_F.
\]

For any CM field \( K \), \( K^+ = K \cap \mathcal{R} \) denotes the maximal real subfield of \( K \).

Now, let \( P_1^+, \ldots, P_r^+ \) be the primes in \( F^+ \) which ramify in \( E^+ \) and split in \( F \), \( P_i^+ \)
non \( p \)-place.
Gal(E/F) = Gal(E/F) = G.

Now, let M = Con_{F^+|F}(P_1^+, \ldots, P_r^+) = \psi_1 \psi_1^J \ldots \psi_i \psi_i^J \ldots \psi_r \psi_r^J, Con_{F|E}\psi_i = (H^{(i)}_1 \ldots H^{(i)}_g)_i := Q_i^{e_i} and N = \prod_{i=1}^r Q_i Q_i^J.

By (9) we have the exact sequence

(10) \hspace{1cm} 1 \longrightarrow F_{p}^{\delta E} \longrightarrow pC_N^- \longrightarrow pC_E^- \longrightarrow 1

and $\lambda_N = \lambda_E + t \cdot \delta_E$ with $t = \sum_{i=1}^r g_i$.

PROPOSITION 7.

$\psi = \text{conorm} : C_M^-(p) \longrightarrow C_N^-(p)^G$ is onto.

PROOF.

It suffices to show that every invariant class contains an invariant ideal.

From the exact sequence

\[ 1 \longrightarrow P_N^- \longrightarrow I_N^- \longrightarrow C_N \longrightarrow 1, \]

we obtain the exact sequence

\[ 1 \longrightarrow P_N^G \longrightarrow I_N^G \longrightarrow C_N^G \longrightarrow H^1(G, P_N^-). \]
We denote again by $I_N$ the ideals which are in $C_N(p)$, and the same convention for $P_N$. Then we have the exact sequence

$$\mathbb{P}_N - \mathbb{I}_N \to \mathbb{I}(C_N(p))^G \to H^1(G, P_N^*)$$

Therefore it suffices to show that $H^1(G, P_N^*) = \{1\}$.

Now

$$1 \to \left( U_E \cap E_{N_1}^* \right)^* = W_E \cap E_{N_1}^* \to E_{N_1}^* \to P_N \to 1$$

is exact.

$W_E \cap E_{N_1}^*$ is a torsion group, $P_N^*/P_N$ is a 2-group and $G$ is a $p$-group, so:

$H^n(G, W_E \cap E_{N_1}^*) = H^n(G, (W_E \cap E_{N_1}^*)(p)) = H^n(G, W_E(p) \cap E_{N_1}^*) = H^n(G, \{1\}) = \{1\}$ by Lemma 5, and $H^n(G, P_N^*) = H^n(G, P_N^*)$. Here $H^n$ denotes the Tate cohomology.

Therefore we have $H^n(G, P_N^*) = H^n(G, E_{N_1}^*)$.

Now $H^1(G, E_{N_1}^*) = \{1\}$ (the proof is similar to that of Hilbert's Theorem 90).

Therefore Proposition 7 follows.

\[\star\]

**PROPOSITION 8.**

$pC_N^*$ is a free $F_p[G]$-module and $pC_N^* = F_p[G]^{\lambda_{F_p \cdot \delta_E}}$.

**PROOF.**

Consider $M = pC_N^*$ as $F_p[G]$-module. Then,

$$\dim_{F_p} M^G = \dim_{F_p} pC_N^G \leq \dim_{F_p} pC_M^* = \lambda_{M^*}^.$$ 

$$\dim_{F_p} M = \lambda_{M^*}^ = \lambda_{E^*}^ + t - \delta_E^\ast, t = \sum_{i=1}^{r} g_i e_i = |G|. \text{ Thus}$$

$$\lambda_{F_p} = \lambda_{E^*}^ + t - \delta_E^\ast$$

$\lambda_{E^*}^ = \sum_{i=1}^{r} g_i e_i = |G|$. Thus
dim_{F_p}M = \sum_{i=1}^{r} g_i \delta_E = \lambda_E + \sum_{i=1}^{r} \frac{g_i e_i}{e_i} - \delta_E = \lambda_E + |G| \sum_{i=1}^{r} \left( \frac{1}{e_i} \right) - \delta_E.

Now by Kida's formula ([4], [15], [21]):

\lambda_E = |G| \cdot (\lambda_F - \delta) + \delta + \sum_{w^+} (e(w^+/v^+) - 1),

where the sum is taken over all finite non p-places \( w^+ \) of \( E^+ \) which split in \( E \) and \( \delta = \delta_E = \delta_F \). So,

\[
\sum_{w^+} (e(w^+/v^+) - 1) = \sum_{i=1}^{r} g_i (c_i - 1) = \sum_{i=1}^{r} \left( g_i e_i - \frac{g_i e_i}{e_i} \right) = |G| \cdot \left( \sum_{i=1}^{r} \left( 1 - \frac{1}{e_i} \right) \right).
\]

Hence, \( \lambda_E = |G| \cdot (\lambda_F - \delta) + \delta \), and

\[\dim_{F_p}M = \lambda_E + \sum_{i=1}^{r} g_i - \delta = \lambda_E + \sum_{i=1}^{r} \left( \frac{1}{e_i} \right) - \delta = |G| \cdot \left\{ \lambda_F - \delta + \sum_{i=1}^{r} \left( 1 - \frac{1}{e_i} \right) + \sum_{i=1}^{r} \left( \frac{1}{e_i} \right) \right\} + \delta - \delta

= |G| \cdot (\lambda_F - \delta + r) = |G| \cdot \lambda_M = |G| \cdot \dim_{F_p}C_M \geq |G| \cdot \dim_{F_p}M^G.
\]

By Kato's Lemma ([27], Proposition 2, page 564) we have that \( M \cong F_p[G]^u \) and \( \dim_{F_p}M = |G| \cdot u = |G| \cdot (\lambda_F - \delta + r) \). Therefore, \( M \cong pC_N = F_p[G]^{\lambda_F + r - \delta_E}. \)

**LEMMA 6. (Schanuel's lemma for injective modules).**

Let \( Y_1, Y_2 \) be injective modules over a ring \( R \), and suppose that we have 2 exact sequences or \( R \)-modules:

\[
\begin{align*}
0 & \longrightarrow A \longrightarrow Y_1 \longrightarrow B_1 \longrightarrow 0 \\
0 & \longrightarrow A \longrightarrow Y_2 \longrightarrow B_2 \longrightarrow 0
\end{align*}
\]
Then $Y_1 \oplus B_2 = Y_2 \oplus B_1$.

**PROOF.**

Dual to the projective case.

**THEOREM 5.**

With the notations as above, if $E/F$ is ramified, then the sequence:

$$1 \longrightarrow \left( \bigoplus_{i=1}^{r} F_p[G/G_i] \right) / F_p^\delta \longrightarrow F_p[G]^\lambda \longrightarrow F_p[G]^{\lambda^t r \delta^t E} \longrightarrow pCE \longrightarrow 1$$


**PROOF.**

The exact sequence (10) is, in fact, $F_p[G]$-exact. It is clear that as $F_p[G]$-module, we may identify $F_p^\delta$ with $\left( \bigoplus_{i=1}^{r} F_p[G/G_i] \right) / F_p^\delta$ The uniqueness is consequence of the injectivity of $F_p[G]^{\lambda^t r \delta^t}$ and Lemma 6.

In [13] the operation $\Omega^\#$ is defined as follows:

For any exact sequence of $R$-modules ($R$ an algebra over a field),

$$0 \longrightarrow A \longrightarrow Y \longrightarrow B \longrightarrow 0,$$

with $Y$ injective, write $B = B_1 \oplus B_2$ where $B_2$ is injective and $B_1$ has no injective components. Then $\Omega^\#A = B_1$. $\Omega^\#$ is the dual of the loop-operation $\Omega$. Since for $F_p[G]$-modules to be projective, injective or free is equivalent we have
COROLLARY 1.

\[ pC_E = \Omega^\# \left\{ \left( \bigoplus_{i=1}^{r} F_p[G/G_i] \right) / F_p^{\delta} \right\} \oplus F_p[G]^u \] (for some u) as \( F_p[G] \)-modules.

From the Corollary, we can give explicitly the structure of \( pC_E \) in some particular cases. First we take \( \delta = 0 \).

In this case we have:

\[ \Omega^\# \left( \bigoplus_{i=1}^{r} F_p[G/G_i] \right) = \bigoplus_{i=1}^{r} \Omega^\# \left( F_p[G/G_i] \right) \] (see [13]).

Now we consider:

\[ \mu : F_p[G/G_i] \rightarrow F_p[G] \] given by

\[ \mu \left( \sum_{\sigma \in G/G_i} a_\sigma \sigma \right) = \sum_{g \in G} b_g g, \text{ with } b_g = a_\sigma \text{ if } g \in \sigma. \]

It can be verified that \( \mu \) is \( F_p[G] \)-homomorphism and it is injective.

So, \( 0 \rightarrow F_p[G/G_i] \rightarrow F_p[G] \rightarrow F_p[G]/F_p[G/G_i] \rightarrow 0 \) is exact.

Therefore, we have \( \Omega^\# \left( F_p[G/G_i] \right) = F_p[G]/F_p[G/G_i] = T_i \) and since \( F_p[G/G_i] \) is an indecomposable \( F_p[G] \)-module, it follows from [13] that \( T_i \) is indecomposable.

On the other hand we have: \( \dim_{F_p} T_i = |G| - \frac{|G|}{|G_i|} = |G| - \frac{|G|}{p^{e_i}} \). Thus, if the ramification index of the prime \( P_i \) in \( E \) is \( p^{e_i} \) with decomposition group \( G_i \), we will have: \( \dim_{F_p} T_i = p^n - p^{n-e_i} \) where \( |G| = p^n \).

We can, now, state

THEOREM 6.

If \( \delta = 0 \), \( pC_E = \left( \bigoplus_{i=1}^{r} T_i \right) \oplus F_p[G]^{\lambda F} \) as \( F_p[G] \)-modules, where \( T_i = \left( F_p[G]/F_p[G/G_i] \right) \) is an indecomposable \( F_p[G] \)-module and \( \dim_{F_p} T_i = p^n - p^{n-e_i} \).

PROOF.
We have  $pC_E^- = \Omega^\delta\left( \bigoplus_{i=1}^{r} F_p[G/G_i] \right) \oplus F_p[G]^u = \left( \bigoplus_{i=1}^{r} T_i \right) \oplus F_p[G]^u$.

Hence  $\lambda_E^- = u \cdot |G| + \sum_{i=1}^{r} \left( p^n - p^{n-1} \right) = |G| \cdot \left\{ u + r - \sum_{i=1}^{r} \left( \frac{1}{c_i} \right) \right\}$.

On the other hand, by Kida's formula:

$\lambda_E^- = |G| \cdot (\lambda_F^- + r - \sum_{i=1}^{r} \left( \frac{1}{c_i} \right))$. Therefore $u = \lambda_F^-$. 

Another particular case is when there is one fully ramified prime, say $P_r$, in $E/F$.

In this case, we have $G_r = G$, so $F_p[G/G_r] = F_p[G]$. Thus we have

$\left( \bigoplus_{i=1}^{r} F_p[G/G_i] \right) / F_p^\delta \approx \left( \bigoplus_{i=1}^{r-1} F_p[G/G_i] \right) \oplus F_p^{1-\delta}$,

$\Omega^\delta\left( \bigoplus_{i=1}^{r} F_p[G/G_i] \right) / F_p^\delta \approx \bigoplus_{i=1}^{r-1} \left( F_p[G]/F_p[G/G_i] \right) \oplus \Omega^\delta F_p^{1-\delta}$

$= \bigoplus_{i=1}^{r-1} \left( F_p[G]/F_p[G/G_i] \right) \oplus \left( F_p[G]/F_p \right)^{1-\delta}$.

Then $pC_E^- = \left( \bigoplus_{i=1}^{r-1} T_i \right) \oplus \left( F_p[G]/F_p \right)^{1-\delta}$ and again by Kida's formula, $u = \lambda_F^-$. Hence we have

**THEOREM 7.**

If there is at least one fully ramified prime in $E/F$ we have

$pC_E^- = \left( \bigoplus_{i=1}^{r-1} T_i \right) \oplus \left( F_p[G]/F_p \right)^{1-\delta}$  $\oplus F_p[G]^{\lambda F}$ as $F_p[G]$-modules, $T_i$ indecomposable $F_p[G]$-module, $T_i = F_p[G]/F_p[G/G_i]$, $\dim F_p T_i = p^n - p^{n-e_i}$.

Now we study the unramified case. First we consider again the general case:
Let $P_j^+, \ldots, P_r^+$ be the primes in $F^+$ which ramify in $E^+$ and split in $F$, $P_r^+$ non-regular (if $r$ may be 0).

Now we consider $P_{r+1}^+, \ldots, P_{r+t}^+$ any set of primes in $F^+$ which split in $F$ and do not ramify in $E^+$. Finally consider $P_{r+t+1}^+, \ldots, P_{r+t+v}^+$ any set of primes in $F^+$ which are inert in $F$ and do not ramify in $E$. Also we assume that $p^\infty\mid (\partial_{F^+}/P_i^+)^*$ for all $1 \leq i \leq r+t+v$.

Consider $M = D \times C \times A$ where $D = \prod_{i=1}^r P_i^+$, $C = \prod_{j=1}^t P_{r+j}^+$, $A = \prod_{k=1}^v P_{r+t+k}^+$. $M$ is an ideal in $F^+$. Now let $\text{Con}_{F^+|E^+}P_i^+ = Q_i^1$ for $i=1, \ldots, r$, $\text{Con}_{F^+|E^+}P_{i+r}^+ = Q_i = P_i^+$ for $i = r+1, \ldots, r+t$, and $\text{Con}_{F^+|E^+}Q_i = (H_i^{(i)} \ldots H_i^{(i), e_i}) : = \Delta_i$.

Note that $e_i = 1$ for $i = r+1, \ldots, r+t+v$.

Let $N = \left\{ \prod_{i=1}^{r+t} (\Delta_i \Delta_i^j) \right\} \cdot \left\{ \prod_{j=r+t+1}^{r+t+v} \Delta_j \right\}$, $\text{Con}_{F|E}A = A_1$, $\text{Con}_{F^+|E^+}D = D_1$, $\text{Con}_{F^+|E^+}C = C_1$, $N = D_1 D_1 C_1 C_1 A_1$. Then we have $f(H_j^{(i)} | Q_i) = 1$ for all $i = 1, \ldots, r+t+v$ (see [15], page 266).

Now $W(p) \subset \partial_{F^+}/Q_i = \partial_{E}/H_j^{(i)} \Leftrightarrow p^\infty\mid (\partial_{F^+}/P_i^+)^*$. We have:

\[
\left( \frac{T_M}{P_M} \right)^* (p) = \left\{ \prod_{i=1}^{r+t} (L_i \times L_i) \times \prod_{j=r+t+1}^{r+t+v} L_j \right\} \left( \frac{W(p)}{W(p)} \right)^\delta =
\left[ \prod_{i=1}^{r+t} (L_i(p) \times L_i(p)) \times \prod_{j=r+t+1}^{r+t+v} L_j(p)^* \right] / W(p)^\delta = (W(p)^{r+t} \times W(p)^v) / W(p)^\delta = W(p)^{r+t+v}.
\]

Again we have the exact sequence:

\[
1 \rightarrow \left( \frac{T_M}{P_M} \right)^* (p) = W(p)^{r+t+v} \rightarrow C_M(p) \rightarrow C_F(p) \rightarrow 1.
\]
Also, $\rho_{CM} \to \rho_{CF}$ is onto (Proposition 5, there, the fact we needed was $W(p) \subset (\theta_F/P_i)\ast$).

So we have the exact sequence

$$1 \to F_p^{t+1+v-\delta} \to \rho_{CM} \to \rho_{CF} \to 1.$$

We have the corresponding exact sequence for $N$.

Therefore $\lambda_{CM}^* = \lambda_{CF}^* + r + t + v - \delta$ and $\lambda_{CN}^* = \lambda_{CF}^* + \sum g_i + |G| \cdot t + |G| \cdot v - \delta$.

As before we have that $\rho_{CM}^* \to \rho_{CN}^G$ is onto and

$$p(T_{M/P_M})^* = \left\{ \bigoplus_{i=1}^r F_p[G/G_i] \bigoplus \left( \bigoplus_{j=1}^t F_p[G] \right) \right\} / F_p^\delta \text{ as } F_p[G]-\text{modules.}$$

Then we obtain

$$\dim_{F_p} \rho_{CN}^G \leq \dim_{F_p} \rho_{CM}^* = \lambda_{CM}^* \text{ and therefore}$$

$$|G| \cdot \dim_{F_p} \rho_{CN}^G \leq |G| \cdot \lambda_{CM}^* = |G| \cdot (\lambda_{CF}^* + r + t + v - \delta).$$

Now using again Kida’s formula, we have:

$$\dim_{F_p} \rho_{CN}^G = \lambda_{CN}^* = \lambda_{CF}^* + \sum g_i + |G| \cdot t + |G| \cdot v - \delta = |G| \cdot \lambda_{CM}^* \geq$$

$$|G| \cdot \dim_{F_p} \rho_{CN}^G.$$

So by Kato’s lemma, $\rho_{CN}^G$ is a free $F_p[G]$-module and $\rho_{CN}^G = F_p[G]^{\lambda_{CF}^* + r + t + v - \delta}$.

So we have

**Proposition 9.**

$$1 \to \left\{ \bigoplus_{i=1}^r F_p[G/G_i] \bigoplus F_p[G]^{t+v} \right\} / F_p^\delta \to F_p[G]^{\lambda_{CF}^* + r + t + v - \delta} \to \rho_{CN}^G \to 1$$

is $F_p[G]$-exact.

**Remark 2.**

Now if we assume $E/F$ unramified, that is, $r = 0$, then if $\delta = 0$, take $t = v = 0$, hence:
0 —> 0 —> \( F_p[G]^\lambda \cap \) \( p \cdot \sigma \) \( p \cdot \sigma \) —> 0 is exact and therefore we obtain
\[ F_p[G]^\lambda \cap \cong p \cdot \sigma \]

If \( r = 0, \delta = 1 \), take \( t = 1, v = 0 \) and then
\[ 0 —> F_p[G]/F_p —> F_p[G]^\lambda \cap —> p \cdot \sigma \cap \sigma \cap —> 0 \text{ is exact.} \]

To study this last exact sequence, we use the dual concept, that is:
For any \( F_p[G] \)-module \( M \), define \( M^* = \text{Hom}_{F_p}(M, F_p) \) with \( F_p[G] \)-module structure defined by:
\[ (g \cdot f)(x) = f(g^{-1} \cdot x). \]
We have \( \text{dim}_{F_p} M^* = \text{dim}_{F_p} M \) and \( (M^*)^* \cong M \) as \( F_p[G] \)-modules.

Now if \( M, N, P \) are \( F_p[G] \)-modules and
\[ 0 —> M —> N —> P —> 0 \text{ is } F_p[G]-\text{exact, then} \]
\[ 0 —> P^* —> N^* —> M^* —> 0 \text{ is } F_p[G]-\text{exact, where} \]
\[ h^*(\sigma) = \sigma \circ h, \sigma \in P^* \text{ and } g^*(\gamma) = \gamma \circ g, \gamma \in N^*. \]

In particular if \( M = N_1 \oplus N_2 \), then \( M^* = N_1^* \oplus N_2^* \) and \( N \) is an indecomposable \( F_p[G] \)-module if and only if \( N^* \) is.

\[ \star \]

**LEMMA 7.**

\[ F_p[G]^* \cong F_p[G], (F_p[G]/F_p)^* \cong I_G \text{ as } F_p[G]-\text{modules, where} \]
\[ I_G = \{ \sum_{\sigma \in G} a_{\sigma} \sigma \in F_p[G] \mid \sum_{\sigma \in G} a_{\sigma} \sigma = 0 \}. \]

**PROOF.**

Let \( \mu : F_p[G]^* —> F_p[G] \) be given by \( \mu(\phi) = \sum_{g \in G} \phi(g)g \). Then \( \mu \) is \( F_p[G] \)-isomorphism.

Now \( \mu^{-1}(I_G) \cong I_G \) and \( \phi \in \mu^{-1}(I_G) \) iff \( \sum_{g \in G} \phi(g) = 0 \).
Since $N = (F_p[G])^G = F_p \left( \sum_{g \in G} g \right) = F_p$, $F_p$ as trivial $F_p[G]$-module, $(F_p[G]/F_p)^*$

$= \text{Hom}_{F_p} (F_p[G]/N, F_p) = \{ \psi : F_p[G] \to F_p, \psi \text{ $F_p[G]$-homomorphism and } N \subset \text{ker } \psi \} = \{ \psi \in F_p[G]^* | \psi \left( \sum_{g \in G} g \right) = \sum_{g \in G} \psi(g) = 0 \} = \mu^{-1}(I_G) = I_G.$

Now we return to our case, $E/F$ unramified, $\delta = 1$. Then

$$0 \longrightarrow F_p[G]/F_p \longrightarrow F_p[G]^{\lambda_F} \longrightarrow \mathcal{C}_E \longrightarrow 0$$

is exact, so

$$0 \longrightarrow \left( \mathcal{C}_E \right)^* \longrightarrow \left( F_p[G]^{\lambda_F} \right)^* \cong F_p[G]^{\lambda_F} \longrightarrow \left( F_p[G]/F_p \right)^* \cong I_G \longrightarrow 0$$

is also $F_p[G]$-exact.

Let $d = \text{the minimum number of generators of } G$. Then by § 2, we have

$$\left( \mathcal{C}_E \right)^* \cong F_p[G]^{\lambda_F - d} \oplus T^* \text{ where } T^* \text{ is an indecomposable } F_p[G]-\text{module},$$

$$\dim_{F_p} T^* = 1 + (d - 1) \cdot |G|.$$

Hence $\mathcal{C}_E = F_p[G]^{\lambda_F - d} \oplus T$, and we have proved

**Theorem 8.**

If $E/F$ is unramified, $d = \text{the minimum number of generators of } G$, then

$$\mathcal{C}_E = F_p[G]^{\lambda_F - 2d} \oplus T \text{ as } F_p[G]-\text{modules, where } T \text{ is an indecomposable } F_p[G]-\text{module such that } \dim_{F_p} T = 1 + (d - 1) \cdot |G|.$$

Finally, we will give the structure of $\mathcal{C}_E(p)$ as $Z_p[G]$-module.
First assume $\delta = 1$, that is $W(p) \subset F$. Let $S$ be any finite set of places on $F^+ = F \cap \mathfrak{R}$ including all the $p$-places. Let $M^+ = \text{the maximal } p\text{-extension over } F^+ \text{ unramified outside of } S$. Then $\text{Gal}(M^+/F^+) = \text{Gal}(M/F)$, $M = M^+ F$ and $\text{Gal}(M/F) = G_1$ is a free pro-$p$ group with minimal number of generators equal to $\lambda^+_F + t$ where $t$ is the number of finite non-$p$-places in $S$ which split in $F$ and ramify in $M^+$ (see [15], Theorem 3, page 276).

\[
\begin{array}{ccc}
M^+ & \longrightarrow & M \\
\downarrow & & \downarrow \\
E^+ & \longrightarrow & E \\
\downarrow & & \downarrow \\
F^+ & \longrightarrow & F \\
\end{array}
\quad \left\{ \begin{array}{c}
G_2 \\
G_1 \\
\end{array} \right. 
\]

Let $S_1$ be the set of places in $E^+$ above $S$, and let $t_1$ be the number of finite non-$p$-places in $S_1$ which split in $E$ and ramify in $M^+$. Let $G_2 = \text{Gal}(M/E)$.

We have the following exact sequence of groups:

\[0 \longrightarrow G_2 \longrightarrow G_1 \longrightarrow G \longrightarrow 0.\]

Let $d = \text{the minimal number of generators of } G$ and consider $H$ a free pro-$p$-group in $d$ generators.

Then we have an exact sequence of groups

\[0 \longrightarrow P \longrightarrow H \longrightarrow G \longrightarrow 0.\]

Therefore as $Z_p[G]$-modules we have: $G_2^{ab} = P^{ab} \oplus Z_p[G]^{\lambda^+_F + t - d}$ where for any group $A$ we denote $A^{ab} = A/(\text{commutator subgroup of } A)$ ([41], Corollary 1.2 page 209 and [38] page 544).

On the other hand we have the exact sequence of groups:
Now if we assume $t = 0$, that is $M^+$ is the maximal $p$-extension of $F^+$ unramified outside of the $p$-places, then $C_E(p) \cong H^1(G_2, W(p))$ as $Z_p[G]$-modules.

Now $W(p) = Q_p/Z_p$ as groups and since $\delta = 1$, $W(p) \subset F$, $G_2$ acts trivially on $W(p)$, hence: $H^1(G_2, W(p)) = \text{Hom}(G_2, W(p)) = \text{Hom}(G_2, Q_p/Z_p)$, $\text{Hom}$ denotes homomorphisms of groups.

Since $Q_p/Z_p$ is abelian, $\text{Hom}(G_2, Q_p/Z_p) = \text{Hom}(G_2, Q_p/Z_p)$.

Now for any $Z_p[G]$-module $T$, define: $\chi(T) = \text{Hom}_{Z_p}(T, Q_p/Z_p)$ with the $G$-structure given by

$$(g \cdot i)(x) = f(g^{-1} \cdot x) \text{ for } g \in G, f \in \chi(T), x \in T.$$ 

We omit the proof of the following

**Lemma 8.**

(i) $\chi(T_1 \oplus T_2) = \chi(T_1) \oplus \chi(T_2)$

(ii) $\chi(Z_p[G]) = Q_p/Z_p[G]

(iii) $\chi(Z_p) = Q_p/Z_p$ with $G$ acting trivially on $Q_p/Z_p$

Now let $d = \text{the minimum number of generators of } G$, and we have the following $Z_p[G]$-exact sequence:

$$0 \rightarrow p^{ab} \rightarrow Z_p[G]^h \rightarrow I_G \rightarrow 0$$

where $h \geq d$, $I_G = \{ \sum_{\sigma \in G} a_{\sigma} \sigma \in Z_p[G] \mid \sum_{\sigma \in G} a_{\sigma} = 0 \}$ ([41], Satz 1.1, page 208).

Moreover, if $h = d$, $p^{ab}$ is indecomposable $Z_p[G]$-module ([41]); therefore as $Z_p[G]$-modules we have $C_E(p) = \text{Hom}(G_2, W(p)) = \text{Hom}(G_2^{ab}, Q_p/Z_p) = \ldots$
Hom_{Z_p}(G^a, Q_p/Z_p) \approx \chi(G_2^a) = \chi(P^a \oplus Z_p[G]^{\lambda F d}) = \chi(P^{ab}) \oplus \chi(Z_p[G]^{\lambda F d}) = T \oplus (Q_p/Z_p)[G]^{\lambda F d}.

Since as groups we have \( C^*(p) = (Q_p/Z_p)^{\lambda E} \) and by Kida's formula:
\[
\lambda^* = 1 + |G| \cdot (\lambda^F - 1) = |G| \cdot (\lambda^F - d) + |G| \cdot (d - 1) + 1,
\]
it follows that
\[
T \approx (Q_p/Z_p)^{1+|G|^*(d-1)}.
\]
Also, since \( P^{ab} \) is an indecomposable \( Z_p[G] \) -module, \( T = \chi(P^{ab}) \) is an indecomposable \( Z_p[G] \) -module (Lemma 8 (i)).

Now assume \( \delta = 0 \), that is, \( W(p) \) is not contained in \( F \). We keep the assumption \( E/F \) unramified.

As in [15, page 283 (7)], we have the following exact sequence of \( Z_p[G] \) -modules
\[
0 \longrightarrow C^E(p) \longrightarrow A \longrightarrow \oplus B_{v^+} \longrightarrow 0.
\]

Here \( A = (Q_p/Z_p)[G]^{\lambda F + t} \) as \( Z_p[G] \)-modules and \( B_{v^+} \) are defined similarly as in [15]. So in the unramified case \( \oplus B_{v^+} = 0, t = 0, A = C^E(p) = (Q_p/Z_p)[G]^{\lambda E} \) as \( Z_p[G] \)-modules. Hence we have proved

**THEOREM 9.**

If \( E/F \) is unramified, \( d = \) the minimum number of generators of \( G \), then:
\[
C^E(p) \approx (Q_p/Z_p)[G]^{\lambda F \cdot \delta t} \oplus T^\delta \text{ with } T \text{ indecomposable } Z_p[G]\text{-module, and}
\]
\[
T \approx (Q_p/Z_p)^{1+|G|^*(d-1)} \text{ as groups.}
\]

**REMARK 3.**

Theorem 9 gives us another proof of Theorem 8. We just consider the elements of order dividing \( p \).
CHAPTER II

AN ANALOGUE OF A CONJECTURE OF GROSS

§1. Introduction.

In this chapter, we are concerned with a problem in the theory of congruence function fields which is analogous to a conjecture of Gross in Iwasawa Theory. If $k$ is a finite field of characteristic $p$, $p$ an odd prime, and $K_0$ is a field of algebraic functions of one variable with $k$ as its exact field of constants, let $K_\infty$ be a $\mathbb{Z}_p$-extension of $K_0$ which is either a purely constant extension or one with no new constants. Let $S$ be a finite set of prime divisors of $K_0$ such that when no new constants are introduced, $S$ is the set of ramified primes and they ramify fully. The $S$-class group of $K_\infty$ is defined in the usual way as the direct limit of the corresponding groups at finite levels. The topological group $\Gamma = \text{Gal}(K_\infty/K_0)$ operates on the $p$-part of the $S$-class group in a natural way. Is the subgroup consisting of invariant classes finite? In the number field case, if $K_\infty/K_0$ is the cyclotomic $\mathbb{Z}_p$-extension of fields of CM-type, Gross' conjecture ([6], [10], [17]) states that the number of invariant $S$-classes under the action of $\Gamma$ on the minus part of the $p$-class group of $K_\infty$ is finite, if $S$ is the set of ramified primes. This conjecture has been verified for absolute abelian fields ([9], [10]). Concerning our analogous question, it is easily seen that the answer is in the affirmative if $K_\infty/K_0$ is a constant $\mathbb{Z}_p$-extension, where $p$ is any prime. In § 3, we indicate how this can be carried out and also how the cohomology of $S$-units can be calculated. In the geometric case, using a formula of Witt ([42]) for the norm residue symbol in cyclic extensions of $p$-power degree of local fields of characteristic $p$, we give necessary and sufficient conditions (Theorem 10) for this group to be finite for a class of $\mathbb{Z}_p$-extensions. In the end we give examples of fields for which the analogue of Gross' conjecture is true, and also give examples of fields for which it fails to hold. To find a
necessary and sufficient condition for the validity of the analogue of Gross' conjecture for an arbitrary $\mathbb{Z}_p$-extension remains an open problem.

§2. Geometric Extensions.

Let $k$ be a finite field, $|k| = p^u = q$, $p$ a prime number. Let $K_0$ be a function field with $k$ as its exact field of constants. For each natural number $n$, let $K_n/K_0$ be a cyclic extension of degree $p^n$ such that:

(i) For each $n$, $K_n \subset K_{n+1}$, $[K_{n+1} : K_n] = p$,

(ii) The field of constants of $K_n$ is $k$,

(iii) $K_\infty = \bigcup_{1 \leq n < \infty} K_n$,

and the prime divisors in the set $S$ of ramified primes of $K_n/K_0$ are fully ramified.

We have that $K_\infty/K_0$ is a $\mathbb{Z}_p$-extension, that is $\Gamma = \text{Gal}(K_\infty/K_0) = \mathbb{Z}_p$. In this situation, the $S$-class group is defined as the inductive limit of the corresponding groups at finite level. The topological group $\Gamma$ acts in a natural way on $C_\infty,S$, the $p$-part of the group of $S$-classes of $K_\infty$. In this section, we find necessary and sufficient conditions for the finiteness of $C_{\infty,S}^\Gamma$, the subgroup consisting of the invariant classes, for a class of $\mathbb{Z}_p$-extensions.

REMARK 4.

Let $E/K$ be a finite Galois extension of fields, complete under a discrete valuation, $P$ the prime in $K$, $Q$ the prime in $E$. If $E/K$ is totally and tamely ramified, then $E = K(\Pi)$, such that the irreducible polynomial is $\text{Irr}(\Pi,x,K) = x^e - \pi$ where $e = [E : K]$ is the ramification index, and $\pi, \Pi$ are primes elements of $P$ and $Q$ respectively (Lang[22], Hasse[11]). In particular, $K$ must contain the $e$-th roots of 1. By the reciprocity law, an abelian unramified geometric extension must be finite. It follows that for a prime $l \neq p$, $l$ an odd prime, geometric $\mathbb{Z}_l$-extensions of function fields $K_0/k$ do not exist if $k$ is a finite field.
First, we obtain a formula, ((22) below), for the number of ambiguous \( S \)-classes in a cyclic extension \( L/K \) of congruence function fields, where \( S \) is any finite set of prime divisors of \( K \). (We also denote by \( S \) the set of prime divisors of \( L \) which lie over these prime divisors).

We have the following exact sequences

\[
\begin{align*}
(12) & \quad 1 \longrightarrow E_S \longrightarrow L^* \longrightarrow P_S \longrightarrow 1, \\
(13) & \quad 1 \longrightarrow P_S \longrightarrow I_S \longrightarrow C_S \longrightarrow 1,
\end{align*}
\]

where \( E_S \) is the set of \( S \)-units in \( L \), \( P_S \) is the set of \( S \)-principal divisors in \( L \), \( I_S \) is the set of all the \( S \)-divisors in \( L \) and \( C_S = C_{L,S} \) is the group of \( S \)-classes of \( L \), (if \( S \neq \emptyset \), \( C_S \) is finite ([30], proposition 1)).

If \( G = \text{Gal}(L/K) \), (13) gives us, in cohomology, the exact \( G \)-sequence:

\[
(14) \quad 1 \longrightarrow P_S^G \longrightarrow I_S^G \longrightarrow C_S^G \longrightarrow H^1(P_S) \longrightarrow 1 \longrightarrow H^1(C_S) \longrightarrow H^0(P_S) \longrightarrow \cdots,
\]

where \( H^1(A) \) denotes \( H^1(G, A) \), \( A \) any \( G \)-module. Note that \( H^1(I_S) = \{1\} \) because \( I_S \) is a direct summand of \( I \), the divisor group, as \( G \)-module.

(See [33] for the basic results in cohomology theory of groups to which we do not refer explicitly.)

Therefore, from (12), (13) and (14), we have the exact \( G \)-sequences:

\[
\begin{align*}
(15) & \quad 1 \longrightarrow \frac{I_S^G}{P_S^G} \longrightarrow C_S^G \longrightarrow H^1(P_S) \longrightarrow 1, \\
(16) & \quad E_S^G = E_{K,S} \longrightarrow L^G = K^* \longrightarrow P_S^G \longrightarrow H^1(E_S) \longrightarrow 1, \\
(17) & \quad 1 \longrightarrow H^1(P_S) \longrightarrow H^2(E_S) \xrightarrow{\phi} H^2(L^*).
\end{align*}
\]
Also, we have 
\[ H^2(E_S) = H^0(E_S) = \frac{E^G_S}{N_{L/K}E^*_S} \] and 
\[ H^2(L^*) = H^0(L^*) = \frac{L^*G}{N_{L/K}L^*}. \]

Therefore, \[ H^1(P_S) = \ker \phi = \frac{(E^G_S \cap N_{L/K}L^*)}{N_{L/K}E^*_S}. \]

From (14) we obtain:

\[ [ C^G_{L,S} : 1 ] = [ H^1(P_S) : 1 ] \cdot [ I^G_S : P^G_S ] \]

\[ = \frac{[ E^G_S \cap N_{L/K}L^* : N_{L/K}E^*_S ] \cdot [ I^G_S : I_{K,S} ] \cdot [ I_{K,S} : P_{K,S} ]}{[ P^G_S : P_{K,S} ]} \]

Also, we have that

\[ [ I_{K,S} : P_{K,S} ] = [ C_{K,S} : 1 ], \]

\[ I^G_S : I_{K,S} ] = e = \prod_{i=1}^{r} e_i, \]

\[ [ P^G_S : P_{K,S} ] = [ H^1(E_S) : 1 ] \quad \text{(by (16))}, \]

where \( e_i \) are the ramification indices for the primes in \( K \) which are ramified in \( L/K \) and are not in \( S \).

Hence using (14) - (21) we obtain

\[ [ C^G_{L,S} : 1 ] = \frac{[ C_{K,S} : 1 ] \cdot e \cdot \phi(E_S)}{[ E^G_S : E^*_S \cap N_{L/K}L^* ]}, \]

where \( \phi(E_S) = \) the Herbrand quotient of \( E_S = \frac{[ H^0(E_S) : 1 ]}{[ H^1(E_S) : 1 ]}. \)
Coming back to our situation, let $T_0$ be any finite set of prime divisors in $K_0$. $T_n$ the prime divisors in $K_n$ above $T_0$. We assume that $T_0$ contains at least one ramified prime $Q$, and therefore this prime is fully ramified.

Let $E_{n,T_n}$ be the set of $T_n$-units in $K_n$. From (22) we have

\[
[C_{T_n}^{G_n} : 1] = \frac{[C_{K_0,T_0} : 1] \cdot e_n \cdot \phi(E_{K_n,T_n})}{[E_{K_0,T_0} : E_{K_0,T_0} \cap N_{0,K_n}^*]},
\]

where $e_n = [I_{K_n,T_n}^{G_n} : I_{K_0,T_0}]$ and $G_n = \text{Gal}(K_n/K_0) = \frac{\mathbb{Z}}{p^n\mathbb{Z}}$.

Also, using an argument similar to that in the proof of Theorem 2.5, page 147 in [19], we have

\[
\phi(E_{K_n,T_n}) = \prod_{P \in T_0 \setminus \{Q\}} e_p f_p = p^{n(v-1)} \cdot \prod_{P \in T_0} f_p
\]

where $T_0$ = prime divisors in $T_0$ which are not ramified,

$v$ = number of prime divisors in $T_0$ which ramify,

$f_p$ = degree of inertia of the prime divisor $P$.

From (23) we obtain

\[
[C_{K,0,T_0} : 1] \cdot \left\{ \prod_{P \in T_0} f_p \right\} \cdot e_n \cdot p^{n(v-1)}
\]

\[
[C_{K_n,T_n}^{G_n} : 1] = \frac{[C_{K_0,T_0} : 1] \cdot \left\{ \prod_{P \in T_0} f_p \right\} \cdot e_n \cdot p^{n(v-1)}}{[E_{K_0,T_0} : E_{K_0,T_0} \cap N_{0,K_n}^*]}.
\]

Now, if we take $T_0 = S = \text{the set of ramified primes}$, then we have

$S = T_0 = T_n$ for all $n$, $|S| = t = v$, $e_n = 1$, and

\[
\left|C_{K_n,T_n}^{G_n} \right| \sim \frac{p^{n(t-1)}}{[E_{K_0,S} : E_{K_0,S} \cap N_{0,K_n}^*]}.
\]
where for two sequences of numbers \(\{B_n\} \) and \(\{C_n\}\), \(B_n \sim C_n\) means that \(\lim_{n \to \infty} \frac{|B_n|}{|C_n|} = d\), \(d\) a positive real number.

Denoting \(E_{K_0,S}\) by \(E_{0,S}\) and \(E_{K_n,S}\) by \(E_{n,S}\), we state

**PROPOSITION 10.**

If \(K_\infty/K_0\) is as above, then:

(i) \(E_{n,S} = E_{0,S}\) for all \(n\).

(ii) \(E_{n,S} = k^* \times \mathbb{Z}^{t-1}\) for all \(n\).

**PROOF.**

Let \(G_n = \langle \sigma \rangle\) and consider \(\omega \in E_{n,S}\). Since \((\omega) = \prod_{P \in S} p^{\alpha(P)}\), \(P\) fully ramified for all \(P \in S\), we have \((\omega^{1-\sigma}) = (1)\). Therefore \(\omega^{1-\sigma}\) is a unit of \(K_n = k^*\); hence \(\omega^{1-\sigma} = \eta \in k\). This implies \(\eta^{p^n} = N_{n,0}\eta = N_{n,0} \omega^{1-\sigma} = 1\), and hence \(\eta = 1\). This shows (i).

To prove (ii), consider \(I(S)\) the set of divisors generated by elements in \(S\). \(I(S)\) is a free group of rank \(t\). The degree function: \(d : I(S) \longrightarrow \mathbb{Z}\) is non-trivial. Therefore, the elements of degree 0 in \(I(S)\) form a free group of rank \(t-1\). Denote this last set by \(I_0(S)\). If \(h\) is the class number of \(K_0\), and if \(P(S) = P \cap I(S)\) then \(P(S) \subset I_0(S)\) and \(I_0(S)^h \subset P(S)\), hence \(P(S)\) is a free abelian group of rank \(t-1\). Finally, since the torsion elements of \(E_{0,S}\) consist of the units of \(K_0 = k^*\), we have \(E_{0,S} = k^* \times \mathbb{Z}^{t-1}\). This is (ii).

\(\bigstar\)

From Proposition 10, we obtain that

\(N_{n,0}E_{n,S} = E_{0,S}^{p^n}\) and \([E_{0,S} : N_{n,0}E_{n,S}] = p^{n(t-1)}\).

Therefore, using these facts we obtain from (25):

\[
|C_{K_n,S}^{G_n}| = \frac{[E_{0,S} : N_{n,0}E_{n,S}]}{[E_{0,S} : E_{0,S} \cap N_{n,0}K_n^*]} = [E_{0,S} \cap N_{n,0}K_n^* : N_{n,0}E_{n,S}] .
\]
If we replace $C_{K_n,s}$ by its $p$-primary part $A_{K_n,s}$, (26) clearly remains valid.

The natural map $i: A_{K_n,s} \rightarrow A_{K_{n+1},s}$ is injective; therefore, we have

\[ A_{\infty}^\Gamma = \bigcup_{1 \leq n < \infty} A_{K_n,s}^G. \]

Thus the finiteness of $A_{\infty}^\Gamma$ is equivalent to the statement:

\[ [ E_{0,s} \cap N_{n,0} K_n^* : N_{n,0} E_{0,s} ] \sim 1, \]

i.e., this set of indices remains bounded for all $n$.

From (26), these two facts are equivalent to

\[ [ E_{0,s} : E_{0,s} \cap N_{n,0} K_n^* ] \sim p^{n(t-1)}. \]

We state this equivalence in the following

**PROPOSITION 11.**

Let $K_{oo} / K_0$ be a $Z_p$-extension of function fields as defined in the beginning of this section. Then the following are equivalent:

(i) $A_{\infty}^\Gamma$ is finite,

(ii) $[ E_{0,s} : E_{0,s} \cap N_{n,0} K_n^* ] \sim p^{n(t-1)}$,

(iii) $[ E_{0,s} \cap N_{n,0} K_n^* : N_{n,0} E_{0,s} ] \sim 1$.

We state this equivalence in the following

**PROPOSITION 11.**

Let $K_{oo} / K_0$ be a $Z_p$-extension of function fields as defined in the beginning of this section. Then the following are equivalent:

(i) $A_{\infty}^\Gamma$ is finite,

(ii) $[ E_{0,s} : E_{0,s} \cap N_{n,0} K_n^* ] \sim p^{n(t-1)}$,

(iii) $[ E_{0,s} \cap N_{n,0} K_n^* : N_{n,0} E_{0,s} ] \sim 1$.

Now, if we consider a cyclic extension $L/K$ of local fields of degree $p^n$ given by

the Witt vector $(\beta_0, \beta_1, \ldots, \beta_{n-1})$, then to test if an element $\alpha \in K$ is a norm from $L$, we use the following criterion due to Witt [42]:

$K$ is isomorphic to a "Laurent series" field $k'((T))$, $k'$ a finite field. Let $F$ be the unramified extension of $Q_p$ such that $\mathcal{O}_F / M_F = k'$, where $\mathcal{O}_F$ is the ring of integers of $F$ and $M_F$ is the maximal ideal of $\mathcal{O}_F$. Choose $A, B_0, B_1, \ldots, B_i, \ldots, B_{n-1}$ in $\mathcal{O}_F((T))$ such that $A \equiv \alpha \mod M_F, B_i \equiv \beta_i \mod M_F, 0 \leq i \leq n - 1$, congruence defined

coefficientwise. Let $\text{Res} \left( \frac{dA}{A} \right) \left[ \frac{B_0^{p^{n-1}}}{p^n} + \ldots + \frac{B_{n-1}}{p} \right] = \gamma \in F$. Let $\text{Tr} = \text{Trace from } F$
to $Q_p$. Then $\text{Tr} \gamma = \frac{m}{p^n} = b + \frac{a}{p^n}$, with $b \in Z_p, a \in Z, 0 \leq a < p^n$. $\text{Tr} \gamma \mod 1 = \frac{a}{p^n}$.

Then $\alpha$ is a norm from $L \iff \text{Tr} \gamma \equiv 0 \mod 1$.

**REMARK 5.**

By the Grunwald-Hasse-Wang Theorem, there exists a normal extension $E/Q$ with $\text{Gal}(E/Q) \cong \text{Gal}(F/Q_p)$, i.e., $p$ is inert in $E/Q$ ([25], Theorem 5). Also $\vartheta_E/M_E = \vartheta_F/M_F$ ([11], page 143), and $\vartheta_E \subset \vartheta_F$. Hence we may assume that the elements $A, B_0, B_1, \ldots, B_{n-1}$ are chosen in $\vartheta_E(T)$. Therefore $p^n \text{Tr} \gamma \in Z_p \cap Q = Z(p)$, where $Z(p)$ denotes the localization of $Z$ at the prime ideal $(p)$.

**REMARK 6.**

If the Witt Vector $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ determines the tower of fields $K_0 = K \subset K_1 \subset \ldots \subset K_n = L$, then $K_i = K_{i-1}(v_i), v_i^p - v_i = z_{i-1} + \beta_{i-1}$, with $z_{i-1} \in K_{i-1}, v_i \in K_i$. We also have $K_i = K_{i-1}(v_i + \beta_{i-1})$, so that $(v_i + \beta_{i-1})^p - (v_i + \beta_{i-1}) = v_i^p - v_i + p_{i-1} - \beta_{i-1} = z_{i-1} + \beta_{i-1}$. Hence, $L/K$ is defined also by the Witt vector $(\beta_0^{j_0}, \beta_1^{j_1}, \ldots, \beta_{n-1}^{j_{n-1}})$ with $j_0, j_1, \ldots, j_{n-1}$ any non-negative integers.

**REMARK 7.**

In the notation of the section, by Hasse's Norm Theorem, any $A$ in $K_0$ is a global norm from $K_n \iff$ it is a local norm for all the primes. Since $S$ consists of precisely the ramified primes and all units are norms in an unramified local extension, it follows that an $S$-unit is a global norm $\iff$ it is a local norm for all the primes in $S$.

By Remark 6 (see also [42]), in a local extension we have that
For the set $S = \{P_1, P_2, \ldots, P_t\}$ of ramified prime divisors of the $\mathbb{Z}_p$-extension $K_\infty/K_0$, we consider integers $a_i, b_i, h_i$, such that $p_{i,\beta}$ is of degree 0 and $\left(\frac{p_{i,\beta}}{p_{i,t}}\right)^{h_i} = (\delta_i)$ is principal in $K_0$. Let $\pi_{j,i}$ be a representative in characteristic 0 of $\delta_j$ when we complete at $P_i$, as in the statement of the Witt's criterion, $1 \leq i, j \leq t - 1$. Also, if $K_\infty/K_0$ is given by the Witt vector $(\beta_0, \beta_1, \ldots, \beta_{n-1}, \ldots)$, let $B_{n,i}$ be a representative in characteristic 0 of $\beta_n$, when we complete at $P_i$, $i = 1, \ldots, t - 1$; $n = 0, 1, \ldots$. Then, we define

$$a_{j,i}^{(n,m)} = \text{Tr Res} \left[ \left\{ \frac{d\pi_{i,i}}{d\pi_{j,i}} \right\} \cdot B_{n,i}^{p_{i,j}} \cdot d\pi_{i,i} \right] \in \mathbb{Z}(p), 1 \leq i, j \leq t - 1. \quad (27)$$

We have

$$a_{j,i}^{(n,m)} \equiv a_{j,i}^{(n,k)} \mod p^{m+1} \text{ for all } k \geq m. \quad (28)$$

Let $\alpha = \delta_{1, t-1} \ldots \delta_{i, i} \ldots$ be an $S$-unit in the subgroup generated by the $\delta_i$, a subgroup of finite index in the group of all $S$-units. Then, $A_i = \pi_{1,i}^{e_1} \pi_{2,i}^{e_2} \ldots \pi_{t-1,i}^{e_{t-1}}$ is a representative of $\alpha$ in characteristic 0 when we complete at $P_i$.

Then from (27) we obtain:

$$\text{Tr Res} \left( \frac{dA_i}{A_i} \right) \cdot \left( \sum_{s=0}^{n-1} \frac{B_{s,i}^{p^{n-1-s}}}{p^{n-s}} \right) = \sum_{j=0}^{t-1} \left[ \frac{1}{p^n} e_j c_{j,i}^{(n)} \right],$$

where

$$c_{j,i}^{(n)} = \sum_{s=0}^{n-1} p^s a_{j,i}^{(s,n-1-s)}, n \geq 1. \quad (29)$$

So, we have, using (28),
Thus, 

\[(30)\quad c_{j,i}^{(n+1)} = c_{j,i}^{(n)} + p^n a_{j,i}^{(n,0)} \mod p^n.\]

Now, since \(\alpha\) is an S-unit:

\(\alpha\) is a global norm (in \(K_n/K_0\)) \(\iff\) \(\alpha\) is a local norm at \(P_i\) for \(1 \leq i \leq t - 1\)

\(\iff\) \(\sum_{j=1}^{t-1} \epsilon_j c_{j,i}^{(n)} \equiv 0 \mod p^n, i = 1, \ldots, t - 1.\)

Let

\[(31)\quad C_n = \begin{bmatrix}
    c_{1,1}^{(n)} & c_{2,1}^{(n)} & \cdots & c_{t-1,1}^{(n)} \\
    c_{1,2}^{(n)} & c_{2,2}^{(n)} & \cdots & c_{t-1,2}^{(n)} \\
    \vdots & \vdots & \ddots & \vdots \\
    c_{1,t-1}^{(n)} & c_{2,t-1}^{(n)} & \cdots & c_{t-1,t-1}^{(n)}
\end{bmatrix} \in M_{(t-1,t-1)}(\mathbb{Z}_p).\]

Then, by (30), we have

\[(32)\quad C_{n+1} = C_n + p^n D_n, n \geq 1,\] with \(D_n\) a matrix in \(\mathbb{Z}_p\).

Now we state

**Lemma 9.**

The sequence \(\{C_n\}_{n=1}^{\infty}\) is Cauchy in \(M_{(t-1,t-1)}(\mathbb{Z}_p)\).

**Proof.**

Follows obviously from (32).
Let \( C = \lim C_n \).

We will show that if \( C \) is non-singular, the analogue of Gross' conjecture is true (Proposition 12). Then, under the assumption that \( C \) has rational coordinates, we shall show that the converse is also true (Proposition 15).

First assume that rank \( C = t - 1 \). In this case, we have that there exists an \( N \) such that for all \( n \geq N \), rank \( C_n = t - 1 \), i.e., \( \det C_n \neq 0 \).

For any sequence \( \{b_n\}_{n=1}^{\infty} \) of elements in \( \mathbb{Q}_p \), if \( \nu_p \) denotes the valuation with respect to the prime \( p \), we have that if \( \lim b_n = b_0 \), then \( \lim \nu_p(b_n) = \nu_p(b_0) \). In particular, \( \lim \nu_p(\det C_n) = \nu_p(\det C) = a \in \mathbb{Z} \). So, there exists an \( N \) such that for all \( n \geq N \) we have, \( \nu_p(\det C_n) = a \).

On the other hand, we have that

\[
\nu_p(\det C_n) = \nu_p \left( \sum_{\sigma \in S_{t-1}} (-1)^{\text{sgn} \sigma} \prod_{i=1}^{t-1} c_{i,\sigma(i)}^{(n)} \right) \geq \min_{i,j} \{ \nu_p(c_{i,j}^{(n)}) \},
\]

\( S_{t-1} \) the symmetric group of degree \( t - 1 \). Hence, \( \nu_p(c_{i,j}^{(n)}) \leq a \), for some \( i,j \).

In \( \mathbb{Q}_p \), if \( X = (x_1, \ldots, x_{t-1}) \in \mathbb{Q}_p^{t-1} \), define

\[
\|X\|_p = \max_{1 \leq i \leq t-1} \{|x_i|_p\} \quad \text{or equivalently} \quad \nu_p(X) = \min_{1 \leq i \leq t-1} \{\nu_p(x_i)\}.
\]

\( \| \cdot \|_p \) is a norm and satisfies \( \|X + Y\|_p \leq \max \{\|X\|_p, \|Y\|_p\} \).

If \( E = (e_{i,j}) \) is any matrix in \( \mathbb{Q}_p \), i.e., \( E \in M_{t-1,t-1}(\mathbb{Q}_p) \), define

\[
\|E\|_p = \max_{i,j} \{|e_{i,j}|_p\} \quad \text{or} \quad \nu_p(E) = \min_{i,j} \{\nu_p(e_{i,j})\}.
\]

From (34), we have that if \( E \) and \( D \) are two matrices, then

\[
\|ED\|_p \leq \|E\|_p \cdot \|D\|_p \quad \text{or} \quad \nu_p(ED) \geq \nu_p(E) + \nu_p(D).
\]

If \( E \) is invertible, \( 0 = \nu_p(E \cdot E^{-1}) \geq \nu_p(E) + \nu_p(E^{-1}) \).

Therefore, if \( E \) is invertible, we obtain
It follows that, in our case, $v_p(C_n) \leq a$, and $v_p(C_{n}^{-1}) \leq -v_p(C_n)$.

On the other hand,

$$C_{n}^{-1} = (\det C_n)^{-1} \begin{bmatrix} \xi_{1,1}^{(n)} & \xi_{1,2}^{(n)} & \cdots & \xi_{1,t-1}^{(n)} \\ \xi_{2,1}^{(n)} & \xi_{2,2}^{(n)} & \cdots & \xi_{2,t-1}^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi_{t-1,1}^{(n)} & \xi_{t-1,2}^{(n)} & \cdots & \xi_{t-1,t-1}^{(n)} \end{bmatrix} \in M_{(t-1,t-1)}(Q_p),$$

where $\xi_{i,j}^{(n)}$ denote the cofactors of the matrix $C_n$. Write $C_{n}^{-1} = (b_{i,j})_{1 \leq i,j \leq t-1}$.

Since $C_n \in M_{(t-1,t-1)}(Z_p)$, we have that $\xi_{i,j}^{(n)} \in Z_p$, so $v_p(\xi_{i,j}^{(n)}) \geq 0$ and then

$$v_p(b_{i,j}) = v_p((\det C_n)^{-1} \xi_{i,j}^{(n)}) = -v_p(\det C_n) + v_p(\xi_{i,j}^{(n)}) \geq -a + 0 = -a.$$ Therefore

$$v_p(C_{n}^{-1}) = \min_{i,j} \{v_p(b_{i,j})\} \geq -a,$$ that is

$$-v_p(\det C_n) = -a \leq v_p(C_{n}^{-1}) \leq -v_p(C_n).$$

**Lemma 10.**

$$C \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_{t-1} \end{pmatrix} = 0 \iff \alpha = \delta_{1}^{\varepsilon_1} \cdots \delta_{i}^{\varepsilon_i} \cdots \delta_{t-1}^{\varepsilon_{t-1}} \in \bigcap_{n \geq 0} N_{n,0} K_n.$$

**Proof.**
If \( \alpha \in \mathbb{N}_{n,0} K_n \) for all \( n \), then by the Witt criterion, \( C_n \left( \begin{array}{c} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_{t-1} \end{array} \right) \equiv 0 \mod p^n \) for all \( n \). Therefore \( \left( \begin{array}{c} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_{t-1} \end{array} \right) = \lim_{n \to \infty} C_n \left( \begin{array}{c} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_{t-1} \end{array} \right) = 0. \)

Conversely, if \( \left( \begin{array}{c} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_{t-1} \end{array} \right) = 0 \), then \( \lim_{n \to \infty} C_n \left( \begin{array}{c} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_{t-1} \end{array} \right) = 0. \) Hence we have congruences: \( \sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n)} \equiv 0 \mod m_n \), \( i = 1, \ldots, t-1 \), where \( m_n \) is the minimum satisfying the congruence, for all \( i \). Then \( \lim m_n = \infty. \)

We claim that \( m_n \geq n \) for all \( n \). Assume that \( m_n < n \) for some \( n \). From (32) we obtain:

\[
\sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n+1)} = \sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n)} + p^n \sum_{j=0}^{t-1} \varepsilon_j d_{j,i}^{(n)} \text{ for all } i.
\]

For some \( i \), we have \( v_p \left( \sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n)} \right) = m_n < n \leq v_p \left( p^n \sum_{j=0}^{t-1} \varepsilon_j d_{j,i}^{(n)} \right). \) Therefore,

\[
v_p \left( \sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n+1)} \right) = m_n. \text{ It follows that } v_p \left( \sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(k)} \right) = m_n \text{ for all } k \geq n.
\]

Thus, \( \lim_{n \to \infty} C_n \left( \begin{array}{c} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_{t-1} \end{array} \right) \neq 0 \), a contradiction. Therefore \( m_n \geq n \) for all \( n \), hence by the Witt's criterion \( \alpha = \delta_1^{\varepsilon_1} \cdots \delta_i^{\varepsilon_i} \cdots \delta_{t-1}^{\varepsilon_{t-1}} \) is norm for all \( n \).

\[
\text{PROPOSITION 12.}
\]

Let \( C \) be as above. Then if \( C \) is invertible, the analogue of Gross' conjecture holds.
PROOF.

If \( \alpha = \delta_1^{e_1} \cdots \delta_i^{e_i} \cdots \delta_{t-1}^{e_{t-1}} \) is a norm from \( K_n \), by the Witt's criterion, we have that

\[
C_n\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{t-1} \\ \end{pmatrix} = \begin{pmatrix} \rho_1 \\ \rho_2 \\ \vdots \\ \rho_{t-1} \\ \end{pmatrix} \equiv 0 \pmod{p^n}. \text{ Then, } C_n\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{t-1} \\ \end{pmatrix} = C_n^{-1}\begin{pmatrix} \rho_1 \\ \rho_2 \\ \vdots \\ \rho_{t-1} \\ \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{t-1} b_{1,j} \rho_j \\ \sum_{j=1}^{t-1} b_{2,j} \rho_j \\ \vdots \\ \sum_{j=1}^{t-1} b_{t-1,j} \rho_j \\ \end{pmatrix},
\]

(38) \[ e_i = \sum_{j=1}^{t-1} b_{i,j} \rho_j, \; v_p(e_i) \geq \min \{v_p(b_{i,j}) + v_p(\rho_j)\} \geq v_p(C_n^{-1}) + n \geq n - a, \]

for all \( n \geq N \).

Therefore, we have

(39) \[ [ E_{0,S} : E_{0,S} \cap N_{n,0} K_n^* ] \geq p^{(n-a)(t-1)} \sim p^{n(t-1)}. \]

On the other hand

(40) \[ [ E_{0,S} : E_{0,S} \cap N_{n,0} K_n^* ] \leq [ E_{0,S} : N_{n,0} E_{n,S} ] = [ E_{0,S} : E_{n,S} ] \sim p^{n(t-1)}. \]

From (39) and (40) we obtain

(41) \[ [ E_{0,S} : E_{0,S} \cap N_{n,0} K_n^* ] \sim p^{n(t-1)}. \]

From Proposition 11 and (41) we obtain Proposition 12.

Now, we assume for the rest of the section that \( C \) has rational coordinates.
PROPOSITION 13.

C is invertible iff \( E_{0,S} \cap ( \cap_{n \geq 0} N_{n,0} K_n ) = k^* \).

PROOF.

Assume first that \( C \) is invertible. We have shown in the proof of Proposition 12 that \( R \cap ( \cap_{n \geq 0} N_{n,0} K_n ) = \{1\} \), where \( R \) is a subgroup of \( E_{0,S} \) of finite index \( h \).

Therefore, if \( \alpha \in E_{0,S} \cap ( \cap_{n \geq 0} N_{n,0} K_n ) \), then \( \alpha^h = 1 \), that is \( \alpha \in k^* \). Since \( k \) is perfect, \( k^* \subset E_{0,S} \cap ( \cap_{n \geq 0} N_{n,0} K_n ) \).

Conversely, if \( E_{0,S} \cap ( \cap_{n \geq 0} N_{n,0} K_n ) = k^* \), and \( C \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{t-1} \end{pmatrix} = 0 \), then by Lemma 10,

\[
\alpha = \delta_{e_1} \ldots \delta_{e_i} \ldots \delta_{e_{t-1}} \in E_{0,S} \cap ( \cap_{n \geq 0} N_{n,0} K_n ) = k^* \Rightarrow e_1 = e_2 = \ldots = e_{t-1} = 0, \text{ that is, } C \text{ is invertible.}
\]

\( \diamond \)

PROPOSITION 14.

The analogue of Gross conjecture is true \( \Leftrightarrow \) \( C \) is invertible.

PROOF.

\( \Rightarrow \) Already proved in Proposition 12.

\( \Leftarrow \) If possible, let \( C \) be not invertible. By Proposition 13, there exists a non-constant \( \alpha \) in \( E_{0,S} \cap ( \cap_{n \geq 0} N_{n,0} K_n ) \). We have that \( E_{0,S} \approx \text{finite group} \times \mathbb{Z}^{t-1} \), \( t = |S| \)

= the number of ramified primes. Therefore, \( T = \langle \alpha \rangle \times \mathbb{Z}^{t-2} \) is of finite index in \( E_{0,S} \).

By Proposition 11, the analogue of Gross' conjecture is true \( \Leftrightarrow \) for \( n >> 0 \), we have \( [T \cap N_{n,0} K_n : T \cap N_{n+1,0} K_{n+1}] = p^{t-1} \). Now \( T \cap N_{n,0} K_n = \langle \alpha \rangle \times L \), with \( L = \mathbb{Z}^{t-2} \), \( T \cap N_{n+1,0} K_{n+1} \supset \langle \alpha \rangle \times LP \) (because if \( y \in L, y = N_{n,0} z, z \in K_n \subset K_{n+1}, N_{n+1,0} z = N_{n,0}(N_{n+1,n} z) = N_{n,0} z^P = y^P \)). So
Thus, under the assumption that the matrix has rational coordinates, we have proved

**THEOREM 10.**

The following conditions are equivalent:

(i) $A_\infty$ is finite, that is, the analogue of Gross' conjecture holds,

(ii) $[ E_{0,S} : E_{0,S} \cap N_{n,0} K_n^* ] \sim p^{n(1-1)}$,

(iii) $[ E_{0,S} \cap N_{n,0} K_n^* : N_{n,0} E_{n,S} ] \sim 1$,

(iv) $[ E_{0,S} \cap N_{n,0} K_n^* : E_{0,S} \cap N_{n+1,0} K_{n+1}^* ] = p^{n-1}$ for $n >> 0$,

(v) $C$ is invertible,

(vi) $E_{0,S} \cap ( \cap N_{n,0} K_n^* ) = k^*$.

We leave the proof of the following refinement of Proposition 13, (it gives the precise rank of the group of universal norms), as an exercise for the reader:

**PROPOSITION 15.**

Assume that $C \in M_{t-1,t-1} \left( Z(p) \right)$, and rank $C = r \leq t - 1$. Then
\[
\text{rank}_Z \left( E_{0,S} \cap ( \cap N_{n,0} K_n^* ) \right) = t - 1 - r.
\]

**REMARK 8.**

Let $K_0 = k(x)$ and $L_\infty$ be an extension of degree 2 of $K_\infty$, and Galois over $K_0$. Then $\text{Gal}(L_\infty/K_0) \cong \Gamma \times C_2$, where $C_2$ is the cyclic group of order 2. Let $L_0 = L_\infty^\Gamma$ be the fixed field of $L_\infty$ under $\Gamma$. Then we can define the minus $S$-units as in the
number field case. In this situation, the analogue of Theorem 1 can be proved in the same way as above.

§3. Constant Extensions.

In this section, $K_{\infty}/k_{\infty}$ is the constant $\mathbb{Z}_p$-extension obtained from the congruence function field $K_0/k_0$, where $p$ is any prime, not necessarily equal to the characteristic.

There is a natural map $\varphi_\infty: C_{\infty} \to C_{\infty, S_{\infty}} = C_S$ with a finite cokernel ([30], Proposition 1), where $C_{\infty}$ is the group of all divisor classes of degree 0. It is well known that $C_\infty(p)^\Gamma = C_0(p)$ is finite and that $C_\infty(p) = \left( \frac{Q_0}{\mathbb{Z}_p} \right)^{\lambda}$ with $0 \leq \lambda \leq 2g$, with $g$ the genus of $K_0$. Therefore the following Proposition follows from the theory of compact noetherian $\mathbb{Z}_p$-modules ([17], Lemma 3).

PROPOSITION 16.

In any constant $\mathbb{Z}_p$-extension $K_{\infty}/K_0$ of function fields of one variable, $C_S(p)^\Gamma$ is finite for any finite non-empty set $S$ of prime divisors in $K_0$. The analogue of Gross' conjecture holds in this case.

For the cohomology of $S$-units, the following Theorem is, now, easily proved using Proposition 16 (analogue of Gross' conjecture), the analogue of Auslander-Brumer and Chase-Harrison-Rosenberg seven term exact sequence ([17], Proposition 1, page 191), and formulas similar to (22) - (26).

THEOREM 11.

Let $K_{\infty}/K_0$ as above. If $n_0$ is such that for $n \geq n_0$ the primes in $S_{n_0}$ remain inert, then

(i) $E_{n,S_n} = E_{n_0,S_{n_0}} \cdot k_n.$

(ii) $[ E_{n_0,S_{n_0}} : N_{n,n_0} E_{n,S_n} ] \sim p^{(t-1)n}.$
(iii) \[ \{ E_{n_0, n_0} : E_{n_0, n_0} \cap N_{n, n_0} K_n^* \} \sim p^{(t-1)n}. \]
(iv) \[ \{ E_{n_0, n_0} \cap N_{n, n_0} K_n^* : N_{n, n_0} E_n, S_n \} \sim 1. \]
(v) \[ H^1(\Gamma, E_{\infty, S_{\infty}}) \text{ is finite and } H^2(\Gamma, E_{\infty, S_{\infty}}) = \left( \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \right)_t, t = |S_\infty|, \Gamma = \mathbb{Z}_p. \]

§4. Examples.

In this section, we are concerned with a special case where the conditions of Theorem 10 of § 2 are met. We use the notation of § 2.

In this section, the field of constants will be \( k = F_p \), the finite field with \( p \) elements, \( K_0 = F_p(x) \), \( p \) an odd prime. The Witt vector corresponding to the extension \( K_\infty/K_0 \) will be \( \beta = (\beta_0, \beta_1, \beta_2, \ldots) \). Also, let \( B_i \) be an element in characteristic 0 corresponding to \( \beta_i \), as explained in the Witt's criterion. By abuse of notation, we shall use the same symbol to denote an element in characteristic \( p \) and its corresponding element in characteristic 0.

**EXAMPLE 1.**

Let \( B_0 = \frac{1}{(x-a)(x-b)} \) with \( a, b \in \mathbb{Q}_p, a \neq b, B_i = 0 \text{ for } i \geq 1 \). Let \( A = \frac{(x-a)^e}{(x-b)} \) be an arbitrary (modulo \( F_p \)) \( S \)-unit. (Here \( S = \{ P_a, P_b \} \) where divisor of \( (x-a) = \frac{P_a}{P_\infty} \) and divisor of \( (x-b) = \frac{P_b}{P_\infty} \).

A will be a global norm iff \( \lim_{n \to \infty} \text{res}_{P_a} B_0^n \cdot \left( \frac{dA}{A} \right) \neq 0 \), because of the product formula for the norm residue symbol, and \( C \) is 1 x 1 matrix.

Now \( \text{res}_{P_a} B_0^{n-1} \cdot \left( \frac{dA}{A} \right) = \frac{-e \cdot (2p^{n-1})!}{(p^{n-1})^2 \cdot (a-b)^{2p^{n-1}}} \). On the other hand, we have \( v_p(p^{r!}) = p^{r-1} + \ldots + p + 1 \text{ ([22]). Therefore } v_p\left( \frac{(2p^{n-1})!}{(p^{n-1})^2} \right) = 0. \) Thus
\[ C_n = \frac{-(2p^{n-1})!}{(p^{n-1}!)^2 \cdot (a-b)^{2p^{n-1}}} \] is invertible and then \( C = \lim_{n \to \infty} C_n \) is invertible. Therefore, the analogue of Gross' conjecture holds in this case.

**EXAMPLE 2.**

This is an example where the analogue of Gross' conjecture does not hold. We will construct an extension defined by a Witt vector such that we have only two (fully) ramified prime divisors and \( C_n \equiv 0 \mod p^n \) for all \( n \). Therefore \( C = \lim_{n \to \infty} C_n = 0 \).

Let \( B_0 = \frac{3x^2-1}{x^2 \cdot (x-1)} \). In this case, \( S = \{ P_0, P_1 \} \). Consider \( A = \left( \frac{1-x}{x} \right)^e \). Then, \( B_0 \cdot \frac{dA}{A} = -e \cdot \left( \frac{3x^2-1}{x^3 \cdot (x-1)} + \frac{3x^2-1}{x^2 \cdot (x-1)^2} \right) dx \), therefore \( B_0 \cdot \left( \frac{dA}{A} \right) = -D_x \left\{ e \cdot \frac{3x+1}{(2x^2 \cdot (x-1)^2)} \right\} \). Thus \( C_1 = (0) \). Assume we have constructed \( B_0, B_1, \ldots, B_{n-1} \) such that \( C_i \equiv 0 \mod p^i \) for \( i = 1, 2, 3, \ldots, n \). From (30) and from the fact that \( C_n \equiv 0 \mod p^n \), it follows that \( C_{n+1} = p^n (a_n + b_n) \), where \( a_n = a_{1,1}^{(n,0)} \) and \( b_n \in \mathbb{Z}_p \). We will have \( C_{n+1} \equiv 0 \mod p^{n+1} \) \( \iff \) \( a_n + b_n \equiv 0 \mod p \). Consider now \( B_n = \frac{r_n}{x \cdot (x-1)} \). Then \( a_n = 2r_n \). Finally, since \( p \) is odd, we can choose \( r_n \) in \( \mathbb{Z} \) such that \( 2r_n \equiv -b_n \mod p \). Thus the analogue of Gross' conjecture does not hold in this extension.

**EXAMPLE 3.**

Let \( k = \mathbb{F}_p \), \( K_0 = k(x) \). Let \( y = \sqrt{x} \). Let \( B_0 = \frac{x+1}{x-1} \), \( B_n = \frac{r_n}{x-1} \), \( r_n \) to be determined. Consider \( K_\infty \) the \( \mathbb{Z}_p \)-extension over \( K_0 \) determined by this Witt vector. Now, if \( L_0 = k(y) = k(\sqrt{x}) \), let \( L_\infty \) be the \( \mathbb{Z}_p \)-extension of \( L_0 \) given by the same Witt vector \( (B_0 = \frac{y^2+1}{y^2-1}, B_1 = \frac{r_1}{(y-1) \cdot (y+1)}, \ldots, B_n = \frac{r_n}{(y-1) \cdot (y+1)}, \ldots) \) viewed in \( L_0 \). In this case, the minus \( S \)-units are the same as the \( S \)-units. An easy calculation shows that the matrix \( C_1 \) for the minus \( S \)-units of \( L_\infty /L_0 \) is equal 0. As in
Example 2, we choose $r_n$ such that $C_n \equiv 0 \mod p^n$. Therefore $C = \lim_{n \to \infty} C_n = 0$ and the analogue of Gross' conjecture does not hold in this case for minus $S$-units.

**REMARK 9.**

Example 3 shows that the "true" analogue of Gross' conjecture, that is, for minus $S$-units does not hold for an arbitrary $\mathbb{Z}_p$-extension.

**REMARK 10.**

Hayes ([12]) defined the analogue of cyclotomic extensions for function fields; however for a prime power modulus the $p$-extensions so obtained are not cyclic in general as is easily seen by comparing the exponent of the different of these extensions with the exponent obtained by Schmid ([31]). There seems to be no theory of $\mathbb{Z}_p$-extensions of cyclotomic function fields.
BIBLIOGRAPHY


