**Palestine Journal of Mathematics**

**Vol. 3(1) (2014)**, 1–10 

# Galois module structure of the $p$–subgroup of the minus part of the ray class group in $\mathbb{Z}_p$–extensions

F. Jarquín-Zárate and G. Villa-Salvador

Communicated by Jose Luis Lopez-Bonilla

MSC 2010 Classifications: 11R23; 11R18; 11R29; 11R32.

Keywords and phrases: $\mathbb{Z}_p$–extensions; Iwasawa's theory; integral representation; Galois module structure; injective module; class group.

**Abstract.** Let $p$ be an odd prime number and let $L/K$ be an arbitrary finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type. In this paper, assuming that the Iwasawa $\mu^-$–invariants of $K$ and $L$ are zero, we obtain the Galois module structure of $\mathscr{C}_{\mathfrak{B}}^-(p)$, the $p$–subgroup of the minus part of the ray class group of $L$, and of ${}_p\mathscr{C}_{\mathfrak{B}}^-$, the elements of $\mathscr{C}_{\mathfrak{B}}^-(p)$ of order a divisor of $p$, associated to the modulus $\mathfrak{B}$ of $L$ induced by a modulus $\mathfrak{A}$ of $K$, which contains in its support the non–$p$–prime divisors of $K^+$ ramified in $L^+$ and split in $K$, and also contains in its support a finite collection of non–$p$–prime divisors of $K^+$ that do not ramify in $L^+$; they may split in $K$ or be inert in $K$. That is, we obtain explicitly the decomposition of $\mathscr{C}_{\mathfrak{B}}^-(p)$ (of ${}_p\mathscr{C}_{\mathfrak{B}}^-$) as a direct sum of indecomposable $\mathbb{Z}_p[G]$–modules ($\mathbb{F}_p[G]$–modules) with respect to the modulus $\mathfrak{B}$.

## 1 Introduction

The Riemann-Hurwitz formula, in the context of algebraic function fields of one variable, is used to calculate the genus of a Riemann surface or a curve. In 1979, Yûji Kida [6] proved an analogous formula for number fields. Namely, for a finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type ($p$ an odd prime number), Kida's formula computes the Iwasawa $\lambda^-$–invariant of a $\mathbb{Z}_p$–cyclotomic field of CM–type. Later, in 1980, Kenkichi Iwasawa [4], using Galois representations, obtained a generalization of this formula valid for fields other than CM-fields. In all this development, the structure as Galois module of the $p$–subgroup of the minus part of the class group $\mathscr{C}_L^-(p)$ of a field of CM–type $L$ is important.

In general, to obtain the Galois module structure of the $p$–subgroup of the minus part of the class group $\mathscr{C}_L^-(p)$, that is, to get the decomposition of $\mathscr{C}_L^-(p)$ as a direct sum of indecomposable $\mathbb{Z}_p[G]$–modules, the following technique has been used successfully. Consider the $p$–Sylow subgroup of the minus part of the ray class group $\mathscr{C}_{\mathfrak{N}}^-(p)$ where $\mathfrak{N}$ is the modulus in $L$ induced by a modulus $\mathfrak{M}$ which contains in its support all the non–$p$–prime divisors of $K^+$ ramified in $L^+$ and split in $K$. Then, consider the exact sequence of $\mathbb{Z}_p[G]$–modules

$$0 \longrightarrow \mathfrak{R} \longrightarrow \mathscr{C}_{\mathfrak{N}}^-(p) \longrightarrow \mathscr{C}_L^-(p) \longrightarrow 0, \tag{1.1}$$

where $\mathfrak{R}$ is the kernel of the natural map characterized in [10], by Villa and Madan.

In (1.1), $\mathscr{C}_{\mathfrak{N}}^-(p)$ is associated with the modulus $\mathfrak{N}$, which contains in its support all the non–$p$– prime divisors of $K^+$ ramified in $L^+$ and split in $K$, and also its support contains a finite collection of non–$p$–prime divisors of $K^+$ unramified in $L^+$ which may be split or inert in $K$ (see [9] p.343.) The natural question is, which is the structure of $\mathscr{C}_{\mathfrak{B}}^-(p)$ as $\mathbb{Z}_p[G]$–module, if $\mathfrak{B}$ is an arbitrary modulus in $L$?

The main objective of this article is to answer the question in the case that $\mathfrak{B}$ is a modulus of $L$ induced by a modulus $\mathfrak{A}$ of $K$ which contains in its support a finite number of non–$p$–prime divisors of $K^+$ ramified in $L^+$ and split in $K$ and a finite collection of non–$p$–prime divisors of $K^+$ ramified in $L^+$ that may be split or inert in $K$. That is, we obtain explicitly, for this type of modulus $\mathfrak{B}$, the decomposition as a direct sum of indecomposable $\mathbb{Z}_p[G]$–modules of $\mathscr{C}_{\mathfrak{B}}^-(p)$. This structure is the content of Theorem 4.1. We also derive the modular structure of ${}_p\mathscr{C}_{\mathfrak{B}}^-$, the $p$–part of $\mathscr{C}_{\mathfrak{B}}^-(p)$, i.e., we obtain the decomposition of ${}_p\mathscr{C}_{\mathfrak{B}}^-$ as a direct sum of indecomposable $\mathbb{F}_p[G]$–modules. The result is Corollary 4.3.

The organization of this paper is as follows. In Section 2, the necessary notation and basic results on $\mathbb{Z}_p$–extensions are collected. In Section 3, we obtain an implicit characterization of $\mathscr{C}_{\mathfrak{B}}^-(p)$ as $\mathbb{Z}_p[G]$–module. This is given in the Theorem 3.5. Finally, in Section 4 we obtain the Galois module structure of $\mathscr{C}_{\mathfrak{B}}^-(p)$ and of ${}_p\mathscr{C}_{\mathfrak{B}}^-$.

## 2 Notation and some preliminaries on $\mathbb{Z}_p$–extensions

We establish in this section the necessary notation and the auxiliary results on $\mathbb{Z}_p$–extensions, where $\mathbb{Z}_p$ denotes the ring of $p$-adic integers. In what follows $p$ denotes an odd prime number. If $L$ is an algebraic number field, a monomorphism $\phi : L \to \mathbb{C}$, where $\mathbb{C}$ denotes the field of complex numbers, is called *an embedding of* $L$. An embedding $\phi$ of $L$ is said to be *real* if $\phi(L) \subseteq \mathbb{R}$, where $\mathbb{R}$ denotes the field of real numbers, and $\phi$ is called *an imaginary embedding* of $L$ if $\phi(L) \nsubseteq \mathbb{R}$. If all the embeddings of $L$ are real, $L$ is called *a totally real field*. If all the embeddings of $L$ are imaginary, $L$ is called *a totally imaginary field*. Denote by $J$ complex conjugation. If $J(L) = L$ and $\sigma \circ J = J \circ \sigma$ for all embeddings $\sigma$ of $L$, $L$ is called a *$J$–field*.

If $L$ is a totally imaginary field and it is a quadratic extension of a totally real field, $L$ is called a *CM–field*. A CM–field $L$ is also called *a field of CM–type*. We have that, in particular, a CM–field $L$ is a $J$–field.

We denote by $L^+ := L \cap \mathbb{R}$ the maximal real subfield of a CM–field $L$. If $L$ is a field of CM–type, then $L$ is invariant over complex conjugation $J$ and the Galois group of the extension $L/L^+$ satisfies $\mathrm{Gal}(L/L^+) \cong \langle J \rangle$, the group generated by complex conjugation.

A *$\mathbb{Z}_p$–extension* of a number field $L$ is a Galois extension $L_\infty/L$ such that $\mathbb{Z}_p \cong \mathrm{Gal}(L_\infty/L)$, the additive group of $p$–adic integers.

Let $\zeta_{p^n}$ be a primitive $p^n$–th root of unity in $\mathbb{C}$. It is well known that $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is a cyclic extension of degree $p^{n-1}(p-1)$. Let $\mathbb{Q}_{n-1}$ be the unique subfield of $\mathbb{Q}(\zeta_{p^n})$ such that $[\mathbb{Q}_{n-1} : \mathbb{Q}] = p^{n-1}$. We have $\mathbb{Q} = \mathbb{Q}_0 \subseteq \mathbb{Q}_1 \subseteq \cdots \subseteq \mathbb{Q}_n \subseteq \cdots$. We define $\mathbb{Q}_\infty := \cup_{n=0}^{\infty}\mathbb{Q}_n$. Then $\mathbb{Z}_p \cong \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Hence $\mathbb{Q}_\infty/\mathbb{Q}$ is a $\mathbb{Z}_p$–extension. The field $\mathbb{Q}_\infty$ is called *the cyclotomic $\mathbb{Z}_p$–extension* of $\mathbb{Q}$.

It is well known that any number field $L$ admits at least one $\mathbb{Z}_p$–extension, namely $L\mathbb{Q}_\infty/L$ which is called *$\mathbb{Z}_p$–cyclotomic extension of $L$* or *$\mathbb{Z}_p$–cyclotomic field* (see [11] p. 128). We will be using the term $\mathbb{Z}_p$–cyclotomic field. Also, $L$ is called a *$\mathbb{Z}_p$–field* if $L$ is the $\mathbb{Z}_p$–cyclotomic extension of some number field $K$.

Let $L$ be a number field. We shall denote by $P_L := \{(\alpha) | \alpha \in L^*)\}$ *the subgroup of principal divisors of* $L$, $I_L$ *the divisor group of* $L$ and $\mathscr{C}_L := I_L/P_L$ denotes *the class group of* $L$.

Given $L/L_0$ a $\mathbb{Z}_p$–extension of some number field $L_0$, let us consider the sequence $L_n$ of associated intermediate fields of the extension $L/L_0$. Let $I_{L_n}$ be the divisor group, $P_{L_n}$ the subgroup of principal divisors and $\mathscr{C}_{L_n}$ the class group of $L_n$. If $0 \leq n \leq m$, consider the natural embeddings $I_{L_n} \longrightarrow I_{L_m}$. We have that $I_L \cong \varinjlim I_{L_n}$, $\mathscr{C}_L \cong \varinjlim \mathscr{C}_{L_n}$ and $\mathscr{C}_L(p) \cong \varinjlim \mathscr{C}_{L_n}(p)$, where $\mathscr{C}_{L_n}(p)$ denotes the $p$–torsion of $\mathscr{C}_{L_n}$, (see [3] p. 263). We have that $\mathscr{C}_L$ is a torsion abelian group.

Let $L/L_0$ be a $\mathbb{Z}_p$–extension and $p^{q_n}$ the highest power of $p$ dividing the class number of $L_n$. Then there exist three integers $\nu, \lambda, \mu$ independent of $n$ with $\lambda, \mu \geq 0$, and an integer $n_0$, such that $q_m = \mu p^m + \lambda m + \nu$ for all $m \geq n_0$, (see [2], Theorem 11, p. 224). The integers $\nu, \lambda, \mu$ are known as *the Iwasawa invariants* associated to the field $L$. In this case, we use the notation

$\nu_L, \lambda_L$ and $\mu_L$.

It is well known that, if $L$ is a $\mathbb{Z}_p$–field of CM–type, then $L^+$ is a $\mathbb{Z}_p$–field. Therefore, there exist Iwasawa invariants associated to $L^+$, which will be denoted by $\nu_{L^+}, \lambda_{L^+}, \mu_{L^+}$. Let $\nu_L^- := \nu_L - \nu_{L^+}$, $\lambda_L^- := \lambda_L - \lambda_{L^+}$ and $\mu_L^- := \mu_L - \mu_{L^+}$.

We define $W_n := \{\zeta \in \mathbb{C} | \zeta^n = 1\}$ the group of $n$-th roots of unity, $W = \cup_{n=1}^{\infty} W_n$, $W(p) = \cup_{n=0}^{\infty} W_{p^n}$ and for a field $L$, $W_L := W \cap L$ the group of roots of unity in $L$. Let

$$\delta_L := \begin{cases} 1 \text{ if } W(p) \subseteq L, \\ 0 \text{ otherwise.} \end{cases}$$

Note that $\delta_K = \delta_L$, since $L/K$ is a $p$–extension.

There is a basic relationship between the Iwasawa invariants $\lambda_L^-$ and $\lambda_K^-$ given by the following proposition.

**Proposition 2.1.** *Let $L/K$ be a finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields with Galois group $G = \mathrm{Gal}(L/K)$, such that $\mu_L^- = 0$ and $\mu_K^- = 0$. Let $P_1^+, \ldots, P_t^+$ be the non–$p$–primes of $K^+$ i.e., $P_i^+|_{\mathbb{Q}} \neq p$, ramified in $L^+$ and split in $K$. Let $\mathrm{Con}_{K^+/K}(P_i^+) = P_i P_i^J$ be the conorm map of $P_i^+$. Let $G_1, \ldots, G_t$ be the decomposition groups of $P_1, \ldots, P_t$. Then*

$$\lambda_L^- - \delta_L = |G|(\lambda_K^- - \delta_K) + \sum_{i=1}^{t} \left( |G| - \frac{|G|}{|G_i|} \right).$$

*Proof.* See [6] p. 519. □

Given a number field $L$, a formal product $\mathfrak{M} := \prod_{\wp \in \mathbb{P}_L} \wp^{n_{\mathfrak{M}}(\wp)}$ where $n_{\mathfrak{M}}(\wp) \in \mathbb{N} \cup \{0\}$ and $n_{\mathfrak{M}}(\wp) = 0$ for all but a finite number of elements of $\mathbb{P}_L$, the collection of prime divisors of $L$, is called *a modulus* of $L$. Moreover, $n_{\mathfrak{M}}(\wp) = 0$ or 1 when $\wp$ is a real prime divisor and $n_{\mathfrak{M}}(\wp) = 0$ if $\wp$ is a complex prime divisor.

For any finite set $\{\wp_1, \wp_2, \ldots, \wp_k\}$ of different prime divisors of $L$, we define the modulus $M := \prod_{i=1}^{k} \wp_i^{\rho_i}$, $\rho_i > 0$. Associated with the modulus $M$ we have the following groups: $I_M := \{\mathfrak{D} | \mathfrak{D}$ is divisor of $L$ relatively prime to $M\}$, $T_M := \{(\alpha) | \alpha \in L^*, (\alpha)$ relatively prime to $M\}$, $P_M := \{(\alpha) | \alpha \in L^*, \alpha \equiv 1 \bmod M\}$, and $\mathscr{C}_M := I_M / P_M$ which is called *the ray class group*.

For a finite $p$–extension of $\mathbb{Z}_p$–fields of CM–type $L/K$, there exist finitely many primes of $K^+$ ramified in $L^+$.

Frow now on: $L/K$ denotes a finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type with Galois group $G = \mathrm{Gal}(L/K)$ and such that $\mu_L^- = 0$ and $\mu_K^- = 0$.

Consider the diagram

$$\begin{array}{ccc} L^+ & \longrightarrow & L \\ \uparrow & & \uparrow \\ K^+ & \longrightarrow & K \end{array}$$

Let $\{\wp_1^+, \wp_2^+, \ldots, \wp_t^+\}$ be the set of the non–$p$–prime divisors of $K^+$, that is $\wp_i^+|_{\mathbb{Q}} \neq p$, ramified in $L^+$ and split in $K$. Let $\{\wp_{t+1}^+, \ldots, \wp_{t+u}^+\}$ be any set of non–$p$–prime divisors of $K^+$ split in $K$ and unramified in $L^+$. Finally, let $\{\wp_{t+u+1}^+, \ldots, \wp_{t+u+v}^+\}$ be an arbitrary set of non–$p$–prime divisors of $K^+$ inert in $K$ and unramifed in $L$. Moreover, we assume that $p^\infty || \left(O_{K^+}/\wp_i^+\right)^* |$ for $1 \leq i \leq t+u+v$, where $O_{K^+}$ denotes the ring of integers of $K^+$ (see [4] p. 268). Let $U := DD^JCC^JQ$ where $D := \prod_{i=1}^{t} \wp_i^+$, $C := \prod_{j=1}^{u} \wp_{t+j}^+$, and $Q := \prod_{k=1}^{v} \wp_{t+u+k}^+$. We have that $U$ is a modulus of $K^+$. Let $D_s := \prod_{i=1}^{s} \wp_i^+$, with $s \leq t$ and

$$\mathfrak{A} := D_s D_s^J CC^J Q. \tag{2.1}$$

The modulus $\mathfrak{A}$ divides the modulus $U$.

Let $\text{Con}_{K^+/K}(\wp_i^+) = \wp_i\wp_i^J$, $i \in \{1,\dots,t+u\}$, $\text{Con}_{K^+/K}(\wp_i^+) = \wp_i = \wp_i^+$, $i \in \{t+u+1,\dots,t+u+v\}$ and $\text{Con}_{K/L}(\wp_i) = (H_1^{(i)}\cdots H_{g_i}^{(i)})^{e_i} =: N_i^{e_i}$, $i \in \{t+u+1,\dots,t+u+v\}$.

Note that $e_i = 1$ for all $i \in \{t+1,\dots,t+u+v\}$ and $f(H_j^{(i)}|\wp_i) = 1$ for every $i \in \{1,\dots,t+u+v\}$ (see [4] p. 266).

We define $\mathfrak{N}$ and $\mathfrak{B}$ as the moduli of $L$ given by:

$$\mathfrak{N} := \left(\prod_{i=1}^{i=t+u} N_i N_i^J\right)\left(\prod_{j=t+u+1}^{j=t+u+v} N_j\right) \quad \text{and} \tag{2.2}$$

$$\mathfrak{B} := \left(\prod_{i=1}^{i=s} N_i N_i^J\right)\left(\prod_{i=t+1}^{i=t+u} N_i N_i^J\right)\left(\prod_{j=t+u+1}^{j=t+u+v} N_j\right), s \le t. \tag{2.3}$$

That is, considering $Q_1 := \text{Con}_{K^+/L^+}(Q)$, $D_1 := \text{Con}_{K^+/L^+}(D)$ and $C_1 := \text{Con}_{K^+/L^+}(C)$, we have in $L$ the modulus $\mathfrak{N} := D_1D_1^JC_1C_1^JQ_1$ induced by the modulus $U$. Furthermore, if $\widetilde{D_s} := \text{Con}_{K^+/L^+}(D_s)$, then $\mathfrak{B} := \widetilde{D_s}\widetilde{D_s}^JC_1C_1^JQ_1$ is a modulus of $L$, i.e., $\mathfrak{B}$ is induced by the modulus $\mathfrak{A}$. We have that $\mathfrak{B}$ divides $\mathfrak{N}$. More precisely, to obtain the modulus $\mathfrak{B}$, some ramified non–$p$–prime divisors in the support of the modulus $\mathfrak{N}$ are removed.

**Remark 2.2.** Let $A$ be a $\mathbb{Z}_p[G]$–module, $p \neq 2$. Then $A \cong A^+ \oplus A^-$, where $A^\pm := \{a \in A | a^J = \pm a\}$. (See [3] p. 308). Also, we define $A(p) := \{a \in A|$ order of $a$ is a power of $p\}$.

In our case, the class group $\mathscr{C}_L$ of $L$ is expressed as

$$\mathscr{C}_L \cong \mathscr{C}_L^- \oplus \mathscr{C}_L^+ \text{ and therefore } \mathscr{C}_L(p) \cong \mathscr{C}_L^-(p) \oplus \mathscr{C}_L^+(p).$$

In particular, for the ray class group induced by the modulus $\mathfrak{B}$, we have

$$\mathscr{C}_{\mathfrak{B}}(p) \cong \mathscr{C}_{\mathfrak{B}}^-(p) \oplus \mathscr{C}_{\mathfrak{B}}^+(p).$$

The main objective of this article is to find the explicit structure as $\mathbb{Z}_p[G]$–module of $\mathscr{C}_{\mathfrak{B}}^-(p)$, *the $p$–subgroup of the minus part of the ray class group of* $L$ associated to the modulus $\mathfrak{B}$ of $L$. That is, we obtain explicitly the decomposition of $\mathscr{C}_{\mathfrak{B}}^-(p)$ as a direct sum of indecomposable $\mathbb{Z}_p[G]$–modules, where $\mathfrak{B}$ is a modulus in $L$ given by (2.3).

If $L/K$ is a finite Galois $p$-extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type with $G = \text{Gal}(L/K)$, it was established in [9] and [10] the exact sequence of $\mathbb{Z}_p[G]$–modules

$$0 \longrightarrow \frac{\overset{t}{\underset{i=1}{\oplus}} R[G/G_i] \oplus R[G]^a}{(Re^*_{t_a})^{\delta_L}} \longrightarrow \mathscr{C}_{\mathfrak{N}}^-(p) \longrightarrow \mathscr{C}_L^-(p) \longrightarrow 0, \tag{2.4}$$

where $G_i$ denotes a decomposition group of the prime divisor $\wp_i$ of $K$, $G/G_i$ denotes the set of left cosets, $R[G/G_i]$ is the $\mathbb{Z}_p[G]$–module $\left\{\sum_{\sigma\in G/G_i} a_\sigma\sigma \;\middle|\; a_\sigma \in R\right\}$ with the natural action and

$$Re^*_{t_a} := \left\{\left(\sum_{\sigma_1\in G/G_1} x\sigma_1, \dots, \sum_{\sigma_t\in G/G_t} x\sigma_t, \underbrace{\sum_{\sigma\in G} x\sigma, \dots, \sum_{\sigma\in G} x\sigma}_{a}\right) \;\middle|\; x \in R\right\},$$

that is, $Re^*_{t_a}$ is isomorphic to $R := \dfrac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}$ embedded diagonally in $\overset{t}{\underset{i=1}{\oplus}} R[G/G_i] \oplus R[G]^a$.

Let $M$ be a $\mathbb{Z}_p[G]$–module and let $0 \longrightarrow M \longrightarrow Y \longrightarrow P \longrightarrow 0$ be any exact sequence of $G$–modules, with $Y$ an injective $\mathbb{Z}_p[G]$–module. We write $P = P^{(1)} \oplus P^{(0)}$ with $P^{(1)}$ an injective $\mathbb{Z}_p[G]$–module and with $P^{(0)}$ having no $\mathbb{Z}_p[G]$–injective components. Let $\Omega^\#(M) := P^{(0)}$, which is called *the dual of the Heller's loop–space operator of* $M$. The $\mathbb{Z}_p[G]$–module $\Omega^\#(M)$ is unique up to isomorphism. Note that $\Omega^\#$ is well defined since the Krull-Schmidt-Azumaya Theorem (see [1], (6.12), p 128) holds for $\mathbb{Z}_p[G]$–modules.

**Proposition 2.3.** *Let $G$ be a finite $p$-group and let $H$ be a subgroup of $G$. Then*

i) $R[G/H]$ *and* $\dfrac{R[G]}{R[G/H]}$ *are indecomposable* $\mathbb{Z}_p[G]$*–modules.*

ii) $\Omega^\#(R[G/H]) \cong \dfrac{R[G]}{R[G/H]}$ *as* $\mathbb{Z}_p[G]$*–modules.*

iii) *If* $M_1$ *and* $M_2$ *are* $\mathbb{Z}_p[G]$*–modules, then* $\Omega^\#(M_1 \oplus M_2) \cong \Omega^\#(M_1) \oplus \Omega^\#(M_2)$.

iv) *If* $M$ *is an injective* $\mathbb{Z}_p[G]$*–module, then* $\Omega^\#(M) \cong \{0\}$.

*Proof.* See [5], Proposition 2.8, p. 108. □

Let $G$ be a finite $p$–group and let $M$ be a $\mathbb{Z}_p[G]$–module such that *the Pontryagin's dual* $\mathfrak{X}(M) := \mathrm{Hom}_{\mathbb{Z}_p}(M, R)$ of $M$ is finitely generated, and such that $M$ is a $\mathbb{Z}_p$–injective module. Then, as groups, $M \cong R^{s_0}$ with $s_0 < \infty$. If ${}_pM$ denotes the elements of $M$ of order a divisor of $p$, then ${}_pM$ is a finitely generated $\mathbb{F}_p[G]$–module and it is called *the $p$–part of $M$*, where $\mathbb{F}_p$ denotes the finite field of $p$ elements.

**Theorem 2.4.** *Let $M$ and $G$ be as in the above notation. If ${}_pM \cong \mathbb{F}_p[G]^n \oplus U$ with $\mathbb{F}_p[G]$ not a component of $U$ and $M \cong R[G]^m \oplus V$ where $R[G]$ is not a component of $V$, then $n = m$.*

*Proof.* See [8], Lemma 3, p. 81. □

## 3 An exact sequence for $\mathscr{C}^-_{\mathfrak{B}}(p)$

The main objetive in this section is to establish an exact sequence of $\mathbb{Z}_p[G]$–modules characterizing implicitly the structure of $\mathscr{C}^-_{\mathfrak{B}}(p)$. First, we obtain some results for a $\mathbb{Z}_p$–cyclotomic field of CM–type and then for $L/K$, a finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type.

**Lemma 3.1.** If $L$ is a $\mathbb{Z}_p$–cyclotomic field of CM–type, $\mathfrak{N}$ and $\mathfrak{B}$ are moduli of $L$ as in (2.2) and (2.3), respectively, then the natural map $\varphi : \mathscr{C}^-_{\mathfrak{N}}(p) \longrightarrow \mathscr{C}^-_{\mathfrak{B}}(p)$ is an epimorphism.

*Proof.* Since $\mathfrak{B}$ divides $\mathfrak{N}$, i.e., $\mathfrak{N} = \mathfrak{B}\mathfrak{D}$ for some divisor $\mathfrak{D}$, the natural inclusion maps $I_{\mathfrak{N}} \subseteq I_{\mathfrak{B}}$ and $P_{\mathfrak{N}} \subseteq P_{\mathfrak{B}}$ induce the epimorphism $\varphi_0 : \mathscr{C}_{\mathfrak{N}} \longrightarrow \mathscr{C}_{\mathfrak{B}}$. Since $\mathscr{C}_{\mathfrak{N}}$ and $\mathscr{C}_{\mathfrak{B}}$ are torsion groups and $L$ is a $J$–field, the result follows. □

**Proposition 3.2.** *If $L$ is a $\mathbb{Z}_p$–cyclotomic field of CM–type, $\mathfrak{N}$ and $\mathfrak{B}$ are moduli of $L$ as in* (2.2) *and* (2.3) *respectively, then we have the exact sequence of groups*

$$0 \longrightarrow W(p)^{t_0 - s_0} \longrightarrow \mathscr{C}^-_{\mathfrak{N}}(p) \longrightarrow \mathscr{C}^-_{\mathfrak{B}}(p) \longrightarrow 0,$$

*where* $t_0 := (u+v)|G| + \left(\sum_{i=1}^t |\frac{G}{G_i}|\right)$ *and* $s_0 := (u+v)|G| + \left(\sum_{i=1}^s |\frac{G}{G_i}|\right)$.

*Proof.* From [9] p. 342, we obtain an exact sequence of groups

$$0 \longrightarrow W(p)^{t_0-\delta_L} \longrightarrow \mathscr{C}_{\mathfrak{N}}^-(p) \longrightarrow \mathscr{C}_L^-(p) \longrightarrow 0.$$

Using the same idea for $1 \leq s \leq t$ we have the exact sequence of groups

$$0 \longrightarrow W(p)^{s_0-\delta_L} \longrightarrow \mathscr{C}_{\mathfrak{B}}^-(p) \longrightarrow \mathscr{C}_L^-(p) \longrightarrow 0.$$

Since the modulus $\mathfrak{B}$ divides the modulus $\mathfrak{N}$, from Lemma 3.1 we have that

$$0 \longrightarrow \ker(\rho) \longrightarrow \mathscr{C}_{\mathfrak{N}}^-(p) \overset{\rho}{\longrightarrow} \mathscr{C}_{\mathfrak{B}}^-(p) \longrightarrow 0 \tag{3.1}$$

is an exact sequence. Therefore we have the commutative diagram of $\mathbb{Z}_p$–modules

$$\begin{array}{ccccccccc}
0 & \longrightarrow & W(p)^{s_0-\delta_L} & \longrightarrow & \mathscr{C}_{\mathfrak{B}}^-(p) & \longrightarrow & \mathscr{C}_L^-(p) & \longrightarrow & 0 \\
 & & \uparrow \widetilde{\rho} & & \uparrow \rho & & \uparrow \mathrm{id} & & \\
0 & \longrightarrow & W(p)^{t_0-\delta_L} & \longrightarrow & \mathscr{C}_{\mathfrak{N}}^-(p) & \longrightarrow & \mathscr{C}_L^-(p) & \longrightarrow & 0
\end{array}$$

Using the Snake Lemma, we obtain the exact sequence

$$0 \longrightarrow \ker(\widetilde{\rho}) \longrightarrow \ker(\rho) \longrightarrow 0.$$

That is, $\ker(\widetilde{\rho}) \cong \ker(\rho)$. It is easy to see that

$$\ker(\widetilde{\rho}) \cong W(p)^{t_0-s_0}. \tag{3.2}$$

Finally, the result follows from (3.1) and (3.2). □

**Corollary 3.3.** *If $L$ is a $\mathbb{Z}_p$–cyclotomic field of CM–type and $\mathfrak{B}$ is modulus of $L$ as in* (2.3)*, then, as groups*

$$\mathscr{C}_{\mathfrak{B}}^-(p) \cong R^{\lambda_{\mathfrak{B}}} \text{ with } \lambda_{\mathfrak{B}} = |G|(\lambda_K^- + t + u + v - \delta_K) - \sum_{i=s+1}^{t} \left|\frac{G}{G_i}\right|.$$

*Proof.* Since $\mathscr{C}_L^-(p) \cong R^{\lambda_L^-}$ as $\mathbb{Z}_p$–modules (see [4] p. 264), using similar arguments we obtain $\mathscr{C}_{\mathfrak{B}}^-(p) \cong R^{\lambda_{\mathfrak{B}}}$ as $\mathbb{Z}_p$–modules. From (2.4) and Kida's formula we obtain

$$\mathscr{C}_{\mathfrak{N}}^-(p) \cong R^{|G|(\lambda_K^- + t + u + v - \delta_K)} \text{ as groups.}$$

On the other hand we have $W(p) \cong R$, and from Proposition 3.2 we obtain

$$\lambda_{\mathfrak{B}} = |G|(\lambda_K^- + t + u + v - \delta_K) - (t_0 - s_0).$$ □

**Proposition 3.4.** *Let $L/K$ be any finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type and suppose that $\mu_L^- = 0$ and $\mu_K^- = 0$. If $\mathfrak{B}$ is a modulus of $L$ given by* (2.3)*, the structure of the $\mathbb{Z}_p[G]$–module $\mathscr{C}_L^-(p)$ is characterized by the following exact sequence of $\mathbb{Z}_p[G]$–modules*

$$0 \longrightarrow \frac{\bigoplus_{i=1}^{s} R[G/G_i] \oplus R[G]^{u+v}}{Re^*_{s_{u+v}}} \longrightarrow \mathscr{C}_{\mathfrak{B}}^-(p) \longrightarrow \mathscr{C}_L^-(p) \longrightarrow 0. \tag{3.3}$$

*Proof.* The case $s = t$ was obtained (for the $p$–part) in Proposition 9 p. 344 of [9] and Theorem 1 p. 257 of [10]. The same ideas apply to the case $1 \leq s \leq t$. □

**Theorem 3.5.** *Let $L/K$ be an arbitrary finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type and suppose that $\mu_L^- = 0$ and $\mu_K^- = 0$. Then we have an exact sequence of $\mathbb{Z}_p[G]$–modules*

$$0 \longrightarrow \bigoplus_{i=s+1}^{t} R[G/G_i] \longrightarrow \mathscr{C}_{\mathfrak{N}}^-(p) \longrightarrow \mathscr{C}_{\mathfrak{B}}^-(p) \longrightarrow 0, \tag{3.4}$$

*where the moduli $\mathfrak{N}$ and $\mathfrak{B}$ of $L$ are defined by* (2.2) *and* (2.3)*, respectively.*

*Proof.* $\mathscr{C}_{\mathfrak{B}}^-(p)$ is completely characterized from the Schanuel's Lemma and (3.4). From (3.3), we obtain the exact sequences of $\mathbb{Z}_p[G]$–modules

$$0 \longrightarrow \frac{\bigoplus_{i=1}^{t} R[G/G_i] \oplus R[G]^{u+v}}{Re^*_{t_{u+v}}} \longrightarrow \mathscr{C}_{\mathfrak{N}}^-(p) \longrightarrow \mathscr{C}_L^-(p) \longrightarrow 0,$$

$$0 \longrightarrow \frac{\bigoplus_{i=1}^{s} R[G/G_i] \oplus R[G]^{u+v}}{Re^*_{s_{u+v}}} \longrightarrow \mathscr{C}_{\mathfrak{B}}^-(p) \longrightarrow \mathscr{C}_L^-(p) \longrightarrow 0.$$

Since the modulus $\mathfrak{B}$ divides the modulus $\mathfrak{N}$, from Lemma 3.1 we obtain the commutative diagram of $\mathbb{Z}_p[G]$–modules

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{\bigoplus_{i=1}^{s} R[G/G_i] \oplus R[G]^{u+v}}{Re^*_{s_{u+v}}} & \longrightarrow & \mathscr{C}_{\mathfrak{B}}^-(p) & \longrightarrow & \mathscr{C}_L^-(p) & \longrightarrow & 0 \\
 & & \uparrow \widetilde{\varphi_1} & & \uparrow \varphi_1 & & \uparrow \mathrm{id} & & \\
0 & \longrightarrow & \dfrac{\bigoplus_{i=1}^{t} R[G/G_i] \oplus R[G]^{u+v}}{Re^*_{t_{u+v}}} & \longrightarrow & \mathscr{C}_{\mathfrak{N}}^-(p) & \longrightarrow & \mathscr{C}_L^-(p) & \longrightarrow & 0
\end{array} \tag{3.5}$$

Using the Snake Lemma, we obtain the exact sequence

$$0 \longrightarrow \ker(\widetilde{\varphi_1}) \longrightarrow \ker(\varphi_1) \longrightarrow 0.$$

That is, $\ker(\widetilde{\varphi_1}) \cong \ker(\varphi_1)$. Furthermore, it is easy to see that

$$\ker(\widetilde{\varphi_1}) \cong \bigoplus_{i=s+1}^{t} R[G/G_i]. \tag{3.6}$$

Finally, the result follows from (3.5) and (3.6). □

**Corollary 3.6.** *We keep the notation as above. For ${}_p\mathscr{C}_{\mathfrak{B}}^-$, the $p$-parte of $\mathscr{C}_{\mathfrak{B}}^-(p)$, we have an exact sequence of $\mathbb{F}_p[G]$–modules*

$$0 \longrightarrow \bigoplus_{i=s+1}^{t} \mathbb{F}_p[G/G_i] \longrightarrow {}_p\mathscr{C}_{\mathfrak{N}}^- \longrightarrow {}_p\mathscr{C}_{\mathfrak{B}}^- \longrightarrow 0,$$

*where the moduli $\mathfrak{N}$ and $\mathfrak{B}$ of $L$ are defined by* (2.2) *and* (2.3)*, respectively.*

*Proof.* Since $\overset{s}{\underset{i=1}{\oplus}} R[G/G_i]$ is a sum of $p$-divisible $\mathbb{Z}_p[G]$–modules, it is a $p$-divisible module. From (3.4), we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \overset{s}{\underset{i=1}{\oplus}} R[G/G_i] & \longrightarrow & \mathscr{C}_{\mathfrak{N}}^-(p) & \longrightarrow & \mathscr{C}_{\mathfrak{B}}^-(p) & \longrightarrow & 0 \\ & & \downarrow \hat{p} & & \downarrow \hat{p} & & \downarrow \hat{p} & & \\ 0 & \longrightarrow & \overset{s}{\underset{i=1}{\oplus}} R[G/G_i] & \longrightarrow & \mathscr{C}_{\mathfrak{N}}^-(p) & \longrightarrow & \mathscr{C}_{\mathfrak{B}}^-(p) & \longrightarrow & 0 \end{array}$$

where $\hat{p} : A \longrightarrow A$ is given by $\hat{p}(a) := pa$, for all $a \in A$, with $A$ any $\mathbb{Z}_p[G]$–module. Using the Snake Lemma and that ${}_p(R[G/G_i]) \cong \mathbb{F}_p[G/G_i]$, the result follows. □

## 4 The Galois module structure of $\mathscr{C}_{\mathfrak{B}}^-(p)$ and ${}_p\mathscr{C}_{\mathfrak{B}}^-$

The main goal in this section is to obtain the structure, as Galois module, of the $p$–subgroup of the minus part of the ray class group $\mathscr{C}_{\mathfrak{B}}^-(p)$ and of ${}_p\mathscr{C}_{\mathfrak{B}}^-$, the elements in $\mathscr{C}_{\mathfrak{B}}^-(p)$ of order dividing $p$. That is, we obtain explicitly the decomposition, as a direct sum of indecomposable $\mathbb{Z}_p[G]$–modules and of indecomposable $\mathbb{F}_p[G]$–modules, of $\mathscr{C}_{\mathfrak{B}}^-(p)$ and ${}_p\mathscr{C}_{\mathfrak{B}}^-$, respectively, where $\mathfrak{B}$ is a modulus of $L$ given by (2.3).

**Theorem 4.1.** *Let $L/K$ be an arbitrary finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type with Galois group $G = \mathrm{Gal}(L/K)$ and suppose that $\mu_L^- = 0$ and $\mu_K^- = 0$. Then the structure of $\mathscr{C}_{\mathfrak{B}}^-(p)$ as $\mathbb{Z}_p[G]$–module is given by*

$$\mathscr{C}_{\mathfrak{B}}^-(p) \cong R[G]^{\lambda_K^- - \delta_K + s + u + v} \oplus \left( \overset{t}{\underset{i=s+1}{\oplus}} \frac{R[G]}{R[G/G_i]} \right),$$

*where $\lambda_K^-$ denotes the minus Iwasawa $\lambda$–invariant of $K$, $t$ is the total number of ramified non–$p$–prime divisors, $s \leq t$ is the number of non–$p$–prime divisors of $K^+$ ramified in $L^+$ and split in $K$, $u$ is the number of non–$p$–prime divisors of $K^+$ split in $K$ and unramified in $L^+$ contained in the support of $\mathfrak{A}$ given by* (2.1)*, and $v$ is the number of non–$p$–prime divisors of $K^+$ inert in $K$ and unramified in $L$.*

*Proof.* Using (3.4) and that $\mathscr{C}_{\mathfrak{N}}(p)$ is an injective $\mathbb{Z}_p[G]$–module (see [10], Proposition 3, p. 257), we obtain the exact sequence of $\mathbb{Z}_p[G]$–modules

$$0 \longrightarrow \overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i] \longrightarrow R[G]^{\lambda_K^- + t + v + u - \delta_K} \longrightarrow \mathscr{C}_{\mathfrak{B}}^-(p) \longrightarrow 0. \tag{4.1}$$

From the Krull-Schmidt-Azumaya Theorem, we obtain

$$\mathscr{C}_{\mathfrak{B}}^-(p) \cong R[G]^{\alpha} \oplus M, \text{ where } M \text{ does not have } R[G] \text{ as a component.}$$

Now, we must find the value of $\alpha$ and decompose $M$ as a direct sum of indecomposable $\mathbb{Z}_p[G]$–modules. Applying the dual of Heller's loop operator in (4.1) and using Proposition 2.3, we have

$$M \cong \mathbf{\Omega}^{\#} \left( \overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i] \right) \cong \overset{t}{\underset{i=s+1}{\oplus}} \left( \mathbf{\Omega}^{\#} R[G/G_i] \right) \cong \overset{t}{\underset{i=s+1}{\oplus}} \frac{R[G]}{R[G/G_i]}.$$

On the other hand, to compute $\alpha$, we use the technique used to obtain the injective component of $\mathscr{C}_L^-(p)$ given in [7]. We have the exact sequence of $\mathbb{Z}_p[G]$–modules

$$0 \longrightarrow \overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i] \longrightarrow R[G]^c \longrightarrow \mathbf{\Omega}^{\#}\left(\overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i]\right) \longrightarrow 0,$$

where $c$ is the minimal natural number such that exists a $\mathbb{Z}_p[G]$–monomorphism

$$\rho : \overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i] \longrightarrow R[G]^c.$$

Since $R[G]^c$ and $R[G]^{\lambda_K^- + t + v + u - \delta_K}$ are injective $\mathbb{Z}_p[G]$–modules, using Schanuel's Lemma, we obtain

$$R[G]^c \oplus R[G]^\alpha \oplus \left(\overset{t}{\underset{i=s+1}{\oplus}} \frac{R[G]}{R[G/G_i]}\right) \cong \mathbf{\Omega}^{\#}\left(\overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i]\right) \oplus R[G]^{\lambda_K^- + t + v + u - \delta_K}.$$

From the Krull-Schmidt-Azumaya Theorem, we have

$$R[G]^c \oplus R[G]^\alpha \cong R[G]^{\lambda_K^- + t + v + u - \delta_K},$$

i.e., $\alpha = \lambda_K^- + t + v + u - \delta_K - c$. Now, to obtain $c$, we compute

$$c = \dim_{\mathbb{Z}_p}\left(\overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i]\right)^G = \dim_{\mathbb{Z}_p}\left(\overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i]^G\right) = \dim_{\mathbb{Z}_p}\left(\overset{t}{\underset{i=s+1}{\oplus}} R\right) = t - s.$$

Finally, $\alpha = \lambda_K^- + t + v + u - \delta_K - (t - s) = \lambda_K^- + s + v + u - \delta_K$. □

**Remark 4.2.** The exponent $\alpha$ of the injective summand in Theorem 4.1 can also be obtained as follows.

From the exact sequence (4.1) and the Krull-Schmidt-Azumaya Theorem we have the exact sequence of $\mathbb{Z}_p[G]$–modules

$$0 \longrightarrow \overset{t}{\underset{i=s+1}{\oplus}} R[G/G_i] \longrightarrow R[G]^{\lambda_K^- + t + v + u - \delta_K} \longrightarrow R[G]^\alpha \oplus \left(\overset{t}{\underset{i=s+1}{\oplus}} \frac{R[G]}{R[G/G_i]}\right) \longrightarrow 0,$$

that is

$$\begin{aligned} |G|\alpha =& |G|(\lambda_K^- + t + v + u - \delta_K) - \sum_{i=s+1}^{t} \left|\frac{G}{G_i}\right| - |G|(t - s) + \sum_{i=s+1}^{t} \left|\frac{G}{G_i}\right| \\ =& |G|(\lambda_K^- + t + v + u - \delta_K + s - t) = |G|(\lambda_K^- + s + v + u - \delta_K), \end{aligned}$$

i.e., $\alpha = \lambda_K^- + s + v + u - \delta_K$.

**Corollary 4.3.** *We keep the notation as above. Let $L/K$ be any finite Galois $p$–extension of $\mathbb{Z}_p$–cyclotomic fields of CM–type and suppose that $\mu_L^- = 0$ and $\mu_K^- = 0$. Then the structure of ${}_p\mathscr{C}_{\mathfrak{B}}^-$ as $\mathbb{F}_p[G]$–module is given by*

$${}_p\mathscr{C}_{\mathfrak{B}}^- \cong \mathbb{F}_p[G]^{\lambda_K^- - \delta_K + s + u + v} \oplus \left(\overset{t}{\underset{i=s+1}{\oplus}} \frac{\mathbb{F}_p[G]}{\mathbb{F}_p[G/G_i]}\right).$$

*Proof.* If follows from Theorems 2.4 and 4.1 since

$$_p(R[G]) \cong \mathbb{F}_p[G] \quad \text{and} \quad {}_p\left(\frac{R[G]}{R[G/G_i]}\right) \cong \frac{\mathbb{F}_p[G]}{\mathbb{F}_p[G/G_i]}. \qquad \square$$

**Remark 4.4.** Theorem 4.1 generalizes Proposition 3, p. 257 of [10]. Corollary 4.3 generalizes Proposition 8 p. 336 of [9].

**Remark 4.5.** For the case of the Galois structure as $\mathbb{Z}_p[G]$-module ($\mathbb{F}_p[G]$-module) of $\mathscr{C}_L^-(p)$ $({}_p\mathscr{C}_L^-)$ there is a difference depending on whether $\delta_L = 0$ or 1. However, the Galois structure as $\mathbb{Z}_p[G]$-module ($\mathbb{F}_p[G]$-module) of $\mathscr{C}_{\mathfrak{B}}^-(p)$ $({}_p\mathscr{C}_{\mathfrak{B}}^-)$ is of the same type independently of $\delta_L$.

## References

[1] C. W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders*, Pure and Applied Mathematics. Wiley-Interscience, New York Vol. I, 1981; Vol. II, 1987.

[2] K. Iwasawa, On Γ–extensions of Algebraic Number Fields, *Bull. Amer. Math. Soc.* **65** (1959), 183-226.

[3] K. Iwasawa, On $\mathbb{Z}_p$–extensions of Algebraic Number Fields, *Ann. of Math.* **98** (1973), 246-326.

[4] K. Iwasawa, Riemann-Hurwitz formula and $p$–adic Galois representation for number fields, *Tôhoku Math. J.* **33** (1981), 263-288.

[5] F. Jarquín-Zárate and G. Villa-Salvador, On the non-injective component as Galois module of generalized Jacobians, *Journal of Algebra, Number Theory: Advances and Applications,* **2** (2) (2009), 99-128.

[6] Y. Kida, $\ell$–Extensions of CM–fields and cyclotomic invariants, *Journal of Number Theory* **12** (1980), 519–528.

[7] P.R. López-Bautista and G.D. Villa-Salvador, Integral Representation of $p$–Class groups in $\mathbb{Z}_p$–Extensions and the Jacobian Variety, *Can. J. Math.* **50** (1998), 1253–1272.

[8] M. Rzedowski–Calderón, G.D. Villa–Salvador and M.L. Madan, Galois Module Structure of Tate Modules, *Math. Z.* **224** (1997), 77–101.

[9] G.D. Villa-Salvador and M.L. Madan, Structure of Semisimple Differentials and $p$–Class Groups in $\mathbb{Z}_p$–Extensions, *manuscripta math.* **57** (1987), 315–350.

[10] G.D. Villa-Salvador and M.L. Madan, Integral Representations of $p$–Class Groups in $\mathbb{Z}_p$–Extensions, Semisimple Differentials and Jacobians, *Arch. Math.* **56** (1991), 254–269.

[11] L.C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. **83**, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

### Author information

F. Jarquín-Zárate, Universidad Autónoma de la Ciudad de México, Academia de Matemáticas. Plantel San Lorenzo Tezonco, Prolongación San Isidro No. 151, Col. San Lorenzo, Iztapalapa, C.P. 09790, D.F., Mexico.
E-mail: `fausto.jarquin@uacm.edu.mx`

G. Villa-Salvador, Centro de Investigación y de Estudios Avanzados del I.P.N., Departamento de Control Automático, Apartado Postal 14-740, 07000 México, D. F., Mexico.
E-mail: `gvilla@ctrl.cinvestav.mx`

Received: January 4, 2013.

Accepted: April 7, 2013.